APRIL 2026

Deterring, Detecting, and Mitigating Insider Threat During Emerging Global Conflict

BTAC BULLETIN
BEHAVIORAL THREAT ANALYSIS CENTER

SPECIAL ISSUE

Potential Rationale(s) for Insider Threat Actors

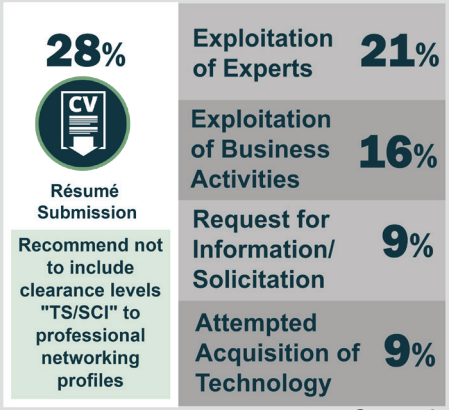
During Emerging Global Conflict

An individual's progression along the Pathway to Intended Violence[1] or the Critical Pathway to Insider Risk[2] is often fueled by personal and organizational grievances and stressors. Global conflict introduces new complexities that may amplify organizational risks beyond typical concerning workplace behaviors. This may result in moral conflicts for employees who feel personal, political, cultural, or religious connections, perspectives or obligations, which differ from their organization. Sophisticated adversaries may seek to leverage developing grievances to influence employees and encourage polarization with the larger goal of disrupting Department of War (DoW) capabilities, Defense Industrial Base production, or public infrastructure, among others. If employers do not recognize and assess these stressors, an individual's progression toward violence, sabotage, espionage, or unauthorized disclosure can be accelerated. Therefore, it is critical to have capabilities in place to deter, detect, and mitigate these risks, as historical data indicates a clear correlation between increased media reporting on geopolitical conflicts and a rise in unauthorized disclosures. During these times, InT programs should refine user activity monitoring (UAM) triggers and collaborate with OPSEC and INFOSEC stakeholders to implement enhanced controls on conflict-related products.

Global uncertainty can result in feelings of uneasiness, anxiety, depression, fear, and anger and can exacerbate stress including in the workplace. This psychological impact has the potential to increase unintentional acts of Insider Threat (InT) through human error such as security violations and unauthorized disclosures. Additionally, the psychological impact may contribute to workplace conflict, decline in performance, development of grievances, and the development or exacerbation of preexisting mental health difficulties.Individuals struggling may deviate from their baseline behavior by withdrawing, appearing distracted, missing deadlines, or becoming more confrontational or passive than normal.

Supervisors play a critical role in maintaining a healthy workplace. Leaders should remain attentive to changes in employee behavior, performance, or engagement and address concerns early through supportive and respectful conversations. Creating a culture of psychological safety is essential. Employees should feel comfortable raising concerns, asking for assistance and using available resources like Employee Assistance Programs (EAPs), behavioral health services, and Equal Employment Opportunity without fear of stigma or negative consequences.

METHODS OF OPERATION



Source 3

As geopolitical tensions continue to evolve, DoW employees should be aware that foreign intelligence services sometimes use deceptive tactics to target individuals with access to sensitive information. One common approach is the use of fraudulent job postings on professional networking sites. These opportunities may appear legitimate but are designed to gather information about your role, the technologies used in your workplace, your organization's structure, or simply to start a relationship that could later be exploited.

WATCH FOR RISK INDICATORS

- IT use behavior (e.g. access request outside scope of duties, excessive printing, file up/ download increase to personal accounts)
- Unusual Foreign Contacts / Travel
- File modification (e.g. deceptive renaming, changing type (extension), or removing keywords to avoid detection)
- Stated support or preference for adversary goals or positions

LEADERSHIP MITIGATION STRATEGIES

Engage & Communicate

- Engage privately and listen closely if concerns arise
- Utilize "difficult conversation" skills
- Discuss specific events and avoid inflammatory language
- Clarify policies and expectations

Secure & Educate

- Reiterate rules on social media and remind DoW personnel of their responsibility not to post comments or material that denigrates another military or civilian member of the DoW team.[4]
- Conduct briefings on recognizing propaganda
- Balance vigilance for employee privacy and rights

Report & Consult

- Cultivate a "see something, say something" culture
- Leverage organizational partners, such as human resouces, legal, and security for support
- Protect information and report unsolicited contacts

REPORT INSIDER THREAT BEHAVIOR

Report insider threat behavior to: leadership, security office, component insider threat hub/ program, local law enforcement, and/or Federal Bureau of Investigation (FBI).

1. Calhoun, F.S. & Weston, S.W. (2003). Contemporary threat management: A guide for identifying, assessing, and managing individuals of violent intent. San Diego, CA: Specialized Training Services. 2. Shaw, E., & Sellers, L. (2015). Application of the critical-path method to evaluate insider risks. Studies in intelligence, 59(2), 1-8. 3. DCSA. (2025). 2025 Targeting U.S. Technologies: A Report of Threats to Cleared Industry. https://www.dcsa.mil/Portals/128/Documents/CI/DCSA-TA-26-001%20Targeting%20US%20Technologies%20FY25.pdf 4.U.S. Department of Defense. (2021, August 24). Online Information Management and Electronic Messaging (DoDI 8170.01). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/817001p.pdf