Wikileaks Vault 7: CIA's Operations Security Apocalypse

The Agency is paying for its unwillingness to take OPSEC seriously

> A nation can survive its fools, and even the ambitious. But it cannot survive treason from within. An enemy at the gates is less formidable, for he is known and carries his banner openly. But the traitor moves amongst those within the gate freely, his sly whispers rustling through all the alleys, heard in the very halls of government itself. For the traitor appears not a traitor; he speaks in accents familiar to his victims, and he wears their face and their arguments, he appeals to the baseness that lies deep in the hearts of all men. He rots the soul of a nation, he works secretly and unknown in the night to undermine the pillars of the city, he infects the body politic so that it can no longer resist. A murderer is less to fear. — Marcus Tullius Cicero

Unlike most of the public, my initial reaction to Wikileaks release of documents detailing CIA's cyber-spying was not one of shock at CIA's vast hacking capabilities. As a former intelligence officer, I was not surprised by the breadth of CIA's capabilities, what shocked me, was the depth of CIA's counterespionage incompetence. I was aware of existing gaps in CIA's Operations Security (OPSEC), but I had never dreamt CIA security was so broken we would witness a counterespionage failure of this scope, one that places Edward Snowden in the Junior Varsity league of intelligence leaks, and renders Chelsea Manning almost inconsequential by comparison. But on March 7, 2017, the unimaginable happened as Wikileaks began publishing details of CIA's cyber-spying capabilities, a stunning acquisition by Julian Assange.

https://twitter.com/wikileaks/status/839100679625060353

It would be misleading to say I did not see the potential for a counterespionage disaster of biblical proportions brewing at CIA, in part because as a CIA Whistleblower, I have unintentionally become part of CIA's failed OPSEC narrative. I have witnessed CIA treat OPSEC with a disdain that is remarkable for an agency considered paranoid about OPSEC by many in the Intelligence Community, who are on the outside looking in. I was once one of those people looking in at CIA from the outside, as an analyst at the Defense Intelligence Agency (DIA), from 2006 until I transferred to CIA in the summer of 2009. DIA taught me OPSEC. From my initial training in DIA's "Tomorrow's Intelligence Professionals" to my deployment to Iraq with The Joint Special Operations Command, I learned good OPSEC could mean the difference between life and death. I also witnessed what I perceived to be the paranoia of CIA analysts, who refused to share intelligence with DIA and others in military intelligence. I mistakenly thought the behavior of CIA analysts was indicative of CIA's strong OPSEC culture. I naively assumed CIA's OPSEC posture was much stronger than what we had at DIA and in the military community. At the time, I had no idea CIA took a laxer approach to OPSEC than DIA. I did not understand that the pushback I had

experienced during my deployment to Iraq was simply bureaucratic game playing by CIA analysts who cared more about preserving their diminishing position in the intelligence community than seriously countering terrorism.

I would not understand CIA's contempt for OPSEC until I arrived at Langley on July 5, 2009 as a Clandestine Service Trainee. I would not grasp the extent of CIA's non-existent OPSEC posture until I found myself in the middle of a CIA Security debacle barely three months later, beginning in late-October of the same year. After a fellow Clandestine Service Trainee made spurious allegations against me, CIA's Office of Security began treating me as a mole within the CIA's ranks. The ineptness of CIA's Office of Security in my case illustrates why CIA has been unable to detect the real moles burrowing their way into the Agency's most closely guarded programs, expressly, CIA's biases lead it to focus on the wrong employees as potential threats. To make a long story short, in October 2009, CIA committed me against my will to Dominion Hospital in Falls Church, Virginia. At Dominion, psychiatrists acting on behalf of CIA's Office of Medical Services, detained me, interrogated me, and attempted to force me to take anti-psychotic drugs, all in the name of proving I was a threat to national security whose Top Secret Clearance should be revoked.

There was one significant problem with CIA's conduct: I was an undercover officer, and CIA Security and Medical Officers leaked highly classified information in zealous pursuit of their objective — proving I was a national security threat. These officers openly and proudly refused to follow basic OPSEC procedures, calling me paranoid and mocking me when I resisted their brazen disregard for protecting classified information. They insisted I speak to them on unsecured phone lines and they transmitted classified materials about my case via unsecured mail, email and fax. CIA Security and Medical Officers revealed my classified identity to Dominion Hospital Staff and Washington, DC police officers, in violation of the Intelligence Identities Protection Act of 1982. The ultimate shock to my OPSEC sensibilities would come when CIA psychiatrist Mary Newman along with psychiatrists Richard Roth and Gary Litovitz at Dominion Hospital, labeled me psychotic, citing my unwillingness to compromise on basic OPSEC procedures as a symptom corroborating the false diagnosis they gave me. I was appalled and continue to be appalled by the ignorance CIA employees have displayed of basic OPSEC. At the time, I was fighting CIA's unrelenting attacks on my civil rights, trying to keep my head above water, and could not invest much time or effort in confronting the issue.

Almost eight years later and CIA's OPSEC posture has not changed. A little over two years ago, CIA Security informed me that I had classified material at my residence in Spain, but refused to provide me with a legal and secure way to return these materials to them. While writing a memoir about my experiences at CIA, CIA's Publication Review Board never provided me with a secure manner to deliver my manuscript, instead demanding I send potentially classified materials via my Gmail account. CIA emailing me to inform me that something I had submitted via Gmail for pre-publication review was classified became routine. Keep in mind, CIA's emails always came after

what they claimed was classified information had already been compromised. Why was the information compromised? Because CIA had directed me to send documents containing potentially classified information to them in an unsecure manner, most commonly via Gmail. CIA has continued to rebuff my requests to set up a more secure means to communicate. When my Chromebook with a copy of my memoir was stolen from my hotel room in Paris on Christmas Day in 2014, CIA refused my entreaties to speak to them about an obvious security breach. A month later, CIA would write me at my address in Spain, informing me significant portions of my memoir was classified. Whoever stole my computer, by CIA's own admission, had gained access to significant amounts of classified information. But to CIA, this was a non-issue.

After CIA informed me that I had classified information at my overseas residence, their Security Officers directed me to return it to them via international mail for destruction. In keeping with CIA's total disregard for anything related to information security, there was a problem with CIA's proposal. Namely, placing classified material in the mail, international or domestic, is illegal because it is not a secure means to transport sensitive material and risks exposing classified material to our adversaries. When I refused to comply with their unlawful order, CIA Security Officers berated me, including James in CIA's Security Operations Center (SOC), who identified himself as CIA management, calling me a hypocrite for refusing to violate US espionage laws. James also invoked the name of CIA's Director of Support, Jeanne C. Tisinger, saying she had personally approved me shipping classified documents via an international carrier.

I have digital recordings of my interactions with staff in the SOC and other CIA support personnel. I began making these recordings in response to the extraordinary ways in which they were ordering me to mishandle classified material. The fact that I was able to digitally record CIA Officers making incriminating statements, speaks volumes to their unawareness of basic OPSEC. I could write a book on the OPSEC failures I have lived through dealing with CIA personnel, a book that would shock the conscience of anyone familiar with the basic countermeasures necessary to protect highly sensitive intelligence information. With all of this background, upon reflection, the shock I initially experienced upon learning of CIA's historic counterespionage failure was unwarranted. The real surprise is given CIA's sloppy approach to OPSEC, this counterespionage disaster did not occur sooner.

My experience is not an isolated incident, over the years there have been several widely reported cases of CIA's inability to protect highly sensitive material. In 2011, CIA compromised the identity of several of its agents reporting on Iran by using poor OPSEC while allegedly conducting meetings at a Pizza Hut in Lebanon. These spies were CIA agents targeting Iran and Hizbollah.

CIA's poor OPSEC also led the Italians to detect the Agency's illegal rendition of one of their

residents, Abu Omar, a Muslim Cleric in Milan. What led the Italian's back to CIA? CIA's poor OPSEC. CIA Operations Officers used their cell phones and credit cards in a manner that allowed Italian authorities to systematically unmask their identities.

As someone whom CIA labeled "paranoid," "delusional," and "psychotic," for attempting to follow basic security procedures, although I was initially surprised by CIA's monumental loss of highly classified materials related to its Cyber Intelligence program, in retrospect, I certainly understand how it happened. Julian Assange's analysis of CIA's breathtaking loss of classified information is dead-on when he says, "This is an historic act of devestating incompetence to have created such an arsenal and stored it all in one place and not secured it."

https://twitter.com/wikileaks/status/839133866002681856

The most damning part of Wikileaks massive disclosure was not CIA's hacking capabilities, (although to the general public, it understandably is…) but the fact that someone was able to exfiltrate this amount of information from CIA's protected network, under the nose of CIA's Office of Security and counterespionage personnel. Anyone who has worked in intelligence knew CIA had an advanced ability to hack into our electronic devices, we can assume the Chinese, Russians and other sophisticated intelligence services do as well, which is why OPSEC has always been fundamental to the effective operation of intelligence services worldwide. Since leaving CIA, I have always assumed the US government and/or other actors have compromised my computers and other devices, and acted accordingly. The documents released by Wikileaks show CIA was doing exactly what we would expect them to do: researching, developing and refining methods to go after their worldwide targets. During an interview in 2012, then CIA Director David Petraeus explained the Agency's goals with regards to our everyday electronics, saying, "Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters — all connected to the next-generation internet using abundant, low-cost, and high-power computing." What we have today, is confirmation that many of the things Petraeus alluded to in 2012, and much more, have become a reality at Langley.

The real story here is how CIA lost control of such a significant amount of information and why post- Edward Snowden (Snowden as we know him would not exist had CIA not granted him a clearance, handing him the keys to the Intelligence Community kingdom), CIA is still relying on the same antiquated security procedures for vetting current and prospective employees and securing its information. Why hasn't CIA caught up with 21st century technology? I knew CIA was at risk based on my personal experience with CIA Security Officers who did not have a basic grasp of OPSEC, Information Security or Information Technology. During the intervening years, I have written to the Federal Bureau of Investigation, the chairmans of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, and many others about

CIA's untenable OPSEC posture. My warnings have fallen on deaf ears…and today, CIA is confronted with ostensibly the largest loss of sensitive intelligence in its history.

Will CIA reform its security apparatus? I will be surprised if it does. I am tempted to laugh and say, "I told you so."…I must admit, I am relishing the pure, unadulterated schadenfreude of this moment. After all CIA put me through, I deserve it. At the same time, as a former intelligence professional, I understand the importance of secret intelligence to the preservation of our democracy. The Intelligence Community cannot sustain these continued losses and remain effective. The question remains, when will the Intelligence Community begin to take security reform seriously? If it continues along the same path, these losses will occur with increased frequency, as would be "copycat" leakers are emboldened by others' successes, creating a cascade effect. CIA can do amazing things with technology, nevertheless, CIA's adversaries can undermine CIA in amazing ways using that same technology. On March 7, 2017, CIA's defenses suffered a stunning defeat at the hands of a formidable asymmetric adversary, Wikileaks. Only time will tell if CIA is willing to do what is needed to recover from this devastating and unprecedented loss. CIA and the entire Intelligence Community would do well to heed the words of Cicero as they move forward following the latest catastrophic attack from within.