INSTITUTE FOR DEFENSE ANALYSES

Military Authorizations in a Connected World: The Department of Defense's Role in Influence Operations

Michelle G. Albert, *Project Leader*
George A. Thompson
Thomas H. Barth

June 2020

IDA Non-Standard
NS D-11022

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a nonprofit corporation that operates three Federally Funded Research and Development Centers. Its mission is to answer the most challenging U.S. security and science policy questions with objective analysis, leveraging extraordinary scientific, technical, and analytic expertise.

About This Publication

This work was conducted by the IDA Systems and Analyses Center under contract HQ0034-14-D-0001, Project C5199, "Future Information Operations," for the IDA. The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgements

Priscilla E. Guthrie

For More Information

Michelle G. Albert, Project Leader
malbert@ida.org, 703-845-6674

Margaret E. Myers, Director, Information Technology and Systems Division
mmyers@ida.org, 703-578-2782

Rigorous Analysis | Trusted Expertise | Service to the Nation

INSTITUTE FOR DEFENSE ANALYSES

IDA Non-Standard NS D-11022

Military Authorizations in a Connected World: The Department of Defense's Role in Influence Operations

Michelle G. Albert, *Project Leader*

George A. Thompson

Thomas H. Barth

Executive Summary

The revelation that Russia's Internet Research Agency conducted a sophisticated disinformation campaign in the run-up to the 2016 U.S. presidential election exposed to the public an attack surface that is difficult to understand, categorize, and bound. This attack surface is also difficult to defend. Today's global media ecosystem enables the easy and almost instantaneous spread of information around the world. Although some counties, such as China, have erected barriers to restrict the Internet, others envision an open platform in which anyone can contribute and freely access content. Unfortunately, an open platform is easily exploited by malicious actors like Russia who want to infiltrate networks and run campaigns based on prepositioning assets to hold critical infrastructure at risk and encourage social division through the manipulation of social and traditional media. Especially vulnerable are societies with strong democratic institutions that hesitate to employ censorship.

This global media ecosystem has enabled a new, different type of attack surface and a rash of new vulnerabilities. Critical infrastructure is run on Internet-enabled and -connected systems. Information of a personal or sensitive nature, including financial records and personal health information (PHI), is stored online, where it is subject to theft and can be used to steal a user's identity. Social media sites contain large amounts of voluntarily shared information that advertising companies use to create detailed profiles of individual and group preferences, habits, spending patterns, and political views. This information can be aggregated and sold by social media sites like Facebook. These new attack surfaces can be exploited by a technologically sophisticated adversary.

These types of cyber activities occur in the gray zone,[1] which falls between diplomatic engagement and military action and encompasses activities that do not merit a conventional military response. The cyber threat in the gray zone comprises espionage, threats to critical infrastructure, and disinformation campaigns. There has been a marked rise in gray zone conflict. This paper, however, is not a review of the literature available on the gray zone. Instead, it looks at the relationship between current trends in influence operations and a traditional state of war, specifically the erosion of distinctions between wartime and peacetime activity and the emergence of a gray zone of blended activity. This paper also

[1] The gray zone refers to "employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces" (International Security Advisory Board (ISAB), (January 3, 2017), *Report on Gray Zone Conflict*, https://www.state.gov/documents/organization/266849.pdf).

looks at how microelectronics-based technologies, which are driving today's global media ecosystem, have affected the scope and focus of both civilian life and defense and intelligence activities. The development rate of microelectronics-based technologies has outstripped the development of the necessary usage and regulatory frameworks on the civilian side and doctrine and authorities on the military side. The rise in these technologies, and the influence operations they enable, has created a challenge regarding the development of related military doctrine, as it ideally should evolve at a rate comparable to the evolution of the platforms and systems supporting the operators. This doctrine must account for the lack of borders in cyberspace.

There is no single answer or method for defending against influence operations in the global media environment. Addressing the threat of adversary influence operations requires public and private sector participation and a three-pronged approach of regulation, education, and government agency action. Broad regulation is a Congressional responsibility and could restrict the dissemination of information shared online in certain circumstances. Education and media literacy campaigns can give the public tools to help them identify disinformation and think critically about information they interact with online.

Making people aware of disinformation campaigns is a first step, but stopping current campaigns and deterring new ones require further action. A whole-of-government approach to fighting disinformation would focus agency authorities and resources where they're needed most. The Department of Defense (DoD) has the technical resources to lead such an effort but is limited by policy and law. Partnering with other agencies may enable DoD to provide cyber capabilities and expertise when and where needed.

Contents

1. Introduction

A. Global Shifts and the Gray Zone

The global media ecosystem has changed dramatically in the past two decades. Despite a few notable examples, the Internet has transcended borders and enabled unprecedented access to information. It has affected how we consume news, spend our money, engage with politics, and live our lives.

During these two decades, the U.S. military was focused on the Middle East. Russia and China, however, have been focused on great power competition. Russia is attempting to reestablish its historical sphere of influence and become, once again, a global power. Russia's actions in Crimea and the Ukraine, engagement in Syria, and commitment to developing a new generation of advanced weapons systems speaks to this. China is using its economic power to extend its global power and influence: It is developing advanced weapons systems, building islands in the South China Sea, making incursions into other countries' territorial waters, and embarking on its Belt and Road Initiative, a huge infrastructure project that would connect China with Pakistan, India, and other countries in Southeast Asia and East Africa.[2] Though the U.S. still retains military supremacy, both Russia and China have developed substantial cyber capabilities and the supporting doctrines for their use.

Our increasingly hyper-connected world creates a new, qualitatively different type of attack surface and a corresponding increase in vulnerability. It also upends traditional notions of conflict. In this digitized world, it is far easier, and requires fewer resources, to attack than to defend. Today, an adversary could be another nation, a terrorist group, or a single hacker. Cyberattacks against critical infrastructure (e.g., water, finance, or healthcare) can weaken our defenses, put sensitive information at risk, and affect lives. The bulk of these activities occur in the *gray zone*,[3] which occupies the area between diplomatic engagement and military action and comprises activities that maintain sufficient plausible deniability to discourage a conventional military response.

---

[2] Chatzky, A. and McBride, J., (May 21, 2019), "China's Massive Belt and Road Initiative," *Council on Foreign Relations*, https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

[3] The *gray zone* refers to "employing instruments of power—often asymmetric and ambiguous in character—that are not direct use of acknowledged regular military forces" (International Security Advisory Board (ISAB), (January 3, 2017), Report on Gray Zone Conflict, https://www.state.gov/documents/organization/266849.pdf).

In the gray zone, the cyber threat comprises espionage (for both intelligence and intellectual property), threats to critical infrastructure, and disinformation campaigns.[4] Cyberattacks on critical infrastructure that result in physical effects are generally considered acts of war, but other activities and effects that do not manifest physically are more difficult to categorize. There are currently no international standards or norms for cyber activity, which gives adversaries significant legal leeway that, in conjunction with difficulties regarding definitive attribution, hampers government response.

These shifts have prompted a rise in gray zone activities. This paper, however, is not a review of the extensive and growing body of literature available on the gray zone. Instead, it focuses on the intersection of media and advanced technology in the context of established trends in military doctrine and current and future gray zone activities, specifically disinformation campaigns and influence operations.

B. Microelectronics and Doctrine Development

Though the intent of war may not change, the character of war—where it is fought; the methods and tactics used; the social, cultural, and political influences behind it; and the players involved—is subject to change. War is an interaction between communities, and its character depends on the tools and technologies used to shape those interactions.[5] The Department of Defense's (DoD) *2018 National Defense Strategy* recognizes that the current and future operational environment is "affected by rapid technological advancements and the changing character of war."[6] The most rapid advancements are occurring in microelectronics. This unprecedented revolution is well-appreciated by the world's militaries, which seem to be attempting to emulate the battlefield sensing and command, control, and communications (C3) capabilities currently deployed by the U.S. military.

The microelectronics revolution has also changed how society collects, manages, and acts on information. Cell phones, Voice-over Internet Protocol (VoIP), social media sites, and e-commerce platforms (e.g., Amazon and business-to-business equivalents), to name a few, have deeply affected civilian life. They have also affected the scope and focus of

---

[4] The Atlantic Council has a similar characterization of potential adversary activities in the gray zone: "As revisionist states leverage disruptive technologies to undermine US interests across the world at a level beneath the threshold of armed conflict, this digital gray zone sees near-constant espionage, sabotage, and influence operations" (Watts, J., Jensen, B., Work, J.D., Whyte, C., and Kollars, N., (September 2019), Alternate Cybersecurity Futures, Atlantic Council Scowcroft Center for Strategy and Security).

[5] Brown, Z.T., (March 12, 2019), "Unmasking War's Changing Character," *Modern War Institute*, https://mwi.usma.edu/unmasking-wars-changing-character/.

[6] Department of Defense, (2018), *Summary of the 2018 National Defense Strategy of the United States of America*, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

defense and intelligence activities. DoD defines *information operations* as "the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[7] The U.S. military participates in a wide range of military operations. Military operations may include defense support of civil authorities, peace operations, noncombatant evacuation, foreign humanitarian assistance, and nation building. [8]An *information-related capability* (IRC) is a "tool, technique, or activity employed within a dimension of the information environment that can be used to create effects and operationally desirable conditions."[9] Based on the nature of information operations, the authority for the U.S. to conduct information operations requires a detailed and rigorous legal interpretation of authority and/or the legality of specific actions.[10] This paper uses the term *influence operations*, which are the coordinated application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster and promote certain attitudes, decisions, or behaviors in a target audience.[11] Influence operations may take place during either military operations or gray zone activities, and the practitioners reside in either military or non-military organizations.

The development rate of microelectronics-based civilian or military technologies has outstripped the development of the necessary regulatory and usage frameworks in the civilian sector and doctrine and authorities in the military sphere. It is not uncommon for new technologies or new applications of existing technologies to create a temporary advantage for the innovator and early adopters while doctrine and defensive technologies adjust. The use of tanks for blitzkrieg, a mass of aircraft carriers to attack a harbor, air power for strategic bombing, and commercial airliners as precision-guided weapons are all examples of known technologies applied in novel and unexpected ways. In the microelectronics arena, new and unforeseen applications of rapidly evolving technology are commonplace.

Predicting a new application of a current microelectronics technology is difficult. It is even more difficult to predict when a new, disruptive, or qualitatively different technology may be created. Computing power as a function of cost has been increasing

---

[7] Joint Publication 3-13, (November 27, 2012), *Information Operations*, incorporating Change 1, November 20, 2014.

[8] Ibid.

[9] Ibid.

[10] Ibid.

[11] Larson, E.V. et al., (2009), "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," *Rand*, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.

exponentially over the past 50 years and is expected to continue to do so. This increase in computing power leads to an increase in opportunities and risks for military use of microelectronics-based technologies. New and emerging technologies will make it easy to track individual opinions, biases, interests, and beliefs. Recent activity in this arena—namely, using social media to influence elections and sow discord in targeted populations—is highly visible and highlights the difficulties of keeping up with technology innovation.

C. Research Focus

This paper looks at the relationship between influence operations and a traditional state of war, specifically the erosion of the distinction between wartime and peacetime activity and the emergence of a gray zone of blended activity. Cyber operations are part of this blended activity, but this paper does not focus on cyber operations for purposes of sabotage or to create kinetic effects. Instead, this paper focuses on influence operations conducted in the cyber domain. This includes techniques and tactics that fall both inside and outside Title 10 authorities for U.S. military activities and Title 50 authorities for intelligence activities. The media, particularly social media, is a major player, and activity is affected by technology innovation and the novel use of existing technologies. Today, we are in a reactive state, scrambling to keep pace with technology and respond to its effects.

This paper also addresses the question of authority: Who should be responsible for defending against and responding to influence operations? The instruments of national power are defined as diplomatic, informational, military, and economic (DIME).[12] Dividing diplomatic, military, and economic power among the proper authorities is mostly straightforward. In the U.S., diplomatic power belongs to the Department of State, military power to DoD, and economic power includes the Department of the Treasury and the Department of Commerce. Informational power is more difficult to assign and categorize. Most U.S. government agencies could reasonably lay claim to responsibility for some aspects of informational power, but the private sector, especially media and tech companies, has influence as well. Regulating and applying informational power requires the use of government and non-government channels.

[12] Theohary, C.A., (March 5, 2018), CRS Report 7-7500, "Information Warfare: Issues for Congress," *Congressional Research Service*.

2. The Evolution of Influence Operations

A. Historical Use of Propaganda and Influence Operations

Propaganda, the predecessor to influence operations, is the deliberate spreading of information or rumor to either help or harm a cause, institution, or person.[13] Today, propaganda may also be defined as "a consistent, enduring effort to create or shape events to influence the relations of the public to an enterprise, idea or group."[14] Propaganda is a means by which to win the struggle for the hearts and minds of the people, a method that relies on emotion as much as information.

The earliest uses and forms of propaganda used symbolism, such as architecture, coins, and oral tradition, to glorify leaders and secure their power. Alexander the Great, for example, replaced the face of Hercules, son of Zeus, on Greek coins with his own face. This change implied that Alexander was a real-life son of Zeus, simultaneously deifying him and establishing his power and right to rule. The imposing facades and white-stone columns of modern government buildings are an attempt to capture some of the Roman Empire's manufactured glory.

The printing press made producing literature faster, easier, and less expensive, resulting in massive cultural changes. The Protestant Reformation, the Renaissance, and the Scientific Revolution were accelerated by the mass production and dissemination of literature.[15] Mass production methods also made it easier to both inform and persuade. The distribution of pamphlets and newspapers expanded during the Revolutionary War: At one point, there were more than 70 newspapers in circulation. There was a corresponding boom in political cartoons, with Benjamin Franklin publishing the first cartoon in an American newspaper in 1754. The cartoon, a snake cut into eight pieces with the slogan, "Join or Die," was meant to compel the colonies to create a union.[16] During World War I, the U.S. Division of Pictorial Publicity used posters to sell the war to an isolationist America. The most famous is the poster showing Uncle Sam pointing at the viewer over the words, "I

---

[13] "propaganda," *Merriam Webster*, https://www.merriam-webster.com/dictionary/propaganda, accessed October 5, 2018.

[14] Bernays, E., (2005), *Propaganda*, New York: Ig Publishing. (Original work published 1928).

[15] Dewar, J.A., (1998), "The Information Age and the Printing Press: Looking Backward to See Ahead," *Rand*, https://www.rand.org/pubs/papers/P8014/index2.html.

[16] Ibid.

want you for U.S. Army."[17] The image is stern and compelling, reminding viewers of their duty to serve their country in a time of war.

Radio increased connectivity, giving people all over the world shared experiences and enabling information to be spread instantaneously. President Franklin Delano Roosevelt used direct radio broadcasts, known as his "fireside chats," to communicate directly with the public during the Great Depression and World War II (WWII). The chats had an informal tone, which greatly appealed to Roosevelt's audience, and ended on a patriotic note with "The Star Spangled Banner."[18] But increased connectivity engendered risk as well. One of the most famous radio broadcasters, Tokyo Rose,[19] used her platform to play American music and spread demoralizing propaganda to U.S. military personnel stationed in the Pacific theater during WWII. The effects of the propaganda on the troops was minor, but the information she revealed concerning U.S. ship and troop movements worried the Army.[20]

Television and movies brought patriotism into homes and theaters. The U.S. government established the Office of War Information (OWI), its propaganda arm, in 1942. The OWI's Bureau of Motion Pictures used live footage from major WW2 fronts and stories about home-front activities to create newsreels that played in theaters before the movies started. These newsreels were motivational tools that highlighted the bravery of U.S. military personnel abroad and incited patriotism at home.[21]

Television and radio also brought news broadcasts to the masses. In 1949, the Federal Communications Commission (FCC) worried that the three main television networks (NBC, ABC, CBS) could use their near-monopoly on nationwide broadcasting to bias public opinion. To counter this, the FCC determined that FCC-licensed broadcasters for television and radio should include controversial issues of public importance in their broadcasts and air differing and opposing views of these issues. This became the Fairness

---

[17] Cook, J., (July 28, 2014), "The Posters That Sold World War I to the American Public," *Smithsonian Magazine*, https://www.smithsonianmag.com/history/posters-sold-world-war-i-american-public-180952179/, accessed October 2, 2018.

[18] Biser, M., "The Fireside Chats: Roosevelt's Radio Talks, The White House Historical Association," https://www.whitehousehistory.org/the-fireside-chats-roosevelts-radio-talks, accessed October 4, 2018.

[19] Tokyo Rose is thought to either be one woman, Iva Toguri d'Aquino, who was convicted of treason in 1948, or a group of women broadcasting under the pseudonym ("Iva Toguri d'Aquino and 'Tokyo Rose,'" FBI, https://www.fbi.gov/history/famous-cases/iva-toguri-daquino-and-tokyo-rose, accessed October 3, 2018).

[20] "Iva Toguri d'Aquino and 'Tokyo Rose,'" FBI, https://www.fbi.gov/history/famous-cases/iva-toguri-daquino-and-tokyo-rose, accessed October 3, 2018.

[21] Stewart, P.W., (2015), "A Reel Story of World War II: The United News Collection of Newsreels Documents the Battlefield and the Home Front," *Prologue Magazine*, Fall 2015, 47(3), https://www.archives.gov/publications/prologue/2015/fall/united-newsreels.html.

Doctrine.[22] Though the Fairness Doctrine was meant to balance reporting of controversial issues, news organizations and others criticized it for impinging on the rights of journalists. The FCC repealed it in 1987. The repeal is noted as the impetus for the rise of conservative talk radio, which commands impressive audiences and has widespread political influence.[23]

The United States Information and Educational Exchange Act of 1948, otherwise known as the Smith-Mundt Act,[24] restricted disseminating U.S. government-created media domestically. U.S. government-run media outlets such as Voice of America and Radio Free Asia were only able to publish and broadcast information to foreign audiences to avoid subjecting U.S. citizens to government propaganda.[25] This changed with the Smith-Mundt Modernization Act of 2012, which authorized the Secretary of State and the Broadcasting Board of Governors to make information intended for foreign dissemination available within the U.S. It also amends the Foreign Relations Authorization Act for Fiscal Year 1986 and Fiscal Year 1987 to prohibit Department of State and Broadcasting Board of Governors funds from being used to spread propaganda in the U.S.[26]

Advertising uses propaganda techniques to convince consumers that, by purchasing a product, they are filling a need or desire that will ensure a better life, increase social standing, or cement moral superiority. Advertising sells ideas, which in turn sell products. Advertisers sell these ideas through stories, capturing narratives that already exist in society and appealing to consumer desire to be uplifted or improved. These stories rely on imagery and symbolism and use cultural tropes to create an aspirational lifestyle.

All of these propaganda techniques have applications in modern influence operations, and the range of applications has greatly expanded in cyberspace.

B. Characteristics of Information Operations and Influence Operations

Information operations occur within, and are intended to affect, the *information environment*, which DoD defines as "individuals, organizations, and systems that collect,

---

[22] Fletcher, D., (February 20, 2009), "The Fairness Doctrine," *Time*, http://content.time.com/time/nation/article/0,8599,1880786,00.html.

[23] Clogston, J.F., (2016), "The Repeal of the Fairness Doctrine and the Irony of Talk Radio: A Story of Political Entrepreneurship, Risk, and Cover," *Journal of Policy History*, 28(2), 375-396, doi:10.1017/S0898030616000105.

[24] United States Information and Educational Exchange Act of 1948, 22 U.S.C. § 1461.

[25] Metzgar, E.T., (January 21, 2013). "Smith-Mundt reform: In with a whimper?" *Columbia Journalism Review*, https://archives.cjr.org/behind_the_news/smith-mundt_modernization_pass.php.

[26] Smith-Mundt Modernization Act of 2012, H.R. 5736, 112th Cong., (2012).

process, disseminate, or act on information."[27] They also comprise different types of operations. *Psychological operations* involve the use of propaganda to shape the motives and behavior of a government, group, or individual. *Military deception* uses false information or disinformation to mislead an adversary into making a decision or taking an action that benefits the U.S.[28] *Cyberspace operations* involve "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace."[29] These objectives range from accessing information, to spreading information, to creating some physical effect, such as degrading site performance or accessing critical infrastructure. DoD doctrine separates cyberspace operations and information operations, but they are inextricably linked. Though the information environment includes both cyberspace and the physical world, and cyber operations extend beyond accessing and disseminating information, cyberspace is where most information operations are occurring today.

DoD does not have a formal definition of influence operations. For this paper, we consider influence operations to use true information, propaganda, misinformation (unintentionally false information), and disinformation (intentionally false information) to achieve a desired outcome. Figure 2-1, below, highlights the differences between DoD-defined information operations and influence operations. Target audiences range from individuals, to groups, to entire populations, and there are varying methods for reaching an intended target. Influence operations have two components: the message and the delivery method. One method is the use of mass media—TV, newspapers, radio, etc.—to reach the broadest possible audience. But using mass media subjects a message to editing, which may change its meaning, or outright rejection. Another method is to use less regulated means of communication to ensure the message is unadulterated. These means include flyers, posters, word of mouth, or postings online on social media sites or other message boards.[30]

---

[27] Ibid.

[28] Theohary, C.A., (March 5, 2018), CRS Report 7-7500, "Information Warfare: Issues for Congress," *Congressional Research Service*.

[29] Joint Publication 3-12, (June 8, 2018), *Cyberspace Operations.*

[30] Larson, E.V. et al., (2009), "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities," *Rand*, https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.

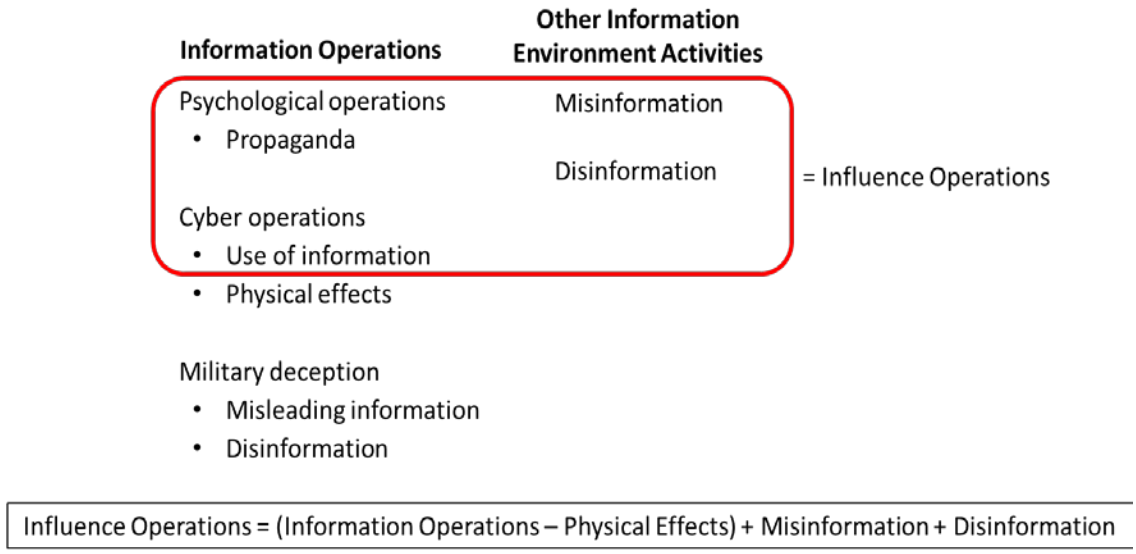

Figure 2-1. Information and Influence Operations

Conducting effective influence operations requires thorough knowledge and understanding of the target audience's demographics, ideals, beliefs, attitudes, values, decision-making processes, and receptiveness to information. The source of the information intended to influence needs to seem authentic and credible to gain the audience's trust, and the information itself must be packaged for maximum appeal.[31] The environment today is saturated with information. For an influence operations campaign to be successful, it must reach the target audience. Information must be both familiar and novel to foster engagement.[32]

C. How Technology Has Affected Influence Operations

The basic tenets of propaganda and influence operations have not changed over time. Instead, the means by which they are employed have changed. The advent of the Internet changed how information is presented and consumed. This change represents an inflection point in technology development that created a new attack surface for influence operations.

In the Internet's early days, many media outlets were initially reluctant to create robust digital offerings because of skepticism about the Internet and paltry online advertising revenues. But as the Internet started to dominate the media landscape, attitudes changed. Publications had to shift from print to digital to stay afloat, even as they struggled with a drop in ad revenue. This shift required new strategies for attracting and maintaining

[31] Ibid.

[32] Vosoughi, S., Roy, D. and Aral, S., (March 9, 2018), "The spread of true and false news online," *Science*, 359, 1146-1151.

online readership and new standards for online publication. Rather than waiting for the next day's newspaper or tuning in to the evening news, readers embraced the immediacy of the Internet and sparked the information-saturated 24-hour news cycle. The race to be first—to break news, draw readers, get the clicks needed to drive advertising revenue—took precedence over the need to be correct. Reader attention spans shortened, which drove demand for shorter articles and "clickbait" headlines that are designed to attract readers but do not always reflect the content of the article. Clickbait headlines are designed to evoke some sort of emotional response, which prompts the reader to click on a link to see more. That link often leads to a site featuring paid advertisements. Site owners depend on user interaction with the advertisements to generate this income, thus increasing the demand for clickbait.[33]

Site owners, publishers, and advertisers rely on the algorithms that control the content a user sees on search engines and social media sites. Economic pressures drove publishers and advertisers to monetize user data. The algorithms gather as much information about users as possible, including location, age, education, political beliefs, contacts, pop culture preferences, and what posts garner the most likes or activity. The algorithms then tailor the available content to best suit each user's preferences while also taking into account whether the site was paid to promote a post and how other people in the user's network have interacted with a post.[34] Personalized content drives continued use of the site, which increases advertising revenues and gives the algorithm even more information. Algorithms are not concerned whether a post is innocuous, provocative, or extremist, as long as it fosters engagement.[35]

The Internet's immediacy and ease of access also precipitated the rise of niche publications and blogs that catered to specific audiences. These sites created communities of people that revolve around personal identity, interests, hobbies, or ideology. This led to the creation of algorithm-generated online echo chambers, in which beliefs and views are met with similar and supporting narratives. Echo chambers have become a hallmark of social media sites, which began as a way for people to connect with others but have evolved into platforms for sharing news and spreading opinion and ideology. Social media echo chambers, driven by algorithmic tailoring, validate and amplify existing beliefs and

---

[33] Bradshaw, S. and Howard, P.N., (January 29, 2018), "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life," *Knight Foundation*, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

[34] Hern, A., (May 22, 2017), "How social media filter bubbles and algorithms influence the election," *The Guardian*, https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles.

[35] Fischer, M. and Taub, A., (April 25, 2018), "How Everyday Social Media Users Become Real-World Extremists," *The New York Times*, https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html.

opinions and exclude narratives that challenge them. Today, it is easier than ever to find communities of like-minded people online and to isolate yourself from opinions that differ from your own.

3. The Current Influence Operations Environment

The current environment is driven by online connection and engagement. Content—articles, video, images—drives user engagement with news stories, advertising, and ecommerce sites. The expectation is to be connected constantly, which has led to an always-on business culture and the blurring of the distinction between work life and home life, between real life and virtual life. It has also led to mental health issues[36] and precipitated a rise in online harassment, known as cyberbullying.[37] Though more sites now verify identities for user accounts, the practical anonymity of the Internet—whether real or perceived—provides a pass for sharing hurtful and incendiary information without fear of attribution.

The biggest appetite in this environment is for data. Email services, search engines, ecommerce sites, and social media sites collect data from user accounts. Social media is designed to hold and keep user attention; more data is collected and revenue generated the longer a user scrolls.

A. Social Media

Today, more than half of all social media users use a social media site for news, and one in 10 users rely on social media as their only news source.[38] Social media users have the ability to pull content they deem interesting or relevant and share it with others, rather than relying on news organizations and publications to push content to them.[39]

This has sparked a rise in citizen journalism. Users not affiliated with a news organization are able to post pictures and video of an event or spread breaking news, providing valuable eyewitness accounts of events as they happen. News of the 2008

[36] Twenge, J.M. and Campbell, W.K., (2018), "Associations between screen time and lower psychological well-being among children and adolescents: Evidence from a population-based study," *Preventive Medicine Reports*, Vol. 12, December 2018, pp. 271-283, https://doi.org/10.1016/j.pmedr.2018.10.003.

[37] Federal Trade Commission, (September 2011), "Cyberbullying," *Federal Trade Commission Consumer Information*, https://www.consumer.ftc.gov/articles/0028-cyberbullying.

[38] Bradshaw, S. and Howard, P.N., (January 29, 2018), "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life," *Knight Foundation*, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

[39] Ibid.

bombings in Mumbai, for example, was broken over Twitter, and pictures were posted to Flickr, a photograph-sharing site.[40] Video, such as the cellphone videos exposing police brutality and racism,[41] has provided evidence for indictments and criminal cases and reshaped national narratives on police behavior and accountability.

The issue with citizen journalism, however, has to do with reliability and trust. Journalists who work for news organizations and publications are held to standards that promote credibility, such as fact checking. Citizen journalists are not subject to these standards and are thus more likely to take something out of context or spread false information. Misinformation is more likely to go viral than the truth,[42] and though some have issued corrections or tried to retract false information, their attempts do not reach the same number of people as their original assertions did.[43]

False or misleading information, whether mistakenly shared by citizen journalists or deliberately spread to manipulate others, is often novel, especially compared with true information, and presented in a manner meant to provoke outrage, which practically guarantees engagement. Interacting with false information can lead users down rabbit holes,[44] following threads that often lead to polarizing information that can spur offline action.

Increasingly, what happens online has real-world effects. Twitter, for example, has been used to coordinate disaster response efforts, organize grassroots political campaigns, harass journalists and other public figures, foment revolution, and affect jobs. The #MeToo movement revealed episodes of sexual harassment and assault perpetrated by prominent men and some women. Each reveal precipitated a backlash in which Twitter users demanded that the accused resign and organized boycotts of the accused's company or commercial interests. Many resigned or were removed from their positions. Some cases,

---

[40] Beaumont, C., (November 27, 2008), "Mumbai attacks: Twitter and Flickr used to break news," *The Telegraph*, https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

[41] Denby, G., (October 18, 2014), "Videos of Deadly Police Encounters Grab the Media Spotlight, but Why?" *NPR*, https://www.npr.org/blogs/codeswitch/2014/10/08/354507430/videos-of-deadly-police-encounters-grab-media-spotlight.

[42] Vosoughi, S., Roy, D. and Aral, S., (March 9, 2018), "The spread of true and false news online," *Science*, 359, 1146-1151.

[43] Singal, J., (October 19, 2016), "'Citizen Journalism' Is a Catastrophe Right Now, and It'll Only Get Worse," *New York Magazine*, http://nymag.com/intelligencer/2016/10/citizen-journalism-is-a-catastrophe-itll-only-get-worse.html.

[44] The term "down the rabbit hole" originated with Lewis Carroll's book *Alice in Wonderland*, in which Alice falls into and down a rabbit hole that eventually leads her to Wonderland. Today, the term "rabbit hole" refers to "a complexly bizarre or difficult state or situation conceived as a hole into which one falls or descends," especially "one in which the pursuit of something (such as an answer or solution) leads to other questions, problems, or pursuits" ("rabbit hole," *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/rabbit%20hole, accessed October 1, 2019).

such as those regarding Harvey Weinstein[45] and Bill Cosby,[46] resulted in criminal investigations and trials. The #MeToo movement has also sparked a nationwide discussion of harassment, power dynamics, and appropriate behavior in the workplace.

In the summer of 2018, two dozen people in India were killed by lynch mobs because they were suspected of participating in child-kidnapping rings or plots to harvest organs. The mobs were fueled by unfounded rumors spread on WhatsApp, an encrypted messaging platform owned by Facebook.[47] WhatsApp trades on end-to-end encryption, which allows only two people, the sender and the intended recipient, to read a message. End-to-end encryption keeps data encrypted both in transit and at rest, even at the server. This means services like WhatsApp cannot access the messages transmitted through its server.[48] It also poses a challenge to law enforcement or other government agencies that may want access to messages as evidence for criminal or terrorist investigations. WhatsApp has a Law Enforcement Online Request system to handle requests for account records, but does not consider message content as part of disclosures compelled by U.S. law.[49]

Russia embarked on a massive hacking, disinformation, and political ad campaign leading up to the 2016 U.S. presidential election. The Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and National Security Agency (NSA) concluded that Russian-backed hackers were behind the breach of the Democratic National Committee's (DNC) computer server and shared thousands of emails with WikiLeaks to discredit the DNC and jeopardize Hillary Clinton's prospects as the Democratic nominee for president. The Internet Research Agency (IRA), a Russian entity, created fraudulent Facebook accounts, political pages, and event pages meant to exploit existing fault lines in American culture and amplify existing fears, a classic propaganda strategy the Russians

---

[45] Gonzalez, S., France, L.R. and Melas, C., (October 4, 2018), "The year since the Weinstein scandal first rocked Hollywood," *CNN*, https://www.cnn.com/2018/04/05/entertainment/weinstein-timeline/index.html.

[46] Bowley, G. and Hurdle, J., (April 26, 2018), "Bill Cosby Is Found Guilty of Sexual Assault," *The New York Times*, https://www.nytimes.com/2018/04/26/arts/television/bill-cosby-guilty-retrial.html?rref=collection%2Fnewseventcollection%2FThe%20Cosby%20Trial&action=click&contentCollection=Television&module=inline&region=Marginalia&src=me&version=newsevent&pgtype=article.

[47] Dwoskin, E. and Gowen, A., (July 23, 2018), "On WhatsApp, fake news is fast—and can be fatal," *The Washington Post*, https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html?noredirect=on&utm_term=.05a5faed4172.

[48] Unith, N., (September 5, 2018), "What is End-to-End Encryption?" *Lifewire*, https://www.lifewire.com/what-is-end-to-end-encryption-4028873.

[49] WhatsApp, (2019), "Information for Law Enforcement Authorities," https://faq.whatsapp.com/en/android/26000050/?category=5245250.

had also deployed during the Cold War.[50] The fraudulent accounts mimicked social media activists on both sides of the political divide and organized real-life protests with legitimate activist groups.[51] The campaign was intended to bolster support for Donald Trump, the Republican nominee, and deter would-be Clinton supporters. This influence campaign is not a one-time event: Two years after the presidential election, Facebook uncovered a similar and more sophisticated influence campaign targeting the 2018 U.S. midterm elections.[52]

Special Counsel Robert Mueller, who was assigned to investigate Russian interference in the 2016 presidential election and possible links between Russian officials and Trump associates, filed two indictments related to his investigation. The first, filed in February 2018, charged the Internet Research Agency, 13 Russian citizens, and two other Russian companies with interfering with the U.S. political system and electoral process, including the 2016 presidential election.[53] The second, filed in July 2018, charged 12 members of the Main Intelligence Directorate of the Russian General Staff (known as the GRU) of hacking into email accounts affiliated with Hillary Clinton's presidential campaign and computer networks belonging to the Democratic Congressional Campaign Committee and the Democratic National Committee, stealing documents, and releasing those documents to affect the outcome of the election.[54] Mueller also warned Congress that the 2016 election was just the beginning in terms of foreign interference. The indictments did not stop the activity, and attempted interference can and will continue.

Social media is also prime grounds for terrorist group recruitment and radicalization. The terrorist group the Islamic State of Iraq and al-Sham (ISIS), also known as the Islamic State of Iraq and the Levant (ISIL), ran a sophisticated, multi-faceted propaganda campaign to glorify its mission and make life under the caliphate seem like paradise.[55] Recruiters

---

[50] Deeks, A., McCubbin, S., and Poplin, C.M., (October 25, 2017), "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.

[51] Roose, K., (August 1, 2018), "Facebook Grapples with a Maturing Adversary in Election Meddling," *The New York Times*, https://www.nytimes.com/2018/08/01/technology/facebook-trolls-midterm-elections.html.

[52] Ibid.

[53] Department of Justice Office of Public Affairs, (February 16, 2018), "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System," https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

[54] Kahn, M., (July 13, 2018), "Document: Special Counsel Indicts 12 Russian Intelligence Officers for Hacking DNC and Clinton Campaign," *Lawfare*, https://www.lawfareblog.com/document-special-counsel-indicts-12-russian-intelligence-officers-hacking-dnc-and-clinton-campaign.

[55] Koerner, B.I., (2016), "Why ISIS Is Winning the Social Media War," *Wired*, https://www.wired.com/2016/03/isis-winning-social-media-war-heres-beat/#slide-5.

used social media to establish relationships with potential recruits, establishing a sense of intimacy and camaraderie to manipulate recruits into joining.[56]

Many, if not most, recent lone-wolf terrorist attacks, including the plague of mass shootings terrorizing the U.S., have roots in online communities and social media sites. Some online communities—echo chambers that validate perceived grievances and advocate violence in response—encourage shootings or other violent acts. Dylann Roof, who shot and killed nine African Americans in the Emanuel African Methodist Episcopal Church in Charleston, South Carolina, in June 2015, self-radicalized using white supremacist and neo-Nazi websites. Roof's exposure to these sites began with a Google search for "black on white crime" following the Trayvon Martin case.[57] Google's algorithm led him to sites peddling racist propaganda and falsified statistics about black-on-white crime.[58] Roof immersed himself in these sites, eventually creating his own site and writing a racist manifesto.

B. How the Current Environment Has Made the U.S. More Vulnerable to Adversary Influence Operations

The continuous expansion of the Internet creates an ever-growing and ever-changing attack surface. With more people online and more places for them to communicate come more opportunities to spread fake news or narratives meant to manipulate people.[59] It is far easier for one person or a group to spread propaganda than it is for an organization to stop all instances of it.

Growing mistrust of the media opens avenues for propaganda and fake news. Much of this mistrust is based on the perception of bias in the news or of a powerful publication using its platform to push a particular agenda.[60] In the U.S., this is seen in the competition between so-called liberal media (e.g., *The New York Times*, *The Washington Post*) and conservative media (e.g., Fox News, *The Wall Street Journal*). This is also common in the United Kingdom (U.K.): U.K. publications make no secret of their political leanings, and

---

[56] Erelle, A., (June 2, 2015), "How One Journalist Found Herself Courted by ISIS," *Vogue*, https://www.vogue.com/article/in-the-skin-of-a-jihadist-isis-recruitment-network-excerpt-anna-erelle.

[57] Collins, C., (2017), "The Miseducation of Dylann Roof," *Teaching Tolerance*, https://www.tolerance.org/magazine/fall-2017/the-miseducation-of-dylann-roof.

[58] Ibid.

[59] Anderson, J. and Rainie, L., (October 19, 2017), "The Future of Truth and Misinformation Online," *Pew Research Center*, http://www.pewinternet.org/2017/10/19/the-future-of-truth-and-misinformation-online/.

[60] Newman, N. and Fletcher, R., (2017), "Bias, Bullshit and Lies: Audience Perspectives on Low Trust in the Media, Digital News Project 2017," Reuters Institute for the Study of Journalism and University of Oxford, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-11/Nic%20Newman%20and%20Richard%20Fletcher%20-%20Bias%2C%20Bullshit%20and%20Lies%20-%20Report.pdf.

U.K. tabloids such as the Daily Mail are notorious for sensationalized stories. Often, the content of the editorial pages, which represent the views of the publication itself, is conflated with the news pages, which aim for objectivity. Political polarization generates mistrust, no matter the publication's commitment to fact checking and other journalistic standards.

For many readers, it is difficult to define a distinct line between real news and fake news. Instead, they consider the differences to lie along a spectrum comprising real news, opinion pieces, propaganda, and fake news.[61] Information that is accurate and fairly presented is considered more trustworthy, but mistrust comes from perceptions of bias or spin. Though some information can be easily identified as false or misleading, the spectrum suggests that what is considered fake news is somewhat up to the reader. If certain information reinforces a reader's beliefs or views, then the reader is more likely to consider the information true. If the information suggests something different, the reader may attribute that difference to political beliefs. If the information directly contradicts certain beliefs or views, the reader is more likely to dig in his or her heels and cling to that belief. This is known as "the backfire effect."[62] The backfire effect makes it easy for readers to dismiss factual information as fake news because it conflicts with what they believe. It also leaves readers open to propaganda and misinformation that reinforce their beliefs.

Social media algorithms provide an easy conduit for such information. A search that begins with innocuous content can quickly lead to propaganda or even content espousing hate speech or promoting violence. Algorithms are also increasingly able to target small, specific groups of people. This makes it easy for advertisers—and adversaries—to target groups as well. The Russian Internet Research Agency's propaganda campaign on Facebook in 2016 created numerous accounts and events that targeted narrow interest groups on both sides of the political spectrum. The Internet Research Agency also deployed more than 150,000 Twitter accounts to post messages before the 2016 Brexit referendum that urged Britain to leave the E.U. Most of the messages focused on stoking existing fears about Muslims and immigrants, two issues that were proving divisive in the debates around the referendum.[63] The Twitter messages employed the same strategy that the Internet Research Agency used in the U.S. Rather than creating something new, the Internet Research Agency used algorithmic targeting to identify current issues under discussion and

---

[61] Ibid.

[62] Silverman, C., (June 17, 2011), "The Backfire Effect: More on the press's inability to debunk bad information," *Columbia Journalism Review*, https://archives.cjr.org/behind_the_news/the_backfire_effect.php.

[63] Kirkpatrick, D.D., (November 15, 2017), "Signs of Russian Meddling in Brexit Referendum," *The New York Times*, https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html.

contribute to them. It is much easier to exploit existing divisions than it is to create new ones.

4. Technology and the Evolving Threat

A. Technology in the Current Information Environment

The current environment is marked by the confluence between cyber capabilities and influence operations. Social engineering campaigns, which include phishing, spear phishing, and baiting, take advantage of human nature to induce individuals to unknowingly infect their computer systems with malware, which leaves their systems vulnerable to information theft and ransomware scams. Phishing and spear phishing use email or other types of communication that seem legitimate to establish trust with the target and convince the target to click on an infected link or divulge sensitive information. Baiting exploits human curiosity by, for example, leaving malware-infected devices lying around in the hopes that people will find them and load them onto their computers.[64] Artificial intelligence (AI) is enabling bots to appear more human, making it difficult to differentiate between real users and bots. These social engineering campaigns are based on old methods that deployed print, radio, TV, and even word of mouth. Many of these methods have become ubiquitous, and people learned over time how to identify and ignore the most blatant examples. But the recent revolution in data management has changed this paradigm.

There is now an unprecedented amount of personal data in the public sphere. This is enabled by Moore's Law, which predicted an exponential increase in computer functionality for a given cost.[65] As a result, the cost of collecting and analyzing data has dropped dramatically, and it is expected to continue dropping. In this interconnected world, where almost everyone has a cell phone and is engaged with social media, where most emails are scanned for content, and where records of electronic financial transactions are vacuumed up, we leave digital footprints that can be easily tracked by social media and advertising companies. These companies are primarily interested in making money, and buying or selling data is a lucrative model. The expansion of semiconductor-based products (e.g., computers, smartphones, and cars) will most likely continue for the foreseeable future, making the collection and analysis of these digital footprints even more pervasive than it is now.[66]

---

[64] Lord, N., (September 11, 2018), "What is Social Engineering? Defining and Avoiding Common Social Engineering Threats," *Digital Guardian*, https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

[65] Moore, G.E., (April 19, 1965), Electronics, Vol. 38, No. 8.

[66] There are arguments that the scaling predicted by Moore's Law may be ending in the next decade, but the industry has already begun the research and development into alternate architectures and technology

Nefarious foreign actors have been using this data in social engineering and influence operations efforts against the U.S.; Russia's interference in the 2016 U.S. presidential election is the most prevalent example. Recent advances in AI, image and video analysis, and data mining, combined with the technology of the coming decade, open up the potential for more powerful influence operations. It is possible that advanced computing will enable targeted advertising messages delivered by email or telephone that are indistinguishable from messages sent by humans and use detailed psychological profiles to tailor messages to specific targets.

Technology in the current environment can be divided into three frameworks: sensing, processing, and acting. Sensing relates to means of gathering data. Processing is both storing and accessing the sensed (gathered) data and analyzing that data to discover and extract useful information. Acting relates to how that information is used.

1. Sensing

Technologies that fit in the sensing framework gather data to create a digital footprint.

Constant surveillance has become the norm today. Cameras have long been ubiquitous in airports, around government buildings, and in other public places, but technologies such as facial recognition are making it easier to track specific people. The United Kingdom is one of the most-watched countries in the world, with approximately one closed-caption television (CCTV) camera for every 32 people.[67] Cameras also record location information, and apps like Instagram take advantage of this by providing the option to geotag pictures.

It's not just cameras that track location and habits: License plate readers, online browsers, and even phone touchscreens track where we are and what we do. Location services on our cell phones, active on applications ranging from Google Maps to Instagram, keep tabs on our whereabouts and where we often go. Stingrays—cell-site simulators pretending to be legitimate cell phone towers—track phone locations and log the unique identifying numbers of all cell phones and mobile devices in a given area. They can also intercept information about calls placed and some types of data use.[68]

Online, browser search history, time spent on certain sites, interaction with links or ads, and even email is scanned for information. Google's predictive search function provides autocomplete options for a user's search as it is typed in. The resulting drop-down

---

to continue scaling without necessarily continuing to decrease the dimensions of the actual semiconductor.

[67] Lewis, P., (March 2, 2011), "You're being watched: there's one CCTV camera for every 32 people in UK," *The Guardian*, https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

[68] Electronic Frontier Foundation (EFF), "Cell-Site Simulators/IMSI Catchers," accessed December 13, 2018, https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

list reflects both what the user has previously searched for and what is commonly searched for among a larger group. Algorithms also notice user interest, whether browsing to a site online or mentioned in the body of an email, and respond with related ads or other content. It is increasingly common to see ads relating to a certain product or service almost immediately after looking at said product or service online.

Online behavior tracking and email scanning, as well as records of online financial activity, are leading to the creation of larger, more detailed digital footprints. These footprints can be used to discern an individual's demographic information, location, purchasing history, political preferences, and more. Active digital footprints comprise information deliberately placed online, such as on a social media site or in an email. Passive digital footprints are collected without user knowledge and involve search histories, online surveys, and online purchases.

Tracking purchases and other financial information has gotten easier as financial transactions have shifted from cash to electronic. Online banking is becoming more popular, and banks are developing apps to make managing bank accounts more convenient. Banks and credit reporting agencies also track online financial activity to develop user profiles and determine user credibility and trustworthiness.

2. Processing

The processing framework refers to using the data gathered by sensing technologies to create detailed profiles. The huge amounts of data gathered also enable machine learning and AI capabilities by training the algorithms underpinning those capabilities to recognize certain patterns.

Big data—datasets or groups of datasets too large for traditional processing techniques[69]—has become big business. Big data can be analyzed to reveal patterns, trends, and other associations often relating to online behavior. Data analytics is a means of turning data into useful information. Data mining is a process for finding patterns, anomalies, and other relationships among large datasets to predict trends or other outcomes. Companies gather, buy, and sell information about current and potential future customers to learn more about those customers and develop strategies to increase revenues and decrease costs. Much of this data gathering and selling is legal and involves collecting information considered part of the public record (e.g., property records, census data, birth records, voter registration information, etc.) or voluntarily put online (e.g., social media, purchasing history, browsing history, etc.). Many sites include disclaimers about data gathering in their Terms of Service agreements.

---

[69] "Big data," *Merriam-Webster Dictionary*, accessed December 26, 2018, https://www.merriam-webster.com/dictionary/big%20data?src=search-dict-hed.

When Facebook and other social media sites first launched, no one understood the amount of information they would collect and how that collection would affect individual privacy. Now, the consequences of such information collection are known, but there is still little oversight for how this information is and should be used. Cambridge Analytica, a voter-profiling firm, acquired information from more than 87 million Facebook profiles to target voters prior to the 2016 U.S. presidential election. This information was acquired without users' permission, which violates Facebook's Terms of Service. Facebook is investigating the breach and is the target of a Federal Trade Commission (FTC) investigation examining whether Facebook violated an earlier FTC agreement to protect user information from third-party applications.[70]

Some data use is regulated. Credit and consumer reporting agencies' use of consumer reports for credit checks, insurance, and employment are regulated under the Fair Credit Reporting Act (FCRA), which defines appropriate use of consumer reports, restricts how medical information can be used and shared, and gives people the ability to access and correct errors in their credit reports.[71] Section 5 of the Federal Trade Commission Act prohibits "unfair or deceptive acts or practices in or affecting commerce," and defines unfair acts as acts that cause substantial injury, cannot be reasonably avoided, and are not outweighed by benefits, and deceptive acts as acts that mislead the consumer.[72] Whether an act is considered unfair, deceptive, or both is determined on a case-by-case basis.

Other data use is not regulated. People search sites, for example, provide personal information such as aliases, birthdates, addresses, education history, employment history, marital history, social media activity, property records, court records, and family history for free or a minor fee.[73] This information can be used for *doxing*, the act of publishing personal information online, often for coercion or revenge.[74] Hacked and stolen data is sold on the dark web for malicious purposes, such as credit card theft, identity theft, or blackmail.

---

[70] Kang, C., (March 20, 2018), "Facebook Faces Growing Pressure Over Data and Privacy Inquiries," *The New York Times*, https://www.nytimes.com/2018/03/20/business/ftc-facebook-privacy-investigation.html.

[71] Fair Credit Reporting Act, revised September 2018, 15 U.S.C. § 1681.

[72] Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, 15 U.S.C. § 45.

[73] Grauer, Y., (March 27, 2018), "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?" *Motherboard*, https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

[74] "Doxing," *Technopedia*, accessed December 26, 2018, https://www.techopedia.com/definition/29025/doxing.

3. Acting

Acting refers to using the data in processed profiles to achieve an end, whether that is for maintaining and improving security, targeting, changing legitimate opinions, or convincing or manipulating people to do something.

Data collection and analysis can instigate and influence action, whether to boost security, prevent criminal activity, or track disease outbreaks. Data mining and analytics tools such as Palantir collect information from emails, financial documents, phone records, and other sources to search for potential links. Palantir has been used to track improvised explosive devices (IED), detect fraud, conduct criminal investigations, and screen travelers in airports. Tools like Palantir have been a boon for security organizations, but they also present risks and challenges. There is no mechanism to determine whether the information collected is valid. Incorrect and misleading information collected in Palantir has resulted in mistaken arrests.[75]

Verifying information is one issue; deciding what is an appropriate use of the information is another. Some current uses, though performed in the name of security and stability, raise doubts. China's estimated 200 million surveillance cameras use facial recognition to not only look for fugitives and criminal suspects, but to identify jaywalkers and people in debt as well. Pictures of people guilty of minor infractions, along with their names and identification numbers, are displayed to encourage public shaming.[76] China is also in the process of establishing a nationwide social credit score system by the end of 2020. The system is currently being piloted in a few cities. Under this system, good behavior can raise scores and bad behavior, which ranges from committing fraud to smoking in smoke-free zones, can lower scores. Those with higher scores would receive perks, such as deposit-free apartment rentals and better placement on dating sites. Those with lower scores would be penalized; penalties include losing employment and educational opportunities as well as travel bans.[77]

B. The Future Environment

The global trend toward universal surveillance will continue as more technologies track our activity both online and offline. As the price of microelectronics-based surveillance tools has dropped dramatically, along with legitimate fears of crime and

---

[75] Waldman, P., Chapman, L., and Robertson, R., (April 19, 2018), "Palantir Knows Everything About You," *Bloomberg*, https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

[76] Mozur, P., (July 8, 2018), "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," *The New York Times*, https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

[77] Nittle, N., (November 2, 2018), "Spend 'frivolously' and be penalized under China's new social credit system," *Vox*, https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games.

nefarious state-sponsored monitoring, increased surveillance has become the norm. From the security services' perspective, universal surveillance means more information about potential terrorist activity and a better chance of stopping terrorist attacks before they happen. For countries like China, with a history marked by political upheaval, surveillance seems the ticket to preventing civil unrest and maintaining political power. From the commercial perspective, surveillance can also translate to increased profits. The algorithmic, advertising-driven Internet model depends on data. As the Internet of Things (IoT) continues to grow, and more records and systems are networked, data will become even more valuable.

Increased networking and data collection expands the potential attack surface. More data means more information about potential targets and target groups. More online systems means more access points to exploit. A state's surveillance capability could be weaponized against itself and used for a cyberattack or influence operations campaign.

Increased data collection also means a corresponding drop in privacy and a higher risk of data breaches and identity theft. A rash of high-profile data breaches over the past few years—Equifax, Marriott, the Office of Management and Budget (OMB), and Blue Cross Blue Shield, to name a few—have highlighted the vulnerabilities inherent to large data-storage systems. It is far easier to attack such a system than it is to defend one, and the increasing value of data gives plenty of incentive for data exfiltration. Electronic medical records (EMR), for example, can fetch $100 or more on the black market.

Encryption, already used in messaging apps such as WhatsApp, will continue to rise in popularity. These apps enable the free flow of information, with no means of determining whether the information is polarizing or harmful. Other apps, such as Twitter and Instagram, have direct message features to ensure more private communications. For the past few years, governments have requested backdoors into encrypted technologies for use during criminal investigations. The Five Eyes alliance—the U.S., the U.K., Canada, Australia, and New Zealand—argued that encryption has helped criminals evade the law. Tech companies, however, insist that providing backdoors would compromise user privacy and create an attack point for hackers.[78]

It will become increasingly more difficult to determine the authenticity of information online. Audio and video recordings have allowed an eyewitness view into events and have corroborated or invalidated witness accounts of what actually happened. But it is becoming easier to create faked audio and video that is almost indistinguishable from the real thing. Known as *deepfakes*, these audio and video clips make it possible for malicious actors to make it seem like someone did or said something that he or she never did or said, opening

[78] *The Week*, (September 3, 2018), "Why the Government wants a mandatory 'backdoor' on encrypted technology," https://www.theweek.co.uk/96224/why-the-government-wants-a-mandatory-backdoor-on-encrypted-technology.

up myriad avenues for disinformation.[79] Currently, the most prevalent type of deepfake involves grafting a celebrity's head onto a porn actor's body. But it would be an easy transition to deepfakes meant to destroy reputations, rig elections, erode trust in public institutions, and jeopardize national security.

Researchers are developing methods to detect deepfakes, but these methods require ample time and resources. Deepfakes are often based on audio or video available online. Looking for older versions of the material online may indicate whether it was manipulated. A frame-by-frame analysis of a deepfaked video can reveal glitches, such as fuzziness around facial features, unnatural movement, and skin tone discrepancies.[80] The Defense Advanced Research Projects Agency's (DARPA) MediFor (media forensics) program is working to create an automated system that assesses a video or image's integrity[81] by assigning an integrity score based on a series of recognizable tells, or flaws, in the video or image. The challenge with recognizing tells is that the neural networks used to create deepfakes can be trained to avoid them.

Making the public aware of deepfakes is necessary to combat their effects, but this awareness can also lead to "reality apathy," which occurs when the public becomes so accustomed to misinformation that they stop trusting what they see and hear and assume everything is meant to mislead.[82] It can also lead to the "liar's dividend," which, in the face of a glut of faked content and an audience ready to doubt the authenticity of an audio or video recording, makes it easier for someone to dispute the veracity of a true recording.[83] One proposed solution is known as lifelogging—or alibi services—that use body cameras and related technologies to record nearly every aspect of someone's life to prove their location and what they said or did at any given time.[84] Although this might serve as protection against deepfakes, it is also incredibly invasive and would remove much of the comfort from personal life.

---

[79] Chesney, R. and Citron, D., (2019), "Deepfakes and the New Disinformation War: The Coming Age in Post-Truth Geopolitics," *Foreign Affairs*, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

[80] Marconi, F. and Daldrup, T., (November 15, 2018), "How *The Wall Street Journal* is preparing its journalists to detect deepfakes," *NeimanLab*, http://www.niemanlab.org/2018/11/how-the-wall-street-journal-is-preparing-its-journalists-to-detect-deepfakes/.

[81] Turek, M., "Media Forensics (MediFor), *Defense Advanced Research Projects Agency (DARPA)*, https://www.darpa.mil/program/media-forensics.

[82] Warzel, C., (February 11, 2018), "He Predicted the 2016 Fake News Crisis. Now He's Worried About an Information Apocalypse," *Buzzfeed News*, https://www.buzzfeednews.com/article/charliewarzel/the-terrifying-future-of-fake-news.

[83] Chesney, R. and Citron, D., (2019), "Deepfakes and the New Disinformation War: The Coming Age in Post-Truth Geopolitics," *Foreign Affairs*, https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

[84] Ibid.

There is no single answer or method for employing defensive measures against the risks of this future environment. Increased connectivity brings greater risk, and each organization or individual accessing networked systems and resources must weigh the desire for convenience versus the need for privacy and security. Addressing the risks and opportunities of the future environment requires both government and private sector participation.

5. Addressing the Current Threat

Addressing the threat of adversary influence operations requires a multi-pronged approach. No single organization has the necessary authority and reach.

A. Privacy and Regulation

1. Federal Privacy Laws and Regulation

The U.S. does not grant an explicit right to privacy. The fourth amendment of the U.S. Constitution protects "persons, houses, papers, and effects against unreasonable searches and seizures."[85] In the digital age, interpretation of "papers and effects" has broadened to include email and other online communications.

Generally, privacy law refers to laws regulating the collection, storage, and use of personally identifiable information (PII). These laws cover certain aspects of personal privacy. The Privacy Act of 1974 sets conditions for federal agencies' collection, maintenance, use, and dissemination of information about individuals maintained in systems of records. It prohibits the disclosure of a record about an individual without that individual's consent unless the disclosure fits one of 12 statutory exemptions.[86] The Right to Financial Privacy Act prohibits financial institutions from releasing customer financial records to the government except in accordance with narrowly defined provisions.[87] The Health Insurance Portability and Accountability Act (HIPAA) sets privacy and security standards for personal health information (PHI).[88]

Online communications fall under the Electronic Communications Privacy Act of 1986,[89] which revised federal wiretapping and eavesdropping provisions to protect certain wire, oral, and electronic communications from unauthorized interception, access, use, and

[85] U.S. Const. amend. IV

[86] Privacy Act of 1974, 5 U.S.C. § 552a (1974) (as amended January 12, 2018).

[87] The Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq.

[88] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (1996).

[89] The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2522 and 18 U.S.C. § 2701-2711 (1986).

disclosure.[90] The Federal Trade Commission (FTC) enforces online privacy through privacy policies and statements. The FTC also manages the Children's Online Privacy Protection Act (COPPA), which gives parents the right to control what information websites collect about children aged 13 and younger. Websites need to get parental consent to collect information about children, enable the parents to decide how that information is used, and give parents the option to opt-out of information collection.[91]

Other than the laws listed above, the focus online is on self-regulation. Websites create their own privacy policies that users must agree to before availing themselves of online services. These policies are long and difficult to understand, stuffed with legal jargon and vague language that allows for broad interpretation and plausible deniability should something go awry.[92] These policies put the onus on the user to read and understand what he or she is signing up for, which includes mass data collection. In 2018, California passed The California Consumer Privacy Act of 2018, which gives California residents the right to know what information companies are collecting, the right to opt out of having personal information sold to other companies, and protection against companies that do not adequately protect personal information.[93] So far, California is the first state to implement such a measure; other states are considering similar measures.

Social media companies such as Facebook have requested that the U.S. government impose its own data protection regulations, possibly because weak federal regulation would usurp strong state regulation. However, these companies have already complied with the E.U.'s General Data Protection Regulation (GDPR), which was passed on April 14, 2016, and enforced on May 25, 2018. The GDPR is meant to protect all E.U. citizens from data and privacy breaches. It applies to all companies processing data of E.U. citizens, regardless of where the company is located, which means that Facebook and other U.S. social media companies must comply. GDPR provisions include guidelines for privacy policies and user consent to collect data, the right of users to know what data is being collected and why, the inclusion of privacy provisions when designing a system, and the right to be forgotten, which gives users the right to have their personal data erased.[94] This

---

[90] "Internet privacy laws revealed – how your personal information is intercepted online," *Thompson Reuters Legal*, accessed June 19, 2019, https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.

[91] The Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6508 (1998).

[92] Litman-Navarro, K., (June 12, 2019), "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster," *The New York Times*, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?searchResultPosition=8.

[93] The California Consumer Privacy Act of 2018, California Code § 1798.100-1798.115 (1998).

[94] "GDPR Key Changes," *EUGDPR.org*, accessed 20 June 2019, https://eugdpr.org/the-regulation/.

compliance only applies to E.U. users; social media companies do not extend GDPR protections to U.S. users.

The GDPR provides a template for possible federal regulation. The U.S. Congress is working on a consumer privacy law, at least 15 related privacy bills have been filed, and a group of six senators are preparing to introduce another comprehensive privacy bill this year.[95] The challenges regarding federal privacy regulations are that they need to be comprehensive enough to protect PII but not so stifling as to prevent innovation in data sharing and aggregation in areas that can benefit U.S. citizens, such as public health, cybersecurity, and disaster response.

Federal regulation could be a boon to personal privacy protection (or, conversely, weak regulation could codify unsavory corporate behavior), but it is unlikely to stop groups such as the Internet Research Agency. Most of the information used in the Internet Research Agency's disinformation campaigns is voluntarily shared on social media sites and online message boards.

2. Speech Regulation

There is an ongoing debate about regulating hate speech and disinformation on social media. On one hand, social media companies such as Facebook and Twitter have created public forums for users to share and debate opinions. On the other, these companies are uniquely positioned to regulate false or misleading information posted on their sites.

The Communications Decency Act of 1996, 47 U.S.C. § 230, states "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[96] This means social media companies are not held accountable for views expressed on their sites. But the Act also exempts companies from liability if they commit "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene [which has its own legal definition], lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected,"[97] meaning that social media companies can determine what can and cannot be posted on their sites to an extent.

So far, the onus has been on companies to regulate themselves. Most newspapers, magazines, and other publications employ fact checkers to verify the accuracy of quotes

---

[95] Lefkowitz, P. M., (June 25, 2019), "Why America Needs a Thoughtful Federal Privacy Law," *The New York Times*, https://www.nytimes.com/2019/06/25/opinion/congress-privacy-law.html?searchResultPosition=2.

[96] Communications Decency Act of 1996, 47 U.S.C. § 230.

[97] Ibid.

and other claims. Facebook has internal guidelines for removing hate speech on its platform and has posted an explanation of how it addresses such speech and the challenges of doing so on its Newsroom site.[98] Facebook has also, in response to a year-long civil rights audit, updated its enforcement policies against harmful content and formalized its Civil Rights Task Force, which will address areas such as content policy, privacy, AI, and elections.[99] In 2017, Twitter updated its policy concerning what content violates its rules and terms of service to include consideration of whether a particular tweet is newsworthy or in the public interest.[100] In that vein, Twitter instituted a policy in 2019 to flag, but not remove, content from major political leaders that violates Twitter's rules. The content will be hidden behind a notice from Twitter: "The Twitter Rules about abusive behavior apply to this Tweet. However, Twitter has determined that it may be in the public interest for the Tweet to remain available."[101] Twitter users interested in reading the flagged content can click through the notice to read the flagged material.[102]

While these policies and initiatives present a solid foundation for regulating hate speech and disinformation, self-regulation presents several challenges. For platforms as large as Facebook and Twitter, finding and accurately categorizing each instance of hate speech, incitement to violence, and disinformation is incredibly difficult, if not impossible. Determining the context of a post or tweet, especially when regulators may only see the flagged post or tweet and may not be familiar with the cultural context of the post, makes it difficult to determine its intent. Monitors also often only have a minute to make a decision whether to flag or delete a post, and they do so with little to no oversight. As a result, monitors have unknowingly taken down innocuous posts and left up posts with potentially harmful content.

Further company-led regulation could and does include editorial boards, fact checkers, and reconfigured algorithms that flag potentially controversial content for further

---

[98] Allan, R., (June 27, 2017), "Hard Questions: Who Should Decide What Is Hate Speech in an Online Global Community?" *Facebook Newsroom*, https://newsroom.fb.com/news/2017/06/hard-questions-hate-speech/.

[99] Sandberg, S., (June 30, 2019), "A Second Update on Our Civil Rights Audit," *Facebook Newsroom*, https://newsroom.fb.com/news/2019/06/second-update-civil-rights-audit/.

[100] Twitter Public Policy (@Policy), "Among the considerations is 'newsworthiness' and whether a Tweet is of public interest 3/6," September 25, 2017, 3:05 p.m. Tweet.

[101] Twitter Safety, (June 27, 2019), "Defining public interest on Twitter," *Twitter Blog*, https://blog.twitter.com/en_us/topics/company/2019/publicinterest.html.

[102] On May 28, 2020, the White House issued an "Executive Order on Preventing Online Censorship" that targets social media and search engine companies, accusing them of exercising political bias when flagging questionable content. The order proposes a broad range of executive and legislative actions. These actions, and their expected legal challenges, will take time to occur. Their implications for this paper's subject matter could be significant, but they are not predictable with any certainty at this time. (The White House, (May 28, 2020), "Executive Order on Preventing Online Censorship," https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/.)

review. For news publications, waiting to post certain material, such as hacked communications, until it can be verified and put into context would prevent public misconceptions of an incomplete story. The siren call of the 24-hour news cycle and the desire to be the first to break news are difficult to ignore, but in this Internet-first age, context is everything.

B. Develop a Media Literacy Campaign

Teaching and reinforcing media literacy[103] is critical for creating an informed populace that would not be so easily hoodwinked by influence operations and disinformation campaigns. Media literacy enables a populace to carefully consume information and think critically about the information's message, intent, context, and source.

Disinformation is spread by organized campaigns and people who believe the disinformation to be true. Fighting disinformation with facts can trigger the backfire effect, but teaching the public to differentiate between true information and disinformation empowers people to educate themselves.

Some efforts to promote media literacy are already underway. The French government is working with schools and journalists on a media literacy effort aimed at students. Teachers receive annual training in media literacy, and journalists volunteer to visit schools to show students how easy it is to create media for a disinformation campaign and teach them to discern the difference between actual and fabricated information, pictures, and videos.[104] In one class, students were first shown a video espousing a conspiracy theory about CIA involvement in the spread of AIDS in Cuba, and then shown a second video explaining how the first fake video was made and why it seemed so persuasive.[105] Pillar 4 of the European Union's (EU) *Action Plan against Disinformation*, "Raising Awareness and Improving Societal Resilience," highlights the importance of an

---

[103] The Center for Media Literacy defines media literacy as a "framework to access, analyze, evaluate, create and participate with messages in a variety of forms—from print to video to Internet. Media literacy builds an understanding of the role of media in society as well as essential skills of inquiry and self-expression necessary for citizens of a democracy" (Center for Media Literacy, "Media Literacy: A Definition and More," accessed January 2, 2019, https://www.medialit.org/media-literacy-definition-and-more).

[104] Satariano, A. and Peltier, E., (December 13, 2018), "In France, School Lessons Ask: Which Twitter Post Should You Trust?" *The New York Times*, https://www.nytimes.com/2018/12/13/technology/france-internet-literacy-school.html.

[105] Beardsley, E., (May 3, 2018), "A Conspiracy Video Teaches Kids A Lesson About Fake News," *NPR*, https://www.npr.org/sections/ed/2018/05/03/601839776/a-conspiracy-video-teaches-kids-a-lesson-about-fake-news.

informed populace in the fight against disinformation and calls for campaigns to improve EU citizens' media literacy.[106]

In the U.S., several states, including California, Washington, Connecticut, Rhode Island, and New Mexico, have passed laws or resolutions promoting media literacy in schools.[107] However, like regulation, it is not clear what effect a media literacy campaign will have overall. An educated, informed populace is a benefit to society. But disinformation campaigns rely on blatant emotional appeals. Posts are designed to evoke anger, fear, or sadness—any emotion that would generate a strong, possibly hasty response. It can be difficult to think critically about a post or other piece of information when it elicits a strong reaction.

C. DoD's Role

The *2018 National Defense Strategy* recognizes that the strategic environment the U.S. military must operate in is "an increasingly complex global security environment, characterized by overt challenges to the free and open international order and the re-emergence of long-term strategic competition between nations."[108] This increasingly complex global security environment also recognizes that the U.S. homeland is no longer a sanctuary. The strategy explains that the U.S. homeland is now targeted by terrorists who want to harm U.S. citizens; conduct malicious cyber activity against infrastructure that is essential to U.S. national security, economic security, and public health; and use areas of competition short of open warfare, such as information warfare, ambiguous or denied proxy operations, and subversion to achieve their ends.[109] To counter the coercion and subversion in competition short of conflict, the DoD's strategic approach is to support U.S. government interagency efforts and work by, with, and through allies and partners to secure national interests.[110] A strategic approach that advocates working by, with, and through others suggests DoD either does not or should not have a leading role in the government's efforts to counter adversary information operations, save for information operations that directly target U.S. forces.

---

[106] European Commission, (May 12, 2018), *Action Plan against Disinformation*, Brussels: High Representative of the Union for Foreign Affairs and Security Policy.

[107] Zubrzycki, J., (July 28, 2017), "More States Take On Media Literacy in Schools," *Education Week*, http://blogs.edweek.org/edweek/curriculum/2017/07/media_literacy_laws.html.

[108] Summary of the 2018 National Defense Strategy of the United States of America, *Sharpening the American Military's Competitive Edge*, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, p. 2.

[109] Summarized from the 2018 National Defense Strategy Summary, pp. 2–3.

[110] Summarized from the 2018 National Defense Strategy Summary, p. 5.

1. 2018 Cyberspace Strategy Symposium

The rationale for a supporting role against adversary information operations short of open conflict was highlighted during U.S. Cyber Command's (CYBERCOM) inaugural Cyberspace Strategy Symposium, which was held at the National Defense University in February 2018. This day-long event showcased leaders from CYBERCOM and its partners inside and outside government pondering the challenges ahead for cyberspace operations.[111] The Symposium consisted of four panels, each of which discussed a key cyberspace topic: (1) Cyber and the Information Environment, (2) Speed and Agility for Defense and Offense, (3) Integrating Cyberspace Operations into the Joint Force, and (4) Defend the Nation. Panels one and four identified critical issues concerning DoD's role in responding to adversary information operations. Panel one determined that the integration of cyberspace and information operations was not new; over the last several years, our adversaries have been aggressive and innovative while using a range of tools in cyberspace. The panel went on to describe how adversaries are employing information operations continuously short of armed conflict. Adversaries do not see a distinction between cyber and information operations and understand the importance of connectivity, content, and cognition. As the U.S. government has sub-divided its information operations concepts and activities among the Under Secretary of Defense for Policy (USD(P)), the Under Secretary of Defense for Intelligence (USD(I)), the Joint Staff, the Combatant Commands, the Service Component Commands, and the Functional Commands,[112] it has not been effectively adapting to the changes U.S. adversaries have been employing.[113] Panel one concluded by identifying the following four issues for further exploration:

1. The relationship between cyber, what was historically called command and control (C2) warfare (adversary focused), and influence operations (which are not just adversary focused), and how to integrate these capabilities.
2. Relevance of concepts like area of responsibility and red-blue-gray space to the cyberspace domain.
3. How cyber is a subset of information operations.

---

[111] Nakasone, P.M., (2018), "Preface," *USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings*, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.

[112] Joint Publication 3-13, (November 27, 2012), *Information Operations*, incorporating Change 1, 20 November 2014.

[113] USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings, https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427, page 2.

4. Assumptions about the battlespace. Adversaries do not see the distinction we do and operate more effectively at scale using a full range of tools.[114]

Panel four's discussion concerned Defend the Nation, the first objective of the *2018 National Security Strategy*. The panel noted that what it means to defend the nation and its interest in cyberspace, as well as what DoD's role should be, was poorly developed and garnered little consensus. The panel also identified a key issue for further exploration: "Is there a threshold of support that DOD should be expected to provide when a state or other sophisticated adversary attacks our [nation's] critical information? When is it appropriate for industry and States to call on DOD for support? The value of standing Defense Support for Civil Authorities to shorten the decision cycle and make requests routine."[115] The challenges summarized by panel one's discussion on cyber and the information environment along with panel four's frustration with the poorly defined Defend the Nation mission reflect the constraints in DoD policy on information operations and the military's doctrine for conducting information operations.

DoD Directive 3600.01 states that information operations will be the principal mechanism used during military operations to integrate, synchronize, employ, and assess a wide variety of information-related capabilities in concert with other lines of operations to affect adversaries' or potential adversaries' decision making while protecting our own.[116] The key phrase in this directive is "during military operations." Although not defined in either military doctrine or U.S. Code, the initiation of military operations in the U.S. requires some level of authority, whether authorized by the President, the Congress, or the Secretary of Defense. Additionally, military doctrine highlights significant legal considerations military commanders and planners should consider before conducting information operations.

> IO planners at all levels should consider the following broad areas within each planning iteration in consultation with the appropriate legal advisor:
>
> 1. Could the execution of a particular IRC be considered a hostile act by an adversary or potential adversary?
>
> 2. Do any non-US laws concerning national security, privacy, or information exchange, criminal and/or civil issues apply?
>
> 3. What are the international treaties, agreements, or customary laws recognized by an adversary or potential adversary that apply to IRCs?

---

[114] USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings, page 2.

[115] USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings, page 8.

[116] Under Secretary of Defense for Policy (USD(P)), (May 2, 2013), Department of Defense Directive 3600.01, Information Operations, incorporating change 1, May 4, 2017, https://www.esd.whs.mil/Directives/issuances/dodd/, page 1.

4. How is the joint force interacting with or being supported by US intelligence organizations and other interagency entities?[117]

The limitations and constraints expressed in both DoD policy and its military doctrine make it difficult for DoD to determine how to respond to adversary influence operations and what would constitute a proportionate response. For DoD, information operations are key to winning "the battle of the narrative," which pits adversary attempts to influence the perception of different populations against U.S. efforts to do the same.[118] The battle of the narrative is an integral part of irregular warfare and requires creating a coherent message, working with the host nation or local partner to boost their legitimacy, disseminating the message to the local population and other key audiences, and delegitimizing the adversary's message and goals.[119]

The battle of the narrative, however, is applicable beyond irregular warfare. The emergence of the gray zone and the blurring of what constitutes wartime and peacetime activity have instigated a constant battle to control the narrative and influence the ideas and actions of target populations. To respond to adversary influence operations short of conflict, DoD will need to be imaginative within the bounds of law, policy, and capabilities to integrate information operations and cyberspace capabilities to counter and contest its adversaries globally.[120]

2. Title 10 and Title 50 Authorities

Title 10 and Title 50 of the U.S. Code refer, respectively, to the statutory authorities granted to DoD and the intelligence community (IC). Title 10 delineates the functions, duties, and responsibilities of the U.S. Armed Forces and gives the Secretary of Defense authority and control over DoD, including its subordinate agencies and commands. It also establishes the combatant commands (COCOM) and gives the COCOMs statutory authorities. COCOM commanders report directly to the Secretary of Defense.[121] Title 50 establishes authorities for the IC and is generally thought of as the basis for the CIA's

---

[117] Joint Publication 3-13, (November 27, 2012), *Information Operations*, incorporating change 1, November 20, 2014, http://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/3-0-Operations-Series/, page III-3.

[118] Department of Defense, (May 17, 2010), *Irregular Warfare: Countering Irregular Threats Joint Operating Concept Version 2.0*, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.

[119] Ibid.

[120] How the Department of Defense will need to respond was taken from the USCYBERCOM *2018 Cyberspace Strategy Symposium Proceedings*, p. 2.

[121] 10 U.S.C. §§ 101-18525.

authority to conduct intelligence operations and covert actions. But Title 50 also establishes the Secretary of Defense's control over the intelligence agencies that are part of DoD, including NSA and the Defense Intelligence Agency (DIA).[122]

One difference between Title 10 and Title 50 is the need for Congressional notification. Both Title 10 and Title 50 activities are subject to Congressional oversight: Title 10 activities are overseen by the House and Senate Armed Services Committees (HASC and SASC, respectively), and Title 50 activities are subject to oversight from the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence (HPSCI).[123] But IC activities that fall under Title 50 require notifying Congress, while activities defined as "military activities" fall under Title 10 and do not require a notice to Congress.[124] Another difference between Title 10 and Title 50 is international protection of sovereignty. Intelligence agencies operating outside the U.S. in covert action status, which is covered by Title 50, have reasonable claim to international law protection of sovereignty because covert action status carries a statutory obligation to comply with the U.S. Constitution and U.S. statutes, but nothing else. Title 10 does not carry the same statutory shield against international law objections.[125]

Questions of oversight and responsibility arise when actions could reside under either Title 10 or Title 50. Historically, Congress and other government departments and agencies have considered Title 10 and Title 50 to be separate entities. But the titles themselves, as well as the authorities granted the Secretary of Defense under both Title 10 and Title 50, suggest otherwise. Some of the same activities could fall under either Title 10 or Title 50 depending on their command and control, funding, and mission intent.[126] Both the IC and DoD conduct intelligence gathering, which is generally assumed to fall under Title 50. However, intelligence gathering is included under both Title 10 and Title 50. The Secretary of Defense is able to direct DoD organizations and personnel to execute intelligence activities. If these activities are meant to fulfill national intelligence requirements, then they fall under Title 50. If they meet military intelligence requirements, or are used to prepare for an organized conflict, they fall under Title 10. Military intelligence operations in support of tasking from the Director of National Intelligence (DNI) fall under Title 50 and have to be reported, but intelligence activities in support of tasking from the Secretary

---

[122] 50 U.S.C. §§ 1-2420.

[123] Wall, A.E., (2011), "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal*, Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.

[124] Ibid.

[125] Chesney, R., (April 12, 2018), "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries," *Lawfare*, https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.

[126] Wall, A.E., (2011), "Demystifying the Title 10-Title 50 Debate," *Harvard National Security Journal*, Vol. 3, https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.

of Defense are considered Title 10. If the DoD organizations conducting the activities are also members of the IC, then the activities fall under both Title 10 and Title 50.[127]

In modern operations, particularly in cyberspace operations, the convergence between Title 10 and Title 50 activities becomes more apparent. Generally, exploiting a network or system to gather information but not alter, control, or degrade the function of that network or system is considered an intelligence activity, and international law does not consider intelligence activities to be acts of war. Exploiting a network or system to alter, control, or degrade its function surpasses that threshold and is generally considered an attack.[128] (In the gray zone, international rules of engagement for cyber operations remain fuzzy and undefined.[129]) Cyber operations, however, often require intelligence gathering to assess a network or system in preparation for an attack. Moving from one activity to another—from Title 50 to Title 10—especially when operating in a foreign country, may leave personnel without sovereignty protection and exposes potential international law issues. The challenge is that cyberspace operations often happen quickly. A particular opportunity may arise and be relevant for a short period of time, which makes waiting for legal authorization difficult, especially if foreign governments need to consent to impending action. By the time such authorization is received, the opportunity may be moot.

Title 10-Title 50 convergence also raises questions of who should be responsible for intelligence gathering and other cyber operations. CYBERCOM, the unified combatant command responsible for cyberspace operations, is partnered with the NSA. The Commander, U.S. Cyber Command, is also the NSA director, which underscores the ties between the two organizations. Historically, NSA has been the U.S. government's lead for cyber operations, but CYBERCOM's responsibility and authority is growing. Convergence is complicated for cyber operations and is even more complicated for information operations.

3. Current Activities

Despite DoD's reluctance and confusion over Title 10 and Title 50 authorities, the 2018 midterm elections serve as an example of how DoD can get involved with election security and how laws can change.

The 2019 National Defense Authorization Act (NDAA) expanded CYBERCOM's statutory authorities.[130] The NDAA modifies parts of Title 10 to give DoD the ability to

---

[127] Ibid.

[128] Ibid.

[129] Bing, C., (April 11, 2018), "Command and control: A fight for the future of government hacking," *cyberscoop*, https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.

[130] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).

conduct cyber operations "short of hostilities"[131] and in areas where "hostilities are not occurring,"[132] and defines clandestine military activity in cyberspace as "a traditional military activity."[133] The designation of clandestine online activity as traditional military activity removes the oversight required of clandestine operations as stated under Title 50.

The NDAA also grants CYBERCOM pre-authorization to conduct cyber operations in response to cyberattacks from foreign countries, but only if those attacks meet two conditions: they constitute "an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes," and they come from Russia, North Korea, China, or Iran.[134]

The 2018 U.S. midterm elections, which were subject to repeated attacks from Russia, serve as an example of how DoD can get involved with election security and the fight against disinformation. CYBERCOM supported U.S. European Command, U.S. Northern Command, the Department of Homeland Security (DHS), the Department of the Treasury, and FBI efforts to protect U.S. elections and electoral systems. CYBERCOM also partnered with allied nations to find instances of foreign interference in the midterm elections.[135] To combat disinformation, CYBERCOM and NSA created the Russia Small Group, a taskforce dedicated to deterring and protecting against Russian disinformation and cyberattacks.[136] On the day of the midterm election, the taskforce blocked Internet access to the Internet Research Agency in St. Petersburg, long identified as the locus of Russia's disinformation campaign against the U.S.[137] The taskforce has since been made permanent.

---

[131] 10 U.S.C. § 394(b).

[132] Ibid.

[133] 10 U.S.C. § 394(c).

[134] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).

[135] Lopez, C.T., (May 14, 2019), "Persistent Engagement, Partnerships, Top Cybercom's Priorities," *Department of Defense*, https://www.defense.gov/Newsroom/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.

[136] Nakasone, P.M., (February 14, 2019), Statement before the Senate Committee on Armed Services.

[137] Nakashima, E., (February 27, 2019), "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms," *The Washington Post*, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on.

6. Conclusion

The battle for the narrative presents several unique challenges. Given the onslaught of foreign surveillance into our critical infrastructure and interference with our social media, the question may not be "How do we deal with these intrusions?" but rather, "Are we at war, and did we not realize it?"

Prussian theorist of war Carl von Clausewitz argued that the nature of war describes war's unchanging essence and the character of war describes how war as a phenomenon manifests in the real world. War's nature is violent, interactive, and fundamentally political. War's conduct, however, is influenced by technology; law; ethics; culture; methods of social, political, and military organization; and other factors that change across time and place.[138] Understanding the complexity of and differences among the various approaches to warfare is critical for understanding adversaries, their methods, and their concepts for victory. In the past, U.S. military doctrine has successfully evolved to meet the challenges of conventional warfare, irregular warfare, and terrorism. It evolved to achieve victory during the major wars of the past century, to manage counterinsurgency operations during the Vietnam War, and it continues to evolve today to manage conflicts in Afghanistan, Iraq, and against ISIS. However, this evolution must continue. Multiple foreign adversaries are surveying U.S. cyber systems and pre-positioning offensive cyber weapons that could disrupt mass transit systems, cause power outages, and leave millions of people without healthcare resources. Russian interference in the 2016 U.S. presidential election and 2018 midterm elections caused mass disruption and distrust in U.S. electoral systems and the democratic process. Adversaries continue to exploit social media to manipulate public opinion to sow confusion within our democracy. To embrace the changing conduct of war, the U.S. military should adopt a heuristic construct for conflict as depicted in Figure 6-1 and abandon a binary peace/war distinction.[139]

---

[138] Mewett, C., (January 21, 2014), "Understanding War's Enduring Nature alongside its Changing Character," *War on the Rocks*, https://warontherocks.com/2014/01/understanding-wars-enduring-nature-alongside-its-changing-character/.

[139] Hoffman, F.G., "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges," *Prism* 7, No 4, https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

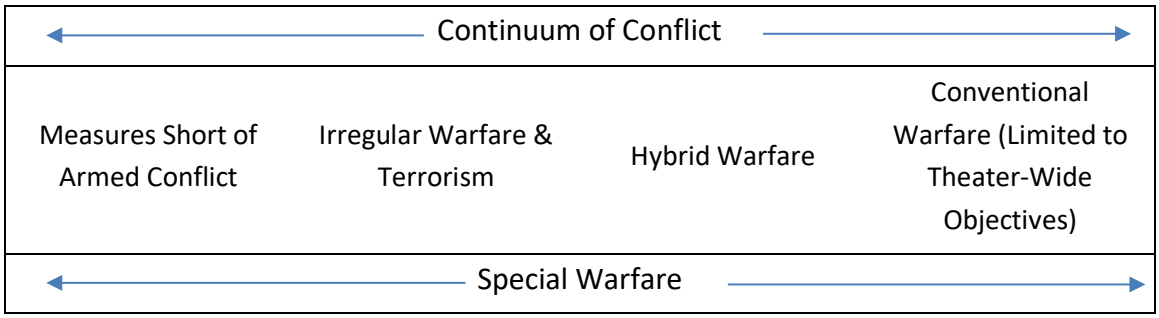

Figure 6-1. Continuum of Conflict

The new battlespace is complex and multi-faceted. Personal information is widely available. Credit card companies, social media companies, health companies, and others possess and trade in staggering amounts of personal information. Though some of this information, such as PHI, is subject to legislative protections, it is also vulnerable to attack. Breaches at Equifax, the Office of Personnel Management (OPM), and Capital One,[140] to name a few, have exposed data belonging to millions of people. Online marketers, social media companies, and Internet service providers (ISP) use surveillance tools to create detailed profiles of individuals' online footprints. This information can be used to create detailed target profiles both for advertising purposes and to enhance an influence operations campaign through personalized, emotional appeals.

Social media companies act like hybrids of intelligence organizations and traditional media companies because they both collect data and curate, post, and deliver news. Their data collection informs their media policy. News posts on social media sites are subject to algorithms that tailor content based on data about individual preferences, previous online activity, and connections, and they present narrow, often biased views of controversial issues. This leads to echo chambers and willing insulation from dissenting or contradictory views and information. Traditional media outlets are dealing with greater public mistrust. Politicians and other prominent figures routinely denounce news they do not agree with as "fake news" to cast doubt on the truth of what is reported and aspersions on the motives of reporters and outlets. As a result, less traditional outlets, often politically polarized, are on the rise. It is far too easy for an adversary to exploit existing divisions in our society and turn people against each other and against the institutions that are supposed to protect and represent them.

Technology is evolving rapidly, and the U.S. government and military are struggling to keep pace. There is an assumption that advances in technology such as raw computing power, data mining, and AI and machine learning will favor defensive actions against

[140] Flitter, E. and Weise, K., (July 29, 2019), "Capital One Data Breach Hits 100 Million; Ex-Amazon Worker Is Charged as Hacker," *The New York Times*, https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html?action=click&module=Top%20Stories&pgtype=Homepage.

influence operations, but that assumption is unsupported. These advances also favor the perpetrators and present obstacles to effective defense. Emotionally intelligent computing is developing rapidly. Deepfake audio and video are becoming increasingly difficult to detect and may have unpredictable effects, especially if integrated into a broad influence operations campaign.

A hallmark of the gray zone is a blurring of boundaries and responsibilities. This new battlespace spans the public and private sectors and encompasses media outlets, social media sites, a range of technologies, and individual citizens. As what constitutes an attack in cyberspace has not been concretely defined (a cyberattack that causes physical effects notwithstanding), it is difficult to determine a proportionate response to foreign adversary incursion into our networks, though the social effects of such incursions have been pronounced. This is a new type of warfare, one that does not adhere to current doctrinal definition.

Given the nebulous nature of the gray zone, it is difficult to define the battlespace, much less victory, especially in the context of influence operations. In fact, the concept of victory as we understand it today may not even exist. Instead, the goal is to maintain an advantage. Battling influence operations campaigns requires a three-pronged approach of regulation, education, and government agency action. Broad regulation is a congressional responsibility. The E.U. can serve as a source for guidelines. Social media companies that operate in Europe are already complying with E.U. regulations; they can certainly apply similar regulations in the U.S.

Education and media literacy campaigns give the public tools to help them identify disinformation and think critically about the information they see and interact with online. The public needs to be aware that there are influence operations campaigns conducted against them and know how to protect themselves. There is room for a government-sponsored national media literacy campaign accessible to all audiences, including students. To be effective, the campaign must focus on authenticity and building trust with the public. But education alone is not a panacea. It is not enough to arm the public with the knowledge of these campaigns; we need to stop current campaigns and prevent new ones.

Doing so requires U.S. government agency involvement. Individual agencies have particular areas of focus and responsibility, and a whole-of-government approach to fighting disinformation would focus agency resources and expertise where they're needed most. DoD has the resources and abilities to be the technical lead but is limited by policy and law. Partnering with DHS, FBI, and other agencies would enable DoD to provide cyber capabilities and expertise where needed. CYBERCOM and NSA's Russia Small Group taskforce, as well as CYBERCOM's partnerships with allied nations and U.S. government agencies, present a model for future DoD involvement in the fight against disinformation, and CYBERCOM's Joint Task Force Ares has partnered with NSA to act as a hub for

whole-of-government cyber planning.[141] DoD is also already partnering with the Department of State's Global Engagement Center, which has been charged to "lead, synchronize, and coordinate efforts of the Federal Government to recognize, understand, expose, and counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national security interests."[142]

This partnership model could be expanded. To do so, we need a better understanding of what each agency can and is willing to do. DHS, for example, is responsible for critical infrastructure. Could they expand their role to a partnership with DoD to better defend infrastructure systems? Could the Department of Commerce use export control authorities to control the export of technologies to countries likely to use them against us? Could we use the Department of Veterans Affairs' (VA) education programs to train entry-level cybersecurity technicians?

DoD needs to determine the best approach to combating and deterring disinformation campaigns. CYBERCOM's pre-authorization to conduct cyber operations against cyberattacks from certain foreign countries defines a proportionate response in specific instances. Knowing that the U.S. can and will respond to an attack is part of an effective deterrence strategy, but defense requires a different approach. Effective defense against influence operations may require the Secretary of Defense to exercise both Title 10 and Title 50 authorities. For DoD involvement in the gray zone, the question is how to operate under these authorities and when to use them.

In addition, establishing rules of engagement for cyberspace would help governments determine proportionate responses to adversary activity and define necessary activities to defend against and deter disinformation campaigns. DoD and the U.S. government as a whole could draw from previous experience countering disinformation and effective programs and legislation already established by other governments to begin creating guidelines for cyber activities.

Fighting and preventing influence operations campaigns needs to become a national priority. Special Counsel Robert Mueller's testimony to the House Judiciary and Intelligence Committees on July 24, 2019, issued a warning about election interference: The 2016 election "wasn't a single attempt. They're doing it as we sit here."[143] Election interference and other influence operations campaigns are going to continue to expand in scope and affect our society and way of life. We need to address this head on.

---

[141] Nakasone, P.M., (February 14, 2019), Statement before the Senate Committee on Armed Services.

[142] National Defense Authorization Act (NDAA) for Fiscal Year 2017, Pub. L. 114-328 § 1287(a)(2).

[143] Hirshfeld Davis, J. and Mazzetti, M., (July 24, 2019), "Highlights of Robert Mueller's Testimony to Congress," *The New York Times*, https://www.nytimes.com/2019/07/24/us/politics/mueller-testimony.html?action=click&module=RelatedLinks&pgtype=Article.

References

Armed Forces, 10 U.S.C. §§ 101-18505.

Beardsley, E. (May 3, 2018). "A Conspiracy Video Teaches Kids A Lesson About Fake News." *NPR*. https://www.npr.org/sections/ed/2018/05/03/601839776/a-conspiracy-video-teaches-kids-a-lesson-about-fake-news.

Beaumont, C. (November 27, 2008). "Mumbai attacks: Twitter and Flickr used to break news." *The Telegraph*. https://www.telegraph.co.uk/news/worldnews/asia/india/3530640/Mumbai-attacks-Twitter-and-Flickr-used-to-break-news-Bombay-India.html.

Bernays, E. (2005). *Propaganda*. New York: Ig Publishing. (Original work published 1928).

"Big data." *Merriam-Webster Dictionary*, accessed December 26, 2018. https://www.merriam-webster.com/dictionary/big%20data?src=search-dict-hed.

Bing, C. (April 11, 2018), "Command and control: A fight for the future of government hacking." *cyberscoop*. https://www.cyberscoop.com/us-cyber-command-nsa-government-hacking-operations-fight/.

Biser, M. "The Fireside Chats: Roosevelt's Radio Talks," The White House Historical Association. https://www.whitehousehistory.org/the-fireside-chats-roosevelts-radio-talks. Accessed October 4, 2018.

Bowley, G. and Hurdle, J. (April 26, 2018). "Bill Cosby Is Found Guilty of Sexual Assault." *The New York Times*. https://www.nytimes.com/2018/04/26/arts/television/bill-cosby-guilty-retrial.html?rref=collection%2Fnewseventcollection%2FThe%20Cosby%20Trial&action=click&contentCollection=Television&module=inline&region=Marginalia&src=me&version=newsevent&pgtype=article.

Bradshaw, S. and Howard, P.N. (January 29, 2018). "Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life." Knight Foundation. https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

Brown, Z.T. (March 12, 2019). "Unmasking War's Changing Character." *Modern War Institute*. https://mwi.usma.edu/unmasking-wars-changing-character/.

California Consumer Privacy Act of 2018, California Code § 1798.100-1798.115 (1998).
Center for Media Literacy. "Media Literacy: A Definition and More." Accessed January 2, 2019. https://www.medialit.org/media-literacy-definition-and-more.

Chatzky, A. and McBride, J. (May 21, 2019). "China's Massive Belt and Road Initiative." *Council on Foreign Relations*. https://www.cfr.org/backgrounder/chinas-massive-belt-and-road-initiative.

Chesney, R. (April 12, 2018). "Title 10 and Title 50 Issues When Computer Network Operations Impact Third Countries." *Lawfare*. https://www.lawfareblog.com/title-10-and-title-50-issues-when-computer-network-operations-impact-third-countries.

Chesney, R. and Citron, D. (2019). "Deepfakes and the New Disinformation War: The Coming Age in Post-Truth Geopolitics." *Foreign Affairs*. https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6508 (1998).

Clogston, J.F. (2016). "The Repeal of the Fairness Doctrine and the Irony of Talk Radio: A Story of Political Entrepreneurship, Risk, and Cover." *Journal of Policy History*, 28(2), 375-396, doi:10.1017/S0898030616000105.

Communications Decency Act of 1996, 47 U.S.C. § 230.

Cook, J. (July 28, 2014). "The Posters That Sold World War I to the American Public." *Smithsonian Magazine*. https://www.smithsonianmag.com/history/posters-sold-world-war-i-american-public-180952179/. Accessed October 2, 2018.

Deeks, A., McCubbin, S. and Poplin, C.M. (October 25, 2017). "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.

Denby, G. (October 18, 2014). "Videos Of Deadly Police Encounters Grab The Media Spotlight, But Why?" *NPR*. https://www.npr.org/blogs/codeswitch/2014/10/08/354507430/videos-of-deadly-police-encounters-grab-media-spotlight.

Department of Defense. (May 17, 2010). *Irregular Warfare: Countering Irregular Threats Joint Operating Concept Version 2.0*. http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joc_iw_v2.pdf?ver=2017-12-28-162021-510.

Department of Defense. (2018). *Summary of the 2018 National Defense Strategy of the United States of America*. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

Department of Justice, Office of Public Affairs. (February 16, 2018). "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System." https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere.

Dewar, J.A. (1998). "The Information Age and the Printing Press: Looking Backward to See Ahead." *Rand*. https://www.rand.org/pubs/papers/P8014/index2.html.

"Doxing." *Technopedia*. Accessed December 26, 2018. https://www.techopedia.com/definition/29025/doxing.

Dwoskin, E. and Gowen, A. (July 23, 2018). "On WhatsApp, fake news is fast—and can be fatal." *The Washington Post*. https://www.washingtonpost.com/business/economy/on-whatsapp-fake-news-is-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5-9d911c784c38_story.html?noredirect=on&utm_term=.05a5faed4172.

Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510-2522 and 18 U.S.C. § 2701-2711 (1986).

Electronic Frontier Foundation (EFF). "Cell-Site Simulators/IMSI Catchers." Accessed December 13, 2018. https://www.eff.org/pages/cell-site-simulatorsimsi-catchers.

European Commission. (May 12, 2018). *Action Plan against Disinformation*. Brussels: High Representative of the Union for Foreign Affairs and Security Policy.

Fair Credit Reporting Act, revised September 2018, 15 U.S.C. § 1681.

Federal Trade Commission. (September 2011). "Cyberbullying." Federal Trade Commission Consumer Information. https://www.consumer.ftc.gov/articles/0028-cyberbullying.

Fischer, M. and Taub, A. (April 25, 2018). "How Everyday Social Media Users Become Real-World Extremists." *The New York Times*. https://www.nytimes.com/2018/04/25/world/asia/facebook-extremism.html.

Fletcher, D. (February 20, 2009). "The Fairness Doctrine." *Time*. http://content.time.com/time/nation/article/0,8599,1880786,00.html.

Flitter, E. and Weise, K. (July 29, 2019). "Capital One Data Breach Hits 100 Million; Ex-Amazon Worker Is Charged as Hacker." *The New York Times*. https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html?action=click&module=Top%20Stories&pgtype=Homepage.

Fortney, L. (December 19, 2018). "Bitcoin Mining, Explained." *Investopedia*. https://www.investopedia.com/terms/b/bitcoin-mining.asp.

"GDPR Key Changes." *EUGDPR.org*. Accessed 20 June 2019. https://eugdpr.org/the-regulation/.

Gonzalez, S., France, L.R., and Melas, C. (October 4, 2018). "The year since the Weinstein scandal first rocked Hollywood." *CNN*. https://www.cnn.com/2018/04/05/entertainment/weinstein-timeline/index.html.

Grauer, Y. (March 27, 2018). "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?" *Motherboard*. https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection.

Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191 (1996).

Hern, A. (May 22, 2017). "How social media filter bubbles and algorithms influence the election." *The Guardian*. https://www.theguardian.com/technology/2017/may/22/social-media-election-facebook-filter-bubbles.

Hirshfeld Davis, J. and Mazzetti, M. (July 24, 2019). "Highlights of Robert Mueller's Testimony to Congress." *The New York Times*. https://www.nytimes.com/2019/07/24/us/politics/mueller-testimony.html?action=click&module=RelatedLinks&pgtype=Article.

Hoffman, F.G. "Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges." *Prism* 7, No. 4. https://cco.ndu.edu/News/Article/1680696/examining-complex-forms-of-conflict-gray-zone-and-hybrid-challenges/.

International Security Advisory Board (ISAB). (January 3, 2017). *Report on Gray Zone Conflict*. https://www.state.gov/documents/organization/266849.pdf.

"Internet privacy laws revealed – how your personal information is intercepted online." *Thompson Reuters Legal*. Accessed June 19, 2019. https://legal.thomsonreuters.com/en/insights/articles/how-your-personal-information-is-protected-online.

"Iva Toguri d'Aquino and 'Tokyo Rose.'" FBI. https://www.fbi.gov/history/famous-cases/iva-toguri-daquino-and-tokyo-rose. Accessed October 3, 2018

John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (2018).

Joint Publication 3-12. (June 8, 2018). *Cyberspace Operations*.

Joint Publication 3-13. (November 27, 2012). *Information Operations*. Incorporating Change 1, November 20, 2014.

Jowett, G.S. and O'Donnell, V. (2012). *Propaganda and Persuasion*, Fifth Edition. Los Angeles: SAGE Publications, Inc.

Kahn, M. (July 13, 2018). "Document: Special Counsel Indicts 12 Russian Intelligence Officers for Hacking DNC and Clinton Campaign." *Lawfare*. https://www.lawfareblog.com/document-special-counsel-indicts-12-russian-intelligence-officers-hacking-dnc-and-clinton-campaign.

Kang, C. (March 20, 2018). "Facebook Faces Growing Pressure Over Data and Privacy Inquiries." *The New York Times*. https://www.nytimes.com/2018/03/20/business/ftc-facebook-privacy-investigation.html.

Kirkpatrick, D.D. (November 15, 2017). "Signs of Russian Meddling in Brexit Referendum." *The New York Times*. https://www.nytimes.com/2017/11/15/world/europe/russia-brexit-twitter-facebook.html.

Lapowsky, I. (April 4, 2018). "Facebook Exposed 87 Million Users to Cambridge Analytica." *Wired*. https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/.

Larson, E.V., Darilek, R.E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L.H. and Thurston, C.Q. (2009). "Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities." *Rand*. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf.

Lewis, P. (March 2, 2011). "You're being watched: there's one CCTV camera for every 32 people in UK." *The Guardian*. https://www.theguardian.com/uk/2011/mar/02/cctv-cameras-watching-surveillance.

Litman-Navarro, K. (June 12, 2019). "We Read 150 Privacy Policies. They Were an Incomprehensible Disaster." *The New York Times*. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?searchResultPosition=8.

Lopez, C.T. (May 14, 2019). "Persistent Engagement, Partnerships, Top Cybercom's Priorities." *Department of Defense*. https://www.defense.gov/Newsroom/News/Article/Article/1847823/persistent-engagement-partnerships-top-cybercoms-priorities/.

Lord, N. (September 11, 2018). "What is Social Engineering? Defining and Avoiding Common Social Engineering Threats." *Digital Guardian*.

https://digitalguardian.com/blog/what-social-engineering-defining-and-avoiding-common-social-engineering-threats.

Marconi, F. and Daldrup, T. (November 15, 2018). "How *The Wall Street Journal* is preparing its journalists to detect deepfakes." *NeimanLab*. http://www.niemanlab.org/2018/11/how-the-wall-street-journal-is-preparing-its-journalists-to-detect-deepfakes/.

Metzgar, E.T., (January 21, 2013). "Smith-Mundt reform: In with a whimper?" *Columbia Journalism Review*, https://archives.cjr.org/behind_the_news/smith-mundt_modernization_pass.php.

Mewett, C. (January 21, 2014). "Understanding War's Enduring Nature alongside its Changing Character." *War on the Rocks*. https://warontherocks.com/2014/01/understanding-wars-enduring-nature-alongside-its-changing-character/.

Mozur, P. (July 8, 2018). "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras." *The New York Times*. https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

Nakashima, E. (February 27, 2019). "U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms." *The Washington Post*. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html?noredirect=on.

Nakasone, P.M. (2018). "Preface," *USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings*. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.

Nakasone, P.M. (February 14, 2019). Statement before the Senate Committee on Armed Services.

National Defense Authorization Act (NDAA) for Fiscal Year 2017, Pub. L. 114-328 § 1287(a)(2).

Newman, N. and Fletcher, R. (2017). "Bias, Bullshit and Lies: Audience Perspectives on Low Trust in the Media." *Digital News Project 2017*. Reuters Institute for the Study of Journalism and University of Oxford. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2017-11/Nic%20Newman%20and%20Richard%20Fletcher%20-%20Bias%2C%20Bullshit%20and%20Lies%20-%20Report.pdf.

Nittle, N. (November 2, 2018). “Spend ‘frivolously’ and be penalized under China’s new social credit system.” *Vox*. https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games.

Privacy Act of 1974, 5 U.S.C. § 552a (1974) (as amended January 12, 2018).

“propaganda.” *Merriam Webster*. https://www.merriam-webster.com/dictionary/propaganda. Accessed October 5, 2018.

“rabbit hole.” *Merriam-Webster*. https://www.merriam-webster.com/dictionary/rabbit%20hole. Accessed October 1, 2019.

Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq.

Roose, K. (August 1, 2018). “Facebook Grapples With a Maturing Adversary in Election Meddling.” *The New York Times*. https://www.nytimes.com/2018/08/01/technology/facebook-trolls-midterm-elections.html.

Satariano, A. and Peltier, E. (December 13, 2018). “In France, School Lessons Ask: Which Twitter Post Should You Trust?” *The New York Times*. https://www.nytimes.com/2018/12/13/technology/france-internet-literacy-school.html.

Silverman, C. (June 17, 2011). “The Backfire Effect: More on the press’s inability to debunk bad information. *Columbia Journalism Review.* https://archives.cjr.org/behind_the_news/the_backfire_effect.php.

Singal, J. (October 19, 2016). “‘Citizen Journalism’ Is a Catastrophe Right Now, and It’ll Only Get Worse.” *New York Magazine*. http://nymag.com/intelligencer/2016/10/citizen-journalism-is-a-catastrophe-itll-only-get-worse.html.

Smith-Mundt Modernization Act of 2012, H.R. 5736, 112th Cong., (2012).

Stewart, P.W. (2015). “A Reel Story of World War II: The United News Collection of Newsreels Documents the Battlefield and the Home Front.” *Prologue Magazine*, Fall 2015, 47(3). https://www.archives.gov/publications/prologue/2015/fall/united-newsreels.html.

The White House. (May 28, 2020). “Executive Order on Preventing Online Censorship.” https://www.whitehouse.gov/presidential-actions/executive-order-preventing-online-censorship/.

Theohary, C.A. (March 5, 2018). CRS Report 7-7500, “Information Warfare: Issues for Congress.” *Congressional Research Service*.

Torpey, K. (February 27, 2018). “Bill Gates: I Don’t Think Bitcoin’s Anonymity Is a Good Thing.” *Forbes*. https://www.forbes.com/sites/ktorpey/2018/02/27/bill-gates-i-dont-think-bitcoins-anonymity-is-a-good-thing/#6f3472fc1395.

Turek, M. “Media Forensics (MediFor).” *Defense Advanced Research Projects Agency (DARPA)*. https://www.darpa.mil/program/media-forensics.

Twenge, J.M. and Campbell, W.K. (2018). “Associations Between Screen Time and Lower Psychological Well-Being Among Children and Adolescents: Evidence From a Population-Based Study.” *Preventive Medicine Reports*, Vol. 12, December 2018, p. 271-283. https://doi.org/10.1016/j.pmedr.2018.10.003.

Twitter Public Policy (@Policy). “Among the considerations is ‘newsworthiness’ and whether a Tweet is of public interest 3/6.” September 25, 2017, 3:05 p.m. Tweet. https://twitter.com/Policy/status/912438046515220480.

Twitter Safety. (June 27, 2019). “Defining public interest on Twitter.” *Twitter Blog*. https://blog.twitter.com/en_us/topics/company/2019/publicinterest.html.

Under Secretary of Defense for Policy (USD(P)). (May 2, 2013). Department of Defense Directive 3600.01, *Information Operations*. Incorporating change 1, May 4, 2017. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/360001p.pdf?ver=2017-06-20-125019-483.

United States Information and Educational Exchange Act of 1948, 22 U.S.C. § 1461.

U.S. Const. amend. IV.

USCYBERCOM. (2018). *USCYBERCOM 2018 Cyberspace Strategy Symposium Proceedings*. https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Cyberspace%20Strategy%20Symposium%20Proceedings%202018.pdf?ver=2018-07-11-092344-427.

Vosoughi, S., Roy, D. and Aral, S. (March 9, 2018). “The spread of true and false news online.” *Science*, 359, 1146-1151.

Waldman, P., Chapman, L., and Robertson, R. (April 19, 2018). “Palantir Knows Everything About You.” *Bloomberg*. https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

Wall, A.E. (2011). “Demystifying the Title 10-Title 50 Debate.” *Harvard National Security Journal*, Vol. 3. https://harvardnsj.org/wp-content/uploads/sites/13/2012/01/Vol-3-Wall.pdf.

War and National Defense, 50 U.S.C. §§ 1-2420.

Warzel, C. (February 11, 2018). “He Predicted The 2016 Fake News Crisis. Now He’s Worried About an Information Apocalypse.” *Buzzfeed News*. https://www.buzzfeednews.com/article/charliewarzel/the-terrifying-future-of-fake-news.

Watts, J., Jensen, B., Work, J.D., Whyte, C., and Kollars, N. (September 2019). “Alternate Cybersecurity Futures.” Atlantic Council Scowcroft Center for Strategy and Security.

The Week. (September 3, 2018). “Why the Government Wants a Mandatory ‘Backdoor’ on Encrypted Technology.” https://www.theweek.co.uk/96224/why-the-government-wants-a-mandatory-backdoor-on-encrypted-technology.

Zubrzycki, J. (July 28, 2017). “More States Take On Media Literacy in Schools.” *Education Week*. http://blogs.edweek.org/edweek/curriculum/2017/07/media_literacy_laws.html.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
00-06-20	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Military Authorizations in a Connected World: The Department of Defense's Role in Influence Operations	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
Michelle G. Albert, George A. Thompson, Thomas H. Barth	C5199
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-11022

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
Institute for Defense Analyses 4850 Mark Center Dr., Alexandria, VA 22311	IDA
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Michelle G. Albert

14. ABSTRACT

Today's Internet-based global media ecosystem, which allows for an unprecedented free flow of information, has given rise to a new type of attack surface. Cyber activities in the gray zone, which falls between diplomatic engagement and military action and includes disinformation campaigns and influence operations, raise questions regarding responsibility and proportionate response. This paper looks at the distinction between influence operations and a traditional state of war, specifically at the emergence of a gray zone of blended activity. Countering and deterring adversary influence operations requires a multi-pronged approach of regulation, education, and government agency action, including Department of Defense technical resources and expertise.

15. SUBJECT TERMS

Influence operations, gray zone, disinformation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Institute for Defense Analyses
Unclassified	Unclassified	Unclassified	Unlimited	55	19b. TELEPHONE NUMBER (Include Area Code)