SAFEGUARDING THE PUBLIC

RUSSIAN INTELLIGENCE POSES A PERSISTENT THREAT TO THE UNITED STATES

THREAT

Despite Russia's substantial military losses since its February 2022 invasion of Ukraine, Russia's intelligence services (RIS) remain a formidable threat to the United States. In recent months, the U.S. government has sanctioned several Russian intelligence operatives and their associates for activities targeting the United States, and authorities across Europe have arrested and charged a number of suspected Russian spies in their nations. Even so, in public remarks in September 2023, FBI Director Christopher Wray warned the number of Russian intelligence officers operating in the United States is "still way too big."

The RIS and their proxies continue to target the United States through espionage, influence operations, and cyber activities while also seeking to degrade U.S. and partner support for Ukraine. The RIS target the U.S. government, commercial and private sectors to gain valuable information regarding U.S. plans and intentions, military and technology advances. They also target the American public to sow dissent in our society.

The RIS seek to achieve Russia's goals by using:

ESPIONAGE

The RIS recruit sources and agents to collect information on economic, political, security, and technological developments affecting Russia's interests. Russia continues to target a wide array of sectors to gain access to information and procure material of interest.

These targeted sectors include government entities, academic institutions and think tanks, non-governmental organizations and activist groups, international organizations, media entities, and high-technology companies.

Through existing professional accesses or networks, the RIS also seek out individuals sympathetic to Russia's causes to serve as collectors within organizations. The RIS reach out through both in-person meetings and online contact, often under the guise of seemingly innocuous professional or personal outreach, to individuals possessing insider knowledge of sectors of interest whom they hope to use as sources.

CYBER ACTIVITIES

The RIS target government, private sector computer networks, and individuals of interest to steal information, track individuals, and prepare for potential disruptive or destructive cyberattacks against critical infrastructure.

They exploit known and unknown software vulnerabilities, often taking advantage of weak security, including slow patching, poor configuration, weak passwords, and lack of two-factor authentication.

MALIGN INFLUENCE

Russia's malign influence efforts are ongoing and blend covert intelligence operations with overt efforts by Russian government agencies, state-funded media, third party intermediaries, and social media personas to sow and exacerbate division among the U.S. public and undermine democratic processes.

Russia seeks to use unwitting U.S. persons and others to propagate information intended to influence the public by forwarding, sharing, liking, or discussing unsubstantiated or misleading narratives, and by spreading stolen, leaked or fabricated information, amplifying the reach of the original information.

IMPACT

The RIS' persistent focus on targeting the U.S. public, private sector, academia, and other institutions is intended to:

- Obstruct U.S. policy goals and erode U.S. strategic advantage through the loss of sensitive U.S. government information, proprietary scientific research, and new technologies.
- Result in economic loss for individuals and U.S. companies through intellectual property theft.
- Weaken public trust in U.S. institutions; increase social divisions that weaken the U.S. domestically and internationally; and enhance support for Russia's preferred policy positions.

For additional information on NCSC awareness materials or publications, visit our website:

WWW.NCSC.GOV

or contact

DNI_NCSC_OUTREACH@DNI.GOV

Find us on Twitter (X):

@NCSCGOV

On LinkedIn:

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

MITIGATION

You are not helpless. These steps can help you, your organization, and your community be more aware of, and better prepared to defend against RIS efforts:

- Maintain Insider Threat awareness through workforce training and by implementing reporting mechanisms; engage in proper vetting of employees, students, and research networks as appropriate; visit the National Insider Threat Task Force resource page for more information.

  WWW.DNI.GOV/INDEX.PHP/NCSC-HOW-WE-WORK/NCSC-NITTF
- Enhance your organization's cyber posture; follow best practices for identity and access management, protective controls, and vulnerability management.
- Verify unsolicited professional outreach; evaluate the origin and professional networks surrounding the source of outreach.
- Evaluate the information source and narratives encountered online, in news media, and mass or social media; seek information from multiple sources; compare information across multiple media platforms.
- Beware of online personas whom you do not know or cannot verify who ask you to forward and post or otherwise spread information.
- Report suspicious activities or outreach by foreign-linked actors to your local FBI field office.

  WWW.FBI.GOV/CONTACT-US/FIELD-OFFICES

0030595