Safeguarding "By, With, & Through" in Strategic Competition: A SOF CI Professional's Perspective

Michael W. Parrott

> Insider threats tear the fabric of trust built between partner forces.

Introduction

U.S. Special Operations Forces (SOF) across the globe often integrate into their operational environment by facilitating partner force engagements through a comprehensive approach that accomplishes the mission at hand. This "by, with, and through" concept is an essential part of America's diplomatic and military power projection. Nowhere is this more evident than in strategic competition, which requires leveraging relationships with allies and partners, to contend with challenges from other states and actors that include the People's Republic

MICHAEL W. PARROTT

Michael W. Parrott serves as the Special Operations Forces Counterintelligence (CI) Integration Course (SCIC) Director at the Joint Special Operations University (JSOU), MacDill Air Force Base, Florida. He is responsible for the development, execution, and instruction of joint force special operations curriculum. He served as a U.S. Army Counterintelligence Technician and Chemical, Biological, Radiological & Nuclear (CBRN) Defense professional prior to his retirement after 24 years of service to the nation. He is a former special operations intelligence management professional. His work has appeared in the Tip of the Spear magazine, the Simons Center's Interagency, and Military Intelligence Corps Association's Vanguard journals. Parrott holds a Master of Arts degree in Strategic Security Studies from the College of International Security Affairs at the National Defense University, a Bachelor of Arts in Homeland Security with a concentration in Terrorism Studies from the American Military University, and an Associate of Applied Science Degree in Intelligence Operations.

of China (PRC), Russia, Iran, and Violent Extremist Organizations (VEO). However, contemporary SOF partner engagements can trace their lineage back to the Office of Strategic Services (OSS) during World War II.[1] The OSS explored the use of partisan forces (like the French Underground, but also similar efforts in many other places) to disrupt, deny, and exploit the Axis Powers. In working with resistance forces, OSS officers quickly discovered the dangers of what is commonly referred to today as “insider threats.”

Insider threats tear the fabric of trust built between partner forces. Trust is not just an essential element for all SOF engagements; it is both the metaphorical and literal lifeblood for these partnerships as U.S. and Coalition forces learned in Afghanistan. In 2012, insider or “green-on-blue” attacks accounted for 15% of coalition force deaths.[2] Again, in 2019, green-on-blue attacks resulted in 172 killed and 85 wounded in 82 separate incidents perpetrated by Afghan soldiers and Taliban infiltrators.[3] In addition to lessons learned by the OSS, today's SOF must not abandon lessons learned from the past 20 years of counterterrorism. Instead, SOF must preserve these lessons and innovate new approaches to confront a more sophisticated insider threat challenge posed by strategic competitors.

The contemporary insider threat challenges SOF are faced with in partnering environments are not unique to special operations; insider threats discussed here can affect businesses, commercial entities, academia, and government institutions. However, the lessons to be learned from historical retrospection and ways to prepare and protect SOF members and their families now and in the future can also help leaders and security professionals in other industries. Many of the lessons and recommendations outlined below can be applied more broadly by insider threat professionals in various sectors; the concepts apply to all organizations…government or civilian. Nevertheless, this article will focus predominately on the SOF nexus, while yielding helpful options for dealing with insider threat dilemmas outside the enterprise.

Contemporary Insider Threat Challenges

As USSOF prepares to train Mexican SOF members in 2024, the threat of attacks by cartel infiltrators or assets within the partner force continues to pose a similar threat to insider attacks in Afghanistan by co-opted Afghan security forces and partner force members. The costs can be very high, as demonstrated by a 2019 insider attack in which "a Taliban infiltrator killed 23 Afghan National Army soldiers in their sleep."[4] SOF were not immune to such attacks. In early 2020, members of 7th Special Forces Group (7th SFG) and allied Afghan Special Operations Forces were conducting a key leader engagement with influential figures in the Sherzad district of Nangahar province. The post incident report indicated the insider attack occurred when, "an individual in an Afghan uniform opened fire on the combined U.S. and Afghan force with a machine gun," resulting in multiple U.S. and Afghan casualties.[5]

Ruthless Mexican cartels – threatened by government security forces and now USSOF trainers (from 7th SFG) – could employ similar tactics.[6] In the late 1990s, the Gulf Cartel convinced over 30 Mexican military members to form a group commonly referred to as Los Zetas.[7] Again, in 2023, Mexican military officials were thrust into the media spotlight as millions of SEDNA (Mexico's Defense Department) documents that contained evidence of collusion between high level military officials within the department and drug cartels were leaked by trusted insiders.[8] In parallel, cartels have also retaliated against host nation security and police officers. In December 2023, cartels killed Mexican police officers believed to have stolen cartel drug shipments.[9] Cartel infiltration, coercion, and brutal tactics paint a grim operating environment, analogous to Afghanistan between 2010 and 2019.

> "
> **As tensions rise, insider risk heightens and the potential for insider attacks grows**

To confront these challenges, an examination of insider incidents and lessons from Afghanistan can help mitigate risks associated to comparable threats today. Continuous vetting, counterintelligence integration, guardian angels, and various assessments helped fetter out insurgent infiltrators in Afghanistan and Iraq. On July 7, 2018, U.S. Security Force Assistance Brigade members succumbed to an insider attack near Tarin Kowt Airfield, Afghanistan. The investigation revealed the quick actions of U.S. soldiers, referred to as Guardian Angels, "played an invaluable role in minimizing the number of casualties," according to the investigating officer's report.[10] The attacker, an Afghan National Army soldier, had no clear motive, which highlighted flaws in the Afghan military's vetting process. Post-attack interviews uncovered that the number of individuals to be vetted overwhelmed the system; many made it through the initial screening process without undergoing the necessary scrutiny or vetting required.[11] All the more reason Coalition Forces employed a continuous vetting process for partner forces and locally-employed persons. A process that enabled security forces to discover connections between trusted insiders and nefarious actors that may have been missed during initial screening interviews or later after an insider was coerced, intimidated, or manipulated by Taliban or insurgents to switch sides. Another technique that proved fruitful was the use of biometrics devices.

Biometric enrollment and screenings of Afghan National Security Force personnel were part of the vetting and recruitment process for all members of the Afghan National Defense & Security Forces.[12] These devices denied anonymity to would-be infiltrators while counterintelligence interviews helped U.S. and coalition forces identify aspiring attackers and adversarial collectors. An assessment by the Special Inspector General for Afghanistan Reconstruction reported no insider attacks nor casualties occurred among U.S. and Coalition forces during the last few months of 2020, which reinforces the additional protective measures instituted helped deter or dissuade insider attacks.[13] However, a key difference between Afghanistan and Mexico is proximity to the U.S. homeland.

The proximity and reach cartels exhibit not only endangers USSOF members in Mexico, but also their families in the U.S.[14] This additional dynamic exacerbates an already complex threat environment for USSOF. USSOF employs counterintelligence professionals to protect, exploit, and neutralize foreign intelligence entity threats at home and abroad. They should undoubtedly play an important role when USSOF elements deploy to Mexico next year. Through effective CI integration and partnerships with U.S. federal, state, and local law enforcement agencies, the threat of cartel retaliation and/or reprisals against USSOF members and families can be identified and neutralized. Border Enforcement Security Task Force (BEST) teams, led by U.S. Immigration and Customs Enforcement (ICE), employed along the southern border have proven to be a useful capability in response to cartel violence and activities

affecting both Mexico and the U.S.[15] The BEST teams have successfully partnered with Mexican law enforcement to interdict and apprehend hundreds of criminals and their illicit cargo. Similarly, the U.S. Drug Enforcement Administration (DEA) uses vetted units. These Sensitive Investigative Units (SIU) leverage trained and vetted foreign police officers to cooperatively investigate specific cases within the host nation that have a U.S. nexus.[16] Therefore, it is incumbent on USSOF leaders to incorporate proven lessons from Afghanistan and throughout history to mitigate insider threats in partnering environments, especially as they prepare to work in Mexico and other high-threat countries.

Strategic Competition and the Insider Threat in Taiwan

Although the U.S. should not abandon lessons already learned, it must anticipate and innovate to address insider threats in a new strategic environment. Nowhere is this challenge more apparent than in USSOF-partner engagement in Taiwan. USSOF continue preparation and training initiatives with Taiwanese counterparts as PRC hostilities mount.[17] Partnerships like these make it increasingly difficult for the PRC to subvert the Taiwanese government or its people; however, they also present opportunities for exploitation, infiltration, co-option, or worse by PRC intelligence and security services.[18] USSOF must adapt to a CI environment more familiar to their predecessors' experiences during the Cold War than the more recent Global War on Terror.

PRC espionage activities in Taiwan are formidable. Peter Mattis and Matthew Brazil have examined decades of spying by Taiwanese individuals and groups on behalf of the PRC and espionage plots involving Taiwanese military members from all echelons up to the three-star level.[19] In 2017, Taiwanese national security officials estimated approximately 5,000 individuals were spying for the PRC in Taiwan.[20] This number continues to grow. From 2002 to 2020, Taiwanese authorities uncovered 60 espionage plots that could be just the tip of the iceberg—and affect those at the tip of the spear.[21] For instance, in August 2023, a Taiwanese pilot was arrested and charged with spying for China, after attempting to steal and defect with a U.S.-made CH-47 helicopter, a workhorse for USSOF, in exchange for $15 million dollars.[22] The arrests of both the pilot and a retired Taiwanese military officer occurred because of a tip-off. A tip, most likely, resulting from Taiwan's aggressive counter-espionage campaign focused on education, awareness, and reporting.[23] Had the PRC acquired the airframe, the People's Liberation Army (PLA) would undoubtedly have reverse-engineered it to fill a gap within the army's current fleet.

Trust is critical to effective partnerships. USSOF members must build trust and relationships with Taiwanese counterparts despite the heightened risk of operating in a critical insider threat environment. The dilemma of how much to reveal versus conceal in working with partner forces place SOF personnel in a precarious position. USSOF currently face the challenge of PRC espionage by proxy through partner engagements. The Global Taiwan Institute asserts that "Taipei has no way–short of accepting unification–to stop Beijing's human and technical intelligence operations."[24] PRC intelligence services target and exploit current and former Taiwanese military and government officials. They have also started using university students to spy within the island nation. The addition of academics and students resembles efforts by the PRC to recruit students studying in the United States, via the Thousand Talents Program, to spy on China's behalf.[25] A practice that is proving fruitful and difficult to detect, exploit, or neutralize. European nations, like Germany, are even sounding the alarm on the unprecedented influx of Chinese students, an "Army of spies".[26] Additionally, in November 2023, 10 active-duty and retired military personnel were indicted by Taiwan on suspicion of spying for China.[27] Currently, insider threat trends within Taiwan focus on political influence, subverting the will to fight, and technology exploitation on behalf of the PRC. A concern for the U.S. defense industry and a wake-up call for USSOF leaders; a clear threat to SOF's competitive advantage.

As tensions rise, insider risk heightens and the potential for insider attacks grows. In the event of hostilities between the PRC and Taiwanese and/or U.S. forces, the PRC could leverage networks of insiders to sabotage or attack Taiwanese defense and resistance structures and organizations. To confront the operating environment's challenges, USSOF can and should remain vigilant and resilient to the effects and impacts insider threats may have on operations, personnel, and partners while limiting the damage that counter-insider threat and counterintelligence efforts can inflict on trust, the *sine qua non* of effective USSOF partnerships.

Mitigating Insider Threats in Partnering Environments

Studying the trends experienced in Afghanistan and during the Cold War can provide USSOF and other government, commercial, and private sectors with valuable insights to help confront insider threats in partnering environments. In Afghanistan, U.S. military leaders sought solutions to green-on-blue attacks. They turned to the U.S. Army's Asymmetric Warfare Group (AWG) for help. The group provided recommendations and useful tools for leaders to use to mitigate the risks associated with partnering with foreign forces. These same tenets and elements can be used to guide intra-organizational insider threat programs as effectively as between organizations. Often, different "branches" of organizations--especially large organizations--have different perspectives, missions, needs, and priorities. The branches must "partner" for an effective insider threat program within the enterprise. This is something we can build upon to connect DoD and non-DoD perspectives.

In June 2011, the AWG created a useful infographic titled, "Insider Threats in Partnering Environments: A Guide for Military Leaders." AWG's guide assists in three areas: awareness, information, and dialogue between US and partner force elements.[28] The guide states that partnering "in itself is a sensitive mission and only by creating trust and having an open dialogue with all forces will the mission be accomplished."[29] To overcome the insider threat the guide provides leaders with observable indicators and decision matrices to assist leaders and staffs with determining acceptable risk categories and mitigation procedures. While there is little to no definitive proof this guide contributed to reduction in the number of insider attacks in Afghanistan two years after it was implemented or if some other factor(s) were to blame. The guide still provides helpful recommendations USSOF leaders should review, and institute as they prepare for partner force engagements in 2024 and beyond.

A retrospective examination of World War II and Cold War era archives provides a treasure trove of useful examples of compromised networks and insider threats applicable to today's strategic competition and partnering environments. In 1942, the United Kingdom's Special Operations Executive (SOE), the British counterpart to America's OSS, experienced one of its most significant compromises of WWII.[30] German security and Nazis captured over 50 clandestine SOE agents in Holland and compromised the entire operation by penetrating the newly formed Dutch resistance forces.[31] In France, over 80 separate resistance groups were established by British Intelligence's special division, commonly referred to as F-Section.[32] The SOE's Prosper Mission, which F-Section played a critical role in, employed Henri Dericourt, a French military officer to secretly control air traffic into the Paris area of operations for the network of spies, saboteurs, and operatives.[33] Unbeknownst to SOE and British intelligence was Dericourt's concealed connection to Hans Boemlburg, the chief of German counterespionage, which resulted in 14 clandestine airfield locations compromised and a number of agents captured, tortured, or killed.[34]

In contrast, Military Assistance Command Vietnam, Studies, and Observation Group (MACVSOG) missions in Vietnam resulted in a mix of success and failure. OP35, MACVSOG cross border operations in Laos and Cambodia, were highly effective "for a myriad of reasons including highly trained and motivated personnel, a depth of experienced in the exact missions they were going to conduct, exemplary leadership at multiple levels and immeasurable amounts of trust amongst those involved."[35] However, OP34s agent operations proved to be disastrous, "costing high attrition amongst the trained Vietnamese agents."[36] Mass training of potential agents and centralized housing of all recruited agents with trainees resulted in operational security degradation and compromise by those without the necessary need-to-know. Due to this mass training, MACVSOG had no way to determine or account for what information was divulged to the enemy by compromised partner force members. A method that reemerged during the Operation Enduring Freedom-Afghanistan, when U.S. and coalition forces trained Afghan security forces en masse, a technique that should not be repeated in the current strategic competition environment within the INDOPACIFIC region.

Similarly, examination of the insider threats in Taiwan today presents distinct challenges and concerns. The language barrier forces USSOF personnel to adapt and develop organic language capacity or rely on contracted linguistic support; a problem shared by the commercial and private sectors. The latter poses an opportunity for PRC penetration, co-option, or coercion for Mandarin Chinese and Taiwanese speakers with families in mainland China. A review of motivations for espionage committed by PRC operatives proves that many reside within the private sector.[37] This creates opportunities to infiltrate and influence the human domain where USSOF are often interfacing and interacting within partnering environments at the spear tip. Like SOF operators – corporate executives and entrepreneurs – face comparable challenges when interacting with foreign business owners or operating in foreign markets.

Counterintelligence professionals within SOF formations or supporting elements can help detect, identify, exploit, and neutralize the threat actors and/or their activities. Additionally, counterintelligence personnel (in any organization) could liaise with host nation security and intelligence forces and resident U.S. interagency personnel to help deny anonymity and operating space to PRC intelligence and security forces seeking to exploit gaps caused by language, culture, or other means. In a recent 2023, *Tip of the Spear* magazine article, I emphasize that more effective counterintelligence integration within SOF is needed, a practice that is vital to countering foreign intelligence threats to USSOF in partnering environments.[38]

Conclusion – A CI Professional's Perspective

Over the course of my 24-year U.S. Army career it became clear that engagements with foreign partners proved to be built on trust, mutual respect, and a fellowship of comrades-in-arms. As a counterintelligence professional, it was necessary to protect the force while ensuring the mission's success without compromising the trust built between USSOF partners and their counterparts. This was often difficult, yet attainable. Many of the approaches and methods used to vet partners, while unorthodox, proved valuable years, even decades later. The implementation of Guardian Angels and counterintelligence interviews of questionable or suspected individuals proved positive and saved lives. Then and now, the adoption of new technological advancements in data management, biometrics devices, and analysis are speeding up the process. By simply gathering biometrics and pertinent assessment information early, it enables partners to be vetted faster. However, the human factor is still must be considered. To build trust amongst partner forces it takes time and focus. Stephen Covey’s book *The Speed of Trust* articulates why character and competence – two traits examined during SOF assessments and selection processes – are vital to building lasting partnerships (relationships).[39] The same can be said about corporate employee interviewing and screening practices. While the speed with which partners can be expedited through the verification process improves the overall amount of time spent training with USSOF members on mission-enhancing skills like shooting, rappelling, patrolling, etc. it is critical that trust is built and maintained throughout the partnership. Most mitigation measures can be implemented with very little effort or impact to the partnering mission. It is incumbent on leaders within USSOF to help educate their members on the need for counterintelligence integration into future events to ensure USSOF members, operations, activities, and investments are protected from foreign intelligence and insider threats in partnering environments. The same, can be said for corporate America that face insider threats from within and on the periphery in business ventures, similar to what SOF faces in partnering environments.

DISCLAIMER

The information and views expressed in this presentation are solely those of the author and do not represent opinions and policies of the Department of Defense, U.S. Government, U.S. Special Operations Command, the Joint Special Operations University, or the institutions with which the author is affiliated.

> “it [is] necessary to protect the force while ensuring the mission’s success without compromising the trust built between … partners. This [is] often difficult, yet attainable.

REFERENCES

1. Diana I. Dalphonse, Chris Townsend, and Matthew W. Weaver Shifting Landscape: The Evolution of By, With, and Through. *The Strategy Bridge*. August 1, 2018. https://thestrategybridge.org/the-bridge/2018/8/1/shifting-landscape-the-evolution-of-by-with-and-through.
2. Bill Roggio & Lisa Lundquist. Green-on-Blue Attacks in Afghanistan: The Data. Real Clear Defense. March 21, 2017. https://www.realcleardefense.com/articles/2017/03/21/green-on-blue_attacks_in_afghanistan_the_data_111015.html.
3. Jared Keller. Insider attacks against US troops in Afghanistan have dropped too a historic low. Here’s why. *Task and Purpose*. February 2, 2021. https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
4. Jared Keller, 2 Feb 2021, https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
5. James Laporta and Tom O’Connor. U.S. and Afghan Special Operations Forces Killed in Deadly Ambush. 8 Feb 2020. https://www.newsweek.com/us-afghan-special-operations-forces-killed-deadly-ambush-1486400.
6. Karol Suarez, The power of blood: Why Mexican drug cartels make such a show of their brutality. USA Today. 18 DEC 2023. https://www.usatoday.com/story/news/nation/2023/12/18/mexican-drug-cartels-brutality-power/71932898007/.
7. Samuel Logan. A profile of Los Zetas: Mexico’s second most powerful drug cartel. Feb 2012, Vol 5, Issue 2. CTC Sentinel. https://ctc.westpoint.edu/a-profile-of-los-zetas-mexicos-second-most-powerful-drug-cartel/.
8. Armando Velasco. Mexico military hack shows revelations of cartel involvement with some defense officials. 18 OCT 2022. Fox News. https://www.foxnews.com/world/mexico-military-hack-shows-revelations-cartel-involvement-with-some-defense-officials.
9. CBS News. Cartel leaders go on killing rampage to hunt down corrupt officers who stole drug shipment in Tijuana. Insider attacks against US troops in Afghanistan have dropped to a historic low. Here’s why. 12 DEC 2023. https://www.cbsnews.com/news/cartel-leaders-kill-corrupt-officers-who-stole-drug-shipment-tijuana-mexico/.
10. Kyle Rempfer. Investigation of 2018 green-on-blue attack criticizes vetting of Afghan forces, praises actions of US riflemen. *Army Times* magazine. 26 Jun 2020. https://www.armytimes.com/news/your-army/2020/06/26/investigation-of-2018-green-on-blue-attack-criticizes-vetting-of-afghan-forces-praises-actions-of-us-riflemen/.
11. Ibid.
12. Krystian Fracik. Insider attacks as one of the main threats to Resolute Support personnel in Afghanistan. *Security & Defence Quarterly* Vol 12, March 2016. https://securityanddefence.pl/Insider-attacks-as-one-of-the-main-threats-to-resolute-support-personnel-in-Afghanistan,103234,0,2.html.
13. Jared Keller. Insider Attacks in Afghanistan 2020. 2 FEB 2021. *Task & Purpose*. https://taskandpurpose.com/news/insider-attacks-afghanistan-2020/.
14. DEA. United States: Areas of Influence of Major Mexican Transnational Criminal Organizations. DEA-DCT-DIR-065-15. July 2015. https://www.dea.gov/sites/default/files/2018-07/dir06515.pdf.
15. Sigrid Arzt. U.S.-Mexico Security Collaboration. The Wilson Center March 31, 2023. https://www.wilsoncenter.org/sites/default/files/media/documents/publication/Chapter%2012-%20U.S.-Mexico%20Security%20Collaboration%2C%20Intelligence%20Sharing%20and%20Law%20Enforcement%20Cooperation.pdf .
16. Ibid.
17. A.B. Abrams. Building a U.S. Special Forces ‘Stealth Network’ on Taiwan. *The Diplomat*. 3 May 2023. https://thediplomat.com/2023/05/building-a-us-special-forces-stealth-network-on-taiwan/.
18. Stavros Atlamazoglou. US Green Berets who’ve trained Taiwanese troops explained how they could fight China and why the US keeps their mission secret. *Business Insider.* 24 OCT 2021. https://www.businessinsider.com/us-green-berets-explain-how-they-train-taiwan-troops-2021-10.
19. Peter Mattis and Matthew Brazil. *Chinese Communist Espionage: An Intelligence Primer*. 2019. Naval Institute Press, Annapolis, Maryland.
20. Chung Li-hua and Jonathan Chin. 5,000 Chinese Spies in Taiwan: Source. *Taipei Times.* 13 March 2017. https://www.taipeitimes.com/News/front/archives/2017/03/13/2003666661.
21. Ibid.
22. Peter Suciu. China Offered Taiwanese Pilot $15 Million to Steal U.S.-Made CH-47 Helicopter. 13 December 2023. https://nationalinterest.org/blog/buzz/china-offered-taiwanese-pilot-15-million-steal-us-made-ch-47-helicopter-207917.
23. Reuters. Taiwan boosts counter-espionage effort after suspected China infiltration. 2 Aug 2023. https://www.reuters.com/world/asia-pacific/taiwan-boosts-counter-espionage-effort-after-suspected-china-infiltration-2023-08-02/.
24. Peter Mattis. 28 September 2016. Spy Games in Taiwan Strait: Taipei’s Unenviable Espionage Problem. Global Taiwan Institute. https://globaltaiwan.org/2016/09/spy-games-in-taiwan-strait-taipeis-uneviable-espionage-problem/.
25. Aaron Jensen. China Expands its Spying Against Taiwan. The Diplomat. 21 March 2017. https://thediplomat.com/2017/03/china-expands-its-spying-against-taiwan/.
26. Ritu Sharma. China’s ‘Army of Spies’ Horrifies Germany; Report Cautions Against Massive Influx of Chinese Students. 3 January 2024. https://www.eurasiantimes.com/china-cranking-up-espionage-activities-in-germany/amp/.
27. Cindy Wang. November 23, 2023. Taiwan Indicted Military Person Suspected of Spying for China. https://www.bloomberg.com/news/articles/2023-11-28/taiwan-indicted-military-personnel-suspected-of-spying-for-china.
28. U.S. Army Asymmetric Warfare Group (June 2011) *Insider Threats in Partnering Environments: A Guide for Military Leaders*.

REFERENCES

29. Ibid.
30. Robert Hutton. Was this the UK's Worst Spy Failure of World War II? 13 May 2022. History Net. https://www.historynet.com/was-this-the-uks-worst-spy-failure-of-world-war-ii/.
31. Paul Lashmar & Chris Staerck. Spy fiasco cost Britain 50 agents. 21 September 1998. *Independent.* https://www.independent.co.uk/news/spy-fiasco-cost-britain-50-agents-1199631.html.
32. Peter Kross. The British Prosper Spy Network: Destroyed to Protect D-Day? September 2007. Warfare History Network. https://warfarehistorynetwork.com/article/the-british-prosper-spy-network-destroyed-to-protect-d-day/.
33. Ibid.
34. Ibid.
35. Daniel J. Staheli. Analysis of Military Assistance Command Vietnam, Studies and Observation Group (MACVSOG) Against the Special Operations Forces Truths. AY 2019-20. https://apps.dtic.mil/sti/trecms/pdf/AD1177859.pdf.
36. Ibid.
37. Nicholas Eftimiades, *China's Espionage Recruitment Motivations: Getting Rid of the MICE* European Intelligence Academy Research Paper Series #5 December 2023. https://www.rieas.gr/images/editorial/EIAPaper5.pdf.
38. Michael W. Parrott, *Foreign Intelligence Threats to SOF – Why Counterintelligence Integration is Vital*. October 2023. Tip of the Spear Magazine. https://www.dvidshub.net/publication/issues/68487.
39. Stephen Covey. *The Speed of Trust*. Pg 30. Free Press. Feb 2008.