AWC Fellows
Strategy Research Project

21st Century Statecraft and the Return of Great Power Competition: An Interagency Framework for Non-Traditional Threats

by

Lieutenant Colonel (P) Michael Rose
United States Army

Under the Direction of:
Simon Miles, Ph.D. and Christopher Bolan, Ph.D.

While a Fellow at:
Duke University

United States Army War College
Class of 2019

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE	*Form Approved--OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 01-03-2019	**2. REPORT TYPE** FELLOWS STRATEGY RESEARCH PROJECT	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE 21st Century Statecraft and the Return of Great Power Competition: An Interagency Framework for Non-Traditional Threats	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER**
6. AUTHOR(S) Lieutenant Colonel (P) Michael Rose United States Army	**5d. PROJECT NUMBER** **5e. TASK NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Faculty Adviser: Simon Miles, Ph.D. Host Institution: Duke University	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Faculty Mentor: Christopher Bolan, Ph.D. U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT Distribution A: Approved for Public Release. Distribution is Unlimited.
To the best of my knowledge this FSRP accurately depicts USG and/or DoD policy & contains no classified information or aggregation of information that poses an operations security risk. **Author:** ☒ **Mentor:** □

13. SUPPLEMENTARY NOTES
Word Count: 11280

14. ABSTRACT

With the reemergence of great power competition, strategic competitors and rogue states pose a variety of threats to the United States and allies, but it is their willingness to operate in the 'gray zone' to press the boundaries of interstate competition short of war and use political warfare to undermine liberal democratic institutions which offers common dangerous characteristics. Russia's deliberate undercutting of competitors and manipulation of weaker states provides a representative example of these types of non-traditional threats. To design an updated interagency framework for non-traditional threats, this paper examines three case studies in interagency organizational design used to counter other non-traditional threats: counterterrorism, counter narcotics trafficking, and America's Cold War efforts to counter Soviet subversion. The proposed framework draws on key characteristics from these case studies for interagency organizational structure to more effectively conduct the art of statecraft short of war. The United States should establish an interagency organizational structure at the strategic and operational levels that has both a defensive and offensive mandate, bridges the foreign and domestic divide in the diplomatic, military, intelligence, and law enforcement communities, and includes public, private, and international partnerships when appropriate.

15. SUBJECT TERMS
Gray Zone, Political Warfare, Joint Interagency Task Force (JIATF)

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT UU	**b. ABSTRACT** UU	**c. THIS PAGE** UU	SAR	54	**19b. TELEPHONE NUMBER** *(w/ area code)*

21st Century Statecraft and the Return of Great Power Competition: An Interagency Framework for Non-Traditional Threats

(11280 words)

Abstract

With the reemergence of great power competition, strategic competitors and rogue states pose a variety of threats to the United States and allies, but it is their willingness to operate in the ‘gray zone’ to press the boundaries of interstate competition short of war and use political warfare to undermine liberal democratic institutions which offers common dangerous characteristics. Russia’s deliberate undercutting of competitors and manipulation of weaker states provides a representative example of these types of non-traditional threats. To design an updated interagency framework for non-traditional threats, this paper examines three case studies in interagency organizational design used to counter other non-traditional threats: counterterrorism, counter narcotics trafficking, and America’s Cold War efforts to counter Soviet subversion. The proposed framework draws on key characteristics from these case studies for interagency organizational structure to more effectively conduct the art of statecraft short of war. The United States should establish an interagency organizational structure at the strategic and operational levels that has both a defensive and offensive mandate, bridges the foreign and domestic divide in the diplomatic, military, intelligence, and law enforcement communities, and includes public, private, and international partnerships when appropriate.

21st Century Statecraft and the Return of Great Power Competition: An Interagency Framework for Non-Traditional Threats

While the United States has routinely made incremental changes to its national security departments and agencies, the most significant changes have occurred when the government focused — or rather, was compelled to focus — on reorganizing the national security structure to address the current threat of the time. Most of these major revisions and new organizations were born from recent failures and in times of crisis. To meet the revived threats posed by renewed great-power competition, specifically non-traditional threats in the gray zone from strategic competitors and rogue states, but most prevalently from Russia, the United States should conduct the next evolution in restructuring interagency organizational design before further evolution and expansion of the threat — or a catastrophic event — necessitates in extremis change as occurred at the end of World War II and following the 9/11 attacks.

At the conclusion of World War II, the Truman administration and Congress completely restructured the organization of America's national security apparatus. Congress' main goal was to prevent another strategic surprise as the intelligence failure to predict the December 7, 1941 attack on Pearl Harbor demonstrated. More forward looking, President Truman was focused on organizing for the future threat posed by the Soviet Union.[1] The result was the National Security Act of 1947, creating the National Security Council (NSC), Secretary of Defense and Defense Department (DoD), and the Central Intelligence Agency (CIA).[2] This foundation effectively supported the United States in creating and maintaining the liberal-democratic world order during the ideological struggle against communism for nearly fifty years and brought about the favorable end to the Cold War. Yet, a future-focused reassessment of national security organizational structure did not occur once the strategic conditions defined by the Cold War changed, giving rise to new strategic threats to the United States such as transnational terrorist organizations.

Following the terrorist attacks on September 11, 2001, Congress and the George W. Bush administration conducted the largest restructuring of the national security apparatus since 1947. Once again, the government organized for the threat, albeit again following a failure. The Intelligence Reform and Terrorism Prevention Act of 2004 established the Director for National Intelligence to replace the CIA director as the head of the Intelligence Community (IC), empowering the position with budgetary and personnel control over all seventeen member-agencies, and the National Counterterrorism Center (NCTC), to bridge the divides associated with terrorism-related intelligence and strategy. It also strengthened Federal Bureau of Investigation's (FBI) mandate as the leading domestic counterterrorism and counterintelligence organization in the government, which, along with the newly created Department of Homeland Security, would be key to defending the homeland and preventing future attacks.[3] Nearly two decades later, these changes have proven effective in defending the homeland from major attack and enabled a strategy of proactive counterterrorism, but strategic conditions have once again changed while the United States focused on the threat of terrorism.

As key guiding documents such as the Director of National Intelligence's (DNI) 2017 Global Trends, the 2017 National Security Strategy (NSS), and the 2018 National Defense Strategy (NDS) attest, terrorism is no longer America's principal national security concern.[4] Since 2014, the United States has faced the return of great power competition with Russia and China, as well as rogue states Iran and North Korea, presenting the United States with asymmetric and subversive challenges. The most severe are aimed at undermining America's, and its partners' and allies', liberal democratic institutions, political systems, and societal cohesion.[5] Thus, the United States is faced with traditional rivals using non-traditional means to exert national power and achieve their political objectives. Russia's deliberate strategy of undercutting competitors and manipulating weaker states is most emblematic of these non-traditional threats. But with much of the nation's national security infrastructure organized on a post–Cold War footing oriented against transnational terrorist organizations, now is the time to ask, "Are we organized for today's non-traditional threats?"

To design an updated interagency framework for non-traditional threats posed by strategic competitors and rogue states, this paper conducts a focused assessment of non-traditional threats with specific emphasis on Russia's methods of subversion and political warfare. It then considers three case studies in interagency organizational design used to counter other non-traditional threats. First, America's post–9/11 counterterrorism organizational structure demonstrates that effective interagency organizations can be implemented in a revolutionary manner following crisis. Second, the counter narcotics trafficking example, beginning in the 1980s and continuing today, shows how interagency organizations can evolve to become more effective by applying the lessons of failure and increasing successes, with organizational adjustments to match a changing threat. Third, the efforts to counter Cold War–era Soviet subversion provide example of centralized strategic decision-making and limited scope interagency organizations against a threat similar to that of today, but with important distinctions.

The proposed interagency framework draws on key characteristics from these case studies that will enable the United States to organize most effectively for the threats of the day.

The organizational interagency cooperation demonstrated by the counterterrorism community, counter-narcotics organizations, and America's Cold War efforts against Soviet subversion provide the U.S. government examples from which to draw upon in organizing for today's non-traditional threats at the strategic and operational levels, prior to crisis, in order to accomplish the objectives set forth in the NSS and NDS. A strategic-level organization is necessary to focus strategic analysis and comprehensive policymaking to take on today's non-traditional threats. But it is also insufficient for the objective if not complemented by one or more operational action arms, empowered with proper authorities to act and to coordinate and synchronize interagency activities meant to identify, disrupt, dismantle, and deter. In the current era of adversaries aggressively pressing the boundaries of international norms and peace to achieve their strategic objectives, the United States must more effectively conduct the art of statecraft short of war. To do so, the United States should establish an interagency organizational structure at the strategic and operational levels that has both a defensive and offensive mandate, bridges the foreign and domestic divide in the diplomatic, military, intelligence, and law enforcement communities, and includes public, private, and international partnerships when appropriate.

What is the Future Threat?

The reemergence of great power competition, as identified in the NSS and NDS, highlights the return of strategic competitors Russia and China, as well as destabilizing rogue states Iran and North Korea.[6] These nations pose a variety of threats to the United States and allies, but it is their willingness to operate in the ‘gray zone’ to press the boundaries of interstate competition short of war and use political warfare to undermine liberal democratic institutions which offers common dangerous characteristics.[7] The rules-based democratic world order does not suit these nations’ strategic ends, therefore they are inclined to challenge these fundamental doctrines in order to either reshape them toward their advantage or diminish the strength of the institutions in order to rebalance power in their favor and close the gap in relative strength.[8] Because the cost of conventional war and risk of escalation to nuclear war are so high, and because the United States retains a decisive conventional military advantage, more and more of this competition will be through non-traditional means.[9]

While all of the above-listed adversaries are executing their own respective versions of a gray zone strategy, Russia’s activities below the threshold of war are most representative of the type of non-traditional threats that the United States must better organize against. Of the adversaries identified in the NSS and NDS, Russia’s application of this strategy may pose the largest threat to the post–World War II democratic liberal order because it so deliberately focuses on the transatlantic institutions and the democratic systems of the United States as well as western and central European nations.[10] Further, the Russian doctrine of “New Generation Warfare,” which increasingly integrates non-military means with military capabilities, provides the most coherent assemblage of a strategy that integrates non-traditional means to achieve political ends.[11] Finally, among the aforementioned state adversaries, revanchist Russia is most aggressively employing political warfare as a component of its strategy. Though there is no universally agreed upon definition of political warfare, George Kennan's description as "the logical application of Clausewitz's doctrine in time of peace" which includes "employment of all the means at a nation's command, short of war, to achieve its national objectives" is the most succinct summation. Political warfare, in Kennan's definition and as displayed by Russia behavior, includes activities that are both overt and covert, spanning from political alliances, economic tools, propaganda and psychological warfare, and support to opposition and resistance groups.[12]

Russia employs cyber warfare and information operations to tamper with elections and exploit contentious social issues in order to sow division, expertly manipulating the social media environment with misinformation. It supports opposition groups in non-aligned, western-leaning former Soviet states; hedges for the future through relationships with select terrorist groups; props up authoritarian dictators with mercenary groups, ostensibly operating outside official government sanction; and conducts political assassination against opposition leaders and outspoken members of the media. It uses economic coercion and energy resources to influence governmental decisions and create dependencies. It foments instability in parts of the developing world, resulting in displaced populations seeking refuge in western Europe, using migration as a destabilizing weapon. The United States is not always the intended target of these malign activities, but its major role in the world is the primary motivator for much of this strategy.[13]

The Russian method of political warfare clearly poses not only external but also internal threats to the United States and other targets. This is particularly true in its use of influence operations to manipulate the information environment, which Russian doctrine uses as a fifth column–like tool of statecraft to destabilize societies and undermine governments from within.[14] Often the ultimate goal is not to change its targets' ideology, but rather to erode confidence in western democratic institutions and society. Russia routinely seeks to intensify division in American society by provoking all sides over contentious issues, intent on calling out and exploiting the vulnerabilities created by U.S. racial and economic diversity.[15] Further and more provocative evidence can be found in Russia's efforts to influence the 2016 presidential election. The U.S. Intelligence Community assesses its intent was consistent with efforts "to undermine the U.S.-led liberal democratic order," but with an increased level of intensity not previously seen.[16] Russia has also targeted other western nations' elections, reinserted itself into the 2018 mid-term elections, and is likely postured to do so again in the 2020 presidential race.[17] Russia is also likely to continue more targeted operations to influence U.S. policy through disinformation, data manipulation, and hack-and-leak operations.[18]

Russia's present-day use of political warfare and the gray zone are not dissimilar to Cold War–era Soviet "active measures," which were used to covertly influence and disrupt adversaries by disseminating a wide array of harmful information and disinformation, creating and supporting proxy groups, and enabling illicit and sometimes violent activities.[19] Contemporary Russian influence operations use similar strategies, but with the added velocity, lower cost, and further reach of modern communications technology.[20] In addition, emerging technology in artificial intelligence and machine learning may soon allow the use of ‘neural networks’ to very accurately impersonate real people online and ‘deep fakes’ to create false images, audio recordings, and videos that never actually happened in real life.[21] When used for malign purpose, these tools can flood the information environment with falsehoods and contradictions, thereby making what is true unknowable in the most extreme cases, or at least disrupting societies, media outlets, and key leaders who have to spend energy perpetually correcting the record. Guarding against the magnitude of potential technologically enabled threats will require greatly increased partnership with the private sector.

In the modern era, private industry has a vast role to play in securing our institutions and social fabric. Acknowledging the information environment is a warfighting domain in a political warfare sense, private digital media companies, as much as any government, own the domain in which struggles for legitimacy and influence are commonly fought. In the absence of effective regulatory norms, adversaries use platforms like Facebook and Twitter to carry out their influence operations with near impunity, often concealing the sponsor of the message or the authenticity of the messenger, let alone the accuracy or truthfulness. The news media has been routinely duped into further spinning the echo chamber of “fake news” in their endless efforts to be the first with a storyline, at times sacrificing a professional responsibility to corroborate the veracity of their information. Adversaries can exploit this unwitting error when news outlets prioritize rapid reporting on trending stories, as adversaries have learned to manipulate what is trending through use of automated tools.[22] More overt are the Russian-sponsored news media such as RT (formerly known as Russia Today) and Sputnik, which broadcast news to U.S. and other audiences around the world that has a decidedly anti-western and pro-Russian slant. Russian use of lobbying firms and special-interest groups enables the purchase of influence in Washington, often via Russian proxies which provide distance for the Russian government.[23] In sum, the openness of American society and the U.S. system of government provide an exceptionally large attack surface for influence operations, much of which flows through the private sector.[24]

The 2016 election tampering provides the most glaring example of Russia's political warfare campaign against the United States. In retrospect, the U.S. government now knows much more about the election tampering than it did during the race. The special counsel investigation led by former FBI Director Robert Mueller and the unclassified Intelligence Community assessment provide evidence that the pieces to the puzzle are largely assembled.[25] However, it is now also clear that the Intelligence Community did know that tampering was occurring in the months leading up to the election. The Obama administration, understandably careful to guard against perceptions of the sitting president influencing the election outcome, did not sound the alarm. Instead, they chose a much more subtle strategy to warn the Russians off and inform the public approximately one month before the election.[26] Neither effort gained traction and the public largely ignored the warning.[27] The episode may not have the appearance of a catastrophic event the way Pearl Harbor or the 9/11 attacks do, but it was nevertheless an intelligence failure as Russia's actions were a "sustained assault on [the United States'] traditional values and institutions of governance."[28] Though not as spectacular as those earlier strategic attacks on the U.S. homeland, the deliberate meddling in the 2016 election constitutes an equivalent violation. Russian subversion blatantly violated the political sovereignty of the United States, which, by the definition of aggression between nations, is equal in severity to violating its territorial integrity.[29]

The United States national security apparatus has not yet fully acknowledged that this was on par with previous catastrophic attacks and a reevaluation of the nation's organizational preparedness for future non-traditional threats is long past due. Though the government is now better able to identify this type of activity, it is still not fully organized to rapidly assess the adversary's effectiveness or overall intentions, nor to formulate disruptive and preventative coordinated action. Former DNI James Clapper, who headed the Intelligence Community during the Russian election meddling, affirmed the gap in capability during that time. The IC's capabilities are oriented outside the United States toward external threats and that, though the community could see that the Russians were attempting to influence voters, they did not have the mandate or means to assess the impacts of the influence campaign.[30] Recent examples that show positive movement in recognizing the severity of the threat are the FBI's establishment of the Foreign Influence Task Force and Justice Department's Cyber-Digital Task Force to investigate and counter foreign influence operations.[31] However, these efforts alone are not sufficient to address the magnitude of the global threat. It is imperative to continue to close this and other gaps by further organizing the interagency for the non-traditional threats Russia and other adversaries pose.

Case Studies in Interagency Organization

Counterterrorism, counter-narcotics, and Cold War–era efforts against the Soviet Union’s active measures and other subversive activities offer three interagency structural examples the U.S. government has used to address non-traditional threats. Though the nature of state-sponsored subversion is unique, the threats posed and parried in these case studies are useful comparisons because of their shared characteristics. First, each represents a transregional or global challenge. Terrorist groups and drug trafficking organizations often operate across borders in ways which transcend the geographic and functional administrative boundaries by which America’s national security departments and agencies organize. Soviet active measures also did not historically operate only inside the borders of the U.S.S.R. or the United States. Rather, their disinformation campaigns, political and economic pressure, support to armed opposition groups, and illicit activities occurred on a global scale.[32] Second, they all thrive in the shadows. Their methods of obscuring and concealing their activities and the manner in which they exploited adversaries' vulnerabilities impede the government’s ability to identify and coordinate action. They also took great effort to obfuscate the origins and their sponsorship of the activities, providing necessary plausible deniability. Third, the organizations and their activities functioned as systems to provide command and control and to conduct their activities. With appropriate resources and focus, national security organizations can map systems and processes to better understand the key nodes and personnel in the organizations, provide predictive analysis of emerging threats, and identify vulnerabilities to exploit in order to disrupt plots or dismantle critical capabilities. Fourth and finally, the U.S. government’s counters included kinetic and non-kinetic means, often in the wheelhouse of law enforcement, counterintelligence, and governance programs, but the military does have expertise and resources that can be brought to bear in coordination with the tools resident in other departments and agencies. The best organizing practices drawn from these three case studies will provide a framework for interagency organizational design to address the non-traditional threats posed by state-sponsored subversion.

Counterterrorism Interagency Cooperation: Revolutionary Change

The 9/11 attacks woke America from its post–Cold War slumber, brought on by a decade of unipolar dominance, and led to sweeping change of the national security structure. The ensuing interagency restructuring shows that revolutionary change can create very effective systems to counter non-traditional threats, even if following a catastrophic event. Almost immediately following the attacks, the George W. Bush administration began making changes in order to better organize for the terrorism threat. The president established the Office of Homeland Security, later to become the Department of Homeland Security.[33] Congress passed the PATRIOT Act, providing sweeping authority to domestic law enforcement agencies, and the Authorization for the Use of Military Force (AUMF), giving the Department of Defense the domestic legal authority to pursue the perpetrators of the attacks and those who harbored them.[34]   The administration also reprioritized terrorism within all departments and agencies, setting the nation on a more vigilant and ready footing. In 2004, the publication of the 9/11 Commission Report and the resultant Intelligence Reform and Terrorism Prevention Act legislated the creation of the Director of National Intelligence to head the seventeen-member Intelligence Community. The act empowered the DNI with budgetary and personnel management authority over the entire IC, critical management authority to prioritize collection and analysis across departments and agencies that had not existed under the previous Director of Central Intelligence model. It also mandated the establishment of the National Counterterrorism Center (NCTC) and provided the DNI the authority to establish additional centers to synchronize the IC against specific threats.[35]

Beginning with NCTC at the strategic level and three operational action arms, the counterterrorism case study showcases the value of complementary strategic and operational organizations, their ability to bridge the foreign and domestic divide, the necessity to have both a defensive and offensive mandate, and the importance of a public-private partnership. NCTC holds four principle missions. First is its responsibility as the IC's primary organization for analyzing and integrating all terrorism- and counterterrorism-related intelligence, excluding strictly domestic terrorists.[36] This assignment is meant to bridge the foreign and domestic divide made apparent by the pre–9/11 failure to overcome the rivalries, bureaucratic cultures, and statutory barriers to sharing between the national intelligence organizations and the law enforcement portions of the IC.[37] Second, NCTC is responsible for counterterrorism strategic operational planning, integrating capabilities from all relevant departments and agencies. It is able to assign roles and responsibilities, but it does not have authority to direct the execution of operations.[38] Therefore, it is not itself an operational arm, but rather ensures whole-of-government unity of effort. Third, it ensures intelligence sharing across departments and agencies as appropriate and that those same organizations have the intelligence support required to execute their respective assigned missions. Similar to bridging the foreign-domestic divide, this responsibility is intended to overcome the IC's failure to "connect the dots" prior to 9/11 where numerous pieces of critical information were spread throughout the interagency, but not aggregated or available to all that needed it to identify and assess the emerging threat.[39] Finally, NCTC is the repository of knowledge for terrorists and terrorist groups regarding membership, capabilities, goals, and strategies.[40]

Three interagency operational-level action arms which complement NCTC's strategic focus are noteworthy examples of successful integration of capability from across the national security departments and agencies. Led by the military, the FBI, and the CIA, respectively, each includes representation of departments and agencies with particular counterterrorism tools and responsibilities from across the government, is empowered with clear authority to act, and coordinates operations slightly differently but in an effectively overlapping manner. Each maintains key international partnerships to share information and extend operational reach. All have an offensive, proactive mindset enabling disruption and prevention of attacks, and also dismantlement of terrorist networks and capability. Finally, each of these interagency organizations has the ability to operate across administrative boundaries in order to counter terrorist groups' transregional methods of operation.

Though Joint Interagency Task Forces (JIATF) were not a new concept prior to 9/11, U.S. Special Operations Command has used them to "achieve unprecedented levels of interagency collaboration" in the fight against terror since then.[41] One particularly successful example is the JIATF established in 2004 by then–Lieutenant

General Stanley McChrystal, commander of a special operations joint task force responsible for counterterrorism operations in Iraq, Afghanistan, and other areas where networks supporting terrorism thrived. General McChrystal's goal in bringing together representatives, and therefore capabilities, of the CIA, FBI, National Security Agency (NSA), National Geospatial-Intelligence Agency (NGA), and Defense Intelligence Agency (DIA) was twofold. Bringing together these experts in their fields greatly increased the effectiveness of principally military operations against Al Qaeda's most senior leaders in Iraq and Afghanistan. They also allowed the task force to leverage the tools resident in each of the other participating members' parent organizations in order to disrupt the international nature of Al Qaeda's support apparatus, a network outside the formal war zones which included recruiters, financiers, logisticians, facilitators, and transiting foreign fighters. According to General McChrystal, establishing the JIATF turned the special operations task force "from a collection of niche strike forces into a network able to integrate diverse elements from the U.S. government into a unified effort."[42] The resultant precision and pace of operations is considered a major contributing factor in turning the tide against Al Qaeda in Iraq beginning in 2007.[43]

CIA's Counterterrorism Center (CTC) offers another example of success in operational interagency coordination. As a part of the CIA, this operational action arm is oriented overseas to disrupt terrorist networks.[44] Established in 1986 and still in existence today, though now more robustly resourced and with a vastly more prominent role, CTC was the CIA's first permanent unit to fuse analysis and operations, a much more commonplace practice now.[45] Also including vast representation from across the interagency, CTC has included from its inception other departments and agencies such as NSA, DIA, FBI, and Department of State, to name only a selection and has a close relationship with NCTC.[46] CTC "targets terrorist leaders and cells, disrupts their plots, severs their financial and logistical links, and makes it difficult for terrorists to find safe haven."[47] While most operations are executed by overseas stations and bases, CTC is the coordination hub, integrating operations and intelligence, for the CIA's war on terror.[48]

The FBI maintains a network of Joint Terrorism Task Forces (JTTFs), serving as hubs for interagency cooperation. These law enforcement–heavy JTTFs include representation from the Intelligence Community, the Department of Homeland Security and other federal law enforcement agencies, plus they add the benefit of local law enforcement. With offices in 104 U.S. cities, the JTTFs expand the reach and integration of the FBI and other federal departments and agencies down to the local level. To coordinate across that number of task force elements, an interagency National Joint Terrorism Task Force resides at FBI Headquarters to ensure information and intelligence sharing between local JTTFs and interagency representatives from across the federal government.[49]

Prior to the attacks on 9/11, the FBI was not centrally focused on terrorism, but on criminal investigations. The attacks highlighted a number of gaps in the country's preparedness to identify and disrupt terrorist attacks, both externally and internally. Among those gaps were failures to share across foreign-focused intelligence agencies and the domestically-focused law enforcement community. Also, the FBI's law-enforcement, evidence-based, culture made it more of a reactive organization, so it was not postured for prevention but for investigation after the fact. Following the attacks, then-Director Robert Mueller prioritized its leading role for domestic terrorism and retooled the bureau to become a more proactive in identifying and preventing attacks. The 9/11 Commission Report concluded that the FBI should remain as lead domestically for counterterrorism and counterintelligence and subsequent legislation strengthened the agency's ability to do so.[50] With the shift in mindset, and prioritization within the FBI of counterterrorism, the bureau expanded its network of JTTFs by tripling the number of offices and quadrupling the membership across the country. This footing has allowed the FBI to coordinate not just greater information sharing, but also effectiveness in pre- and post-crisis coordination because of the standing structure and relationships among agencies and personnel.[51] Through JTTFs and their diverse representation from local, state, and federal government, the FBI now develops leads, cultivates informants, and conducts surveillance to thwart future attacks and punish those who support and conduct them, either in the United States or overseas.[52]

The overlapping of military-, CIA-, and FBI-led efforts balances against vast external threats and the growing threat of homegrown violent extremists, those radicalized usually through online propaganda and inspired or directed by overseas terrorist groups to conduct violent attacks at home. The emergence of the increased domestic threat highlights the importance of a public-private partnership in identifying and preventing attacks, which can be leveraged in a number of ways. The FBI views local law enforcement and their integration into JTTFs as critical for this function. Creating relationships within communities and the corporate sector makes it possible to broadly educate the population on the signs of potential nefarious activity and businesses on financial transactions, purchases, or other activities that indicate a future threat.[53] Another example of public-private partnership is the Lower Manhattan Security Initiative, where the New York City Police Department works with public and private partners to deploy and integrate networked technological capability to aid in securing the city's and nation's critical infrastructure in Manhattan's financial district.[54] Through other tools such as Foreign Intelligence Surveillance Court, and formerly PATRIOT, now FREEDOM Act legislation, the law enforcement and intelligence communities gain access to critical private information for national security purpose. Though this creates a tension with civil liberties which must be reckoned with, many private businesses routinely and willingly fulfill reporting requirements in the interest of security.[55] Finally, digital platforms and social media have taken steps to self-police extremist content and to aid Countering Violent Extremism programs. Technology companies investing in increasingly capable artificial intelligence tools to identify inappropriate content or see indications of threatening behavior provide some optimism for limiting vulnerabilities inherent in the ubiquitous nature of social media.[56]

The counterterrorism case emphasizes the importance of strategic- and operational-level complementary organizations that can integrate intelligence and effects across the foreign and domestic divide. The proactive nature of post–9/11 counterterrorism shows the value of both offensive and defensive capability to protect the homeland and U.S. interests. Operational-level interagency organizations led by the military, CIA, and FBI are complementary, not redundant, because they spread differing approaches and mitigate geographic limitations. Like terrorism, Russia's non-traditional threats have both foreign and domestic components and require far-reaching, coordinated actions that are both defensive and offensive in order to protect democratic institutions and U.S. populations from malign influence. Finally, the examples of public-private partnerships in countering violent extremism are necessary to draw from in mitigating Russia’s use of technology, as is mobilizing the private sector in securing America’s open society and system of governance.

Interagency Cooperation in Counter-Narcotics Trafficking: Evolutionary Change

The current interagency cooperation highlighted by Joint Interagency Task Force South (JIATF South), a counter-narcotics trafficking task force, is another example of a well-organized operational action arm, enabled by a complementary strategic-level policy formulation body, with the ability to coordinate across foreign and domestic lines as well as transregionally across administrative boundaries. However, unlike the sweeping changes represented by the terrorism case, interagency cooperation to counter narcotics trafficking occurred more incrementally over time, in a more evolutionary manner. Rather than a single catastrophic event, the roots of interagency organizations to counter drug trafficking began with the rapid growth of Colombian drug cartels in the 1980s, which overwhelmed traditional law enforcement means to counter drugs and associated crime, and grabbed the public’s attention.

Beginning with amendment of the Posse Comitatus Act in 1981, Congress loosened the restrictions on DoD allowing for a supporting role to civilian law enforcement and the Coast Guard, though still restraining the military from direct participation in domestic law enforcement activities. This opened the door to DoD intelligence and surveillance capabilities, as well as logistical and transportation support, being brought to bear. The first two attempts at interagency cooperation were led by Vice President George H.W. Bush in the early 1980s, drawing all key agencies and departments from across the federal government into a task force oriented on networks smuggling into South Florida and a coordinated border interdiction system in the southwestern United States. Both had only limited effects against trafficking and neither achieved the strategic outcomes expected of cabinet-level coordinating body. In 1986, President Ronald Reagan declared that narcotrafficking was a national security threat, adding necessary weight to the effort. Rather than continue to coordinate operations at the national level, the White House instead identified "lead agencies," conceptually dividing responsibility for portions of drug interdiction across different departments and agencies. For instance, the Customs Service had responsibility for land-based interdiction at the borders while the Coast Guard was responsible for maritime interdictions. However, the lead agency approach did not yield the anticipated improvements in interagency cooperation and the threat of drugs and associated violence remained a prevalent threat, causing Congress to intervene in 1988.[57]

Through the Anti–Drug Abuse Act of 1988, Congress created the Office of National Drug Control Policy (ONDCP) in the Executive Office of the President, the beginnings of a strategic-level organization to coordinate policy. At the time, the ONDCP's main responsibility was to ensure that the strategies of the U.S. government's departments and agencies with a drug control mandate aligned with the President's National Drug Control Strategy. However, ONDCP at the time was not empowered to direct cooperation from any department or agency, as incremental improvements in the ONDCP's ability to oversee policy execution would come years later. Congress also directed that DoD assume the lead agency role for detection and monitoring of drug trafficking into the United States, and identified the Coast Guard as the lead agency for interdiction and arrest, in the 1989 National Defense Authorization Act. Other law enforcement agencies maintained their own roles for interdiction and arrest, furthering the ambiguity of which organization had the lead and when and where. This legislation and the executive's emphasis on drug trafficking led to the earliest manifestations of operational level action arms, led by DoD, to coordinate across the interagency. DoD established joint task forces (JTFs) and operations-intelligence fusion centers that would allow DoD to link operations with law enforcement agencies and the Coast Guard in the geographic combatant commands (GCC) of U.S. Pacific Command (USPACOM), North American Aerospace Defense Command (NORAD), U.S. Southern Command (USSOUTHCOM), and Atlantic Command, a command that was later absorbed into other GCCs.[58]

Creation of the JTFs meant an influx of unique resources to support countering narcotics trafficking. However, the impacts of the JTFs were limited by the continued use of the lead agency approach which created seams between the identification and tracking of smuggling activities and the actual interdiction operations. A hesitancy on the part of law enforcement agencies to share sensitive case information further reduced DoD's ability to orient assets toward known shipments. Adding to the problem, each respective participating agency maintained its own intelligence assessment, which led to multiple, uncoordinated collection plans and targeting priorities. The challenge of having no common intelligence or operating picture was further exacerbated by the lack of tactical control the JTFs held over other agencies' assets supporting operations. Finally, a cultural difference between the DoD and law enforcement communities created a tension in determining when to act. The law enforcement community generally preferred to follow the drugs in order to better understand the whole of the smuggling network and make more future arrests and convictions. Conversely, the JTFs preferred interdiction of shipments at the earliest opportunity because of the massive resources and effort required to track targets. It would take additional legislative empowerment of the ONDCP and innovative employment of greatly reduced resources to overcome these early friction points.[59]

Early in his administration, President Bill Clinton conducted a reassessment of the nation's counterdrug strategy, giving greater emphasis to programs aimed at reducing demand in the United States and disrupting the supply chain by combatting narco-trafficking organizations inside source countries, rather than primarily through interdiction. As a result, interdiction resources and operating budgets were cut dramatically.[60] At the same time, though, the President's order strengthened the role of the ONDCP in three key ways, making it responsible for "leading and coordinating the development, implementation, and assessment of U.S. drug policy."[61] First, the order assigned the director responsibility to assess and certify budgets and oversee National Drug Control Strategy compliance of departments and agencies. As Congress provides separate funding for each department and agency, the ONDCP cannot compel expenditures, but may advocate for adjustments to better support the strategy. Second, ONDCP would be responsible for "oversight and direction of all international counter-narcotics policy development and implementation."[62] Third, it directed the ONDCP to establish a Coordinator for Drug Interdiction to ensure sufficiency of assets for interdiction and their optimal integration. The Interdiction Coordinator is responsible for developing and overseeing the National Interdiction Command and Control Plan, which includes resourcing and synchronizing interdiction activities of relevant departments and agencies. Additionally, new legislation empowered the Director of the ONDCP with the ability direct temporary movement of personnel across agencies and to create counterdrug task forces, as it did in collaboration with DoD, the Coast Guard, and the Customs Service in creating the precursor organizations to what is today JIATF South.[63]

Under the ONDCP's new authority, a National Interdiction Command and Control Plan transitioned the JTFs into a new model, JIATFs, with greater unity of effort including tactical control of assets operating in support of its mission and an intelligence support plan to overcome a lack of actionable intelligence by ensuring relevant agencies had access to the right intelligence in a timely manner. These changes took time to implement, but the JIATF model began to overcome the shortcomings of the previous lead agency model.[64]

The predecessors to JIATF South evolved over time to become more efficient, reinforcing success and closing capabilities gaps. The JIATF conducted two major expansions of its area of responsibility (AOR), becoming an exemplar for future transregional task forces. To meet the changing tactics employed by drug traffickers, the JIATF absorbed responsibility for portions of the Pacific and Atlantic Oceans that were not covered by the owning GCCs. Cross-GCC agreements, mirrored by the interagency partner organizations in the JIATF, allowed the task force to operate across GCC administrative boundaries. Their AOR now included all of SOUTHCOM, and parts of PACOM, NORTHCOM, and operational reach into EUCOM. SOUTHCOM also combined the functions of two previously existing JIATFs into one in order to improve end-to-end mission management and operations-intelligence fusion since one task force had been responsible for counterdrug operations inside source countries and the other for interdictions of shipments that had departed those countries. This made a singular task force organized to understand and affect the smuggling network more effectively as a system, end-to-end from cultivation and manufacturing through shipment to distribution networks in the United States, bridging the foreign-domestic divide. It also allowed the task force to follow interdictions and arrests through prosecution and intelligence exploitation, enhancing the intelligence and operations cycle. The JIATF also improved its ability to integrate all intelligence assets, including human intelligence, imagery intelligence, intelligence related to commercial and private air and maritime traffic, and robust signals intelligence, with these resources growing over time with increased successes. The JIATF expanded its reach through a network of liaison teams in embassies in key countries throughout the region which included intelligence support to the law enforcement attaché operating from embassies and consulates. Not only did this yield better information sharing in both directions, but also with host nation partner law enforcement which enabled greater influence over their operations and the task force's understanding of the networks and key personalities it would target. Finally, integrating international partners extends the JIATF's operational reach for interdictions, arrests, and prosecutions in North, Central, and South America and in Europe.[65]

Today, JIATF South is an interagency intelligence and operations fusion organization that complements the strategic policy function of the ONDCP with a centralized element to coordinate intelligence and disruption operations. Like the counterterrorism interagency task forces, it is a proven success as "a model for whole-of-government problem-solving."[66] The DoD-led task force includes all military services partnering with federal law enforcement agencies and members of the intelligence community, plus at least fourteen partner nations. JIATF South's mission is to "execute detection and monitoring of illicit trafficking across all domains, and facilitate international and interagency interdiction to enable disruption and dismantlement of illicit and converging threat networks in support of national and hemispheric security."[67] The JIATF's effectiveness is measured in volume of drugs seized: in 2017, the task force seized 285 metric tons of cocaine, which nearly tripled the average annual seizures from 1989 through 2000 and far exceeds interdictions by other organizations with a similar mission.[68]

JIATF South's successes are a result of a years-long effort to create a system of trust amongst interagency and international partners and to learn how to best employ and integrate the various capabilities available to the task force. The JIATF demonstrates that success breeds success, that other agencies will seek an increased cooperative relationship as long as the task force provides value back to parent organizations. JIATF South also reinforces that it is essential for contributing partners to be senior and empowered to represent their parent organizations' positions and coordinate resources and action as necessary. The example also demonstrates the unique challenges in leading an interagency organization with few formal agreements between contributing departments and agencies. Leaders must prioritize not only the JIATF's mission, but also the equities of partner organizations and nations by showing an appreciation for partner concerns and a willingness to compromise when methods conflict with partner interests.[69]

Counter-narcotics organizational design further demonstrates the value of complementary strategic and operational level organizations. At the strategic level, though an imperfect design lacking a strategic intelligence analysis function, the ONDCP highlights the particular importance of providing the appropriate level of resourcing for, and focus on, the threat is essential to ensuring legitimacy of the effort across departments and agencies. Operationally, JIATF South provides an exceptional example of how law enforcement, intelligence, and military capabilities can integrate to bridge the foreign and domestic divide, a critical capability to effectively counter the foreign and domestic components of Russian subversion. The counter-narcotics methods highlighted here also offer disruptive, offensive capabilities, organized to interdict the adversary's smuggling capability before their illicit cargo reaches U.S. shores. Likewise, the ability to disrupt Russian non-traditional threats before they can fully manifest and dismantle their infrastructure in order to raise the costs of future malign activity will diminish Russia's effectiveness and contribute to deterring Russian subversion. The example of JIATF South also demonstrates that an integrated task force can overcome the limitations of independent departmental actions as well as a lead agency approach to non-traditional threats, where the whole is greater than the sum of its parts. Present efforts against foreign influence led by the FBI and Justice Department follow the lead federal agency approach and should be bolstered through revised interagency organizational structure.

Interagency Coordination to Counter to Soviet Subversion: Limited Scope

Throughout the Cold War, presidential administrations sought ways to coordinate effective actions to check Soviet aggression while balancing risk through centralized decision-making at the national level, an approach that limited the scope of lower-level interagency coordination. Early in the Cold War, the United States created a number of supporting organizations to counter Soviet influence operations, including the U.S. Information Agency and its numerous publications and public messaging outlets Radio Free Europe, Radio Liberty, and Voice of America. It also created organizations to coordinate covert activities with other foreign policy tools, beginning with the Office of Policy Coordination in the CIA in 1948.[70] Presidents Harry Truman and Dwight Eisenhower each established the cabinet-level coordinating bodies which reported to the National Security Council; the Psychological Strategy Board and the Operations Coordinating Board were organized to integrate diplomatic, defense, and intelligence psychological activities and other national security policy execution in the 1950s.[71] In 1961, John F. Kennedy created the U.S. Agency for International Development (USAID) to provide a mechanism for using foreign aid to counter the spread of communism in the developing world.[72]

During this period, the United States devoted all elements of its national power, including diplomacy, information, the military, economics, and covert tools, to achieve strategic objectives and to counter the Soviet Union. Diplomatic and economic support to Turkey and Greece in 1947 signaled the beginning of the Truman Doctrine of providing assistance to democratic nations under internal and external threat from communism.[73] Soon after, the European Recovery Program, better known as the

Marshall Plan, rebuilt and strengthened European economies in order to create resiliency and keep Western European nations securely democratic. Later, USAID would continue as an institutionalized body to provide development aid as a means of combating the spread of communism.[74] The United States employed information programs to reach populations in denied areas and those at risk of communist ideological expansion. The Departments of State and Defense, as well as the CIA, mounted psychological warfare and other messaging efforts throughout the Cold War. The U.S. Information Agency (USIA) provided the most widespread means for overt information efforts including publications in thirty languages, sponsoring pro-U.S. speakers around the world, promoting the arts and cultural events, and administering media organizations.[75] Military alliances, with the North Atlantic Treaty Organization the preeminent example, further bolstered defense against communist aggression and increased the collective power of coalitions against the Soviet Union. The military interventions in Korea and Vietnam illustrated the United States' willingness to use force to check communist expansion and other interventions in Central and South America show the value of Special Forces in countering communist-backed insurgencies in the western hemisphere.[76]

The United States also used CIA covert action, concealing the hand of the U.S. government, throughout the Cold War to supplement diplomatic, economic, and military efforts or with the CIA in the lead, mounting its own independent operations. Early in the Cold War, the CIA provided covert support to anti-communist political parties, labor unions, media, student organizations, and resistance groups in Europe to create strong and compelling alternatives to communist-backed groups, giving them tools to spread anti-communist, pro-Western messages. These efforts served the government's objective of keeping communist parties from gaining influence and political power worldwide. CIA-led regime overthrows in Iran, Guatemala, and Chile in the 1950s removed Soviet-friendly governments and later CIA-supported guerilla movements in Angola, Nicaragua, and Afghanistan pressured communist governments and Soviet support, albeit all with mixed results and impacts.[77]

As the 1979 Soviet invasion of Afghanistan signaled the end of détente, relations between the United States and Soviet Union deteriorated. President Jimmy Carter intensified U.S. public exposure of the moral failures and human rights violations of the Soviet Union, began support to the Solidarity movement in Poland, and initiated covert support for guerilla groups in Afghanistan and elsewhere. Upon assuming office, Ronald Reagan expanded these efforts and others into the most comprehensive strategy against the Soviet Union of the Cold War, intent on exploiting the vulnerabilities inherent in the Soviet system of autocratic and forceful rule. Though the campaign was fundamentally an interagency effort, its planning and conduct was centrally organized and led by Reagan's White House.[78] However, one small interagency organization had outsized impacts against the Soviet counteroffensive.

In response to the increased pressure, the Soviets ramped up their aggressive campaign to weaken the United States and advance Soviet objectives and communist ideology. Reagan considered these so-called active measures such a threat that he established a small, part-time interagency committee called the Active Measures Working Group (AMWG) which coordinated policy to respond to Soviet disinformation. The working group, chaired by the Department of State's Office of Intelligence and

Research, included members of the NSC, CIA, FBI, USIA, and DoD. The group enabled collaboration amongst the participants with the focus limited to exposing covert attempts to influence foreign and domestic populations, thus reducing the disinformation's effectiveness and increasing political costs to the Soviet Union.[79] Ultimately, the AMWG's main purpose was to educate the American and international audience about active measures and to expose the insidious activities of the Soviets. The working group's first report on Soviet malign activities, *Soviet Active Measures: Forgery, Disinformation, Political Operations*, published on October 9, 1981, caught the public's attention with an inventory of active measures techniques: forgeries, press manipulation, disinformation, political influence, support to opposition movements, economic influence, and employment of compromised academics and journalists.[80]

The seminal example of the working group's ability to counter Soviet active measures was the response to a KGB operation to spread disinformation blaming the United States for the creation of the AIDS virus. Employing techniques common to other active measures, the Soviets planted a story in an Indian newspaper through a forged letter purportedly from a U.S. scientist claiming that AIDS was the product of a military biological weapons program. The story lay dormant for nearly three years before the KGB chose to activate it with another published story, this time in the Soviet Union, which built on and referenced the original story. KGB officers leveraged East German counterpart intelligence service to enlist a German scientist to spread the story through scientific publications, high profile interviews, and eventually seeding the story into a popular novel. With more help from the KGB, the story eventually reached global media in eighty countries. The AMWG worked for more than two years to defeat the story, by generally exposing Soviet disinformation techniques to the media, but also specifically using science to debunk the theories supporting the false narrative that the United States created the virus.[81] The AMWG disclosed the Soviet disinformation operations in its *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-1987*. The exposure embarrassed Soviet leadership, especially at a time when the AIDS virus was spreading through the Soviet Union and around the world while the falsified story obstructed medical research cooperation between the countries. Following a confrontation between U.S. Secretary of State George Schultz and Soviet General Secretary Mikhail Gorbachev, the Soviet Academy of Sciences disavowed the story outright in 1987 and again in 1988.[82]

The United States' Cold War efforts provide a successful example of centralization of planning and execution against the non-traditional threats posed by the Soviet Union. This era also provides an example of a narrowly scoped interagency coordination body's effective efforts to expose Soviet disinformation operations. The centralization of interagency coordination evidenced throughout the Cold War is proportionate to the strategic risk of miscalculation or escalation against another superpower. However, though centralizing decision-making was effective in the conditions of the Cold War, in which the United States faced a single adversary operating in a slower and less technologically enabled environment, those conditions do not exist today. Today, the United States faces not only Russia, but also China, North Korea, Iran, and the continued terrorist threat, all confronting the administration with non-traditional challenges. Modern technology also aids in the speed, reach, and low cost of non-traditional threats, making them all the more prevalent. In today's conditions, choosing to rely primarily on the centralized National Security Council process for interagency coordination and execution decisions will hinder the necessary tempo and volume needed to defend against and deter future threats. The U.S. government must create an interagency organizational structure that enables effective statecraft short of war which keeps pace with the widespread non-standard threats to its national security.

An Interagency Framework for Non-Traditional Threats

Drawing on the examples of counterterrorism, counter-drug, and Cold War counter-subversion interagency organizations, four distinct characteristics in organizational design stand out as being most effective against non-traditional threats. First and foremost, there must be complementary strategic and operational level interagency components. A strategic-level analysis and planning component is necessary to inform national leadership decisions and policy formulation. NCTC offers an ideal model for strategic analysis of all intelligence from across the IC related to state-sponsored subversive activities. NCTC's mission of "analyzing and integrating" all terrorism and counterterrorism information and to ensure proper sharing across departments and agencies is a necessary component to connecting the dots of state subversive activities.[83] NCTC's strategic operational planning mission is also necessary to ensure unity of effort by directing planning and assigning roles and responsibilities across the federal government. A counter-subversion center must be able to at once inform policymaking with fully analyzed intelligence assessments and analysis of policy options and associated risk. Centralizing both in an intelligence center under the DNI will give the president and the National Security Council the best available information in as direct and efficient a manner as possible.

Creating an intelligence center under the Director of National Intelligence allows the DNI to fully exercise his or her authority to set intelligence collection and analysis priorities across the entire IC, and also reprogram funds and personnel to support the new center. The DNI is empowered by legislation to create national intelligence centers as necessary. Under current legislation, only the National Counterterrorism Center and the National Counterproliferation Center are dictated by the law, while establishment of all other centers is at the discretion of the DNI.[84] To ensure an enduring focus on the strategic threat posed by state-sponsored subversion, Congress should modify existing law to compel the creation of a counter-subversion center under the Office of the Director of National Intelligence, with the mission to analyze and integrate all related national intelligence and conduct strategic-level planning to integrate whole-of-government capabilities.

To complement the strategic analysis and planning organization, one or more operational-level action arms are necessary to focus integration of diverse interagency capabilities and multinational partner efforts when appropriate. The counterterrorism task forces and JIATF South provide relevant, but slightly different models for structuring such an organization. All include appropriate representation from departments and agencies, each having delegated authorities within their respective areas of responsibility that, when employed in concert with one another, create a symbiotic effect which multiplies the impact of otherwise isolated tools. It is critical to have not just liaisons, but senior and experienced interagency participants that can represent the positions of their respective organizations and also gain support for action.[85] Leadership of such interagency organizations is an art that balances respect for bureaucratic equities with the drive for mission success. Because department and agency contributions to these interagency organizations is often informal, the return on investment in increased effectiveness must justify the expenditure in personnel and other resources. Building an interagency organization can be a slow and incremental process, but as the counterterrorism and counter-narcotics examples show, success breeds success and over time an interagency counter-subversion operational coordination mechanism will show value.

Where the counterterrorism and counter-drug models differ is in their bureaucratic agency leadership and reporting structure, giving rise to the question of what department or agency would lead interagency operational action arms. Some experts hold that the Department of State should take lead on these issues, as George Kennan argued in his 1948 proposal for a political warfare mechanism.[86] However, as the Active Measures Working Group of the 1980s demonstrates, the State Department may be suited for a defensive effort to expose disinformation in order to reduce its effectiveness or to coordinate imposing after-the-fact costs on Russia, but the culture and expertise within the organization would not provide the depth in operations and intelligence fusion capabilities required to disrupt active plots and dismantle end-to-end networks that support subversive activities. Department of State concurrence with proposed operations is a must, but that role does not require the department to have leadership of action arms. More contemporarily, the CIA may seem viable as the lead agency for this effort, an argument supported by the CIA's mandate to conduct covert action. However, covert action is a necessary, but niche component of an overall operational arm. As in the case of counterterrorism interagency task forces, the CIA could lead one interagency effort that is matched with others from DoD and FBI, or shared leadership of a single organization. As the counterdrug and counterterrorism interagency task forces demonstrate, DoD does have the resources and the institutional expertise to lead an interagency task force, as well as the expertise in fusing intelligence with operations, even when those operations rely on other department and agency authorities for action.

The DoD-led task forces highlighted in the counterterrorism and counterdrug case studies rely on the operational authorities that are exercised through Geographic Combatant Commanders: in JIATF South's case, those of SOUTHCOM, and in the counterterrorism case those of each respective combatant command inside of which operations are executed but under the global responsibility of USSOCOM to "synchronize planning for global operations to combat terrorist networks."[87] While this has given SOCOM the ability to allocate its resources in alignment with counterterrorism priorities, it is still reliant on the relevant GCC to give its approval for any operations.[88] This tradeoff does ensure an agility in resource allocation that would be beneficial to any counter-subversion effort. Conversely, the JIATF South example provides a direct line to one combatant commander, SOUTHCOM, for a threat that originates from that GCC Area of Responsibility, but is fundamentally transregional in nature. Cross-GCC agreements help mitigate the challenges of working across administrative boundaries while keeping the combatant command from which the threat is most prevalently emanating in the lead, EUCOM in Russia's case. The EUCOM commander is dualhatted as NATO's Supreme Allied Commander Europe, so the oversight of a DoD-led effort could be from a unilateral standpoint or quickly become a multinational, NATO effort if and when necessary. To fully address all state-sponsored subversion, any DoD-led effort may require separate operational level interagency task forces with coordinating mechanisms to work across administrative boundaries. Additionally, if SOCOM takes on a greater role in countering state-sponsored subversion, assigning the command responsibility to also manage its unique resources globally will be essential to balance capacity across all the GCCs countering subversive threats and fulfilling its counterterrorism responsibilities.

The three operational examples in the counterterrorism case study demonstrate that multiple concurrent interagency organizations with overlapping, yet not redundant, focus can be a powerful counter to non-traditional threats. The military, CIA, and FBI each hold statutory and delegated authorities which shape the overall nature of their respective counterterrorism operations. In each case, these authorities are blended with other participating departments and agencies, resulting in geographic and functional divisions of labor that add value due to the diversity in methods, global expansiveness, and sheer volume of threats. However, it is important to remain guarded against diffusing future counter-subversion efforts by creating multiple redundant and competing efforts.

Second, the case studies highlight the need for an interagency organizational structure to bridge the foreign and domestic divide that exists between the diplomatic, military, intelligence, and law enforcement communities. Again, NCTC provides a foundation upon which to model a strategic level analytic capability that integrates all sources of intelligence not universally accessible to the entire Intelligence Community. Much like in counterterrorism, most of the IC is outward-facing regarding counterintelligence responsibilities, while the FBI has the largely inclusive mandate for threats inside the United States. Since so much of the subversive threat is both external and internal, counterintelligence and counter-subversion capabilities must work seamlessly across that divide. As the 2016 election tampering highlighted, the intelligence and law enforcement communities have the ability to perhaps identify an ongoing influence operation, but lack the mandate and analytic capability to assess the impacts of influence campaigns. With a view to civil-liberties and privacy considerations, it will be imperative to build in the ability to understand the effects of disinformation in order to tailor counteractions such as public messaging or other tools. JIATF South and the FBI's JTTF are exemplars of coordinating against external threat streams with preventative or punitive actions inside their domestic reach. Interdicting drug shipments before they reach the United States or arresting facilitators and operatives of terrorist groups before they have the ability to act greatly reduces the capabilities of adversary groups to achieve their objectives. Similarly, a counter-subversion task force cannot be limited to only providing a counter-message, but also must identify and interdict foreign agents that are fomenting subversive opposition or coordinating violent or otherwise harmful activities both in the United States and in partner nations. The FBI's new Foreign Influence Task Force is a step in the right direction, but needs other complementary efforts across the foreign and domestic divide.

Third, future interagency organizations must have both a defensive and offensive mandate. The U.S. government needs to not only build resiliency and parry attacks, but to also coordinate action at a tempo and volume which exceeds an adversary's ability to respond and to deter future malign activity. In building resiliency, it is increasingly important to understand the methods that adversaries are employing and the vulnerabilities they are exploiting. Hardening systems where able, such as preventing cyber attacks and hacking, is one component. Educating the population and creating more aware consumers of information will make adversary manipulation more difficult when targets of influence operations are naturally skeptical of questionable news sources and are motivated to do their own fact checking. "Naming and shaming" the perpetrators and sponsors of subversive activity helps educate the population, but more importantly, doubles as a reactive punitive measure because by exposing an operation it disrupts and diminishes the effectiveness of an adversary's investment, increasing their costs.

Other punitive responses to attacks and plots are also necessary both to hold perpetrators to account and increase costs, adding to the overall deterrent effect. Tools available to the government include criminal charges, sanctions, and other financial seizures. In addition, the United States has the ability to respond in symmetric and asymmetric ways with cost-imposing measures. Not only can the government respond to a cyber attack with a cyber attack, but it can also respond to a cyber attack by outing adversary intelligence capabilities or exposing political leaders' corrupt behavior, or, more provocatively, backing opposition leaders and groups in contested areas — or all of the above in a coordinated and synchronized manner.[89]

Moving toward more proactive methods, an interagency coordinating body should focus not only on identifying and illuminating threats, but also on disrupting them upstream, dismantling adversary capabilities to operate, and preempting enemy action. Being this predictive is an intelligence-heavy and undeniably difficult task, best accomplished through real-time multiagency coordination. As the counterterrorism and counter-narcotics examples show, seeing threats emerge and stopping them before they can reach a decisive point — getting ahead of adversaries — is invaluable for national security and for imposing costs. These options are costly for the U.S., but a strictly defensive posture comes with an enduring high price because of the resources necessary to constantly cover so large an attack surface as the U.S. system of government and open society offer.[90] Ultimately, the U.S. objective of giving adversaries more dilemmas all at once than they can reasonably handle is a way of disincentivizing subversive activities. Just as the costs and risks of escalating to conventional or nuclear war drive our competitors into gray zone activities, the United States must look at both reactive and proactive tools, defensive and offensive capabilities, to contribute to comprehensive deterrence that "raises an adversary's perceived cost to an unacceptable level of risk relative to the perceived benefit."[91]

Fourth and finally, to be most effective, any interagency organizational structure should include partnerships with relevant portions of the private sector. The vulnerabilities of America's open society and democratic system highlighted in 2016 make exploiting the private sector attractive to adversaries conducting subversive activities. Like the counterterrorism and counter-narcotics examples, a counter-subversion interagency organization may rely on regulation and the courts to enforce sharing of private information. But including digital media platforms such as Facebook and Twitter, as well as the news media community, as non-conventional partners will optimize U.S. counter-subversion efforts. It is in the interests of digital platforms and media outlets to improve their records in policing malign activities both from an organizational legitimacy and societal duty standpoint. Facebook and Twitter, for example, lost public trust, and monetary valuation, in their handling of Russian interference on their platforms. Executives from both have been called to testify before Congress on multiple occasions regarding their steps to limit vulnerabilities to exploitation.[92] The news media have shown how they still can be manipulated, even as they become more guarded against following trending stories without substantiation.[93] A public-private partnership may be beneficial in developing tools to identify adversary use of automation or validate the objectivity of information sources. Appropriate regulation, or even partnership with government agencies, creates challenges in balancing liberty with security; privacy concerns are legitimate and must be overcome through establishing reasonable protections to protect freedom of speech, data privacy, and independence of a free press. It is important to begin this effort where the government and private companies have shared interests and build upon the trust and cooperation. The FBI’s Foreign Influence Task Force has begun sharing information with technology companies to aid in their self-policing activities.[94] Increasing shared investment in the research and development of artificial intelligence tools to identify bot-driven information trends and deep fakes also suits the interests of all parties and is ongoing.[95] There is much work being done by both private entities and government organizations in parallel, which should be better synchronized to optimize its effectiveness. Private companies and government organizations helping each other to see trends and threats in order to stop them before they manifest is a mutually beneficial and necessary component to an interagency effort to counter non-traditional threats.

Status Quo, Too Risky, or Time for a Change?

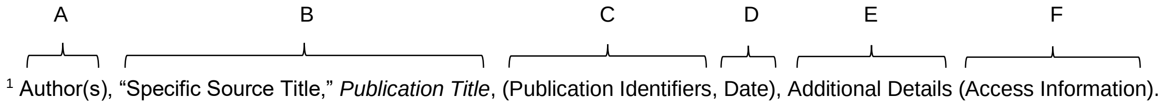
Why would the United States go to such lengths to create more bureaucracy when it is clear that the U.S. government has awoken to the subversive nature of the current threat? Hasn't the government shown it is now better prepared to identify and respond to future malign activities primarily through counterintelligence, economic, diplomatic, and law enforcement channels? The numerous indictments of Russian actors that the Mueller investigation has yielded, the amount of sanctions implemented in response to Russian aggression in Ukraine, and the disruption President Barack Obama caused in kicking out Russian intelligence officers following the election meddling illustrate that the U.S. government is indeed acting.

But it can do more. While the United States has the tools required to counter these threats, the manner in which the government's bureaucracy is organized creates seams that prevent effective whole-of-government cooperation.[96] Russia's reliance on political warfare to weaken democratic institutions, willingness to operate in the gray zone to accomplish what they do not have the power to openly, and intent to intimidate America's partners and allies necessitates revitalizing a focused interagency effort. To guard America's vital national interests requires a mandate to synchronize and direct an array of resilience, defensive, and offensive options at a pace at which the adversary's costs far outweigh the potential gains. Persistently posing more dilemmas than may be handled at once will serve as the nation's best deterrent to malign actions. To do so requires that the United States organize against this and other state-sponsored subversive threats. In today's threat environment of multiple competitors and rogue actors enabled by rapidly advancing technologies, centralizing decision-making through the NSC process will not yield the tempo and breadth needed. Rather, the United States should use the NSC to formulate a strategy that is enabled by a national intelligence center for counter-subversion, which provides strategic intelligence analysis and continually assesses risks of policy choices. Delegating to departments and agencies the authority to act within the confines of the strategy and risk analysis, and creating one or more complementary interagency operational action arms, will provide greater and more widespread effects.

Are not the risks of miscalculation and escalation too great to push back against Russia and other malign actors? Would the United States raising the stakes not just result in adversaries doing the same, escalating perhaps even to the point of military conflict? Simply put, defeating and deterring the threat of state-sponsored non-traditional threats cannot be accomplished through defensive and reactive means alone. To rely on such a strategy cedes the initiative to U.S. adversaries. Because the potential attack surface is so expansive, a defensive strategy puts the national security community in a position of being required to be everywhere at all times, a very costly and distracting method over time. The right approach requires a willingness to increase risk tolerance to employ proactive and asymmetric capabilities, but in a measured way –– and, in so doing, not compromising America's values by resorting to the same tactics Russia has demonstrated.[97] Failure to incorporate measured risk through offensive action will force the nation to deal with these threats in perpetuity.

The strategic environment has changed, and policy-makers clearly appreciate this, but the national security apparatus has yet to adjust. The changes recommended herein are not as sweeping as those compelled in 1947 and 2004, but the United States must make real adjustments to organize for the threat. While the changes also do not need to be revolutionary as in the counterterrorism example, they should be far more timely and comprehensive than the evolutionary counter-narcotics example. The resultant structure must also include more delegation across coordinated efforts than seen in the limited-scope, Cold War–era examples. Interagency approaches are proven to be effective in improving U.S. security and aiding in accomplishing strategic objectives, particularly against non-traditional problem sets. In short, the United States must ensure that the nation is postured with the appropriate interagency organizational design for today's threats — only then will the U.S. government be able to protect the nation from the aggressive strategic competition of today and into the future.

Endnotes



[1] Author(s), "Specific Source Title," *Publication Title*, (Publication Identifiers, Date), Additional Details (Access Information).

[1] Rhodi Jeffreys-Jones, "Why was the CIA established in 1947?" Intelligence and National Security, (12, no.1, 1997), 21-40; Michael Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11* (Lincoln: Potomac Books, 2013), xix-xx.

[2] Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11*, xix; *National Security Act of 1947* (July 26, 1947), Public Law 253, 80th Cong., 1st sess., Chapter 343, https://www.cia.gov/library/readingroom/docs/1947-07-26.pdf (accessed March 21, 2019).

[3] *Intelligence Reform and Terrorism Prevention Act of 2004* (December 17, 2004), Public Law 108-458, 108th Cong, 118 STAT. 3638; Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11*.

[4] Office of the Director of National Intelligence, *Global Trends: Paradox of Progress*, (National Intelligence Council, January 2017), https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf (accessed February 15, 2019); Donald J. Trump, *National Security Strategy of the United States of America,* (Washington, DC: The White House, December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed August 1, 2018); James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America,* (Washington, DC: Department of Defense, January 2018), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (accessed August 1, 2018).

[5] Michael Mandelbaum, *Mission Failure: America and the World in the Post-Cold War Era* (New York: Oxford University Press, 2016), 311-366.

[6] Trump, *National Security Strategy of the United States of America*; Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*.

[7] Hal Brands, “Paradoxes of the Gray Zone,” *Foreign Policy Research Institute*, (February 5, 2016), https://www.fpri.org/article/2016/02/paradoxes-gray-zone/ (accessed on October 28, 2018); Joseph L. Votel, et al, “Unconventional Warfare in the Gray Zone,” *Joint Forces Quarterly*, (80, 1st Quarter 2016), 101-109; Hal Brands and Toshi Yoshihara, “How to Wage Political Warfare,” *The National Interest* (December 16, 2018), https://nationalinterest.org/feature/how-wage-political-warfare-38802 (accessed on February 15, 2019).

[8] Mandelbaum, *Mission Failure: America and the World in the Post-Cold War Era*, 313-366.

[9] Seth G. Jones. “The Return of Political Warfare,” *Center for Strategic & International Studies*, (February 2018); https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180202_Jones_ReturnPoliticalWarfare_Web.pdf?nsT.nzT52.7lzHB.9ZymYwjjgnAHFh4X (accessed on February 15, 2019).

[10] Heather Conley, et al, “The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe,” *Center for Strategic & International Studies*, (October 2016), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/1601017_Conley_KremlinPlaybook_Web.pdf (accessed February 1, 2019).

[11] Linda Robinson, et al, *Modern Political Warfare: Current Practices and Possible Responses*, (Santa Monica: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR1700/RR1772/RAND_RR1772.pdf (accessed on December 1, 2018), 41-124; Heather Conley, et al, “The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe,” x, 3-4.

[12] “George F. Kennan on Organizing Political Warfare," *Wilson Center Digital Archive*, (April 30, 1948), redacted final draft of a memorandum dated May 4, 1948, https://digitalarchive.wilsoncenter.org/document/114320.pdf?v=944c40c2ed95dc52d2d6966ce7666f90 (accessed on February 1, 2019).

[13] “Assessing Russian Activities and Intentions in Recent US Elections,” Intelligence Community Assessment (Washington, DC: Office of the Director of National Intelligence, January 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf (accessed October 30, 2018); John Schaus, et al, “What Works: Countering Gray Zone Coercion,” *Center for Strategic & International Studies*, (July 2018), https://csis-prod.s3.amazonaws.com/s3fs-public/publication/180716_Schaus_WhatWorks.pdf?_2N5GlQNzTKzXCXELkLmjNOhXI8fyMSg (accessed October 28, 2018); Heather Conley, et al, “The Kremlin Playbook: Understanding Russian Influence in Central and Eastern Europe;” Linda Robinson, et al, Modern Political Warfare: Current Practices and Possible Responses, 41-124.

[14] T.S. Allen and A.J. Moore, “Victory without Casualties: Russia’s Information Operations,” *Parameters* (48, no.1, Spring 2018), 59-71.

[15] Schaus, et al, “What Works: Countering Gray Zone Coercion,” 4.

[16] “Assessing Russian Activities and Intentions in Recent US Elections,” ii.

[17] Alina Polyakova and Spencer P. Boyer, “The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition,” *The Brookings Institution* (March 2018), https://www.brookings.edu/wp-content/uploads/2018/03/fp_20180316_future_political_warfare.pdf (accessed February 1, 2019); Matthew Rosenberg, Charlie Savage, and Michael Wines, “Russia Sees Midterm Elections as Chance to Sow Fresh Discord, Intelligence Chiefs Warn,” *New York Times*, (February 13, 2018), https://www.nytimes.com/2018/02/13/us/politics/russia-sees-midterm-elections-as-chance-to-sow-fresh-discord-intelligence-chiefs-warn.html (accessed February 15, 2019); Daniel R. Coats, “Worldwide Threat Assessment of the US Intelligence Community” (written statement for the record for the Senate Select Committee on Intelligence, January 29, 2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf (accessed on January 30, 2019), 7.

[18] Coats, “Worldwide Threat Assessment of the US Intelligence Community,” 7.

[19] Steve Abrams, “Beyond Propaganda: Soviet Active Measures in Putin’s Russia,” *Connections: The Quarterly Journal*, (15, no. 1, 2016), 5-31.

[20] Ibid, 8; Schaus, “What Works: Countering Gray Zone Coercion,” 4.

[21] Coats, “Worldwide Threat Assessment of the US Intelligence Community,” 7; P.W. Singer and Emerson T. Brooking, *LikeWar*, (New York: Houghton Mifflin Harcourt Publishing Company, 2018), 248-254.

[22] Singer and Emerson, *LikeWar*, 138-147.

[23] Alex Altman and Elizabeth Dias, “Moscow Cozies Up to the Right,” *Time*, (March 10, 2017), http://time.com/4696424/moscow-right-kremlin-republicans/ (accessed on March 15, 2019).

[24] Brands and Yoshihara, “How to Wage Political Warfare.”

[25] Larry Buchanan and Karen Yourish, “The Mueller Report is Highly Anticipated. Here’s What We Already Know,” *The New York Times*, (March 20, 2019),

https://www.nytimes.com/interactive/2019/03/20/us/politics/mueller-investigation-people-events.html?emc=edit_na_20190320&nl=breaking-news&nlid=45647227ing-news&ref=cta (accessed on March 21, 2019); "Assessing Russian Activities and Intentions in Recent US Elections."

[26] Philip Ewing, "FACT CHECK: Why Didn't Obama Stop Russia's Election Interference In 2016?," *NPR*, (February 21, 2018), https://www.npr.org/2018/02/21/587614043/fact-check-why-didnt-obama-stop-russia-s-election-interference-in-2016 (accessed on February 15, 2019); "Joint Statement from the Department of Homeland Security and Office of the Director of National Intelligence on Election Security," (October 7, 2016), https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (accessed on February 15, 2019).

[27] James Clapper, *Facts and Fears*, (New York: Viking, 2018), 1-4.

[28] Susan B. Glasser, "Ex-Spy Chief: Russia's Election Hacking was an 'Intelligence Failure,'" *Politico Magazine*, (December 11, 2017), https://www.politico.com/magazine/story/2017/12/11/the-full-transcript-michael-morell-216061 (accessed February 15, 2019).; Clapper, *Facts and Fears*, 4.

[29] Michael Walzer, *Just and Unjust Wars: A Moral Argument with Historical Illustrations*, (New York: Basic Books, 2006, 4th Ed.), 51-73.

[30] Clapper, *Facts and Fears*, 2-3.

[31] "What We Investigate: Combating Foreign Influence," FBI website, https://www.fbi.gov/investigate/counterintelligence/foreign-influence (accessed on March 21, 2019); "Fact Sheet on Department of Justice Cyber-Digital Task Force Report," Department of Justice website, https://www.justice.gov/file/1081871/download (accessed March 21, 2019).

[32] "State Department Special Report 88, Soviet Active Measures: Forgery, Disinformation, Political Operations,"(October 1981), https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf (Accessed 21 March, 2019).

[33] "Creation of the Department of Homeland Security," Department of Homeland Security website, https://www.dhs.gov/creation-department-homeland-security (accessed on March 15, 2019).

[34] "Department of Justice Report, The USA PATRIOT Act: Preserving Life and Liberty," https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (accessed March 21, 2019); *Authorization for the Use of Military Force*, (September 18, 2001), Public Law 107-40, 107th Cong, 115 STAT. 224, https://www.congress.gov/107/plaws/publ40/PLAW-107publ40.pdf (accessed February 15, 2019).

[35] *Intelligence Reform and Terrorism Prevention Act of 2004*.

[36] Ibid, Section 1021.

[37] Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11*, ix-xi; ; *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, (New York: Norton, 2004), 399-428.

[38] *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 1021; “In Focus: National Counterterrorism Center,” *Congressional Research Service*, (July 11, 2018), https://fas.org/sgp/crs/intel/IF10709.pdf (accessed on December 1, 2018).

[39] Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11*, 6-20.

[40] *Intelligence Reform and Terrorism Prevention Act of 2004*, Section 1021; “In Focus: National Counterterrorism Center.”

[41] Christopher Lamb, “Global SOF and Interagency Collaboration,” J*ournal of Strategic Security* (7, no. 2, Special Issue, Summer 2014), 8-20.

[42] Stanley A. McChrystal, *My Share of the Task*, (New York: Portfolio/Penguin, 2013), 117-119, 168-169.

[43] Christopher J. Lamb and Evan Munsing, “Secret Weapon: High-value Target Teams as an Organizational Innovation,” *Institute for National Security Studies Strategic Perspectives* (No. 4, March 2011), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-4.pdf (accessed on November 15, 2019).

[44] Gregory F. Treverton, *Intelligence for an Age of Terror*, (New York: Cambridge University Press, 2009), 55-56.

[45] ”Offices of CIA: History”, CIA website, https://www.cia.gov/offices-of-cia/intelligence-analysis/history.html (accessed on February 15, 2019).

[46] John Deutch, “Fighting Foreign Terrorism,” CIA Website, (September 5, 1996), https://www.cia.gov/news-information/speeches-testimony/1996/dci_speech_090596.html (accessed on February 15, 2019); Michael V. Hayden, “Statement for the Record, Senate Select Committee on Intelligence,” (January 11, 2007), https://www.cia.gov/news-information/cia-the-war-on-terrorism/excerpt-from-d-cia-statement-to-senate-intel-committee.html (accessed on February 15, 2019).

[47] “Spotlight on CIA’s Centers,” CIA Website, https://www.cia.gov/news-information/featured-story-archive/2014-featured-story-archive/spotlight-on-cias-centers.html (accessed on February 15, 2019).

[48] Hayden, “Statement for the Record, Senate Select Committee on Intelligence.”

[49] “Joint Terrorism Task Forces,” FBI website, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces (accessed February 15, 2019).

[50] Allen, *Blinking Red: Crisis and Compromise in American Intelligence after 9/11*, 6-20; *The 9/11 Commission Report*, 399-428; *Intelligence Reform and Terrorism Prevention Act of 2004.*

[51] “Joint Terrorism Task Forces,” FBI website, https://www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces (accessed on February 15, 2019).

[52] Jerome P. Bjelopera, “The Federal Bureau of Investigations and Terrorism Investigations,” *Congressional Research Service*, (April 24, 2013), https://fas.org/sgp/crs/terror/R41780.pdf (accessed February 15, 2019).

[53] Diane Ritchey, “Public-Private Partnerships and the Fight Against Terrorism,” *Security Magazine* (55 no. 10, October 2018), https://search-proquest-com.proxy.lib.duke.edu/docview/2126788346/fulltextPDF/C5216BAFD3EB4AE6PQ/1?accountid=10598 (accessed on February 15, 2019), 16-18.

[54] “Press Release: NEW YORK CITY POLICE DEPARTMENT RELEASES DRAFT OF PUBLIC SECURITY PRIVACY GUIDELINES FOR PUBLIC COMMENT,” New York City website, (February 25, 2009), http://www.nyc.gov/html/nypd/html/pr/pr_2009_005.shtml (accessed on February 15, 2019).

[55] “Department of Justice Report, The USA PATRIOT Act: Preserving Life and Liberty.”

[56] Sheera Frenkel, “Facebook will Use Artificial Intelligence to Find Extremist Posts,” *The New York Times*, (June 15, 2017), https://www.nytimes.com/2017/06/15/technology/facebook-artificial-intelligence-extremists-terrorism.html (accessed on March 15, 2019); Andy Greenberg, “Google’s Clever Plan to Stop Aspiring ISIS Recruits,” *Wired*, (September 7, 2016), https://www.wired.com/2016/09/googles-clever-plan-stop-aspiring-isis-recruits/ (accessed on March 15, 2019).

[57] Evan Munsing and Christopher J. Lamb, “Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success,” *Institute for National Strategic Studies, Strategic Perspectives* (No. 5, Washington, DC: National Defense University Press June 2011), 6-10.

[58] Ibid, 10-11.

[59] Ibid, 11-16.

[60] Ibid, 16-19.

[61] “Office of National Drug Control Policy,” The White House, https://www.whitehouse.gov/ondcp/ (accessed October 28 2018).

[62] Munsing and Lamb, “Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success,” 18; William Clinton, “Presidential Decision Directive/NSC-14,” The White House, (November 3, 1993), https://fas.org/irp/offdocs/pdd/pdd-14.pdf (accessed on December 1, 2019).

[63] Munsing and Lamb, “Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success,” 16-19; *21 USC 1710: Drug Interdiction Coordinator and Committee*, http://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title21-section1710&num=0&edition=prelim (accessed October 28, 2018).

[64] Munsing and Lamb, “Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success,” 18-21.

[65] Ibid, 22-30.

[66] Ibid, 3-4.

[67] "Mission," Joint Interagency Task Force South, http://www.jiatfs.southcom.mil/About-Us/ (accessed October 25 2018).

[68] "Secretary Nielsen Joins President Trump at JIATF-South to Discuss Efforts to Stop Drugs and Criminals from Entering Our Country," Department of Homeland Security website, (April 19, 2018), https://www.dhs.gov/news/2018/04/19/secretary-nielsen-joins-president-trump-jiatf-south-discuss-efforts-stop-drugs-and (accessed on Febrauy 15, 2019); Munsing and Lamb, "Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success," 24.

[69] Ibid, 30-68.

[70] "Office of Policy Coordination, 1948-1952," *Studies in Intelligence*, (17, No. 2-S, Summer 1973), https://www.cia.gov/library/readingroom/docs/1973-06-01.pdf (accessed on March 21, 2019).

[71] Harry S. Truman, "Memorandum From President Truman to the Chairman of the Psychological Strategy Board (Smith)", (June 2, 1951), https://history.state.gov/historicaldocuments/frus1950-55Intel/d119 (accessed on March 21, 2019); Dwight Eisenhower, "Executive Order 10483: Establishing the Operations Coordination Board," (September 2, 1953), https://www.cia.gov/library/readingroom/docs/CIA-RDP80B01676R002700040038-0.pdf (accessed on March 21, 2019); Brands and Yoshihara, "How to Wage Political Warfare," 8-9.

[72] Linda Robinson, et al, *Modern Political Warfare: Current Practices and Possible Responses*, 27-29.

[73] Harry S. Truman, "President Harry S. Truman's Address Before a Joint Session of Congress," (March 12, 1947), http://avalon.law.yale.edu/20th_century/trudoc.asp (accesses March 21, 2019).

[74] Linda Robinson, et al, *Modern Political Warfare: Current Practices and Possible Responses*, 27-29.

[75] Ibid, 19-23.

[76] John D. Waghelstein, "Reading the Tea Leaves: Proto-Insurgency in Honduras," *Center on Irregular Warfare and Armed Groups Case Studies*, (1, November 2012), https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1001&context=ciwag-case-studies (accessed on March 21, 2019).

[77] Linda Robinson, et al, *Modern Political Warfare: Current Practices and Possible Responses*, 15-39.

[78] Brands and Yoshihara, "How to Wage Political Warfare."

[79] Fletcher Schoen and Christopher J. Lamb, "Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference," *Institute for National Strategic Studies, Strategic Perspectives* (no. 11, Series Editor: Nicholas Rostow, Washington, DC: National Defense University Press, June 2012), https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/Strategic-Perspectives-

11.pdf (accessed November 15, 2019); G. McK. Kinahan, "Exposing Soviet Active Measures in the 1980s: A Model for the Bush Administration?" *The Journal of Social, Political, and Economic Studies* (15, no.3, Fall 1990), 301-336.

[80] "State Department Special Report 88, Soviet Active Measures: Forgery, Disinformation, Political Operations."

[81] Thomas Boghardt, "Operation INFEKTION: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign," *Studies in Intelligence*, (53, No. 4, December 2009), https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/pdf/U-%20Boghardt-AIDS-Made%20in%20the%20USA-17Dec.pdf (accessed March 1, 2019).

[82] Ibid; David K. Shipler, "State Department; Little Report, With Right Spin, Makes Big Splash," *The New York Times*, November 5, 1987, https://www.nytimes.com/1987/11/05/us/state-department-little-report-with-right-spin-makes-big-splash.html (accessed on March 21, 2019).

[83] "In Focus: National Counterterrorism Center."

[84] *Intelligence Reform and Terrorism Prevention Act of 2004.*

[85] Munsing and Lamb, "Joint Interagency Task Force-South: The Best Known, Least Understood Interagency Success," 30-68.

[86] "George F. Kennan on Organizing Political Warfare."

[87] Andrew Feickert, "U.S. Special Operations Forces (SOF): Background and Issues for Congress," *Congressional Research Service*, (October 29, 2018), https://fas.org/sgp/crs/natsec/RS21048.pdf (accessed on February 15, 2019).

[88] Ibid.

[89] David E. Sanger, "Obama Strikes Back at Russia for Election Hacking," *The New York Times*, (December 29, 2016), https://www.nytimes.com/2016/12/29/us/politics/russia-election-hacking-sanctions.html (accessed on February 15, 2019).

[90] Brands and Yoshihara, "How to Political Warfare."

[91] Becca Wasser, et al, *Comprehensive Deterrence Forum: Proceedings and Commissioned Papers*, (Santa Monica: RAND Corporation, 2018), https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF345/RAND_CF345.pdf (accessed on December 1, 2019).

[92] Tony Romm and Craig Timberg, "Facebook and Twitter testified before Congress. Conservative conspiracy theorists lurked behind them." *The Washington Post*, (September 5, 2018), https://www.washingtonpost.com/technology/2018/09/05/facebook-twitter-sandberg-dorsey-congress-tech-hearings/?utm_term=.d9158135a809 (accessed March 16, 2019).

[93] Valeria Richardson, "Nick Sandman sues Washington Post for $250 million in first Covington Catholic lawsuit," *The Washington Times*, (February 19, 2019),

https://www.washingtontimes.com/news/2019/feb/19/nick-sandmann-covington-catholic-teen-sues-washing/ (accessed on March 21, 2019).

[94] "What We Investigate: Combating Foreign Influence."

[95] "Artificial Intelligence and National Security," *Congressional Research Service*, (January 30, 2019), https://fas.org/sgp/crs/natsec/R45178.pdf (accessed on March 21, 2019), 11-12.

[96] Brands, "Paradoxes of the Gray Zone."

[97] Brands and Yoshihara, "How to Wage Political Warfare."