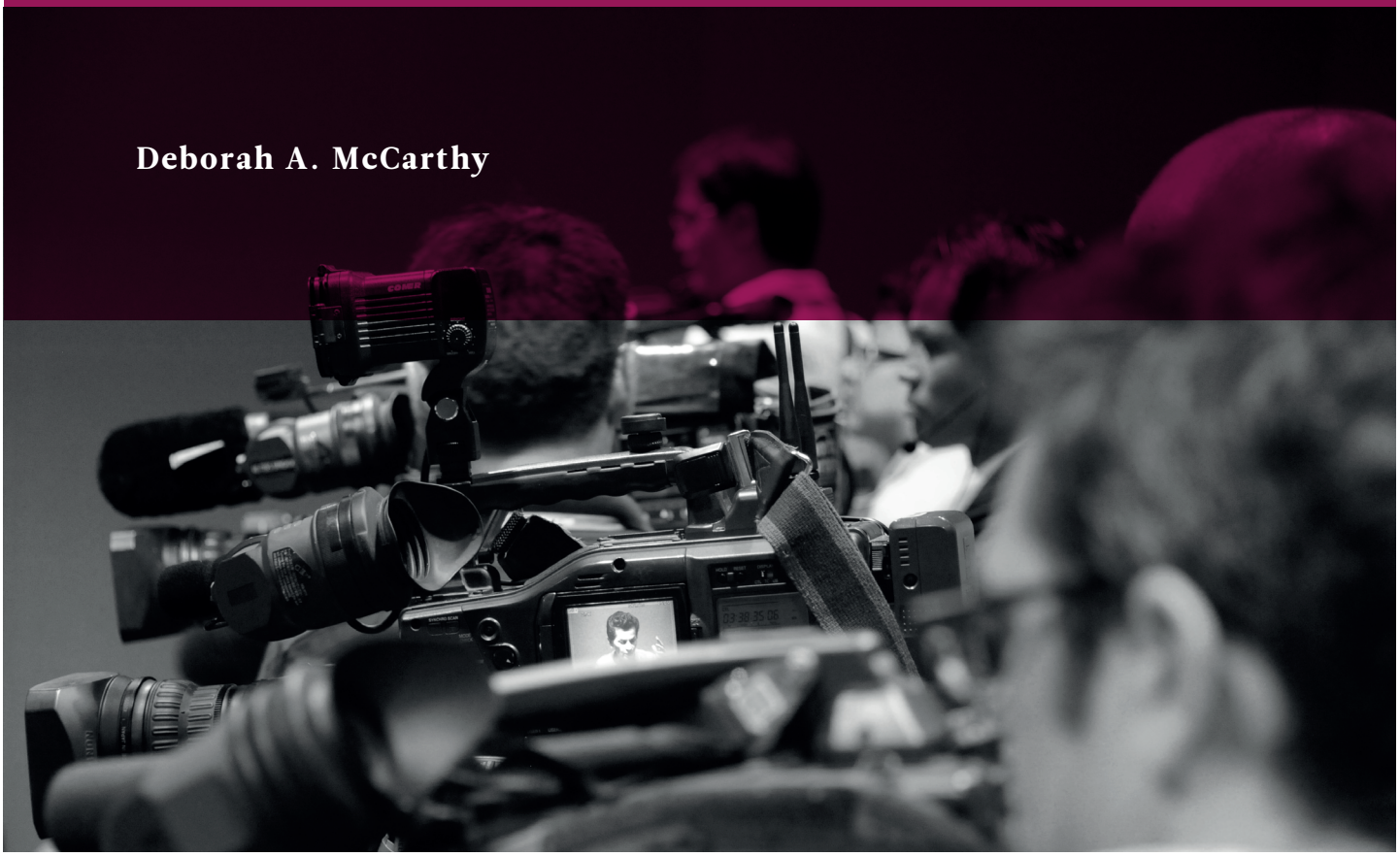
FIIA
BRIEFING PAPER

OCTOBER 2019 / 272

US FOREIGN POLICY TOOLS IN THE ERA OF DISINFORMATION

DEFICIENCIES PREVENT EFFECTIVE RESPONSE TO MALIGN INFORMATION OPERATIONS

Deborah A. McCarthy



FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

US FOREIGN POLICY TOOLS IN THE ERA OF DISINFORMATION

DEFICIENCIES PREVENT EFFECTIVE RESPONSE TO MALIGN INFORMATION OPERATIONS

- Russia, China, Iran and ISIS use information operations to undermine the national security objectives of the United States and its allies.
- The US's international response has been weak.
- Internal constraints have limited more effective counter-measures. In particular, the lack of a coordinated White House-level strategy, dispersed authorities and little cooperation with private social media companies can be identified as causal factors.
- Additional steps by the Trump Administration to counter foreign disinformation will aim to protect the 2020 presidential elections rather than to push back on efforts to undermine US leadership abroad.

DEBORAH A. MCCARTHY

Ambassador (ret.),

Visiting Senior Fellow,

Center on US Politics and Power

Finnish Institute of International Affairs

ISBN 978-951-769-623-4

ISSN 1795-8059

Language editing: Lynn Nikkanen.

Cover photo: Flickr/UNclimatechange. Used under creative commons lisence; the original photo changed to black&white.

FIIA FINNISH INSTITUTE OF INTERNATIONAL AFFAIRS

Arkadiankatu 23 b

POB 425 / 00101 Helsinki

Telephone +358 (0)9 432 7000

Fax +358 (0)9 432 7799

www.fiia.fi

US FOREIGN POLICY TOOLS IN THE ERA OF DISINFORMATION

DEFICIENCIES PREVENT EFFECTIVE RESPONSE TO MALIGN INFORMATION OPERATIONS

INTRODUCTION

US foreign policy interests are being challenged by information and disinformation operations carried out by state actors, such as Russia, China, and Iran, as well as non-state (ISIS) actors. Russian activities to undermine democratic values and to sow discord within NATO are well known. Chinese disinformation actions have included 1) implying that the US was to blame for the massive blackout in Venezuela in March 2019; 2) a media blitz depicting the Hong Kong protests as riots funded by the CIA; 3) the purchase of media outlets and political influence peddling in Australia and New Zealand, two staunch US allies; and 4) the deliberate targeting of US think tanks to influence the US narrative on China.[1] Iranian operations have included using websites in 15 countries during 2018 to disseminate information antagonistic to the US, and the impersonation of authentic Western media outlets to spread false information critical of the United States.[2] ISIS, although defeated militarily in Iraq and Syria, continues to propagate its violent ideology and to recruit through new social media platforms.[3]

The 2017 US National Security Strategy identified the weaponization of information as a threat to the United States, and stated that the States would strengthen public diplomacy, while developing new communication campaigns and platforms. However, the Trump Administration has failed to flesh out a strategy to counter malign information operations *within* the United States, let alone to push back on an *international* scale against efforts to undermine the national security interests of the United States, its allies and partners.

This Briefing Paper aims to dissect the internal constraints underlying the neglect to devise a functional strategy and to coordinate an effective international response. The paper first analyzes the key internal institutional challenges in depth. It then proceeds by exploring the underdeveloped nature of cooperation with external actors. The paper thereafter examines the challenges faced by ongoing coordination efforts in the US government, before concluding by pointing out possible ways forward.

INSTITUTIONAL CONSTRAINTS WITHIN THE DEPARTMENT OF STATE

By law, the Department of State is responsible for countering foreign influence operations *outside* of the United States. However, it has very limited personnel and funding for this purpose. While additional capabilities exist in other US government agencies, notably the Department of Defense, there is currently no interagency coordinating mechanism to develop effective countermeasures.

Beginning during the Cold War and until 1999, the US Information Agency (USIA) was responsible for influencing foreign audiences to advance US national interests. It managed multiple broadcasts such as the Voice of America as well as press and cultural programmes. Many of its activities focused on developing an understanding of non-US audiences in order to push out information on US values, culture and interests.

It was not until the administration of President Reagan, in 1981 to be precise, that the Interagency Active Measures group, led by the Intelligence Bureau of the Department of State, was established to specifically counter Soviet propaganda. Combining information obtained from USIA overseas with intelligence, it produced multiple reports exposing propaganda and disinformation. With the collapse of the Soviet Union, the group was disbanded, producing its last report in 1992.[4]

1 Larry Diamond and Orville Shell, "Chinese Influence and American Interests. Promoting Constructive Vigilance", Report of the Working Group on Chinese Influence Activities in the United States. Hoover Institution, 21 October 2018, https://www.hoover.org/sites/default/files/research/docs/chineseinfluence_americaninterests_fullreport_web.pdf.

2 Kate Conger and Sheera Frenkel, "How FireEye Helped Facebook Spot a Disinformation Campaign", *New York Times*, 23 August 2018, https://www.nytimes.com/2018/08/23/technology/fireeye-facebook-disinformation.html.

3 Catherine A. Theohary, "Information Warfare: Issues for Congress", Congressional Research Service Report R45142, 5 March 2018, https://fas.org/sgp/crs/natsec/R45142.pdf.

4 Seth G. Jones, "Going on the Offensive: A Russia Strategy to Combat Russian Information Warfare", Center for Strategic and International Studies Briefs, 1 October 2018, https://www.csis.org/analysis/going-offensive-us-strategy-combat-russian-information-warfare.

USIA itself was dissolved in 1999. The agency's broadcasting arm was turned over to a new agency called the Broadcasting Board of Governors (now renamed the US Agency for Global Media). Press, cultural and exchange programmes were transferred to the Department of State.

In 2016, by executive order, President Obama designated the Department of State as the lead government agency to counter foreign influence operations outside of the United States that are harmful to US interests.[5] The order created the Global Engagement Center (GEC) to coordinate these efforts. Initially, however, the GEC focused almost exclusively on countering the messaging of international terrorist organizations and violent extremists. Only with the passage by the US Congress of the Countering Foreign Propaganda and Disinformation Act in late 2016[6] was the Center given a second responsibility: to counter state-sponsored disinformation that seeks to undermine the security of the United States, its allies and partner nations.

In mandating the change, Congress was primarily focused on Russian disinformation, as a result of revelations of extensive Russian efforts to influence the 2016 US Presidential elections. The GEC sought to push back on Russia's efforts in Europe to undermine transatlantic unity and the credibility of the US commitment to the region. By the end of the Obama administration, however, the Center had less than 90 people and almost no Russian language experts.

Under the Trump Administration, the GEC expanded its work to include countering Chinese and Iranian information operations. Even so, its efforts got off to a very slow start as then Secretary of State Tillerson froze the hiring of personnel and delayed requesting funding for operations for many months.

Today, the GEC has a modest staff of 75 and an annual budget of $40 million. Due to its small size, it works primarily through partnerships with outside entities to produce content for overseas media and to increase the skills of overseas local journalists and media organizations to detect and expose disinformation. It has some limited technical capability to showcase new technologies and analyze vulnerabilities. On occasion, it works directly with governments. In 2018, for example, it helped the office of the Prime Minister of North Macedonia to address widespread disinformation by Russia to mislead voters in the run-up to the referendum to change the country's name. GEC assistance was part of active US support for the referendum to pave the way for North Macedonia's accession to NATO.

Not all partnerships have been successful. In May 2019, the GEC was forced to suspend its Iran Disinformation Project after it was determined that the partner organization had inappropriately targeted reputable journalists, academics and human rights activities for not being tough enough on Iran. The project worked on social media platforms to expose Iranian disinformation on US foreign policy objectives in the Middle East.

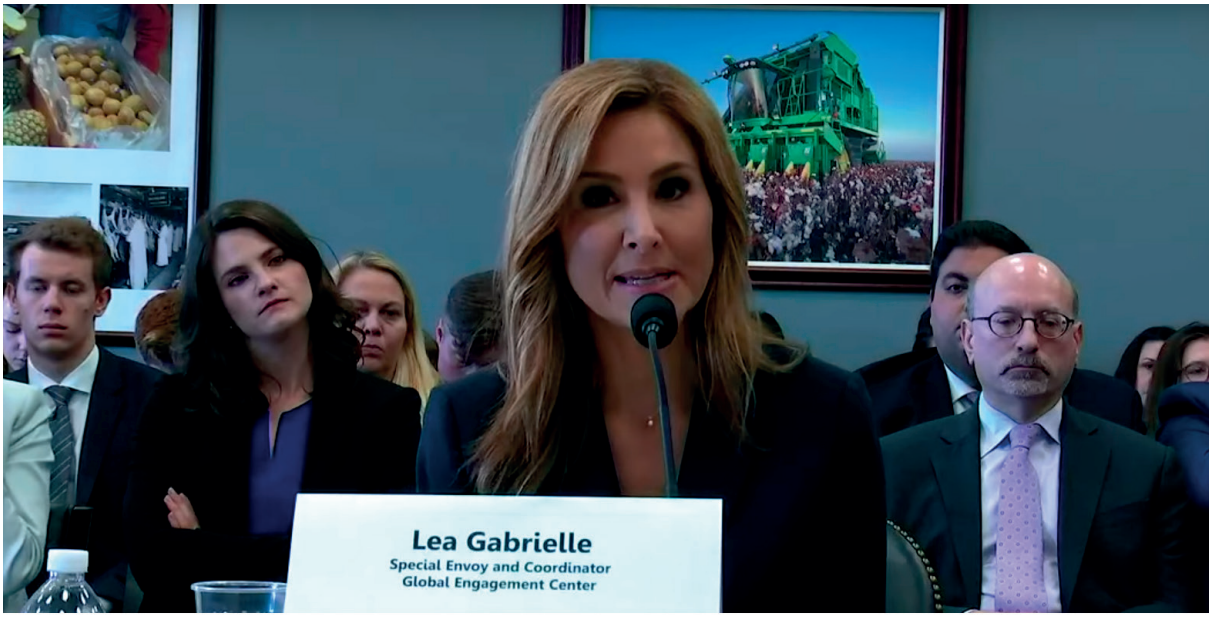
While the GEC has an enormous legal mandate, the responsibility for the day-to-day public messaging on US foreign policy for the Secretary of State lies elsewhere, namely in the senior ranks of the Bureau of Global Public Affairs, making it extremely difficult for the GEC to execute its lead coordinating role across the entire Department of State, let alone across all US government agencies operating overseas.

Beyond the GEC, certain other offices in the Department of State, with different sources of funding, contribute to the effort to fight disinformation abroad. However, as was the case in the early days of the GEC, much of this effort continues to be focused on fighting extremist messaging rather than state-sponsored disinformation/campaigns.

A notable exception is the dedicated work within the Bureau of European and Eurasian Affairs to train journalists in investigative reporting, build independent news platforms and generally support independent local media to uncover and dispel Russian disinformation. In Ukraine's Donbas region, for example, the Bureau funds a news portal which reports on Russia's ongoing aggression against Ukraine. The Bureau also partners with the European Center of Excellence for Countering Hybrid Threats in Helsinki.

5 Executive Order 13721 of March 14, 2016 Developing an Integrated Global Engagement Center To Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584, https://www.govinfo.gov/content/pkg/FR-2016-03-17/pdf/2016-06250.pdf.

6 PUBLIC LAW 114–328—DEC.23, 2016 NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2017: https://www.congress.gov/114/plaws/publ328/PLAW-114publ328.pdf. The Act was enfolded as section 1287.



Lea Gabrielle, Special Envoy and Coordinator of the Global Engagement Center (GEC), made a statement on United States Efforts to Counter Russian Disinformation and Malign Influence for the House Committee on Appropriations on July 2019. She opened up GEC's key ongoing initiatives and capabilities. *Source: House Committee on Appropriations/YouTube screenshot*

DISPERSED EFFORTS BY OTHER US GOVERNMENT AGENCIES

Outside of the Department of State, two other US government agencies are pushing back on state-sponsored disinformation which seeks to undermine US foreign policy interests.

In 2019, the US Agency for International Development launched a Countering Malign Kremlin Influence Framework outlining a new approach to funding programmes in Eastern Europe and Eurasia. The framework repurposed many ongoing projects supporting free and fair elections, anti-corruption efforts and local media. The region, however, only receives approximately four percent of overall US foreign assistance.

Outside of Europe, USAID began a deliberate campaign to be publicly critical of China's predatory approach to development financing. Together with the launch of the new US International Development Finance Corporation (DFC), the objective is to emphasize the pitfalls of Chinese project financing and convince low income countries to pursue an alternate sustainable model of development. However, overall USAID budgets continue to stagnate under the Trump Administration, the bulk of US assistance is still devoted to the Middle East, and the new Corporation has not begun operations.

The US Agency for Global Media (USAGM) collaborates to dispel international disinformation about the United States and its policies by pushing out fact-based news over its multiple broadcast and digital platforms across the globe. Most of its efforts are focused on Russian disinformation about the weakness of the United States, of the NATO alliance and of Western democracies. In 2017 it launched Current Time, a 24/7 Russian-language TV and digital news network, increased broadcasting through the Voice of America's Russian Service and RFE/RL's Radio Svoboda, and expanded news coverage in languages such as Ukrainian, Belarusian, Serbian, and Georgian. It also established two fact-checking websites that investigate misleading statements and stories from Russian officials and state-sponsored propaganda outlets.

Although there is a rapidly growing audience for a number of these anti-propaganda products, the USAGM has not published information on measured results. At $808 million in fiscal year 2019, the global budget of the Agency is not large, and is due to drop significantly in 2020 to $628 million, as part of the overall budget-cutting process mandated by the US government.

Furthermore, the Department of Defense has built up its capacity to respond to foreign information operations. While this has mainly focused on fighting

violent extremist propaganda, more recently the Department has broadened its efforts to state-sponsored information operations.

The Department established the Russian Influence Group[7] co-chaired by the US European Command and the Department of State to share information on programmes and strategies to push back on Russian disinformation. The US European Command also expanded collaborative efforts within NATO, including with the Strategic Communications Centre of Excellence in Riga and the Cyber Defence Centre of Excellence in Tallinn.

To broaden counter-information operations beyond Russia, the Defense Department has established trans-regional Military Information Support Operations (MISO) under the Special Operations Command and is finalizing the creation of a MISO Operations Center to provide US regional Combatant Commands with global messaging capabilities beyond the themes of combatting violent extremism.

Although MISO teams are already deployed in many parts of the world to carry out activities designed to increase support for US military activities, the new steps will bring a more strategic approach to operations. It remains to be seen, however, how the activities will be coordinated with those of the GEC at the Department of State, which has the legal mandate for overseas US government messaging. To avoid conflict, the US Congress recently mandated the Department of Defense to produce a report on how the new MISO activities will be synchronized with those of the GEC.

The US Cyber Command has been given new authorities to defend forward in cyber and is conducting operations to identify and counter information operations. Although not confirmed, the late-2018 strike on the Russian Internet Research Agency in St. Petersburg, which was accused of meddling in the 2016 US presidential elections, was seen as part of a new offensive cyber campaign to impose costs for malign influence in the United States.

The Department of Justice and the Department of the Treasury are also involved in countering disinformation through the use of their authorities to indict and sanction those who conduct foreign information operations against the United States. In March 2018, the Department of the Treasury sanctioned the Russian Internet Research Agency, its employees and financial supporters for tampering with, altering and misappropriating information to influence the 2016 US elections.

Last but not least, the US intelligence community has certain authorities to conduct operations overseas to counter foreign influence. While individual government agencies are pushing back on malign state and non-state information operations outside of the United States, they are doing so without overall White House or National Security Council coordination of strategic messaging, development of countermeasures, or measurement of results.

UNDERDEVELOPED COOPERATION WITH THE PRIVATE SECTOR

Besides an interagency process, another missing element for an effective strategy is an agreement between the US government and the major, privately held US social media companies. Yet it is primarily on these privately owned platforms that the bulk of the disinformation and information campaigns take place. While several of the companies such as Google and Twitter have signed onto the EU Code of Practice to address the spread of online disinformation, no such code has been developed in the United States.[8]

The US Congress held several hearings with executives of major US social media companies during which they were questioned, sometimes sharply, about their privacy protection standards and their slow response to foreign manipulation of their platforms. The concerns of the US Congress are confronting the companies' own concerns about the effect of counter-disinformation mechanisms on their revenue streams and about the possible increased government regulation of social media. This has led to a climate of mistrust that prevents more effective public-private collective action.

The social media companies have been active in fighting disinformation. They have issued new policies and adopted new mechanisms to identify and take down fake accounts and campaigns that seek to mislead. While, like US government agencies, their initial efforts focused on reducing online jihadi propaganda, they are now seeking to address the manipulation of their platforms by Iran, China and Russia as well.

In 2018, the discovery by a US research company of a large social media influence campaign in the United

7 C. Todd Lopez, "Challenging Russian Information Operations Requires Whole-of-Government Approach", Defense News, 14 March 2019, https://www.defense.gov/Newsroom/News/Article/Article/1785455/challenging-russian-information-operations-requires-whole-of-government-approach/.

8 Alina Polyakova and Daniel Fried, "Europe is starting to tackle information. The US is lagging". In Brookings blog: Order from Chaos, 20 June 2019, https://www.brookings.edu/blog/order-from-chaos/2019/06/20/europe-is-starting-to-tackle-disinformation-the-us-is-lagging/.

States linked to Iran led to the takedown of multiple accounts by Facebook. In early 2019, Facebook removed another 500 pages and accounts operated out of Russia. More recently, Twitter, Facebook and Google removed content and suspended accounts linked to a Chinese state-sponsored information operation designed to sow discord and influence perceptions of the Hong Kong protests.

It is important to note that these actions are aimed at stopping what Facebook terms "coordinated inauthentic behavior to mislead others about who they are or what they are doing". The focus, therefore, is less on content than on behaviour. US social media company actions, in other words, are *not* aimed at reducing foreign malign influence operations against US national security interests, but rather seek to prevent misuse of the platforms.[9]

ONGOING EFFORTS TO COORDINATE EFFECTIVE RESPONSES

The US Congress continues to lead in efforts to develop greater coordination across US government agencies to counter foreign information operations. In the 2019 National Defense Authorization Act, the US Congress mandated that the White House appoint someone at the National Security Council to coordinate the interagency process to fight foreign malign influence. It also tasked the Director of National Intelligence to assess the national security threats posed by deep fake technology (digital forgeries of videos, images or audio), noting that it could be a "tool for hostile powers seeking to spread misinformation". These efforts are, however, more focused on preventing foreign influence on the upcoming US presidential elections than on strengthening US government actions to fight disinformation abroad.

There is some talk of the need to re-establish an Interagency Active Measures Group, as existed during the Reagan administration, to expose disinformation and to develop countermeasures. While this would help fill the vacuum on interagency coordination, there are major challenges today in setting up such an entity.[10]

The first challenge is the issue of data collection. A full analysis of foreign influence operations would require domestic data collection. The capability to do so lies with US intelligence and the US military. But, under current legal authorities, they are restricted in their ability to collect information within the United States. Also, US social media companies, for liability, revenue and regulatory reasons, are unwilling to share information on the customer data they collect or on the means they are using to identify fake accounts.

A second challenge is incorporating cyber as part of an integrated approach. Today, malign foreign information operations include hacking into computer systems to obtain information to influence social behaviour, such as the hacking and leaking of the emails of the Democratic National Committee by Russia to influence public opinion on candidate Hillary Clinton in the 2016 presidential election. A new Active Measures Group would have to integrate cyber tools into any strategy, especially the new offensive authorities given to the US Cyber Command. This would require an extensive review of retaliatory risks. Incorporating cyber would also require greater information sharing from private companies. These continue to under-report cyber-attacks, for legal and financial reasons.

Given these difficulties, it is likely that the current system of scattered efforts by government agencies to respond internationally to foreign information operations will continue.

CONCLUSION: THE WAY FORWARD

Any centralization of effort within the White House and the National Security Council in the immediate future will likely focus on protecting US voters and the electoral system from malign foreign interests in the run-up to the 2020 presidential election. A new senior position has already been created within the office of the Director for National Intelligence (DNI) to oversee election security intelligence across the government.

The lack of an integrated pro-active US international strategy to counter malign foreign information operations means that there is a greater need for international cooperation to address this threat. The Global Internet Forum to Counter Terrorism (GICFT)[11] could serve as a model of collaboration across industry, governments, NGOs and multilateral organizations,

9 Nathaniel Gleicher, Head of Cybersecurity Policy Facebook. "Coordinated Inauthentic Behavior", 4 December 2018, https://www.facebook.com/facebook/videos/coordinated-inauthentic-behavior-explained/942418432620984/.

10 Melissa Dalton, Kathleen H. Hicks, Megan Donahoe, Lindsey Sheppard, Alice Hunt Friend, Michael Matlaga, Joseph Federici, Matthew Conklin and Joseph Kiernan, "By Other Means Part II: US Priorities in the Gray Zone", Center for Strategic and International Studies, August 2019, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_II_full_WEB_0.pdf.

11 The Global Internet Forum to Counter Terrorism, https://gifct.org/about/.

but needs to be adapted to the challenges of state-sponsored influence operations. Furthermore, at the regional level, the US can and should increase cooperation with key entities such as the Strategic Communication Task Forces of the European External Action Service.

The Director of National Intelligence warned in testimony in January 2019 that "US adversaries and strategic competitors almost certainly will use online influence operations to try to weaken democratic institutions, undermine US alliances and partnerships, and shape policy outcomes in the United States and elsewhere. We expect our adversaries and strategic competitors to refine their capabilities and add new tactics as they learn from each other's experiences".[12]

The lack of a strategy and an effective interagency coordinating mechanism to respond internationally to malign influence operations by key rivals means that the United States will continue to operate on the defensive in the information space, to its strategic disadvantage. It has the requisite tools and ability to operate effectively on the offensive. It needs to adapt its government organization, develop new policies and have a new 21st century government-private sector compact to meet this long-term global challenge.

12 Daniel R. Coats, "Worldwide Threat Assessment of the US Intelligence Community", 29 January 2019, https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.