

Committee on House Administration

---

# American Confidence in Elections:

## Prohibiting Foreign Interference

**BRADLEY BOWMAN**

**Senior Director**

*Center on Military and Political Power,  
Foundation for Defense of Democracies*

**MAX LESSER**

**Senior Analyst on Emerging Threats**

*Center on Cyber and Technology Innovation,  
Foundation for Defense of Democracies*

**Washington, DC  
December 18, 2024**

Chairman Steil, Ranking Member Morelle, and distinguished members of this committee, thank you for the opportunity to testify today regarding efforts by foreign adversaries to undermine American democracy and the confidence we have in our elections. The committee deserves credit for convening this hearing and calling attention to this incredibly important issue. Before assessing foreign adversary attacks on the 2024 U.S. election, the effectiveness of those attacks, and how the government responded, it is helpful to step back and try to understand the larger context.

*The Information War China, Russia, and Iran Are Waging Against Americans*

China, Russia, and Iran are waging an information war against the United States that includes a focus on the U.S. electoral process, yet many Americans do not realize we are under attack. Nor do they fully appreciate that developments on the battlefield of ideas and beliefs can have a decisive impact on our democracy and the way of life Americans enjoy. This lack of awareness is ideal for Beijing, Moscow, and Tehran — predators like nothing better than hunting slumbering prey.

Americans may not realize they are already in an information war because adversaries attempt to conceal their activities. To make matters worse, Americans often think of international conflict consciously or subconsciously in the context of kinetic war — soldiers, ships, and aircraft battling one another on land, at sea, or in the air. So, when there is no overt conflict, we can be lulled into a false sense of security.

In June, the Foundation for Defense of Democracies (FDD) published a major report entitled “*Cognitive Combat: China, Russia, and Iran’s Information War Against Americans*.”<sup>1</sup> Much of this testimony is based on research conducted for that report, as well as the research and analysis of FDD’s Center on Cyber and Technology Innovation.<sup>2</sup>

An enduring obstacle to understanding information warfare is the lack of consensus about what the phrase actually means. Some definitions are too broad to be useful, and some have the opposite problem. In the June report, we defined information warfare as the messages — and means to convey those messages — that nation-states use to advance political, economic, and security objectives and to strengthen the government’s foundations of power, reinforce those of allies and partners, and undermine those of adversaries.<sup>3</sup>

---

<sup>1</sup> Ed. Bradley Bowman, “Cognitive Combat,” *Foundation for Defense of Democracies*, June 28, 2024. (<https://www.fdd.org/analysis/2024/06/28/cognitive-combat>). The report includes chapters by our FDD colleagues, including a chapter on China by Craig Singleton, on Russia by Ivana Stradner and John Hardie, and on Iran by Mark Dubowitz and Saeed Ghasseminejad.

<sup>2</sup> Max Lesser and RADM (Ret.) Mark Montgomery, “How U.S. Adversaries Undermine the Perception of Election Integrity,” *Foundation for Defense of Democracies*, September 26, 2024. (<https://www.fdd.org/analysis/2024/09/26/how-u-s-adversaries-undermine-the-perception-of-election-integrity>); Max Lesser, “Foreign Malign Election Meddling Persists But Struggles to Gain Traction,” *Foundation for Defense of Democracies*, October 29, 2024. (<https://www.fdd.org/analysis/2024/10/29/foreign-malign-election-meddling-persists-but-struggles-to-gain-traction>).

<sup>3</sup> A more complete definition of information warfare would not focus exclusively on nation-states alone and would include non-state actors such as Hamas and Hezbollah, but the focus of the report was three nation-states: China, Russia, and Iran.

By that definition, China, Russia, and Iran are already waging an information war against our country. Despite their differences, these adversaries of the United States understand that ideas and beliefs play a decisive role in shaping what individuals and nations support or oppose and, ultimately, in determining which actions are taken or avoided.

Armed with this understanding, Beijing, Moscow, and Tehran are methodically targeting three groups. The first and most important target audience for each adversary regime is its own domestic population. The second target audience is Americans, the U.S. government, and its allies and partners. And the third is populations and governments in other countries where these regimes seek to obtain valuable strategic resources or concessions. We will focus on the first two groups for this testimony.

It might seem odd that the primary information warfare focus of Xi Jinping, Vladimir Putin, and Ali Khamenei is their own people. But when one considers the autocratic, authoritarian, and/or totalitarian natures of these regimes, it makes sense. Xi, Putin, and Khamenei must manipulate the flow of information to their people to maintain a monopoly on power. If a government does not enjoy the consent of the governed, the regime must attempt the Orwellian management of information to their oppressed peoples so that they submit to their subjugated state.

Most relevant to this hearing, China, Russia, and Iran also focus their information warfare campaigns on Americans because they believe the United States possesses a unique potential to challenge the regimes' oppression at home and aggression abroad.<sup>4</sup> More specifically, the *existence* and *power* of the United States directly challenge the regimes in Beijing, Moscow, and Tehran.

The mere *existence* of the United States (and its democratic allies) conveys to the people of China, Russia, and Iran that there is an appealing alternative to authoritarianism and autocracy.<sup>5</sup> The regimes and their proxies sometimes respond by suggesting that democracy is inferior or that it cannot work in their respective regions. The former argument is rather predictable for autocrats eager to retain their self-serving grip on power. The latter argument is decisively refuted by the existence of free peoples and democratic governments in Taiwan, Ukraine, and Israel. That explains some of the vitriol we see toward Taipei, Kyiv, and Jerusalem, respectively.

Adversary regimes also realize that American military *power* presents a serious impediment to their regional ambitions. Xi seeks to conquer Taiwan, Putin seeks to subjugate Ukraine, and Khamenei seeks to exterminate the State of Israel. In each case, the United States is a leading obstacle to their aims. That helps explain why each regime is waging information war against the United States.

---

<sup>4</sup> Matt Pottinger, "Remarks by Matthew Pottinger at Parliamentary Intelligence-Security Forum in London," August 31, 2023. (<https://www.fdd.org/analysis/2023/08/31/remarks-by-matthew-pottinger-at-parliamentary-intelligence-security-forum-in-london>)

<sup>5</sup> Stephen Kotkin, a senior fellow at the Hoover Institution, has made this point. An example here: Hoover Institution, "American Character vs. Authoritarian Nature | HISPBC," *YouTube*, September 24, 2024. (<https://youtu.be/korJRqnWhnI?si=4OyXVfG1opveKGEZ>)

These concerns about the existence and power of the United States have motivated our adversaries to adopt a strategy that features three broad objectives, which can be summarized as *divide, degrade, and deceive*. Understanding these objectives can help us respond more effectively.

Our authoritarian adversaries seek to *divide* Americans, pitting us against one another, so that we are as domestically dysfunctional as possible, encouraging us to mistakenly view as enemies fellow citizens of good faith with whom we simply have a disagreement.<sup>6</sup> Authoritarian adversaries want our domestic politics to be as partisan, tribalistic, and vitriolic as possible.<sup>7</sup> They want us at each other's throats so that we are too distracted, divided, and weak to defend ourselves and our interests, hoping we consume our finite time, energy, and resources fighting one another rather than working together to strengthen our country at home and defend our interests abroad.<sup>8</sup>

In addition to attempting to divide Americans, our adversaries also seek to *degrade* our democracy's reputation, both in our eyes and in the eyes of others. If Americans don't respect our democracy, some may be less eager to defend it. Moreover, authoritarian adversaries want our model of representative democracy to look like a less favorable governance alternative compared to authoritarianism and autocracy. An adversary information warfare strategy that frames the United States as a dysfunctional and declining power is designed to serve that objective.

Finally, our adversaries also seek to *deceive* Americans into believing falsely that we have no important interests or values to defend in places such as Taiwan, Ukraine, and Israel.<sup>9</sup> By seeking to drive a wedge between the United States and those three beleaguered democratic partners, authoritarian regimes hope to deprive our partners of American diplomatic, economic, and military support, thereby making those U.S. partners more vulnerable to aggression.

---

<sup>6</sup> David R. Shedd and Ivana Stradner, "The Covert War for American Minds," *Foreign Affairs*, October 29, 2024. (<https://www.foreignaffairs.com/united-states/covert-war-american-minds>)

<sup>7</sup> The Russian media organization Rybar, also known as Storm-1841 or Volga Flood, created multiple inauthentic Telegram channels and X accounts not in its own name that shared polarizing content in attempts to divide Americans and even encourage acts of violence. U.S. Department of State, Rewards for Justice, "Rybar Employees," accessed December 5, 2024. (<https://rewardsforjustice.net/rewards/rybar>); "Iran Steps Into U.S. Election 2024 With Cyber-Enabled Influence Operations," *Microsoft Threat Analysis Center*, August 9, 2024, page 5. (<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/5bc57431-a7a9-49ad-944d-b93b7d35d0fc.pdf>)

<sup>8</sup> A couple of caveats are important: First, we should not reflexively blame problems and divisions in the United States on our adversaries. Unfortunately, we Americans are quite adept at creating our own problems. But it would be dangerous not to recognize that Beijing, Moscow, and Tehran seek to exacerbate and magnify existing social-political fault lines to help pave the way for their wider ambitions. Second, acknowledging that our adversaries are attempting to divide us is not to suggest, of course, that we shouldn't have serious political and policy disagreements. Disagreements can be healthy and are certainly to be expected in our wonderfully diverse, free, and rambunctious democracy. But we need to engage in those debates in a manner that does not create opportunities for our adversaries and that does not inadvertently facilitate their information war against us.

<sup>9</sup> Bradley Bowman and RADM (Ret.) Mark Montgomery, "Supporting America's Allies Puts America First," *National Review*, February 23, 2024. (<https://www.nationalreview.com/2024/02/supporting-americas-allies-puts-america-first>)

Our adversaries seek to achieve their objectives at the lowest cost. They would rather not fight the U.S. military and would rather not see Taiwan, Ukraine, and Israel defending themselves with American weapons. Beijing, Moscow, and Tehran hope that by deceiving Americans into believing that the outcomes in Taiwan, Ukraine, and Israel don't matter Americans will decide not to help those three beleaguered democracies defend themselves and the interests we share. In other words, this element of our adversaries' information warfare campaigns represents a methodical effort to remove U.S. military power and American weapons as obstacles to authoritarian aggression by manipulating the beliefs of Americans.

In summary, China pushes messages via a variety of means that seek to undermine Americans' trust in our leaders, our government, and each other. Simultaneously, Beijing is attempting to manipulate U.S. public opinion regarding Hong Kong, Taiwan, Tibet, and Xinjiang.<sup>10</sup> The Chinese Communist Party hopes these measures weaken and divide Americans and remove any U.S. obstacles to Beijing's control and oppression at home and "might makes right" foreign policy abroad. Russia proliferates messages designed to exploit hot-button domestic issues, stoke division among Americans,<sup>11</sup> and undermine support for Ukraine.<sup>12</sup> The Islamic Republic of Iran, for its part, not only uses information warfare to oppress the Iranian people, threaten dissidents, magnify anti-American voices, and threaten Israel but also seeks to manipulate American opinions and enfeeble U.S. foreign policy.

So, with this broader context in mind, why do our adversaries focus so much attention on our elections?

Carl von Clausewitz, the 19th-century Prussian military theorist, promulgated the concept of a "center of gravity." He defined it as "the hub of all power and movement, on which everything depends."<sup>13</sup> Clausewitz's center of gravity is sometimes characterized by analysts as the source of power and strength — the point against which all efforts should be directed.<sup>14</sup>

This military concept can also be applied in this context. The American center of gravity is our Constitution and the rule of law — as well as free, fair, and trusted elections and the peaceful transfer of power. That is the foundation for who we are as Americans. That is what we must defend to secure our freedom, stability, and way of life. Our adversaries understand that fact, and that is why they are so eager to undermine our elections and their perceived credibility.

---

<sup>10</sup> U.S. Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community," February 5, 2024. (<https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>)

<sup>11</sup> Mark Hosenball, "Russia stocking U.S. racial, social differences ahead of election: sources," *Reuters*, March 10, 2020. (<https://www.reuters.com/article/us-usa-election-security/russia-stoking-u-s-racial-social-differences-ahead-of-election-sources-idUSKBN20X2O3>); Bradley Bowman and Shane Praiswater, "Great Power Competition Comes Home to America," *Defense One*, November 3, 2020. (<https://www.defenseone.com/ideas/2020/11/great-power-competition-comes-home-america/169760>).

<sup>12</sup> Julian E. Barnes and David E. Sanger, "Russia Amps Up Online Campaign Against Ukraine Before U.S. Elections," *The New York Times*, March 27, 2024. (<https://www.nytimes.com/2024/03/27/us/politics/russian-ukraine-us-interference.html>)

<sup>13</sup> Carl von Clausewitz, *On War*, Trans. Peter Paret and Michael Howard (Princeton, New Jersey: Princeton University Press, 1976), page 595.

<sup>14</sup> Antulio Echevarria, "Clausewitz's Center of Gravity," *Naval War College Review*, 2003. (<https://digital-commons.usnwc.edu/nwc-review/vol56/iss1/6>)

A survey of history and international affairs makes clear that the quality of life we enjoy in the United States is not the norm. It is an anomaly, and we should not take it for granted. That means understanding the information war being waged against us and taking steps to defend our democratic and electoral center of gravity are essential.

### *What Just Happened?*

With this context in mind, it is worth assessing adversary attacks on the 2024 election, the effectiveness of those attacks, and how the United States responded.

Russia, Iran, and China aggressively targeted the American democratic process this year. Russia sought to undermine Vice President Kamala Harris's campaign.<sup>15</sup> Iran attacked president-elect Donald Trump's campaign.<sup>16</sup> China, for its part, attacked both major presidential candidates, in addition to certain congressional candidates who are critical of China.<sup>17</sup> In short, both parties and all major presidential candidates were attacked. All three adversaries sought to undermine the faith of Americans in our electoral process.

In other words, anyone who seeks to highlight foreign interference for the purposes of partisan gain is missing the point. It should not matter which party or politician stood to gain or lose from the interference. Not unlike how a family comes together when a single member of the family is hurt, when it comes to foreign adversary interference in our elections, the only question is whether our country and our democratic system were attacked. If the answer is 'yes', then Americans of all political persuasions should act together to better defend our democracy and impose consequences on our adversaries.

So, what steps did U.S. adversaries take to target the 2024 elections?

---

<sup>15</sup> U.S. Office of the Director of National Intelligence, Press Release, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024.

(<https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf>)

<sup>16</sup> Dustin Volz, "Iran Is Working to Undercut Trump in Presidential Election, U.S. Spy Agencies Say," *The Wall Street Journal*, July 29, 2024. (<https://www.wsj.com/politics/elections/iran-is-working-to-undercut-trump-in-presidential-election-u-s-spy-agencies-say-7f67fad7>)

<sup>17</sup> Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (<https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf>); Insikt Group, "Operation Overload Impersonates Media to Influence 2024 U.S. Election," *Recorded Future*, October 23, 2024.

(<https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf>); "Russia, Iran, and China Continue Influence Campaigns in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024. (<https://cdn-dynmedia->

[l.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf](https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf)); "The #Americans: Chinese State-Linked Influence Operation Spamouflage Masquerades as U.S. Voters to Push Divisive Online Narratives Ahead of 2024 Election," *Graphika*, September 2024.

(<https://public-assets.graphika.com/reports/graphika-report-the-americans.pdf>); Steven Lee Myers, "Bots Linked to China Target Republican House and Senate Candidates, Microsoft Says," *The New York Times*, October 23, 2024. (<https://www.nytimes.com/2024/10/23/us/politics/x-bots-china-republicans.html>)

Russia's most significant operations involved a series of hoax videos published in the weeks before the election, several of which went viral.<sup>18</sup> Fortunately, the U.S. government promptly responded in many cases. In one instance, a fake video depicting someone burning ballots in Pennsylvania was debunked by local election officials on the same day the video was posted, and the federal government released an official statement two days later attributing it to Russia.<sup>19</sup> Iran's most significant activity involved a hack-and-leak operation targeting the Trump campaign. While Iran successfully compromised sensitive materials from the Trump campaign, mainstream media outlets did not publish this information.<sup>20</sup> Iran also targeted swing states and minority groups through a series of fake websites, but these do not appear to have gained significant traction.<sup>21</sup>

China largely targeted the election through its flagship influence operation known as "Spamouflage," which involves vast networks of fake accounts on social media. Spamouflage's activity typically pushed out low-quality content that, with a few exceptions, garnered little organic engagement on social media.<sup>22</sup> A notable trend with Spamouflage this election cycle, however, was that it leveraged antisemitic tropes to criticize both the American political system and specific candidates.<sup>23</sup>

---

<sup>18</sup> "Russia Leverages Cyber proxies and Volga Flood Assets in Expansive Influence Efforts," *Microsoft Threat Analysis Center*, September 17, 2024, page 2. (<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-4.pdf>); "Fact Check: Kamala Harris Hit-and-Run Story Stems From Unreliable Website," *Reuters*, September 20, 2024. (<https://www.reuters.com/fact-check/kamala-harris-hit-and-run-story-stems-unreliable-website-2024-09-20/>); "Lead-up to Election Day 2024: Russia, Iran, and China Engaging in Influence Activity in Final Weeks Before Election Day 2024," *Microsoft Threat Analysis Center*, October 23, 2024, pages 4-5. (<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/MTAC-Election-Report-5-on-Russian-Influence.pdf>); Office of Georgia Secretary of State, "Statement from Secretary Raffensperger," October 31, 2024. (<https://sos.ga.gov/news/statement-secretary-raffensperger>)

<sup>19</sup> "Board of Elections Issues Bipartisan Statement on Fake Ballot Video," *Bucks County, Pennsylvania*, October 24, 2024. (<https://www.buckscounty.gov/CivicAlerts.aspx?AID=1151>); "Fact Check: Video of Pennsylvania Mail-in Ballots Being Destroyed Is Fake," *Reuters*, October 31, 2024. (<https://www.reuters.com/fact-check/video-pennsylvania-mail-in-ballots-being-destroyed-is-fake-2024-10-31/>)

<sup>20</sup> Christopher Bing, Raphael Satter, and Gram Slattery, "Exclusive: Accused Iranian Hackers Successfully Peddle Stolen Trump Emails," *Reuters*, October 25, 2024. (<https://www.reuters.com/world/us/accused-iranian-hackers-successfully-peddle-stolen-trump-emails-2024-10-25/>)

<sup>21</sup> Max Lesser and RADM (Ret.) Mark Montgomery, "How U.S. Adversaries Undermine the Perception of Election Integrity," *Foundation for Defense of Democracies*, September 26, 2024. (<https://www.fdd.org/wp-content/uploads/2024/09/fdd-memo-how-u.s.-adversaries-undermine-the-perception-of-election-integrity.pdf>); Max Lesser, "Foreign Malign Election Meddling Persists But Struggles to Gain Traction," *Foundation for Defense of Democracies*, October 29, 2024. (<https://www.fdd.org/wp-content/uploads/2024/10/fdd-memo-foreign-malign-election-meddling-persists-but-struggles-to-gain-traction.pdf>)

<sup>22</sup> Max Lesser, Ari Ben Am, Margot Fulde-Hardy, Saman Nazari, and Paul J. Malcomb, "Much Ado About 'Somethings': China-Linked Influence Operation Endures Despite Takedowns," *Foundation for Defense of Democracies*, March 27, 2024. (<https://www.fdd.org/analysis/2024/03/27/much-ado-about-somethings>); Elise Thomas, "Pro-CCP Spamouflage Campaign Experiments with New Tactics Targeting the U.S.," *Institute for Strategic Dialogue*, April 1, 2024. ([https://www.isdglobal.org/digital\\_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us](https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us))

<sup>23</sup> Wenhao Ma, "China-Connected Spamouflage Networks Spread Antisemitic Disinformation," *Voice of America*, October 4, 2024. (<https://www.voanews.com/a/china-connected-spamouflage-networks-spread-antisemitic-disinformation/7811033.html>)

The U.S. government's response proved relatively effective this election cycle. It preemptively warned Americans of adversaries' tactics, techniques, and procedures, took down infrastructure enabling influence operations, name-and-shamed malign influence actors, and sometimes even debunked falsehoods in near real-time.

U.S. government organizations involved in combating foreign malign influence targeting the 2024 U.S. elections included the Office of the Director of National Intelligence's Foreign Malign Influence Center, the FBI's Foreign Influence Task Force, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of Justice (DOJ), the State Department, and the Treasury Department. The involvement of these departments and agencies, as well as coordination between them, yielded significant results.

Highlights included the DOJ taking down Doppelganger domains and indicting American media executives that acted on behalf of Russia,<sup>24</sup> the Treasury sanctioning various influence actors from Russia and Iran,<sup>25</sup> CISA and the FBI proactively debunking false claims of cyberattacks against voting machines,<sup>26</sup> and the ODNI's regular reports giving an overview of the threat landscape.<sup>27</sup>

The efforts of state and local governments were also critical. The office of the Georgia secretary of state, the Bucks County Board of Elections, and the San Francisco Police Department, for example, all issued statements either directly to the public or to the media debunking videos likely originating from the Russian operation CopyCop.<sup>28</sup>

---

<sup>24</sup> U.S. Department of Justice, Office of Public Affairs, Press Release, "Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere," September 4, 2024. (<https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence>)

<sup>25</sup> U.S. Department of the Treasury, Press Release, "Treasury Sanctions Iranian Regime Agents Attempting to Interfere in U.S. Elections," September 27, 2024. (<https://home.treasury.gov/news/press-releases/jy2621>); U.S. Department of the Treasury, Press Release, "Treasury Sanctions Actors Supporting Kremlin-Directed Malign Influence Efforts," March 20, 2024. (<https://home.treasury.gov/news/press-releases/jy2195>); Eu Disinfo Lab, "What is the Doppelganger Operation? List of Resources," accessed December 5, 2024. (<https://www.disinfo.eu/doppelganger-operation>). Note: While the Treasury press release does not specifically call out Doppelganger, researchers have linked Doppelganger to the companies associated with the individuals sanctioned by Treasury.

<sup>26</sup> U.S. Federal Bureau of Investigation and U.S. Cybersecurity and Infrastructure Security Agency, "Just So You Know: Ransomware Disruptions During Voting Periods Will Not Impact the Security and Resilience of Vote Casting or Counting," August 15, 2024. ([https://www.cisa.gov/sites/default/files/2024-08/Just\\_So\\_You\\_Know\\_Ransomware\\_Disruptions\\_During\\_Voting\\_Periods\\_Will\\_Not\\_Impact\\_the\\_Security\\_and\\_Resilience\\_of\\_Vote\\_Casting\\_or\\_Counting\\_8.15.24\\_V2\\_508c\\_0.pdf](https://www.cisa.gov/sites/default/files/2024-08/Just_So_You_Know_Ransomware_Disruptions_During_Voting_Periods_Will_Not_Impact_the_Security_and_Resilience_of_Vote_Casting_or_Counting_8.15.24_V2_508c_0.pdf))

<sup>27</sup> U.S. Office of the Director of National Intelligence, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024. (<https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf>)

<sup>28</sup> Office of Georgia Secretary of State, "Statement from Secretary Raffensperger," October 31, 2024. (<https://sos.ga.gov/news/statement-secretary-raffensperger>); "Board of Elections Issues Bipartisan Statement on Fake Ballot Video," *Bucks County, Pennsylvania*, October 24, 2024. (<https://www.buckscounty.gov/CivicAlerts.aspx?AID=1151>); "Fact Check: Video of Pennsylvania Mail-in Ballots Being Destroyed Is Fake," *Reuters*, October 31, 2024. (<https://www.reuters.com/fact-check/video-pennsylvania-mail-in-ballots-being-destroyed-is-fake-2024-10-31>); "Fact Check: Kamala Harris Hit-and-Run Story Stems From Unreliable Website," *Reuters*, September 20, 2024. (<https://www.reuters.com/fact-check/kamala-harris-hit-and-run-story-stems-unreliable-website-2024-09-20>)



On Election Day, the FBI quickly responded to hoax bomb threats, assuring the public that none of the threats were credible.<sup>29</sup> CISA, for its part, released a statement the next day affirming the security and integrity of election infrastructure.<sup>30</sup>

In summary, Russia, Iran, and China waged aggressive influence operations targeting America's political system. It is difficult to define with precision the effects of these efforts, but it appears that America proved remarkably resilient. In many instances, efforts of federal and state governments, the private sector, and the research community appear to have thwarted Russian, Iranian, and Chinese efforts to shape voters' preferences and undermine Americans' faith in the fairness and integrity of the democratic process. A Reuters/Ipsos poll released several days after the election found that the majority of Americans believed the election was legitimate and accurate.<sup>31</sup>

That's good news, but Americans should not allow themselves to become complacent. Given the ongoing information war against the United States and the interests of adversaries, we can expect China, Russia, and Iran to continue to attack our electoral processes with increasing ferocity and effectiveness.<sup>32</sup> Just because adversary efforts in 2024 were not more successful does not mean we should assume that will be the case in future elections.

### *Time To Go On the Offensive*

To deter foreign interference in our elections and protect our American center of gravity requires more than effective defenses. Even the best defenses eventually fail if attacks continue unabated. Our adversaries are not deterred from attacking our elections, and those attacks will only increase in frequency and sophistication if they believe they can continue to wage those attacks on our elections at no cost. We must change the cost-benefit analysis of our adversaries. After all, deterrence is strongest when there is both an effective defense and an effective offense. Therefore, we should continue to build the best possible defenses for our elections and electoral processes while simultaneously going on the information warfare offensive against China, Russia, and Iran. Such a campaign could systematically expose each regime's corruption and

---

<sup>29</sup> U.S. Federal Bureau of Investigation, National Press Office, Press Release, "FBI Statement on Bomb Threats to Polling Locations," November 5, 2024. (<https://www.fbi.gov/news/press-releases/fbi-statement-on-bomb-threats-to-polling-locations>)

<sup>30</sup> U.S. Cybersecurity and Infrastructure Security Agency, "Statement from CISA Director Easterly on the Security of the 2024 Elections," November 6, 2024. (<https://www.cisa.gov/news-events/news/statement-cisa-director-easterly-security-2024-elections>)

<sup>31</sup> "Americans accept the election results even if some are unhappy with the outcome," *Ipsos*, November 8, 2024. (<https://www.ipsos.com/en-us/americans-accept-election-results-even-if-some-are-unhappy-outcome>)

<sup>32</sup> In the lead-up to Election Day, researchers and government officials warned that America's adversaries would use AI to improve their influence operations dramatically. While Russia, Iran, and China all used AI-generated content in their influence operations, this did not appear to transform their operations. As per the ODNI, "Generative AI is helping to improve and accelerate aspects of foreign influence operations but thus far the IC has not seen it revolutionize such operations." *Source*: U.S. Office of the Director of National Intelligence, "45 Days Until Election 2024: Election Security Update as of Mid-September 2024," September 23, 2024. (<https://www.odni.gov/files/FMIC/documents/ODNI-Election-Security-Update-20240923.pdf>)

oppression and help the Chinese, Russian, and Iranian people advocate for their own rights, including more representative governance.<sup>33</sup>

Much to the detriment of U.S. interests and the satisfaction of Xi, Putin, and Khamenei, successive U.S. administrations have resisted offensive information warfare efforts inside China, Russia, and Iran for fear of “provoking” them. The result is that the United States has failed to put up a fight, even as all three regimes wage aggressive information war in America. This is the equivalent of a kinetic war in which one combatant is relentlessly firing mortars, rockets, and missiles, and the recipient of the strikes assiduously refuses to respond for fear of provoking an aggressor already launching salvos.

Skeptics of such arguments will no doubt express concern that aggressive U.S. offensive information warfare operations inside China, Russia, and Iran could spark a dangerous escalatory cycle. Curiously, such concerns often seem to emerge only when Americans awake to aggression against them and begin contemplating how to respond.<sup>34</sup>

Admittedly, such concerns about escalation are not entirely ridiculous. But these concerns must be weighed against the dangers associated with accepting the status quo in which we can expect China, Russia, and Iran to target with increasing ferocity and AI-empowered effectiveness<sup>35</sup> the socio-political foundations upon which American stability, liberty, and security stand.

For too long, America has tried a strategy of inaction, at worst, and restraint, at best, when it comes to responding to information warfare aggression by China, Russia, and Iran. The results from this head-in-the-sand strategy are not good, and there is reason to worry the consequences will only get worse without change.

As a result of the ineffective U.S. information warfare defense and an arguably almost non-existent offense, Washington has failed to deter adversary offensive information warfare operations against Americans. That has left China, Russia, and Iran with the impression that they can wage war openly on Americans, our security, our democracy, and our elections with few consequences.

A call for aggressive offensive information warfare operations against China, Russia, and Iran is not a call for Washington to proactively use the U.S. military to conduct regime change. The U.S. experiences in Afghanistan and Iraq serve as a cautionary tale for those contemplating the preemptive use of U.S. military forces to topple any regime, not to mention a nuclear-armed great power adversary.

---

<sup>33</sup> Mark Dubowitz, “Mapping Protests in Iran,” *Foundation for Defense of Democracies*, May 29, 2024. (<https://www.fdd.org/analysis/2023/01/27/mapping-the-protests-in-iran-2>)

<sup>34</sup> Fareed Zakaria, “On GPS: Does the US need a more confrontational China strategy?” *CNN*, April 28, 2024. (<https://www.cnn.com/videos/world/2024/04/28/gps-0428-former-trump-aide-on-china-policy.cnn>)

<sup>35</sup> Russell Hanson, Adam R. Grissom, and Christopher A. Mouton, “The Future of Indo-Pacific Information Warfare: Challenges and Prospects from the Rise of AI,” *RAND Corporation*, March 14, 2024. ([https://www.rand.org/pubs/research\\_reports/RRA2205-1.html](https://www.rand.org/pubs/research_reports/RRA2205-1.html))

An American offensive information warfare campaign in China, Russia, and Iran focused on exposing regime corruption, lies, and oppression<sup>36</sup> and ensuring the respective populations know the truth regarding their regime's foreign and domestic policies is different. More importantly, if Beijing, Moscow, and Tehran don't like having to fend off offensive information warfare operations in their respective countries, perhaps that could prompt them to assess whether it is in their interest to continue information warfare operations against the United States.

### *Some Final Thoughts*

China, Russia, and Iran are waging an information war against Americans with the goals of dividing Americans against one another, degrading our democracy, and deceiving us regarding our foreign policy interests. A major component of these adversary efforts is targeting our democracy and the confidence Americans have in our elections.

Our adversaries understand that free, fair, and trusted elections are the center of gravity for our democracy. That is why China, Russia, and Iran sought to undermine Americans' faith in the fairness and integrity of our democratic process this year. Thankfully, federal and state governments, the private sector, and the research community responded effectively in many cases, and our democracy proved resilient. But we should not be overconfident or complacent. We can expect adversary attacks to grow more sophisticated in the future. Additional steps are needed.

That begins with sounding the alarm for Americans so that we can build bipartisan unity and action to strengthen our electoral defenses. But that is not enough. We must also go on the offensive in the information domain to shift the cost-benefit analysis of our adversaries as they contemplate future attacks on our democracy.

Chairman Steil, Ranking Member Morelle, and distinguished members of this committee, thank you for the opportunity to testify on this important topic.

---

<sup>36</sup> "Executions Surge in Iran and Protests Persist," *Foundation for Defense of Democracies*, May 3, 2024. (<https://www.fdd.org/analysis/2024/05/03/executions-surge-in-iran-as-protests-persist>)