Guest view

The human factor in America's security systems

By Frank G. Splitt

The Daily Herald
Opinion, May 15, 2023

The discoveries of classified documents at former President Donald Trump's Mar-a-Lago estate, at President Joe Biden's former office and Delaware garage, as well as at former Vice President Mike Pence's Indiana home were troubling. They revealed a cavalier attitude toward classified documents by elected officials at the highest level of our nation's government -- certainly not the best examples for others in government and the military charged with safeguarding America's secrets.

Even more troubling have been the intelligence leaks by untrustworthy individuals: the FBI's Robert Hanssen, WikiLeaks' Julian Assange via the U.S. Army's Chelsea Manning, National Security Agency contractor Booz Allen Hamilton's Edward Snowden and Harold Martin III and now the alleged leaker, the Massachusetts Air National Guard's Jack Teixeira.

This image made from video provided by WCVB-TV, shows accused document leaker Jack Teixeira, in T-shirt and shorts, being taken into custody by armed tactical agents on April 13 in Dighton, Massachusetts.

The latest leak is considered to be one of the largest, most wide-ranging military and intelligence breaches in U.S. history with potentially devastating consequences in terms of CIA lives lost, informants compromised or killed, lost trust by U.S. allies, compromised battle plans, the exposure of U.S. counter-intelligence cyberweapons and all the more that is still unknown.

It is beyond my comprehension how the leak suspect Teixeira was able to receive and maintain a top-secret clearance, in spite of his history of making comments about shootings and violence.

Furthermore, how could a low-level IT support technician gain access to highly classified information without a need to know? Something is awry. Why so? It would have been anathema to me, my colleagues and to the government officials to whom we reported during the 1956-1964 time period when we were actively engaged in very highly classified research and development on a variety of military systems that were critical to national security.

To put this time period in perspective, it spanned the presidencies of Dwight Eisenhower, John Kennedy and Lyndon Johnson.

This was also the time when America was in the midst of a Cold War with Russia and, as so-called scientific Cold Warriors, we felt a patriotic duty to handle work-related classified research documents with the utmost care and respect. So sensitive was the nature of the R&D that security clearances, with levels ranging up to Top Secret/Cryptographic "Eyes only," were necessitated with each step up the security ladder demanding ever more arduous scrutiny of my personal, financial, academic and professional life.

How tight were security measures at the time? Consider the following: The security officer who was responsible for oversight of our Tech Center could not enter my crypto-secure office because he did not have the required "need to know," notwithstanding the fact that he was a former FBI agent with a top-secret clearance.

As a consequence of the recent leak, we have lost countless millions of our nation's secrets and counter-intelligence cyberweapons while living at a time perhaps even more dangerous than that of the Cold War.

This situation prompts the following question: What is going on with America's inability to securely transmit and retain highly classified information and what can be done about it? To answer the question we need to identify points of vulnerability to information leaks in a communication system designed to be secure from leaks of information to unintended individuals via encryption codes that are essentially unbreakable.

Such systems are commonly known as COMSEC systems. Ideally, these systems should deny transmitted information access to individuals without a need to know.

Nevertheless, COMSEC transmissions are vulnerable to information interception because of human factors, specifically untrustworthy individuals who have been granted security clearances.

Apparently some of these individuals have been able to gain access to unencrypted information at the source and decrypted information at its destination. Intermediate points of access to the transmission may also be available to these individuals. Such individuals as, for example, Air National Guardsman Teixeira, could also have access to transmission decryption keys.

Thus, COMSEC system vulnerability can obviously be traced to humans and gross deficiencies in the procedures used by the government agencies responsible for granting security clearances and follow-up vetting to maintain those clearances. So too, strict attention needs to be paid to minimizing the granting of “need-to-knows” as well as to eliminating access to decryption keys by network technicians.

The pool of today's candidates for security clearances have come and are still coming, from quite a different America than existed during 1956-1964. That period, in my view, was a time when America's citizens were relatively more patriotic and morally grounded. Today's citizens seem grounded in technology and social media that is rife with conspiracy theories and falsehoods -- seeding further consequential rifts in our politically divided country.

One such consequence was the unprecedented assault on the U.S. Capitol by paramilitary and other hate groups. Now is a time when, for some, it is more important to gain prestige and/or maintain political and personal power than it is to safeguard our national interests.

Therefore, it should come as no surprise that untrustworthy individuals might possibly hold security clearances in government and military service while still others will be put forth to seek security clearances. Clearly, there is an urgent need for more stringent background investigations coupled with periodic vetting of all individuals holding high-level security clearances by a responsible government agency that must be held accountable for any further breaches of security.

Costly though it may be, it's the price that must be paid to help minimize the vulnerability of America's security systems.

Frank G. Splitt
Photo by Julia Wenzelman

Frank G. Splitt, of Mount Prospect, was a McCormick Faculty Fellow of Telecommunications at Northwestern University's McCormick School of Engineering and an Emeritus Vice President of Educational and Environmental Initiatives at Nortel Networks.