SAFEGUARDING THE U.S. DEFENSE INDUSTRIAL BASE AND PRIVATE INDUSTRY AGAINST SABOTAGE

OVERVIEW

The Russian government has been using its intelligence services to plan and conduct *sabotage operations*[a] targeting Europe's defense industrial base (DIB)—including private industry—in an attempt to undermine Allied support for Ukraine. Russia's sabotage activities in Europe increase the risk to U.S. companies abroad and potentially at home. Such sabotage operations can sow fear and doubt, damage important infrastructure, disrupt commerce, or cause injury and death. U.S. companies, particularly those supporting entities involved in the Ukraine conflict or other ongoing geopolitical conflicts, as a best practice should enhance their vigilance and security efforts.

THREAT

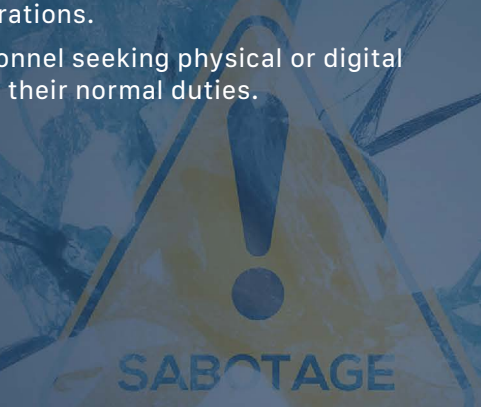
Over the last year, the Russian government and its proxies have planned and directed sabotage attacks against European military installations, foreign defense companies, logistics facilities, and public utilities in an effort to undermine Allied support to Ukraine. Russian intelligence services are recruiting criminals and other proxies to carry out attacks in Europe, and may also try to identify and recruit DIB insiders.

- **April 2024:** U.K. authorities charged several Britons for planning and conducting an arson attack on a Ukraine-linked business in London on behalf of Russian intelligence.
- **June 2024:** Polish authorities announced they had arrested 18 individuals over the past six months on charges including plotting arson and other acts of sabotage across Poland on behalf of Russia and Belarus. One of these fires destroyed a major shopping mall in Warsaw, requiring 200 firefighters to respond.

INDICATORS

Sabotage can involve several steps before actual attacks, including planning, preparation, surveillance, and recruitment. Some acts of sabotage are designed to hide the hand of the perpetrator, appearing to be accidents or equipment failures. Potential sabotage indicators to which you should be alert include:

- Explicit or implied threats to facilities or personnel. Such threats—communicated in person or online—may identify specific attack-planning details, including targets, timeframes, and participant roles.
- Online posts by individuals noting their intent to commit violence, or a direct threat with justification for action.
- Photographic or video surveillance, including drone or small unmanned aircraft systems operating near facilities, staff, or systems, or employees who bring unauthorized cameras, tools, or software into the workplace.
- Physical threats or intrusions, such as unusual loitering or entry attempts by unauthorized personnel, or trespassing and vandalism in and around the facility, which may indicate casing and perimeter security tests.
- Indications that outsiders are eliciting your organization's staff, including individuals contacting employees with requests for proprietary or sensitive information.
- Observed cyber attacks or successful network penetrations.
- Company personnel seeking physical or digital access beyond their normal duties.



[a] *Sabotage, as defined in 18 USC 2155 — is an action to "Intentionally injure, interfere with, obstruct, contaminate, infect, or destroy any national defense material, national defense premises or national defense utilities."*

MITIGATION

You are not helpless in the face of potential threats. Sabotage often hides in existing patterns of activity. Saboteurs look for targets of opportunity and exploit vulnerabilities. Your physical security, cybersecurity, and personnel security protocols can help detect, deter, and mitigate impact through steps such as these:

MAINTAIN KEY PARTNERSHIPS

- **Engage with law enforcement,** local responders, and appropriate intelligence agencies so that your organization stays informed about potential threats, receives guidance on best security practices, and responds effectively to incidents. Know your local and federal law enforcement contacts and familiarize them with your security and safety procedures.
- **Hold routine exercises** with local partners to practice and validate your incident response protocols.

ENHANCE YOUR SECURITY POSTURE

- **Provide regular training** on security awareness to your employees and emphasize the importance of reporting suspicious activities. Employees are your first line of defense.
- **Ensure your physical security, cybersecurity monitoring, and surveillance** of the key nodes in your system can spot potential disruptions. Sabotage can include both physical and cyber components.
  - For additional guidance on mitigating malicious cyber activity, please see the NSA, FBI, CISA and Allied Cybersecurity Advisory "Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure."
- **Identify your most important assets** and prioritize their protection with layered security measures.
- **If you see suspicious activity, report it immediately.** Develop an "anomaly" log to track unusual or suspicious incidents, whether physical or virtual, for security and safety purposes.

BOLSTER PERSONAL SECURITY

- **Personnel can also take steps to improve security practices.** Be mindful of what you post on social media. Those involved in work tied to Ukraine or other geopolitical conflicts should be cautious about disclosing work, travel, personal, and family information online. Adversaries can use this information to identify access, location, and personal vulnerabilities.
- **When traveling abroad,** check the U.S. State Department website at **https://www.state.gov** for travel advisories and monitor current events in the location of your visit. Consider enrolling in the U.S. State Department's Smart Traveler Enrollment Program (STEP). Ensure someone in the U.S. has your travel itinerary and establish check-in times throughout the trip. Do not travel with devices containing sensitive information, and practice good cyber hygiene when using devices abroad.
- **Do not share detailed information** about yourself, family or associates with any individual who has shown an unusual interest in them.
- **Vary routes to and from work** and pay attention to surroundings at home, enroute, and upon arrival at work. Report suspicious incidents to company security and supervisors, and contact your local law enforcement if you feel in danger.
- You can find more tips on personal safety, identifying elicitation, and safe travel protocol at **https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-know-the-risk-raise-your-shield/ncsc-awareness-materials**

BUILD RESILIENCE AND REDUNDANCY INTO YOUR OPERATIONS

- **Diversifying and enhancing the security of your supply chain,** including through due diligence on suppliers and subcontractors, can reduce the impact of potential compromises. These efforts can aid in recovery and deter the saboteur by decreasing the effectiveness of a sabotage attempt.

REPORTING

- If you believe your organization or its operations have been targeted by malicious actors or are at risk of sabotage, contact the Private Sector Coordinator at your local FBI Field Office: **https://www.fbi.gov/contact-us/field-offices**. If you are concerned with an immediate threat to your facility, **call 9-1-1.**
- Report significant cyber incidents to the Cybersecurity and Infrastructure Security Agency (CISA) Incident Reporting System (IRF) at **https://myservices.cisa.gov/irf.** CISA Central provides a critical infrastructure 24/7 watch and warning function and gives all critical infrastructure owners and operators a means to connect with and receive information from all CISA services. Contact CISA Central via phone: **1-844-Say-CISA (844-729-2472)** or email **SayCISA@cisa.dhs.gov**. Additional information is available online at **https://www.cisa.gov/about/contact-us**.
- Cleared contractors should follow reporting requirements per *Code of Federal Regulation (CFR) 32 Part 117, National Industrial Security Program Operating Manual (NISPOM).* For additional information, visit DCSA at **https://www.dcsa.mil,** DCSA Counterintelligence & Insider Threat at **https://www.dcsa.mil/mc/ci,** and *CFR 32 Part 117* at **https://www.ecfr.gov/current/title-32/subtitle-A/chapter-1/subchapter-D/part-117.**
- For more threat awareness materials or publications, visit the National Counterintelligence and Security Center (NCSC) website at **https://www.ncsc.gov** or contact **NCSC_Outreach@odni.gov.**
- Follow NCSC on Twitter (X) **@NCSCgov** and LinkedIn at **https://www.linkedin.com/company/national-counterintelligence-and-security-center** and FBI on Twitter (X) **@fbi,** LinkedIn at **https://www.linkedin.com/company/fbi,** and Facebook at **https://www.facebook.com/FBI for more information.**