POLICY ALERT

28 October 2020

Target: US Society

In a press release on July 24, 2020, National Counterintelligence and Security Center (NCSC) Director William Evanina highlighted foreign threats to the 2020 US election, specifically focusing on China, Iran, and Russia's efforts to undermine US citizens' confidence in their government institutions. Influence measures on social and traditional media to sway US voters' preferences during a particularly contentious election year have been pervasive and diverse. However, we assess that foreign actors' efforts this election season are just the tip of the iceberg.

- Russia's persistent objective is to weaken the United States and diminish our global role, according to the NCSC press release. Russia uses numerous methodologies, including internet trolls and other proxies, to spread disinformation designed to undermine confidence in our democratic processes.

- In his 2017 testimony before the Senate Armed Services Committee's Subcommittee on Cybersecurity, the Rand Corporation's Rand Waltzman informed members that for Russia, information operations (IO) are a perpetual state. The Dictionary of Terms and Definitions in the Field of Information Security written by the Russian Military Academy of the General Staff explains that Russia considers IO as continuous, regardless of the state of relations with any government, while the West sees IO as a limited tactic to be used during hostilities.

Information warfare is complex, sophisticated, less expensive, and more effective at weakening Russia's adversaries than conventional warfare, and we judge that although Russia is focusing on continued modernization of its armed forces, it cannot match us or NATO in conventional strength and will increase its use of the less expensive IO to weaken its adversary.

- Russia's largest State Armaments Program (SAP), approved in 2010 and intended to modernize its military and spend billions of dollars on procurement of new armaments over a 10-year span, was stymied by declining oil prices (at the time the SAP was approved, the Russians counted on oil prices staying above $70 per barrel) and western sanctions. Moscow's new SAP aims to spend roughly $306 billion on military equipment procurement through 2027, and although the sum is approximately the same in rubles as Russia's previous SAP, inflation has kept Russia's modernization goals more modest.

- In an article published by the Brookings Institution, Alina Polyakova explains that the Kremlin is using the West as an external enemy to distract its citizens from the economic, military, and social problems plaguing Russia. "And this is why," she explains, "the Kremlin has launched a strategy of political warfare against the West in the form of disinformation campaigns, support for far-right political parties in Europe, cyberattacks, money laundering, and other tools of influence that allow Moscow to undermine its perceived adversaries at very little cost."

- According to Insikt Group analysis of disinformation pricing on Russian-speaking underground forums by two vendors, the price of disinformation campaigns in the West can cost thousands of dollars – much less than the cost of developing and deploying new weapons systems.

- ✓ $15 for an article up to 1,000 characters
- ✓ $8 for social media posts and commentary up to 1,000 characters
- ✓ $10 for Russian to English translation up to 1,800 characters
- ✓ $25 for other language translation up to 2,000 characters
- ✓ $1,500 for SEO services to further promote social media posts and traditional media articles, with a time frame of 10 to 15 days
- ✓ $150 for Facebook and other social media accounts and content
- ✓ $200 for LinkedIn accounts and content
- ✓ $350–$550 per month for social media marketing
- ✓ $45 for an article up to 1,000 characters
- ✓ $65 to contact a media source directly to spread material
- ✓ $100 per 10 comments for a given article or news story

Russia's disinformation campaign in the 2020 elections may appear contradictory on its face, but we assess that Moscow's efforts are consistent with its long-term strategy to use "active measures" adapted to modern technologies to sow chaos in western societies, weakening the public's confidence in their democratic processes, and damage the foreign policy and defense goals of the United States. Early in 2020, Moscow appeared to have focused on multiple candidates, first supporting Tulsi Gabbard, and later possibly meddling in the Democratic primaries to help Bernie Sanders. The intelligence community also assessed in August that some Kremlin-linked actors have a preference for President Donald Trump.

- Among traditional ways the Soviet Union, and now Russia, have used active measures is disinformation: leaking of false information and rumors to foreign media or planting forgeries in an attempt to deceive the public or the political elite in a given country or countries.

- Defectors have reported that the Soviet Union and its allies circulated forged documents—often purporting to be speeches, letters, or policy statements by United States officials—containing false information and used international front organizations and foreign communist parties to expand the Soviet Union's political influence and further its propaganda.

- The Rand Corporation describes Russian disinformation campaigns as a "firehose of falsehood" that does not target a specific candidate or ideology. Hundreds of Russian Internet troll accounts, many of which were created more than a decade ago, are focusing on divisive social issues to drive a wedge between Americans, their government institutions, and society writ large. The efforts are widespread, feeding Americans a barrage of false, misleading, manipulated information until fatigue sets in and the audience can no longer distinguish truth from fiction.

- In February 2020, amid panic about the coronavirus, the Russian disinformation machine swung into full gear to place blame for the outbreak at the feet of the United States. According to the WHO, conspiracy theories exploiting the fear of contagion are not confined to the dark corners of the Internet but are broadcast on news shows in the Russian mainstream media.

For fans of the show “The Americans,” the following scenario sounds all too familiar: Russian sleeper agents infiltrate American society and live among us for years using fake identities of people who had died years earlier, working to subvert US policy, turn Americans into Russian assets – both witting and unwitting – and gain an advantage over the United States. Today, sleeper troll accounts live among us in the cyber realm. They are part of our social media experience. They publish real hometown news stories to gain our trust, and when the time comes, they are activated and gradually begin to disseminate disinformation, exploiting the trust they have built with audiences over the years.

- In 2018, Twitter discovered dozens of sleeper accounts that were linked to Russia’s Internet Research Agency, many of them mimicking hometown news sites with names such as @Milwaukeevoice or @Seattle_Post, and Facebook that year found similar activity on its platform and removed dozens of pages that violated its community standards against “coordinated inauthentic behavior.”

- In September 2020, Facebook and Twitter removed several hundred additional fake accounts linked to Russian intelligence. The networks Facebook shut down targeted numerous countries around the world, according to the company’s Head of Security Policy. These entities created fictitious or seemingly independent media entities and personas to engage unwitting individuals to amplify their content and drive traffic to other websites controlled by these operations, tailoring their activities to each targeted audience.

- Twitter that month deactivated two networks of accounts that it attributed to Russian state-linked entities, with one linked to previous Russian hacking attempts, and the other promoting the same United World International website that Facebook said was connected to the Internet Research Agency.

Information warfare can cover a vast range of different activities and processes seeking to steal, plant, interdict, manipulate, distort or destroy information. Russian operatives use everything from computers to smartphones, social media, online troll campaigns, text messages, YouTube videos, and other means to impact our society, the way we process information, and the way we interact with our political leaders and even one another.

- According to NATO research, an adversary can achieve effective control of an opponent’s decision making is achieved by allowing him to logically derive his own decision, but one that is predetermined by the other side by shaping the opponent’s objectives and altering his decisionmaking algorithm.

Spreading disinformation to manipulate your adversary’s decision-making process is much more sophisticated than attempting to hack election software. Creating social media accounts and disseminating disinformation is less expensive than sending military hardware across an adversary’s borders. Allowing your adversary to believe that he is making the right decision based on misleading information provides more plausible deniability than hacking voting machines. Russia no longer needs to directly involve itself in active measures. It simply needs to pay a few savvy hackers and online operatives or use unwitting stooges to spread its disinformation and weaken its adversaries.