COLD WAR LESSONS FOR COUNTERING COVERT ACTION

BY NATE LOW

A Russian intelligence agency forged letters from the Ku Klux Klan threatening the lives of black athletes in an upcoming Olympics. The same agency initiated a propaganda campaign against the enhancement of nuclear weapons and covertly organized what appeared to be grassroots protest in the United States. The group also sent pamphlets to civil rights organizations allegedly created by the far-right Jewish Defense League that advocated violence. These divisive actions are not the recent work of a Russian online troll working within the GRU or Internet Research Agency. They are examples from the early 1980s of what the Soviet Union called "active measures," a mix of covert and deceptive operations—including propaganda, disinformation, front groups, media manipulation, political influence operations, and forgeries—intended to influence opinions and/or the actions of individuals and governments.[1] Today, such operations are also referred to as information warfare, and in the digital age, democracies are even more vulnerable to their implementation.

United States policymakers continue to reiterate the need to learn from the 2016 election to formulate a defense for active measures. They tend to characterize Russia's actions as a new type of threat requiring a new tool kit to combat. In doing so, they risk ignoring lessons from our past for confronting these threats. Indeed, methods developed by the U.S. government during the Cold War, such as the establishment of an interagency group that initiated educational programs, the formulation of innovative technical solutions for detection and attribution, and the active funding of independent media abroad, offer an arsenal of tactics for countering active measures today.

The first and most vital facet of any strategy to combat active measures is education. On October 9, 1981, the Active Measures Working Group (AMWG) ignited international interest in Soviet active measures when it published its first report, *Special Report 88, Soviet Active Measures: Forgery, Disinformation, Political Operations*,[2] which defined the terms the U.S. government used in classifying various Soviet tactics in information warfare and identified specific instances of Soviet active measures. Established during the Reagan administration, the AMWG was the first interagency organization dedicated to combating Soviet active measures. It had the publication legitimacy of the State Department and the resources to pronounce where and how forgeries emerged, allowing it to expose falsehoods and educate the public on foreign efforts to distort information.

Similar media and digital literacy training are particularly important in today's information environment. The Soviet act of selective replay in its active measures, which during the Cold War required KGB and other intelligence agents to coerce newspapers or radio broadcasters to publish their material, is now being done by "trolls," automat-

ed bots and unaware citizens on social media. Today, the impetus to detect and shut down fake Twitter accounts, Facebook pages, and Google ads has mostly fallen to technology companies. However, taking lessons from its Cold War history, the U.S. government should complement these efforts by identifying and shutting down suspicious accounts and network activity. Early detection and attribution of fake news will reduce the likelihood that such stories are "replayed" by Kremlin-backed outlets such as RT and Sputnik, making the dissemination of these stories more difficult. The establishment of the Foreign Influence Task Force (FITF) within the FBI to identify and counteract malign foreign influence operations is a promising start. But this effort should involve significant coordination with other intelligence community agencies, as well as with state and local law enforcement partners and election officials. Such a task may require the creation of an independent interagency group similar to the AMWG.

The AMWG also developed a campaign aimed at educating international audiences on Soviet active measures and disseminated its contestation strategy of "Report-Analyze-Publicize." In the spring of 1983, then AMWG Director Dennis Kux and several members of the Group embarked on their first "road show."[3] The Group travelled to two countries per week to brief officials in U.S. embassies and foreign intelligence services and to make presentations to local journalists and media organizations on Soviet disinformation efforts. Today, most countries facing the threat of disinformation don't need to be lectured on its existence. However, a single U.S. government body tasked with coordinating disparate international efforts to counter Russian active measures would be beneficial. The U.S. Agency for International Development's Office of Transition Initiatives (OTI) has started to fulfill this role by traveling to meet with civil society organizations, media groups, and governments in Europe targeted by Russian influence operations. OTI aims to increase access to balanced information, promote constructive political discourse, and support democratic reforms.[4] Using the model of AMWG, the U.S. government should formalize and expand OTI's role as a coordinating body for counter-disinformation efforts.

The next prong of an effective strategy to combat active measures is developing technical expertise and creative technical solutions. During the Cold War, the U.S. government invested in and drew from its own technical know-how to identify active measures, which often took the form of forgeries. For example, in 1983, the Soviets forged diplomatic cables asserting that the United States orchestrated assassination attempts on Pope John Paul II and a Nigerian presidential candidate.[5] According to Kux, the forgeries were excellent, but skilled analysts were able to identify minor errors such as the mis-transliteration of Brazil as "Brasilia" and the use of the word "wet affair," a Soviet euphemism for assassination, which revealed that the documents were of Russian origin.[6]

Today, technological development has created new dangers but also new solutions. With developments in AI such as language and image detection, the U.S. government should be at the forefront of algorithms that autonomously detect fake news sources. While the private sector should be enlisted in this effort, the U.S. government should also fund public and military research into these technologies,

including through National Science Foundation grants and/or through the technical divisions of the armed forces. A third and equally viable path is to direct more public funds to one of America's greatest assets: universities. In March 2018, Harvard's Belfer Center for Science and International Affairs hosted an Information Operations Technical and Policy Hackathon in which students presented ideas such as "honey bots" to counter malicious bots, algorithms that limit echo chambers, and an app called Sanity Check, which uses natural language processing, bot detection, source greylisting, and reverse image searching to identify information operations over social media.[7] Efforts of this nature should be supported in earnest.

Educating the public and increasing our ability to identify and disrupt active measures is important, but the U.S. government must also take its fight abroad. Here, too, there are historical examples to borrow from. As Seth G. Jones identifies in his new book, *A Covert Action*, during the Cold War, the Reagan Administration successfully supported the Solidarity Movement in Poland by covertly providing duplicator machines, paper products, and aiding in the production of propaganda. At the same time, the CIA operated a covert "book program" in which it sent books and periodicals to states in the Soviet Union through front organizations.[8] Using a different type of offensive action, the U.S. government funded Radio Free Europe and Radio Liberty to air its values and create space for independent reporting in biased, Soviet-dominated information environments. Today, as during the Cold War, there is room for different types of offensive action that do not replicate Soviet active measures, but effectively thwart them. The U.S. Cyber Command should establish a group similar to Joint Task Force Ares, which conducted an effective cyber offensive against ISIS, to disrupt the computer networks and operations of foreign adversaries implementing active measures from within their home countries. Policymakers can also publicize possible responses to active measures and pass legislation such as the Defending American Security from Kremlin Aggression Act of 2018. These actions may or may not change Russian behavior, but they signal clear consequences for future active measures.

THE U.S. GOVERNMENT SHOULD FOCUS ON HUMAN SOLUTIONS TO ACTIVE MEASURES BY IMPROVING THE QUALITY OF THE MEDIA ENVIRONMENT AT HOME AND ABROAD

However, the U.S. government must be careful not to securitize the issue. Disinformation and cybersecurity are both threats to democratic processes and interconnected in important ways, but as James A. Lewis of CSIS notes, "information warfare covers a range of activities of which cyber-attacks may be the least important."[9] Policies should recognize the distinction. Hague Centre for Strategic Studies cyber expert Alexander Klimburg identifies that: "especially in the West, we seem conceptually trapped in thinking of the new challenges of cyberspace as being purely technical, instead of being very much human."[10] The U.S. government should focus on human solutions to active measures by improving the quality of the media environment at home and abroad through increased investment in programs like those offered by OTI, Radio Free Europe, and Radio Liberty. Policymakers should also follow the example of countries such as the Czech

Republic and the Ukraine, which have signed decrees prioritizing media literacy in the national curriculum.

A democracy such as the United States is especially vulnerable to information warfare due to its beliefs in transparency and the open exchange of information. Such vulnerability was present throughout the Cold War information wars with the Soviet Union and has only been exacerbated in the digital age. Yet, the methods developed during that time, such as the establishment of an interagency group dedicated to combating active measures through education, the formulation of new technical solutions for detection and attribution, offensive actions such as those offered by U.S. Cyber Command, and funding for free media, remain democracy's best defense.

Nathaniel Low *is a research intern with the Technology Policy Program at CSIS.*

ENDNOTES

1. U.S. Department of State, *Soviet Influence Activities: A Report on Active Measures and Propaganda*, 1986-87 (Washington, D.C.: 1987).

2. U.S. Department of State, *Special Report 88, Soviet Active Measures: Forgery, Disinformation, Political Operations*, (Washington, DC, 1981), https://www.cia.gov/library/readingroom/docs/CIA-RDP84B00049R001303150031-0.pdf.

3. 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* 11, (Washington: NDU Press, 2012), http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/inss/StrategicPerspectives-11.pdf.

4. USAID, "Office of Transition Initiatives (OTI)", https://www.usaid.gov/who-we-are/organization/bureaus/bureau-democracy-conflict-and-humanitarian-assistance/office-1.

5. Schoen and Lamb, 44.

6. Ibid.

7. Josh Burek, "National Student Hackathon Showcases Innovative Proposals to Thwart Cyberattacks and Information Operations," Belfer Center, March 30, 2018, https://www.belfercenter.org/publication/national-student-hackathon-showcases-innovative-proposals-thwart-cyberattacks-and.

8. "Marshall Plan for the Mind: The CIA Covert Book Program during the Cold War," Wilson Center, January 15, 2015, https://www.wilsoncenter.org/event/marshall-plan-for-the-mind-the-cia-covert-book-program-during-the-cold-war.

9. James A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats," (Washington, D.C.: Center for Strategic and International Studies, 2002), p. 7, https://www.csis.org/analysis/assessing-risks-cyber-terrorism-cyber-war-and-other-cyber-threats.

10. Alexander Klimburg, *The Darkening Web: The War for Cyberspace* (New York: Penguin Press, 2017), p. 5.