Forum for American Leadership

Recent Leaks of Intelligence: Causes, Implications, and Steps to Mitigate Future Leaks

May 11, 2023

The recent leak of highly classified documents revealed information potentially damaging to U.S. national security—information that should remain classified because of the risk it has for national security, U.S. persons, and our allies and partners. While this brief will not repost the contents of the documents or comment on their authenticity, it will discuss the consequences of this leak and others before it, and recommend ways to better protect classified information.

The Most Recent Leak and Others Before It

On April 14, 2023, U.S. Air National Guardsman Jack Teixeira was arrested for removing classified documents from a secured work environment and exposing them to the public. The leaked documents initially appeared on a small, now-shuttered Discord server and spread to other servers, as well as on other platforms such as Telegram. In the age of the Internet, leaks can spread virally through social messaging services, illustrating how quickly the damage can metastasize. The documents allegedly contained highly classified information across a wide range of national security issues stemming from the Department of Defense's daily intelligence reports. According to media reports, Teixeira's motivation appears to have been "teaching" the other young people in the small Discord group about national security threats and proving the access he had.

There have been several well-known and publicized intelligence leaks. In 2017, a former Air Force service member and National Security Agency (NSA) translator, Reality Winner, was arrested and charged for providing a classified report to the website The Intercept. Winner was found guilty of leaking the documents to a media organization, spent four years in prison, and was released on probation in 2021.

In 2013, Edward Snowden leaked an enormous tranche of intelligence documents to the *Guardian* and the *Washington Post* revealing the inner workings of the National Security Agency. The U.S. government charged Snowden with espionage and theft of government property. Snowden first fled to China then eventually gained asylum in Russia, where he now lives in exile. The estimated damage from the Snowden leaks ranged into the billions of dollars.

In 2010, then Army Private Chelsea Manning gave Wikileaks 700,000 classified documents from the U.S. military and the State Department, which included videos and diplomatic cables that appeared on the Wikileaks website. Allies and adversaries alike used the leaks to criticize U.S. policy, and U.S. government leaders repeatedly commented on how much damage the leaks had done to U.S. relationships around the globe. Manning spent seven years in prison.

Additionally, recent espionage cases have dealt a significant blow to US national security and intelligence operations. In 2019, a former CIA case officer, Jerry Chun Shing Lee, was sentenced to 19 years in prison for conspiring to provide American intelligence secretes to the Chinese government. Also in 2019, Kevin Patrick Mallory, another former CIA officer, was sentenced to 20 years in prison for transmitting national defense information to a Chinese intelligence officer.

Implications

Consequently, these leaks and espionage cases have given adversaries a window into U.S. collection capabilities and assessments, have put persons in jeopardy, and impacted the relationships and trust of our allies and partners. Further, this revelation of intelligence can lead to the discovery of intelligence collection methods, which can undo thousands of man hours and ultimately millions of dollars of government funding that went into the targeting development and execution of operations, which both increases the safety risk to persons involved and can set back American policymakers' knowledge of the issues collected. The political damage for these events also is incalculable, particularly as Ambassadors' trust with their host governments is undermined, complicating their ability to achieve diplomatic objectives. Foreign governments may determine not to share certain information with us, if they view that this information could be made public and put them under internal domestic scrutiny.

In the aftermath of these leaks and espionage cases, congressional and inspectors general investigations were launched to determine how our national secrets could have been so vulnerable. Unsurprisingly, the most recent leak spurred letters from members of Congress, who are pressing the Department of Defense for accountability and answers regarding the unauthorized disclosure of classified materials. The Chair and Vice Chair of the Senate Intelligence Committee have called for more oversight of intelligence activities and will examine how the Intelligence Community updates individuals' security clearances and new measures for the classification of intelligence.

Perpetrators often have personal or financial motivations for leaking or conducting espionage. In the case of the 21-year-old Air National Guardsman—he appeared to be motivated by ego, desire for acceptance among peers, and perhaps ideology. These are classic red flags for investigators, but it is difficult to quickly identify changes in the mental state or personal interests of someone with access to classified information. To prevent future leaks and reduce the exposure if they do occur, the entire U.S. Intelligence Community (IC) must do better and continue to refine intelligence security practices and processes.

Recommendations

1. **Verify who has a Need-to-Know**: The U.S. government should look at how widely some intelligence is shared internally and make sure that people who do not have a need-to-know information no longer have access to it. There should be a mandated regular review of distribution lists and examination of procedures governing how widely some of the most sensitive secrets are shared. The Pentagon announced that "there have been steps to take a closer look at how this information is distributed and to whom," and since the leak, media has reported that some U.S. officials who used to receive certain highly classified intelligence briefs have stopped receiving them. This is not a DoD problem alone, as most government agencies and departments, including the legislative branch, have access to intelligence reporting and analysis, suggesting a broad review of access to information is important. There should be stricter access controls over who has access to intelligence products and who can download or print them. For example, while an analyst writing across multiple mission sets may need access to a wide range of classified reports and assessments, an IT technician working on system engineering probably does not need regular access to highly classified information.

2. **Beef up Insider Threat Programs**: Updated security policies and behavior-based procedures to monitor unusual or unauthorized use can reduce the risk surface. A combination of processes and technologies combined with the necessary analytical resources to develop behavioral or anomaly-based information security capabilities are needed to detect and prevent data leaks by authorized insiders. While agencies like the FBI and CIA require polygraphs for all employees hired, and again throughout their careers during periodic reinvestigations, polygraphs are not mandatory for all other agencies and departments. Additionally, programs designed to catch disgruntled employees who might want to steal information and weaponize it for financial or political gain are not foolproof either. It may be time to monitor publicly available online activity of those with high-level clearances to see if there are major changes in behavior that warrant a deeper investigation.

3. **Use New Technologies for Detection**: Using big data and artificial intelligence/machine learning, the IC should consider new ways to track access and downloading of information on computer networks to provide a tip off on whether there are anomalies occurring in a user's pattern of behaviors on secure systems that warrant further investigation. For example, if a user suddenly accesses certain classified information that is not in their "need to know" or prints large amounts of information on an issue area that would not normally be in his or her daily practice, that could be flagged as suspicious for monitoring.

4. **Refrain from Reposting Unauthorized Disclosures of Classified Information**: Leaks of classified documents by those with a clearance are a criminal act, punishable by law, and U.S. government employees will be reprimanded for publicly confirming or speaking about leaked information. DoD employees received guidance after the most recent leak to not read or download documents that have appeared in the media or online because "[they] remain classified and should be treated as such." At the same time, we should all be good stewards of this practice and mitigate the risk of the unintended disclosure of classified information, and this is particularly salient for those with a clearance. Additionally, without the full context of the leaked information, U.S. leaders should explain to the public the span and scope of what they are seeing to reduce the risk of misinformation of government information and programs to the public.

5. **Avoid Overcorrection**: Finally, and probably most importantly, while these leaks are damaging and terrible, they should not prevent the massive amount of good work and necessary access that most intelligence officers have and continue to need to have for their job. Going back to the day where information was stove-piped or creating new processes that make it too difficult for intelligence officers to do their jobs in often intense and urgent environments could lead to even more unintended failures. An overcorrection of countermeasures would only add more bureaucratic challenges to an already overburdened process. To this point, ensuring strong security hygiene and proper procedures that are continuously being overseen and enforced by supervisors will help ensure that intervention can take place ahead of any unauthorized disclosures of classified information.

This paper is a product of the Forum for American Leadership's Intelligence Working Group.

The Forum for American Leadership (FAL) is a non-profit organization that presents expert analysis and national security recommendations to policymakers in Congress and the Executive Branch.