Public Integrity, 21: 512–522, 2019

ISSN: 1099-9922 print/1558-0989 online
DOI: 10.1080/10999922.2019.1613832

Routledge
Taylor & Francis Group

Disinformation in Contemporary U.S. Foreign Policy: Impacts and Ethics in an Era of Fake News, Social Media, and Artificial Intelligence

Michael Landon-Murray and Edin Mujkic

University of Colorado Colorado Springs

Brian Nussbaum

University at Albany

Misinformation and disinformation, often in the form of fake news disseminated on social media, are proliferating in the "post-truth" era, with profound implications for public and policy discourse, political accountability and integrity, elections and governance. The United States is grappling with an information landscape eroded by deeply flawed information from a variety of sources, including Russian efforts to undermine its recent presidential election. As it struggles with these problems, the U.S. must also decide if and how to deploy political disinformation. U.S. foreign policy has made significant use of disinformation to influence politics and elections, and as emerging technologies allow new means of producing, disseminating, and amplifying disinformation, American presidents, security officials, and covert operators will weigh their use and usefulness. These technologies will also create new, largely unknown effects, the normative, practical, and governance implications of which must be scrutinized. Despite the attention now focused on disinformation, this angle has received inadequate consideration. This article argues that in rapidly shifting technological and political landscapes, disinformation programs require the highest possible degree of examination and accountability. Congress; the electorate; media; and researchers must engage in the public conversation to ensure that American democratic and ethical values inform U.S. policy.

Keywords: artificial intelligence, covert action, disinformation, fake news, intelligence accountability, misinformation

Information and knowledge are the foundational political resources at citizens' disposal. When those resources are too heavily populated with misinformation; disinformation; propaganda; or conspiracy theory, individual agency is profoundly diminished and informed policy dialog, meaningful political accountability, and healthy democracy become

Correspondence should be sent to Michael Landon-Murray, School of Public Affairs, University of Colorado Colorado Springs, 1420 Austin Bluffs Pkwy, Colorado Springs, CO 80918, USA. E-mail: mlandonm@uccs.edu

virtually impossible. The United States has seen its politics and elections profoundly undermined by both disinformation (intentionally false information to serve an objective) and misinformation (simply incorrect information) in recent years, from internal and external sources. The U.S. itself has a long history of employing disinformation, propaganda, and political interference (Bittman, 1990; Fabre, 2018; Johnson, 1989; Levin, 2016). U.S. disinformation operations have targeted the Soviet Union, as well as regimes in Latin America and the Middle East, and were deployed in the Iran-Contra affair (Bittman, 1990; Zakaria, 2002). Pressures to conduct political and electoral interventions may have subsided somewhat after the Cold War, but emerging geopolitical divisions and the successful use of political disinformation operations by adversaries may make such efforts more attractive and acceptable to U.S. policymakers (Beinart, 2018). Additionally, in an age of social media, fake news and rapid advances in artificial intelligence, disinformation operations take on new forms and will have different, more far-reaching effects. These operations can be conducted remotely at low cost and presented to audiences of millions or even billions. Thus, technology-enabled disinformation is poised to be a very potent tool. It also carries considerable unknowns, a high probability of unintended consequences, and profound questions of governance, accountability, and ethics. Thus, the U.S. finds itself at a critical juncture, and must decide if it is willing, as a matter of public policy in the twenty-first century, to use covert instruments (the focus here being on disinformation) to compromise the integrity of foreign political and democratic systems. Despite growing attention on issues of contemporary political warfare and disinformation, the question of U.S. engagement in cyber disinformation, and the ethics around that, have received much less focus.

The secrecy inherent in covert action creates unavoidable tensions for American democracy. If covert action is to be soundly devised and consistent with U.S. legal and normative parameters, public and Congressional dialog, guidance, and oversight are necessary, supported by specialists in policy and area studies as well as ethics. Policy decisions should not unfold in a vacuum, especially when the rule of law and basic democratic norms seem vulnerable in the U.S. The potentially destabilizing effects of disinformation, at home and abroad, underscore the criticality of broad input. Further, uses of secretive intelligence organs and operations must be continually informed by considerations of ethics and accountability, especially as technology evolves. Intelligence agencies possess tremendous powers; powers that operate mostly out of public sight and that have been repeatedly abused in the past. Moreover, when there are heightened worries about movement in illiberal directions, it is that much more critical to examine the entities that may be employed in that backslide.

This article thus addresses contemporary U.S. policy decisions relating to the use of disinformation to influence political systems and discourses of other nations from the standpoint of ethical and democratic values. To situate the analysis, the article begins with a brief look at the literature on the practice and ethics of U.S. covert action. It then moves to a discussion of the modalities, ethical and practical implications, and governance challenges related to disinformation operations in the age of fake news, social media, and artificial intelligence. The article also briefly presents alternative strategies and policy options, with a focus on public affairs education.

PRACTICE AND ETHICS OF U.S. COVERT ACTION

Covert action entails efforts to influence political; governmental; organizational; social; economic; and military dynamics and events abroad while concealing the role of governmental actors or support, intending to minimize the likelihood of escalation. This includes a range of specific, often interconnected activities short of open military conflict but beyond overt foreign policy and diplomacy: propaganda and information operations; electoral interventions; sabotage; support for coups; and paramilitary operations, among others. Covert tools can be employed against an adversary (including nonstate actors), or in support of a friend or ally, to serve critical U.S. foreign and security interests. Intervening in foreign political systems can sometimes be in the service of democracy in the target nation (Bittman, 1990). In addition to seeking preferred electoral or political outcomes, information and other covert operations can serve to confuse and destabilize populations or manipulate perceptions about the actions or intentions of a state. Thus, there is an intimate coupling of covert political and information operations. In the U.S., the Central Intelligence Agency (CIA) remains the lead entity on covert action. Its covert tools are deployed when a president signs a finding, formally designating a given covert action as essential to U.S. foreign policy and security. A notification is then provided to the intelligence oversight committees in Congress with a few exceptions. Substantive changes, as well as regular updates, are also reported to the oversight committees (Baker, 2010).

On covert action, James A. Barry (1993) has offered "thresholds of increasing ethical concern" from limited to significant, serious, and grave, placing the use of deceptive information in the "serious" category. Loch K. Johnson (1992) similarly models a four-tiered "ladder of escalation," characterizing the use of disinformation as a high-risk operation (third threshold), both in democracies and autocracies. Major covert war, governmental overthrows, and assassinations are among the extreme tools. Intervening in nondemocratic regimes or those violating human rights has been viewed as less ethically wrought (Barry, 1993; Fabre, 2018; Johnson, 1992), but sovereignty issues remain (Beitz, 2005). Covert action and cyber disinformation remain nebulously positioned in the context of international law (Lowenthal, 2017; McClintock, 2017) and domestic laws and regulations, not to mention ethical frames, vary from state to state (Fitzgerald & Brantly, 2017).

Covert action can be used for narrow rather than national interests, including leaders' self-interest (Brantly, 2014). Some have observed that CIA-sponsored coups in Iran (1953) and Guatemala (1954) were in service of select business interests (Perry, 2009). The simple invocation of national interests and security—which may be overstated or simply wrong—is not grounds for using covert means (Beitz, 2005). Melvin A. Goodman (2000) has written that covert action has at times been employed by policymakers simply because the option was there, foregoing careful consideration of potential outcomes. Along these lines, Lowenthal (2017) notes the importance of looking to past operations when assessing proposed ones. Barry (1993) has urged that decision making on covert action apply *jus bellum justum* precepts: just cause and intention; proportionality; proper authority; likelihood of success; lack of viable alternatives; the protection of the innocent; and the minimization of damage. Just war theory has also been applied and examined more broadly in the context of intelligence, as well as other rapidly shifting areas, such as changing environmental dynamics (Hedahl, Clark, & Beggins, 2017; Omand & Phythian, 2013).

Many Americans are likely unaware their government has been a frequent source of electoral and political interference, including meddling in soundly democratic states (Downes & Lilley, 2010; Levin, 2016). This presents uncomfortable questions about the international and democratic place of the U.S. The fundamental integrity of the democratic process is contingent upon informed deliberation and participation (Beitz, 2005). Distortions of reality and information can make it difficult to impossible for the public to track and direct their elected leaders (Nincic, 2003). Hidden support of political leadership can corrupt responsiveness to the electorate (Perry, 2009). Potentially, commitment to democracy contends with security and economic interests (Downes & Lilley, 2010). A 2015 study found that when U.S. policymakers expect a democracy to decline (or "decay"), covert interventions become more likely (Poznansky, 2015).

After the close of the Cold War, Loch K. Johnson (1992) noted there was little systematic understanding of the long-term and unintended effects of covert action. He offered the boiling public discontent with the Iranian Shah, Mohammad Reza Pahlavi, who was ousted and then replaced by the Ayatollah Ruhollah Khomeini, as an example of possible negative consequences. In that case, others have pointed to overt U.S. Iran policy to explain the outcome better (Treverton, 2007). In any event, tactical successes in the short-term can give way to tragic conditions in the longer term. This can include subjecting a targeted nation or group to very dire circumstances, such as the imposition of a violent dictator, as was the case in British Guiana (Kibbe, 2010). And while Dov H. Levin (2016) more recently found that electoral interventions increase the votes received by the favored party by 3%, he concluded that overt interventions are more successful than covert ones, and that insight on key long-term effects remain limited. Additionally, covert campaigns have resulted in excessive cost overruns (Prados, 2006). Once a decision has been made to undertake a specific covert action, operational extrication or termination can be a challenge and achieving objectives can quickly become not only more expensive, but also more expansive and risky (Kibbe, 2010; Treverton, 2007). The likelihood of plausible deniability is thus also reduced.

DISINFORMATION OPERATIONS IN THE TWENTY-FIRST CENTURY: TECHNOLOGIES, ETHICS, AND GOVERNANCE

While Cold War disinformation operations often planted fake stories in print newspapers, today, the Internet; social media; artificial intelligence; and any number of purveyors of bad information make the spread of such stories more rapid, pervasive, and perhaps convincing. In fact, bad information often circulates much more quickly than accurate information and is more likely to be shared, for human, financial, and technical reasons (Meserole, 2018; Polyakova & Gonzalez, 2018; Warzel, 2018). Facebook, riddled in recent years with fake news, has nearly two billion users worldwide (Allcott & Gentzkow, 2017). And today, Americans rely heavily on social media for their news. Of course, it can be challenging to successfully target audiences in a dense and expanding information space, but online micro-targeting and "echo chambers" that supply personalized, comfortable views and information certainly help. Further, flooding outlets with bad information can serve to confuse and overwhelm.

Those who are not "motivated reasoners" can also be duped by false stories. Individual vulnerability to inaccurate information, and outright lies, is somewhat inherent (Feldman, 2009). Further, the capacity of flawed and false information to influence perceptions, even after proven incorrect, has been demonstrated in the context of disinformation operations (Boghardt, 2009). As technologies advance, detection of the untrue will be increasingly challenging, with more people likely to believe in events and conditions that never were. People will encounter very real-seeming (fake) video and audio, the automated production and dissemination of fake news utilizing sentiment analysis and bots able to mirror human emotion (Bakir & McStay, 2017; Polyakova, 2018; Warzel, 2018).

In the context of social media and artificial intelligence, disinformation and misinformation are thus proving extremely powerful, both qualitatively and quantitatively. Policy decisions will need to be made regarding both offensive and defensive approaches to emerging technologies. One of the most fundamental questions for U.S. leaders and the public is whether the government should be in the political disinformation business. The U.S. holds a unique place in the world as a senior democracy and leader, and is itself suffering profoundly from problems of untrue stories and "facts." Spanning "Pizzagate;" the antivaccination movement; a Federal Bureau of Investigation wiretap on Trump Tower (that did not happen); the pervasive consumption of fake news in the 2016 Presidential election (and subsequent disbelief that there were Russian interference efforts); a White House-commissioned voter fraud panel (premised on no evidence) (https://www.whitehouse.gov/articles/presidential-advisory-commission-election-integrity-resources-2); and climate change denialism, more and more Americans are proving susceptible to utter falsehoods and fallacious reasoning, with very real implications for public well-being, dialog, and policy as well as political accountability. To be sure, Americans certainly seem to have a longstanding penchant for the fantastical and unsubstantiated (Andersen, 2017).

Disinformation applications of current and emerging technologies could allow the U.S. to create false speeches or acts from political and religious leaders. Such "footage" might have major geopolitical and diplomatic implications (Warzel, 2018). Of course, these programs will also be available to private, sometimes sophisticated actors, creating another dimension for government to grapple with. These tools can be used to stoke tensions and animosity between and within states and feed false narratives about the past. Leaders will also be able to say that something that *did* happen did not actually happen.

False narratives, as stark as fake video or as subtle as lies intermingled with truth, can also fuel polarized and extreme views, aggravating political and social fissures. This has largely been the recent U.S. experience. Artificial intelligence will allow nefarious actors to simulate citizen input, creating false impressions of constituency preferences when key decisions are made (Warzel, 2018). Such technologies allow actors to propagate disinformation—whether relating to an event or constituent that does not exist—directly to political leaders, who themselves may not be equipped to detect such deception. Increasingly complex networks and campaigns will come with these technological advances. This will create permutations beyond the already maddening labyrinth of bots; troll farms; hacking and leaks; social media manipulation; state-run media and the inundation of competing narratives (potentially from the same source); and the deluge of fake stories.

Thus, foreign political and democratic processes at individual and societal levels can be interfered with in ways not previously possible, at a time when democratic systems and norms are eroding around the globe (Freedom House, 2018). Recent political developments in Hungary; Brazil; Poland; and Turkey are four such examples of eroding democracy. Information landscapes replete with misinformation will spur immense confusion, even resulting in "reality apathy" and its alarming implications for citizen knowledge of governance and public affairs (Warzel, 2018). Dangerous politicians and demagogues can themselves seek to muddy the waters in order to strengthen their own position. Further, as political knowledge and accountability are challenged by a chaotic and conflicting information environment, leaders will have a freer hand to act without meaningful public insight and input (Nincic, 2003).

It is also a virtual certainty that disinformation intended for audiences abroad will be boomeranged back to the U.S. (dubbed the blowback effect), allies, and other democracies. The Internet, social media, and related platforms cross national boundaries. By pumping more junk into cyberspace, U.S. policymakers and operators run the risk of inadvertently compromising domestic informational and political landscapes. While the CIA cannot purposefully target domestic populations with disinformation or other efforts to influence politics and media, it may unintentionally end up doing just that (Kibbe, 2010; Lowenthal, 2017).

If revealed publicly, such campaigns will likely undermine future U.S. efforts to shape narratives and influence opinions in legitimate ways, including through public diplomacy. Engaging publics and leaders of other nations, especially after inevitable revelations about disinformation campaigns, will be difficult. Trust at home will also be eroded, particularly if covert actions are not truly consistent with American interests and values.

Given the above, the new technologies underlying contemporary disinformation suggest impacts that likely exceed, or at least not conform to, the degree of ethical concern and disruption envisioned by Johnson (1992) and Barry (1993). Further, given the unpredictable, lasting effects of these tools, criteria of proportionality; likelihood of success; protection of the innocent; and minimization of damage seem very difficult to measure, let alone ensure. Even in the most just of causes (such as human rights violations), there are likely to be superior or preferable policy options (that come with less in the way of long-lasting harm), and thus the application of the just war framework to advanced cyber disinformation campaigns suggests that few such operations will meet these standards. The unpredictable damage done by advanced disinformation operations, against innocent citizens in democracies and nondemocracies alike (including in the U.S.), will be exceedingly difficult if not impossible to undo, and must be taken into account in decision making. Beyond the residual effects such operations have caused (Boghardt, 2009), correcting evidence can actually bolster some individuals' misinformed and false beliefs, known as the backfire effect (Lewandowsky, Ecker, Seifert, Schwarz, & Cook, 2012). Further, Mark Stout (2017) observes that the ability of cyber influence to achieve actual desired ends remains an open question. However, even the knowledge of possible covert information and electoral interventions can undermine public confidence in political processes (Calabresi, 2017), and if the sole objective is to create utter confusion and "reality apathy," emerging disinformation technologies stand to be quite powerful. It is improbable that disinformation will be disavowed altogether by the U.S., but the many and varied downsides, normative as well as practical, cannot be overlooked, and if fairly assessed, will likely result in the infrequent use of cyber disinformation tools.

The uncertain, uncontrollable effects of modern disinformation, not to mention the profound ethical implications and possible executive abuse, means that robust Congressional involvement in U.S. covert action policy remains imperative. This will ensure such decisions are subject to appropriate oversight and consistent with American values, policy objectives, and statute. In the secretive, classified spheres of intelligence and covert action, Congress serves an especially critical role as the public's proxy. Other key actors, including media and interest groups, are less likely to pull the "fire alarm" in the face of abuses and bad decisions, because many operations will remain unknown. Historically, intelligence oversight has not been a high priority for Congress (Zegart & Quinn, 2010), although the misuse or concealment of covert tools has quickly gotten its attention in the past (Daugherty, 2004; Hastedt, 2017).

Recently, base partisanship has often characterized the behavior of Congress, including the House Intelligence Committee (https://intelligence.house.gov) (Allen, 2018). When legislative oversight diminishes, executive discretion grows. Early and consistent Congressional attention could serve to forestall later executive misuse of disinformation. It cannot be overlooked that a tremendous amount of the misinformation being directed at the American public has come from their President (Peters, 2017; Rose, 2017). His allegiance to facts has been shown wanting on a daily basis (Kessler, Rizzo, & Kelly, 2018). He has also accrued a long list of statements and actions that show contempt for democracy and the rule of law (Just Security, n.d.). His respect for foreign publics and politics is presumably that much less and his inclination seems very much toward the brute application of executive instruments. Reportedly, President Trump implored the Secretary of Defense to have Syria's president, Bashar al-Assad, assassinated—one the most extreme covert actions, and outlawed in the U.S. (Woodward, 2018). At the same time, and as part of what seems to be a broader trend in delegating national security policymaking to lower-level officials, in August 2018, President Trump issued a directive that diminishes the interagency review process for offensive cyber actions (Rudesill, 2018).

Budgeting and funding are key tools to influence covert action. If Congressional committees do not support covert actions, they can choose not to fund them (Daugherty, 2004; Lowenthal, 2017). To this end, Congressional oversight will help ensure that actors in the executive branch are not only considering broader policy and value questions, but also actively seeking less intrusive alternatives, closely linking proportionate actions with clear objectives. These factors inform CIA and executive decision making, but historically and structurally there is good reason to be skeptical (Steiner, 2006). Congress can also informally dissuade covert actions, and has in virtually all recent administrations, lobbying the President to forestall a covert operation (Daugherty, 2004; Lowenthal, 2017).

Congress could also enact legislation controlling disinformation policy. In the extreme form, and perhaps not likely, statute could preclude the U.S. government from spreading false political information, outside the context of warfare, regardless of the cause. It is worth noting that the Iran–Contra affair demonstrated that even strict legislative attempts to control covert action can be ignored or subverted by a determined executive (Currie, 1998).

At a high, unclassified, and normative level, the public sets the parameters of what programs and operations the government and its intelligence services may undertake. To act as the ultimate "principal," it must be a part of the dialog. In the context of covert action, public

debate is essential in determining the appropriateness of objectives and methods (Barry, 1993). However, it is not easy to imagine a civil and relatively dispassionate "national conversation" on this topic, despite the impact these issues have had on American politics (and perhaps *because* of those impacts). With excessive motivated, fallacious reasoning and the starkly different information universes existing in the U.S., meaningful dialog seems to have only an outside chance. This is not a positive note to end on, but maybe the best argument against undermining the integrity of news and information abroad.

CONCLUSION

The U.S. has long engaged in covert political warfare, including disinformation operations. Today, the Internet, social media, and artificial intelligence allow unprecedented reach, and Americans continue to be a target of foreign disinformation. The prospects and ethics of the U.S. engaging in such tactics in this new era have received inadequate attention. As "fake news" is about to be accompanied by "fake events," and other yet unimagined applications, these potentialities must be addressed. Despite a President who describes any inconvenient coverage as "fake news," is a font of misinformation (possibly disinformation) and shows resentment for even the most basic tenets of democracy, the U.S. retains a critical leadership role in the international system. There are currently perverse mirrors of this around the world, as despots make allegations of "fake news" when unflattering stories emerge.

Utilizing emerging technologies in the context of disinformation will not only have destabilizing and unpredictable effects in targeted locales, but will also result in more bad information undermining knowledge, political accountability, and democracy in the U.S. U.S. efforts may be better directed toward measures that will counter adversary disinformation campaigns and create resilience amongst the U.S. population. There is good reason to look at efforts to strengthen education and news literacy (including critical thinking); research and technology; elections systems and practices; information sharing; and international partnerships among other measures (Bodine-Baron, Helmus, Radin, & Treyger, 2018; Conley & Jeangene Vilmer, 2018; Conroy, Rubin, & Chen, 2015; Kahne & Bowyer, 2017). Similarly, the U.S. can learn from other nations and deploy better alternatives to promote its interests, security, and values. This might include the simple dissemination of true information (both abroad and at home), aggressive and open efforts to expose disinformation, and the use of overt policy alternatives which may be more influential in any event and come with much less in the way of ethical compromise and uncontrollable outcomes (Bittman, 1990; Conley & Jeangene Vilmer, 2018; Levin, 2016; Sternstein, 2017).

On the education front, there is a critical role for public affairs programs, which will likely necessitate curricular adaptations. In an increasingly chaotic information and media landscape, strong democracy and civic engagement are premised on the ability to distinguish between reliable and unreliable sources and information, and a 2016 Stanford University study found that American students are not particularly skilled in this regard (Wineburg, McGrew, Breakstone, & Ortega, 2016). Evidence also suggests that media literacy learning opportunities help develop such skills, not political knowledge alone, which can actually embolden motivated reasoning and confirmation biases (Kahne & Bowyer, 2017).

Those entering public service will need to understand and navigate the contemporary landscape, and avoid its pitfalls themselves. They will also need to make sound, ethical decisions in that landscape and design policies and messages that help their publics grapple with dubious and false information. How to use, or not use, advancing disinformation technologies is only one outgrowth that will need to be addressed by practitioners and scholars, and as more is learned about combatting bad information, more can be done in the classroom to create the kinds of public servants the twenty-first century will require. To be sure, other academic programs, from liberal arts to STEM and law, must also prepare students to fulfill their professional responsibilities and conduct themselves ethically in a world replete with misinformation.

ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers and editors for their very helpful feedback, which allowed us to strengthen and clarify central facets of the article.

REFERENCES

Andersen, K. (2017). *Fantasyland: How America went haywire: A 500-year history*. New York, NY: Random House.

Allcott, H., & Gentzkow, M. (2017). Social media and fake news in the 2016 election. *Journal of Economic Perspectives*, *31*(2), 211–236. doi:10.1257/jep.31.2.211

Allen, J. (2018, February 2). Experts warn: Dangerous politicizing of U.S. intelligence. *NBC News.* Retrieved from https://www.nbcnews.com/politics/politics-news/experts-warn-dangerous-politicizing-u-s-intelligence-n844211

Baker, J. E. (2010). Covert action: United States law in substance, process, and practice. In L. K. Johnson (Ed.), *The Oxford handbook of national security intelligence* (pp. 587–607). Oxford, UK: Oxford University Press. doi: 10.1093/oxfordhb/9780195375886.003.0036

Bakir, V., & McStay, A. (2017). Fake news and the economy of emotions. *Digital Journalism*, *6*(2), 154–175. doi: 10.1080/21670811.2017.1345645

Barry, J. A. (1993). Covert action can be just. *Orbis*, *37*(3), 375–390. doi:10.1016/0030-4387(93)90152-3

Beinart, P. (2018, July 22). The U.S. needs to face up to its long history of election meddling. *The Atlantic.* Retrieved from https://www.theatlantic.com/ideas/archive/2018/07/the-us-has-a-long-history-of-election-meddling/565538/

Beitz, C. R. (2005). Covert intervention as a moral problem. In J. Goldman (Ed.), *The ethics of spying: A reader for the intelligence professional* (pp. 206–220). Lanham, MD: Scarecrow.

Bittman, L. (1990). The use of disinformation by democracies. *International Journal of Intelligence and Counterintelligence*, *4*(2), 243–261. doi:10.1080/08850609008435142

Bodine-Baron, E., Helmus, T. C., Radin, A., & Treyger, E. (2018). *Countering Russian social medial influence*. Santa Monica, CA: RAND. doi:10.7249/RR2740

Boghardt, T. (2009). Operation INFEKTION: Soviet bloc intelligence and its AIDS disinformation campaign. *Studies in Intelligence*, *53*(4), 1–24. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/soviet-bloc-intelligence-and-its-aids.html

Brantly, A. F. (2014). Cyber actions by state actors: Motivation and utility. *International Journal of Intelligence and Counterintelligence*, *27*(3), 465–484. doi:10.1080/08850607.2014.900291

Calabresi, M. (2017, May 29). Inside Russia's social media war on America. *Time.* Retrieved from http://time.com/4783932/inside-russia-social-media-war-america

Conley, H. A., & Jeangene Vilmer, J. (2018). *Successfully countering Russian electoral interference*. Washington, DC: Center for Strategic & International Studies. Retrieved from https://www.csis.org/analysis/successfully-countering-russian-electoral-interference

Conroy, N. J., Rubin, V. L., & Chen, Y. (2015). Automatic deception detection: Methods for finding fake news. *Proceedings of the Association for Information Science and Technology*, *52*(1), 1–4. doi:10.1002/pra2.2015.145052010082

Currie, J. T. (1998). Iran-contra and Congressional oversight of the CIA. *International Journal of Intelligence and Counterintelligence*, *11*(2), 185–210. doi:10.1080/08850609808435372

Daugherty, W. J. (2004). Approval and review of covert action programs since Reagan. *International Journal of Intelligence and Counterintelligence*, *17*(1), 62–80. doi:10.1080/08850600490252566 9

Downes, A. B., & Lilley, M. L. (2010). Overt peace, covert war? Covert intervention and the democratic peace. *Security Studies*, *19*(2), 266–306. doi:10.1080/09636411003795756

Fabre, C. (2018). The case for foreign electoral subversion. *Ethics & International Affairs*, *32*(3), 283–292. doi:10.1017/S0892679418000424

Feldman, R. (2009). *The liar in your life: The way to truthful relationships*. New York, NY: Twelve.

Fitzgerald, C. W., & Brantly, A. F. (2017). Subverting reality: The role of propaganda in 21st century intelligence. *International Journal of Intelligence and Counterintelligence*, *30*(2), 215–240. doi:10.1080/08850607.2017.1263528

Freedom House (2018). *Freedom in the world 2018: Democracy in crisis*. Retrieved from https://freedomhouse.org/report/freedom-world/freedom-world-2018

Goodman, M. A. (2000). Espionage and covert action. In C. Eisendrath (Ed.), *National insecurity: U.S. intelligence after the Cold War* (pp. 23–44). Philadelphia, PA: Temple University Press. Retrieved from http://muse.jhu.edu/book/9758

Hastedt, G. (2017). The CIA and Congressional oversight: Learning and forgetting lessons. *Intelligence and National Security*, *32*(6), 710–724. doi:10.1080/02684527.2016.1275137

Hedahl, M., Clark, S., & Beggins, M. (2017). The changing nature of the just war tradition: How our changing environment ought to change the foundations of just war theory. *Public Integrity*, *19*(5), 429–443. doi:10.1080/10999922.2017.1278667

Johnson, L. K. (1989). Covert action and accountability: Decision-making for America's secret foreign policy. *International Studies Quarterly*, *33*(1), 81–109. doi:10.2307/2600495

Johnson, L. K. (1992). On drawing a bright line for covert operations. *American Journal of International Law*, *86*(2), 284–309. doi:10.2307/2203235

Just Security. (n.d.). *Norms watch.* Retrieved from https://www.justsecurity.org/tag/norms-watch

Kahne, J., & Bowyer, B. (2017). Educating for democracy in a partisan age: Confronting challenges of motivated reasoning and misinformation. *American Educational Research Journal*, *54*(1), 3–34. doi:10.3102/0002831216679817

Kessler, G., Rizzo, S., & Kelly, M. (2018, August 1). President Trump has made 4,229 false or misleading claims in 558 days. *The Washington Post.* Retrieved from https://www.washingtonpost.com/news/fact-checker/wp/2018/08/01/president-trump-has-made-4229-false-or-misleading-claims-in-558-days

Kibbe, J. D. (2010). Covert action. In *The Oxford research encyclopedia of international studies*. Oxford, UK: Oxford University Press. doi:10.1093/acrefore/9780190846626.013.135

Levin, D. H. (2016). When the great powers get a vote: The effects of great power electoral interventions on election results. *International Studies Quarterly*, *60*(2), 189–202. doi:10.1093/isq/sqv016

Lewandowsky, S., Ecker, U. K. H., Seifert, C. M., Schwarz, N., & Cook, J. (2012). Misinformation and its correction: Continued influence and successful debiasing. *Psychological Science in the Public Interest*, *13*(3), 106–131. doi:10.1177/1529100612451018

Lowenthal, M. M. (2017). *Intelligence: From secrets to policy* (7th ed.). Thousand Oaks, CA: CQ Press.

McClintock, B. (2017, July 21). Russian information warfare: A reality that needs a response. *RAND.* Retrieved from https://www.rand.org/blog/2017/07/russian-information-warfare-a-reality-that-needs-a.html

Meserole, C. (2018, May 9). How misinformation spreads on social media—and what to do about it. *Brookings Institution.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/05/09/how-misinformation-spreads-on-social-media-and-what-to-do-about-it

Nincic, M. (2003). Information warfare and democratic accountability. *Contemporary Security Policy*, *24*(1), 140–160. doi:10.1080/13523260312331271849

Omand, D., & Phythian, M. (2013). Ethics and intelligence: A debate. *International Journal of Intelligence and Counterintelligence*, *26*(1), 38–63. doi:10.1080/08850607.2012.705186

Perry, D. L. (2009). *Partly cloudy: Ethics in war, espionage, covert action, and interrogation*. Lanham, MD: Scarecrow Press.

Peters, M. A. (2017). Education in a post-truth world. *Educational Philosophy and Theory*, *49*(6), 563–566. doi:10.1080/00131857.2016.1264114

Polyakova, A. (2018, March 22). The next Russian attack will be far worse than bots and trolls. *Brookings Institution.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/03/22/the-next-russian-attack-will-be-far-worse-than-bots-and-trolls

Polyakova, A., & Gonzalez, G. (2018, August 7). Why the U.S. anti-smoking campaign is a great model for fighting disinformation. *Brookings Institution.* Retrieved from https://www.brookings.edu/blog/order-from-chaos/2018/08/07/why-the-u-s-anti-smoking-campaign-is-a-great-model-for-fighting-disinformation

Poznansky, M. (2015). Stasis or decay? Reconciling covert war and the democratic peace. *International Studies Quarterly*, *59*(4), 815–826. Retrieved from https://www.isanet.org/Publications/ISQ/Posts/ID/4740/Stasis-or-Decay-Reconciling-Covert-War-and-the-Democratic-Peace

Prados, J. (2006). *Safe for democracy: The secret wars of the CIA*. Chicago, IL: Ivan R. Dee.

Rose, J. (2017). Brexit, Trump, and post-truth politics. *Public Integrity*, *19*(6), 555–558. doi:10.1080/10999922.2017.1285540

Rudesill, D. S. (2018, August 29). Trump's secret order on pulling the cyber trigger. *Lawfare.* Retrieved from https://www.lawfareblog.com/trumps-secret-order-pulling-cyber-trigger

Steiner, J. (2006). Restoring the red line between intelligence and policy on covert action. *International Journal of Intelligence and Counterintelligence*, *19*(1), 156–165. doi:10.1080/08850600500332532

Sternstein, A. (2017, March 24). Estonia's lessons for fighting Russian disinformation. *Christian Science Monitor.* Retrieved from https://www.csmonitor.com/World/Passcode/2017/0324/Estonia-s-lessons-for-fighting-Russian-disinformation

Stout, M. (2017). Covert action in the age of social media. *Georgetown Review of International Affairs*, *18*(2), 94–103. doi:10.1353/gia.2017.0024

Treverton, G. F. (2007). Covert action: Forward to the past? In L. K. Johnson (Ed.), *Strategic intelligence volume 3: Covert action* (pp. 1–21). Westport, CT: Praeger Security International.

Warzel, C. (2018, February 11). He predicted the 2016 fake news crisis. Now he's worried about an information apocalypse. *BuzzFeed News.* Retrieved from https://www.buzzfeednews.com/article/charliewarzel/the-terrifying-future-of-fake-news

Wineburg, S., McGrew, S., Breakstone, J., & Ortega, T. (2016). Evaluating information: The cornerstone of civic online reasoning. Stanford Digital Repository. Retrieved from https://purl.stanford.edu/fv751yt5934

Woodward, B. (2018). *Fear: Trump in the White House*. New York, NY: Simon & Schuster.

Zakaria, T. (2002, February 25). U.S. planting false stories common Cold War tactic. *Reuters.* Retrieved from https://fas.org/sgp/news/2002/02/re022502.html

Zegart, A., & Quinn, J. (2010). Congressional intelligence oversight: The electoral disconnection. *Intelligence and National Security*, *25*(6), 744–766. doi:10.1080/02684527.2010.537871