FEATURE

Covert Connections

The LinkedIn Recruitment Ruse Targeting Defense Insiders

Lt Col Caleb S. Lisenbee II, USAF

Abstract

Foreign adversaries, particularly China, are exploiting LinkedIn to conduct virtual espionage against current and former US Department of Defense (DOD) members. They create fake profiles and lucrative job solicitations to entice targets into divulging sensitive information or becoming recruited assets. This low-risk, low-cost tactic circumvents robust physical and cybersecurity defenses. Every DOD professional is a potential target, from senior leaders to junior personnel, as adversaries seek insights into future capabilities, vulnerabilities, research, operational concepts, and human intelligence networks. Successful recruitment can devastate national security by enabling technological replication, battlefield strategy countering, and compromising of critical personnel. Consequences for individuals include potential treason charges and ruined careers. To combat this threat, a focused US government counterespionage campaign is recommended, coupled with enhanced training, policies, and legal statutes explicitly addressing virtual espionage. Defensive measures must match the scale and sophistication of the virtual threat.

***

Unsolicited messages on LinkedIn, often masquerading as legitimate business opportunities, have become increasingly prevalent in recent years. These seemingly innocuous communications frequently mask ulterior motives, particularly when honing in on individuals with defense and security backgrounds. Beneath the guise of professional networking lurks a mounting peril of virtual espionage, with foreign adversaries leveraging the platform's perceived reliability to ensnare unwitting recruits for nefarious ends. Take, for instance, the following solicitation: "Paid Consulting Opportunity: I hope you're doing well. I'm currently working with a client who is researching security solutions. Based on your background, I think you'd be a great fit. If you're interested, it would be a ~1 hour phone call, and you would be compensated for your time on the phone with them at a prorated hourly rate of your choosing; typical rate range is $200-300." This message stands as but one among a slew of suspicious unsolicited missives I have encountered on LinkedIn, a platform often hailed as the epitome of trustworthiness, particularly for networking purposes.[1] Many of

[1] Audrey Schomer, "LinkedIn, Pinterest, Instagram Most Trusted Platforms; Facebook Least," *Business Insider*, 26 September 2019, https://www.businessinsider.com/.

my peers—coworkers, colleagues, and friends alike—have attested to receiving similar offers over recent years. Foreign adversaries are leveraging LinkedIn in attempts to recruit both current and former Department of Defense (DOD) members, masquerading under the pretext of consulting, in a bid to gain strategic advantages in the great-power competition. This is facilitated by the low costs and risks associated with utilizing the platform for virtual espionage. In this article, I aim to elucidate this argument by identifying the targeted demographics and the sought-after information or positions by adversaries. Moreover, I will explore the repercussions of these attacks on the nation and the individuals who fall prey to them. Additionally, I will delve into the intricacies of espionage and the underlying psychological mechanisms of social engineering, shedding light on how adversaries pinpoint their targets on LinkedIn. Finally, I will offer recommendations on how to counter this looming threat. The United States possesses the capability to impose costs on adversaries engaged in virtual espionage, effectively making them pay for their transgressions.

As outlined in the current *National Security Strategy*, great-power competition stands as the foremost security challenge confronting the United States, with China emerging as the primary pacing threat. Adversaries persist in their endeavors to gather intelligence, engage in espionage, and pilfer critical information through any available means. Foreign intelligence operatives adeptly exploit human targets to establish connections with high-value individuals (HVI) within a target's professional network. In today's digitally driven world, virtual espionage looms as a formidable menace.

The 2023 US *National Cybersecurity Strategy* (NCS) highlights that "theft of data is growing rapidly and opening up novel vectors for malicious actors to surveil, manipulate, and blackmail individuals."[2] The aspect of manipulation is particularly concerning when considering the exploitation of current and former DOD members for secrets, information, experience, and insights. Technology increasingly intertwines with human life, enhancing and enabling various aspects, including professional networking and collaboration. Social media platforms, particularly Microsoft's professional networking site LinkedIn, offer foreign intelligence services a rich target environment—a fact US counterintelligence chief William Evanina substantiated in 2018.[3]

For security reasons, this article refrains from discussing specific details of the problem, such as the number of reports being investigated by federal law enforce-

[2] *National Cybersecurity Strategy* (Washington: The White House, March 2023), https://www.whitehouse.gov/.

[3] Kevin Ponniah, "How a Chinese Agent Used LinkedIn to Hunt for Targets," *BBC News*, 26 July 2020, https://www.bbc.com/.

ment agencies like the Office of Special Investigations (OSI) regarding suspicious consulting offers over LinkedIn or the extent to which adversary attempts to solicit information or recruit spies from current and former DOD members have increased in recent years. Nevertheless, it is prudent to consider these questions.

That being said, the Defense Counterintelligence and Security Agency (DCSA) offers insight into the magnitude of the issue through statistics from the defense industry. In FY 2022, DCSA received over 26,000 suspicious contact reports from cleared contractor facilities, some of which were linked to social media activity.[4] Furthermore, US and allied intelligence agencies have issued warnings about nations like the People's Republic of China (PRC) engaging in LinkedIn espionage. For instance, in 2018, the US publicly accused the PRC for the first time of leveraging LinkedIn to recruit Americans.[5] Additionally, Gen C.Q. Brown, during his tenure as Chief of Staff (CSAF) of the US Air Force (USAF), alerted all Airmen in a September 2023 email about China's People's Liberation Army (PLA) recruitment efforts "to exploit their knowledge and skill to fill gaps in their military capability."[6]

A 2023 report by the Defense Counterintelligence and Security Agency reveals that social networking ranks among the most common contact methods for adversary intelligence services, particularly those originating from East Asia and the Pacific.[7] A consulting offer serves merely as the initial enticement, paving the way for further exploitation. In the digital age, the acquisition, storage, and analysis of personal information far surpass "any secret police files" compiled by the Soviets during the Cold War.[8] Moreover, advancements in algorithms and artificial intelligence (AI) make analysis even more accessible. This article should be disseminated to all Transition Assistance Program (TAP) offices/facilitators, at the very least, to heighten threat awareness among military personnel transitioning out of service. The following section delves deeper into the target demographic.

---

[4] *Targeting U.S. Technologies: A Report of Threats to Cleared Industry* (Washington: Defense Counterintelligence and Security Agency, 2023), https://www.dcsa.mil/.

[5] Mika Aaltola, "Geostrategically Motivated Co-Option of Social Media: The Case of Chinese LinkedIn Spy Recruitment," Finnish Institute of International Affairs, June 2019, https://www.fiia.fi/; and Warren Strobel and Jonathan Landay, "Exclusive—U.S. Accuses China of 'super Aggressive' Spy Campaign on LinkedIn," *Reuters*, 31 August 2018, https://www.reuters.com/.

[6] Gen Charles Q. Brown, Q., Chief of Staff of the Air Force, US Air Force (USAF), to all Airmen, (USAF), letter/email, subject: PLA Recruitment Efforts, 5 September 2023.

[7] *Targeting U.S. Technologies*, 10.

[8] Raef Meeuwisse, *How to Hack a Human: Cybersecurity for the Mind* (London: Cyber Simplicity, Ltd., 2019), 9.

Who Is Targeted?

Every current and former DOD member present on LinkedIn represents a potential target for LinkedIn espionage. From uniformed military personnel to civilians and defense contractors, current and former DOD members remain susceptible to virtual espionage. These individuals possess valuable information and secrets, may have access to items of interest, or could simply be exploited by foreign intelligence services to navigate a network of human connections to reach a HVIs they seek to exploit. In 2018, the US Assistant Attorney General for National Security highlighted that China "is pursuing its goals through malign behaviors that exploit features of a free-market economy and an open society like ours."[9] LinkedIn provides another vector to do so.

Current and former DOD members become targets because the physical and technical defenses implemented within the DOD are robust and effectively thwart most technical intelligence collection methods. However, the stronger these protective measures become, the greater the vulnerability to social engineering attacks in the virtual realm.[10] Furthermore, "lacking the necessary know-how for weapon systems production has, in fact, become a major obstacle for actors trying to imitate foreign technology—wealthy countries included."[11] Human intelligence (HUMINT) often stands as the sole avenue to endeavor to gain access to an opponent's secret intentions, plans, and technical specifications of weapon systems.[12]

This article emphasizes LinkedIn because DOD TAP offices strongly advocate for the platform among separating/retiring members. Enthusiastic defense professionals often share information to enhance their visibility and attract potential employers. While this practice aids in securing suitable employment or business opportunities, it also amplifies their susceptibility to foreign intelligence services. For instance, an agent for PRC intelligence created a "fake job advertisement" that

[9] John C. Demers, "Statement of John C. Demers, Assistant Attorney General, National Security Division, US Department of Justice, before the Committee on the Judiciary United States Senate for a Hearing on China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses," presented on 12 December 2018, 2, https://www.justice.gov/.

[10] Kevin Mitnick and William L. Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis: Wiley, 2002), 259.

[11] Andrea Gilli and Mauro Gilli, "Why China Has Not Caught Up Yet: Military-Technological Superiority and the Limits of Imitation, Reverse Engineering, and Cyber Espionage," *International Security* 43, no. 3 (2019), 154, https://doi.org/.

[12] David Perry, "Ethics in the Recruiting and Handling of Espionage Agents," in *National Security Intelligence and Ethics*, ed. Seumas Miller, Mitt Regan, and Patrick F. Walsh (New York: Routledge, 2021), 66.

garnered more than "400 CVs [curricula vitae] with 90% of them coming from US military and government personnel with security clearances."[13]

LinkedIn serves as an ideal platform for large-scale espionage operations, enabling simultaneous outreach to thousands of individuals who meet specific targeting criteria. Disclosures from US and allied governments and intelligence agencies indicate that such operations are occurring on a significant scale. For instance, the German Federal Office for the Protection of the Constitution (BfV) reported that more than 10,000 German defense and government practitioners were approached in 2017.[14]

Regardless of the length of one's DOD career or whether they possess sought-after skills, secrets, or insights, they are highly likely to have joined the network of DOD professionals coveted by adversaries. Among these individuals are current or future senior leaders. LinkedIn boasts a user base of more than 40 million decision makers, making it an attractive platform for foreign intelligence services to leverage.[15] The platform's emphasis on professional connections rather than personal friendships makes it an ideal vehicle for exploitation.[16] When accepted into someone's public professional network, a virtual intelligence officer gains immediate cover and credibility. For example, the USAF confirmed that a "security specialist" engaged in a five-year correspondence with Mr. Dickson Yeo, a Singaporean national whose apprehension by US officials in 2020 shed light on this issue concerning the PRC.[17] In an attempt to be helpful, "the security specialist recommended Mr. Yeo on LinkedIn in at least eight categories," which helped further the PRC's ability to headhunt individuals with key positions and sensitive knowledge.[18]

One of the immediate benefits of being accepted into a network of professionals or a professional community is the opportunity to gain valuable insights and information from discussion threads and shared articles posted on LinkedIn. This enables adversaries to remain informed about the latest perceptions, challenges, recommendations, and trends within the DOD community.

---

[13] Ponniah, "How a Chinese Agent Used LinkedIn."

[14] Aaltola, "Geostrategically Motivated Co-Option of Social Media"; and Danielle Wallace, "China's 'prolific' Espionage Scheme Trying to 'Headhunt' British Politicians, Defense Officials, UK Gov't Says," *Fox News*, 17 September 2023, https://www.foxnews.com/.

[15] Aaltola, "Geostrategically Motivated Co-Option of Social Media."

[16] Beata Biały, "Social Media—From Social Exchange to Battlefield," *Cyber Defense Review* 2, no. 2 (Summer 2017), 69–70.

[17] Katrina Manson, Hannah Murphy, and Kadhim Shubber, "LinkedIn Spy Scandal Shines Spotlight on China's Online Espionage," *Financial Times*, 31 July 2020, https://www.ft.com/.

[18] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight"; and Wallace, "China's 'prolific' Espionage Scheme."

Furthermore, junior defense employees or service members, irrespective of rank, title, or position, often find themselves privy to critical military information and thus become targets. A striking example of China "reaching deep within the military ranks" to challenge US military supremacy occurred in 2023 when two junior Navy sailors were charged with allegedly spying for the PRC.[19] These junior members possess intimate knowledge of weapons systems, comprehend the relative strengths and vulnerabilities of these systems, and are well-versed in organizational structures and chains of command.

Active military and civilian members, who have no intention of leaving the DOD in the foreseeable future, remain vulnerable to inadvertently aiding foreign adversaries through enticing consulting offers. A prime example is a seemingly innocuous request for a straightforward report. With a generous compensation package and the simplicity of the task, consultant reports become an avenue for malicious actors to get "a hook" into a potentially valuable source. Furthermore, "the activity itself—writing a short report—is not illegal in many Western countries if no secret or confidential information is revealed."[20]

However, active DOD members are prohibited from working for foreign governments as part of side employment. A guide from Joint Base San Antonio confirms that active, reserve, and guard Airmen are "ineligible for employment by foreign governments or foreign agencies."[21] Violating this rule, whether knowingly or unknowingly, can result in charges of espionage and treason.

Many former DOD members transition to roles within the US's defense industrial base, leveraging their experience to contribute to the development of new and innovative weaponry. In 2022, Federal Bureau of Investigation (FBI) Director Christopher Wray disclosed that "the Bureau had more than 2,000 investigations involving Chinese attempts to steal U.S. technology, and that two such new cases are opened every day."[22]

Further research is necessary to ascertain the duration for which information and insights retain their value and accuracy. Nonetheless, two seasoned intelligence experts and faculty members at the Air War College, possessing extensive knowledge on espionage, have affirmed that even information dating back five years can

---

[19] Nancy A. Youssef and Warren P. Strobel, "Navy Sailors Charged with Allegedly Spying for China," *Wall Street Journal*, 4 August 2023, sec. Politics, https://www.wsj.com/.

[20] Ponniah, "How a Chinese Agent Used LinkedIn"; and Aaltola, "Geostrategically Motivated Co-Option of Social Media," 5–6.

[21] Joint Base San Antonio Legal Assistance Office, "Off-Duty Employment," *JBSA Jurist* 4, no. 3 (March 2018), 1, https://www.jbsa.mil/.

[22] Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China."

remain highly valuable to adversaries in addressing their intelligence gaps.[23] With the targets of adversaries now evident, let us delve into their objectives.

Adversaries' Goals

Foreign adversaries engage in LinkedIn espionage as part of their efforts in the great-power competition to obtain information and strategic advantages. Over the past few decades, adversaries have meticulously analyzed US military capabilities, strategies, and advantages, beginning with the highly sophisticated operations facilitated by space assets, the digital/information domain, and precision bombing during the Persian Gulf War in the early 1990s. To remain competitive, challengers to the United States must consistently inform themselves about the US military and the myriad factors contributing to its success. Of particular interest to adversaries is any insight into the DOD's future force development, capabilities, and strategies for warfare. This encompasses information concerning US plans for defending Taiwan, for which "the Peoples Liberation Army (PLA) has issued contracts to private Chinese companies to gather a range of open-source information," according to the threat-intelligence company Recorded Future.[24]

Any insight obtained would facilitate the PLA's development of its "war plan" and its efforts to counter current and future US weapons and capabilities.[25] In line with this objective, adversaries seek to assess how their military capabilities stack up against those of the United States. Kevin Rudd, former Australian prime minister and current Australian ambassador to the United States, identifies several of these challenging-to-assess factors in his book *The Avoidable War*.[26] The PLA aims to understand the "relative sophistication and survivability of military platforms, systems, and weapons" to discover weaknesses it can attack and exploit. Furthermore, studying US "battlefield experience and training" will enable the PLA to formulate strategies for positioning and operating its forces in ways that catch the US military off guard.[27] Additionally, the PLA seeks to evaluate the United States' "robustness of command, control, communications, and intelligence systems for integrating and sustaining effective joint operations" to identify avenues for isolating, for instance, the US Navy and compelling it to engage in a weakened and disjointed

[23] Elizabeth Tilley and Charles Hans, class discussion on virtual espionage, Air War College, 15 September 2023.

[24] Julian E. Barnes, "China Investing in Open-Source Intelligence Collection on the U.S.," *New York Times*, 1 June 2023, https://www.nytimes.com/.

[25] Jeffrey Richelson, *The U.S. Intelligence Community*, 7th ed. (Boulder, CO: Westview Press, 2016), 10.

[26] Kevin Rudd, *The Avoidable War: The Dangers of a Catastrophic Conflict between the US and Xi Jinping's China*, (New York: PublicAffairs, 2022), 172–73.

[27] Rudd, *The Avoidable War*, 172.

manner.[28] The PRC considers various factors when determining the optimal time and location to act. These factors include the "ability to sustain military budgets over time, as well as the political support and willingness of Washington, Beijing, and relevant allied capitals to develop and maintain military forces."[29] A significant aspect of the PRC's calculations is the presence of nuclear-capable US forces and the "impact of nuclear deterrence in relation to any conventional conflict."[30]

The specific intelligence requirements become clearer following a comparative analysis of relative strengths. A comprehensive review of various books and articles detailing espionage efforts against US military weapon systems yields the following condensed list of sought-after intelligence, sensitive knowledge, and expertise:

1. Propulsion technology, structural designs, and electronics for current and future naval, aerial, and rotary-wing platforms.
2. Space systems for diverse military applications and the associated terrestrial and orbital infrastructure.
3. Advanced munitions technology.
4. Cyber offensive and defensive capabilities, as well as communication and computer technologies.
5. Various weapons' underlying operating systems.[31]

Moreover, critical scientific research is poised to unlock breakthroughs that offer significant military advantages. Intelligence gathering efforts targeting research and development focus on hypersonics, thermodynamics, propulsion, robotics, AI, signal processing, quantum computing, supercomputing, nuclear energy, nanotechnology, semiconductors, and stealth technology.[32] Notably, the DCSA identified half of these scientific domains in its 2023 report on targeted US technologies.

It comes as no surprise that the PRC shows a specific interest in the US capacity to project power across vast distances. In the event of a conflict between the United States and the PRC, their navies would play a pivotal role, as "the PRC sees the likelihood of US and China confrontation at sea."[33] Hence, the PLA is

[28] Rudd, *The Avoidable War*, 172.
[29] Rudd, *The Avoidable War*, 172.
[30] Rudd, *The Avoidable War*, 172.
[31] *Targeting U.S. Technologies*, 11; Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China"; and Joel Brenner, *Glass Houses: Privacy, Secrecy, and Cyber Insecurity in a Transparent World* (New York: Penguin Books, 2013), 74–75.
[32] *Targeting U.S. Technologies*, 11; and Strobel and Landay, "Exclusive—U.S. Accuses China."
[33] Brenner, *Glass Houses*, 75.

particularly keen on US Navy technologies, with a focus on quiet submarine propulsion, torpedoes, as well as carrier and destroyer technologies. Additionally, adversaries acknowledge the global reach of the USAF and therefore target fighter and bomber technologies. Consequently, individuals involved in the development, work, or support of platforms such as the F-35, B-21, and Next Generation Air Dominance (NGAD) are prime targets.

The desired information also encompasses a wealth of data on defense professionals. In 2020, the US Assistant Attorney General for the National Security Division underscored "Beijing's appetite for large volumes of personal data, citing the 2015 OPM hack and the 2017 Equifax breach."[34] A prime example is former Defense Intelligence Agency (DIA) employee Ron Hansen, who was compromised by Chinese intelligence operatives to collect and compile information on his former colleagues and agency.[35] Having discussed the objectives of adversaries targeting the United States, the following section examines the repercussions should they succeed in their LinkedIn espionage efforts.

LinkedIn Espionage Impact

The repercussions for the nation and the individuals compromised by successful foreign adversary LinkedIn espionage operations are profound. The strength and national security of the United States rely on its ability to wield the most advanced, unparalleled technology and weaponry, often deploying them in ways that catch adversaries off guard. Achieving success in combat has always necessitated a technological edge and operational unpredictability. The warfighting concepts, technical innovations, and fielded capabilities of today and tomorrow have been shaped by hard-earned lessons, paid for with the sacrifice of precious lives, billions of taxpayer dollars, and extensive time investments. Effective intelligence utilization is pivotal, not only for enhancing national security but also for fiscal responsibility. As succinctly stated, "Intelligence can help save substantial sums of money by avoiding unnecessary research and development (R&D) and deployment programs."[36] Adversaries engage in LinkedIn espionage to counter

[34] "CSIS: Notes from a CSIS Virtual Event - Countering Chinese Espionage," *Targeted News Service*, 18 August 2020, https://www.proquest.com/.

[35] "Former Intelligence Officer Convicted of Attempted Espionage Sentenced to 10 Years in Federal Prison" (press release, Office of Public Affairs, US Department of Justice, 24 September 2019), https://www.justice.gov/; and Jeff Stone, "LinkedIn Is Becoming China's Go-to Platform for Recruiting Foreign Spies," *CyberScoop* (blog), 26 March 2019, https://cyberscoop.com/.

[36] Richelson, *The U.S. Intelligence Community*, 10.

or replicate US capabilities at a fraction of the cost and with expediency, effectively shifting the burden onto American taxpayers.

Moreover, grave damage ensues when a high-value individual (HVI) is compromised and coerced into collaboration with the adversary, which represents the ultimate objective of LinkedIn espionage. The case of Kevin Mallory, a retired CIA officer initially contacted via LinkedIn, serves as a stark example of this danger. Despite identifying his Chinese contacts as intelligence officers, Mallory still conspired to commit espionage for the PRC.[37] Critical insights into US war plans and most cutting-edge scientific research will severely impact US military power. Consider the ramifications if the United States were to lose the race for AI and quantum computing because the PRC or Russia managed to bypass the safeguards of these R&D efforts. As emphasized, "Adversaries that can mitigate US systems' effectiveness or deploy equal capabilities onto the battlefield will cost US and allied warfighter lives."[38]

It is noteworthy how strikingly similar the US F-22 and the PRC J-20 fighter jets appear in images. One repercussion of failing to effectively counter the threat of virtual espionage is that adversaries will eventually secure access to subject matter experts capable of providing technical insights into the United States' most advanced weaponry and those under development. For instance, the PRC's intelligence asset, Mr. Yeo, initiated contact over LinkedIn with an undisclosed individual facing financial difficulties who was involved in the F-35 program.[39] Additionally, when the PRC possesses planes and warships resembling those of the United States, they likely possess knowledge of US systems' characteristics, while having "modified their own replicas in ways which the US military must guess at."[40]

LinkedIn espionage has the potential to empower adversaries to surpass the United States in existing technologies and outpace it in emerging research fields such as AI and quantum computing. Falling behind in these technological races would significantly impair the United States' ability to wage future wars at the staggering pace necessary to overwhelm enemy forces. As highlighted, "Chinese intelligence services have made an art of exploiting the seam between the classified and the pre-classified, where technologies begin to emerge but under US rules are not yet military R&D."[41] The nation or alliance that harnesses quantum technol-

[37] Strobel and Landay, "Exclusive—U.S. Accuses China."

[38] Defense Counterintelligence and Security Agency, "Counterintelligence - Best Practices for Cleared Industry," 26.

[39] Ponniah, "How a Chinese Agent Used LinkedIn."

[40] Brenner, *Glass Houses*, 75.

[41] Brenner, *Glass Houses*, 77.

ogy will swiftly gain access to knowledge and capabilities that were previously decades or even centuries away. This could position that country at the forefront of human civilization's history, potentially rendering it impossible for competitors to achieve parity, as they would possess the capability to impede and obstruct their progress toward the next level of technological advancement. Consequently, the nation's ability to safeguard its citizens and interests both domestically and internationally would be significantly compromised.

It is imperative to contemplate the ramifications for individuals and their families who fall victim to virtual espionage. Their lives will be thrown into disarray. According to 18 U.S.C § 2381, those found guilty of treason against the United States "shall suffer death, or shall be imprisoned not less than five years and fined under this title but not less than $10,000; and shall be incapable of holding any office under the United States."[42] Furthermore, individuals may endure professional and personal humiliation even in the absence of legal consequences. Their credibility and standing in the community may be irreparably tarnished. Moreover, their prospects for future employment will be severely limited, placing their current quality of life in jeopardy.

The Emoluments Clause of the Constitution extends to military retirees as well. It "prohibits receipt of consulting fees, gifts, travel expenses, honoraria, or salary by all retired military personnel, officer and enlisted, Regular and Reserve, from a foreign government unless Congressional consent is first obtained."[43] Additionally, individuals must exercise caution and refrain from entering into any agreement for compensation with a US company that may be offering services to a foreign government.[44]

The following examples underscore the tangible consequences faced by individuals who have disclosed or attempted to disclose sensitive information, with four instances linked to the PRC and one to Russia. For instance, in January 2024, Navy Petty Officer "Thomas" Zhao was sentenced to two years and fined USD 5,500 for providing pictures and details of naval training and exercises, despite facing a potential 20-year sentence.[45] In 2022, Shapour Moinian, a former Army

---

[42] US Congress, 18 U.S.C § 2381 Ch. 115: TREASON, SEDITION, AND SUBVERSIVE ACTIVITIES.

[43] DOD Standards of Conduct Office, "Department of Defense Standards of Conduct Office > DoD Personnel > Ethics Topics for DoD Personnel > Seeking and Post-Government Employment."

[44] Joint Base San Antonio Legal Assistance Office, "General Law Handouts A Tool for JBSA Separating and Retiring Employees (O-6 and below) Post-Government Employment Restrictions"; USAF Office of the General Counsel, "AFD-111021-024 Pre- and Post -Employment Restrictions For Separating and Retiring Air Force Personnel."

[45] Ives, "U.S. Navy Sailor Who Helped China Is Sentenced to 2 Years in Prison"; and Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China."

helicopter pilot and defense contractor, received a 20-month sentence for divulging aviation-related information.[46] Similarly, in 2019, Ron Hansen, a former DIA case officer, was sentenced to 10 years in federal prison, despite facing a possible life sentence.[47] Also in 2019, Kevin Mallory, a retired CIA officer, was handed a 20-year prison term for colluding with Chinese espionage officers after experiencing financial difficulties and being contacted via LinkedIn.[48]

Ongoing federal cases further underscore the severity of the consequences. For instance, Jareh Dalke, a former National Security Agency (NSA) employee accused of attempting to send classified documents to Russia, faces the death penalty, while Navy Petty Officer Second Class "Patrick" Wei, who received thousands of dollars from PRC intelligence for photos and videos, is potentially facing a life sentence.[49]

It is crucial to recognize that even spouses and family members of current or former DOD members can be targeted. For example, the wife of an unnamed US Army officer assigned to the Pentagon became entangled when Mr. Yeo sent money to her bank account for services her husband purportedly rendered after being recruited via LinkedIn.[50] With an awareness of the repercussions of LinkedIn espionage, the subsequent section will delve into the feasibility of espionage and social engineering.

Espionage and Psychology

Foreign adversaries engage in both traditional espionage and exploit the psychological aspects of social engineering when targeting current and former DOD members through LinkedIn. Espionage constitutes a fundamental component of adversaries' spying and intelligence-gathering activities. It encompasses individuals who divulge sensitive information or secrets to a foreign government or adversary regarding the organization they are affiliated with and have access to. As noted, "Espionage is largely uncodified in international law."[51] Individuals who engage

---

[46] Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China."

[47] Stone, "LinkedIn Is Becoming China's Go-to Platform"; and "Former Intelligence Officer Convicted of Attempted Espionage" (press release).

[48] Strobel and Landay, "Exclusive—U.S. Accuses China"; and Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

[49] "Former NSA Employee from Colorado Pleads Guilty to Trying to Send Classified Documents to Russia," *CBS News*, 23 October 2023, https://www.cbsnews.com/; Kevin Johnson, "Ex-NSA Staffer Charged with Espionage, Allegedly Sought Thousands to Relieve Crushing Debt," USA Today, 29 September 2022, https://www.usatoday.com/; and Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China."

[50] Ponniah, "How a Chinese Agent Used LinkedIn"; and Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

[51] Lester Godefrey, "Shape or Deter?: Managing Cyber-Espionage Threats to National Security Interests," *Studies in Intelligence* 66, no. 1 (March 2022), 2, https://www.cia.gov/.

in espionage on behalf of a foreign entity are commonly referred to as *agents* or *informants*, with the latter being the prevalent term used in the United States, while the adversary is typically termed the *handler* in this context.[52]

HUMINT stands as a pivotal element in espionage operations. It entails the recruitment of foreign nationals to gather intelligence against their own country—a process that historically necessitated approximately seven years for HUMINT officers to attain proficiency.[53] However, what the article refers to as *virtual espionage* now enables the traditional facets of espionage and social engineering to be executed through professional social networking platforms in the digital era. This obviates certain traditional training prerequisites, such as proficiency in weaponry and communication techniques, thereby reducing the time required for intelligence operatives to develop their skills. Moreover, virtual espionage is intricately linked to this phenomenon, consequently mitigating some of the conventional risk factors associated with espionage, such as the prospect of apprehension in a foreign jurisdiction. The arrest of an enemy spy on foreign soil carries political repercussions that are no longer pertinent. Allegations of LinkedIn espionage, emanating from the safety of a desk in China or elsewhere, can be readily refuted.[54]

The traditional informant or spy acquisition cycle comprises five distinct steps:

1. Identifying individuals with access to desired information. In the realm of LinkedIn espionage, consideration should also be given to identifying individuals with valuable social network connections and credibility.
2. Assessing their susceptibility to recruitment.
3. Recruiting or presenting a pitch.
4. Managing the informant or asset.
5. Terminating the relationship, if necessary.[55]

In relation to steps 1 and 2, preparation for social engineering commences with thorough research of the target once an individual has been selected, gathering as much information as possible through various channels. This facilitates the crafting of a tailored solicitation approach, which is then deployed against the target. Additionally, it enables the effective exploitation of individuals who take the bait.[56]

---

[52] "'How Spies Operate," MI5, n.d., https://www.mi5.gov.uk/.

[53] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Los Angeles: CQ Press, 2017), 139.

[54] Lowenthal, *Intelligence*, 143; and Gareth Corfield, "Why LinkedIn Is a Snooper's Paradise," *The Telegraph*, 24 August 2023, https://www.telegraph.co.uk/.

[55] Lowenthal, *Intelligence*, 138.

[56] Meeuwisse, *How to Hack a Human*, 46.

Social engineering plays a central role in the manipulation and enticement of current and former DOD members. Cybersecurity specialist Raef Meeuwisse, in his book *How to Hack a Human: Cybersecurity for the Mind*, dissects social engineering through what he terms a "human hacking kill chain," emphasizing that "the word *engineer* suggests an amount of science" is being employed.[57] In espionage recruitment, the objective is to deceive without arousing the target's suspicion, as any sense of distrust may deter them from connecting on LinkedIn or providing information.[58] Therefore, establishing credibility and trust with the target by fabricating an identity constitutes a crucial initial objective of a social engineering operation and forms part of the first step in making contact through a tailored message.[59] The efficacy of the attack is heightened when accompanied by bait or "offering the target an item he/she will perceive to be valuable, likely notice," and desire to obtain.[60]

Money stands out as one of the most prevalent and enticing motivations for targets, as evidenced by its utilization in the attempted approach against me on LinkedIn. Indeed, it is crucial to highlight the acronym MICE, which stands for money, ideology, compromise, or ego. This acronym is frequently employed to categorize the motivational factors that render individuals susceptible to disclosing information or being recruited for espionage.[61]

Foreign intelligence services exhibit great proficiency in exploiting psychological factors to manipulate motivations, emotions, and decisions. They employ tactics such as bait, time pressure, and fear of missing out.[62] Nudge theory, derived from psychology, "looks at how behaviors and decision-making of individuals can be substantially influenced by subtle and often indirect methods."[63] A potent and ingenious strategy to circumvent psychological defenses involves engineering the situation to appear and flow entirely naturally. This is achieved by incorporating real information that resonates with and is pertinent to the target, acquired through research conducted during the preparation phase. Consequently, the target feels

---

[57] Meeuwisse, *How to Hack a Human*, 26.

[58] Perry, "Ethics in the Recruiting and Handling," 71.

[59] Kevin Mitnick and William L. Simon, *The Art of Intrusion: The Real Stories behind the Exploits of Hackers, Intruders, & Deceivers* (Indianapolis: Wiley, 2005), 46.

[60] Meeuwisse, *How to Hack a Human*, 20-30–46.

[61] Michael Smith, *The Anatomy of a Spy: A History of Espionage and Betrayal* (New York: Arcade Publishing, 2020), 10; and Brenner, *Glass Houses*, 79.

[62] Meeuwisse, *How to Hack a Human*, 28-29–46.

[63] Meeuwisse, *How to Hack a Human*, 47.

as though they are experiencing a typical outcome resulting from a genuine and related situation.[64]

Part of the manipulation process involves making the target feel valued, a tactic achieved through "ego gratification."[65] The adversary will convey to the individual their intelligence and knowledge, express admiration for various attributes, and convey gratitude for the opportunity to receive assistance from such an expert. Psychologists have identified numerous benefits individuals derive from helping others, including empowerment and bolstered self-esteem.[66]

Additionally, favorability bias plays a significant role and is employed through name-dropping to present the intelligence officer as part of a trusted group. Targets tend to respond more positively to individuals within their own circle or if they perceive the attacker to be associated with someone they like or admire.[67] For instance, Mr. Yeo, the PRC's Singaporean intelligence asset, showcased his credentials on LinkedIn as a political risk analyst with connections to hundreds of policy makers in the US capital.[68]

Intelligence services can utilize transactions already completed with a target for implicit blackmail, as accepting payment often signifies a point of no return.[69] A successful contact initiated by the adversary with a target via LinkedIn can swiftly escalate into blackmail before the target even discerns any suspicion. Foreign officers will endeavor to exploit any communication and possibly fabricate a narrative to intimidate and further manipulate their victims. This tactic is inherent to their espionage practices. The subsequent focus of discussion is how LinkedIn is utilized to identify targets.

Locating Targets on LinkedIn

Foreign adversaries leverage LinkedIn due to its low cost and risk. LinkedIn, a US-based company, serves as a platform for professionals worldwide to connect, expand their networks, and advance their careers or secure lucrative business opportunities. This platform is particularly attractive to foreign intelligence services because many current and former DOD professionals, including high-ranking officials, utilize it to promote themselves and their networks.

---

[64] Meeuwisse, *How to Hack a Human*, 46.

[65] Brenner, *Glass Houses*, 79.

[66] Mitnick and Simon, *The Art of Intrusion*, 235.

[67] Mitnick and Simon, *The Art of Intrusion*, 237; Meeuwisse, *How to Hack a Human*, 115.

[68] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

[69] Aaltola, "Geostrategically Motivated Co-Option of Social Media," 6; and Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

For a nominal fee of USD 180 per month, an espionage officer can purchase access to "LinkedIn Recruiter Lite," offering advanced search capabilities and automated recommendations tailored to the desired type of professional.[70] Following his 2020 apprehension by the United States, Mr. Yeo noted the significant assistance provided by an unseen ally—the LinkedIn algorithm—in targeting American military personnel for information and recruitment. The algorithm suggested contacts aligned with his prior LinkedIn searches and connections.[71] Foreign intelligence services can access this platform, even if it's restricted in their country, using workarounds as needed. This method aligns with their operational tactics.

There is a notable correlation between individuals targeted on LinkedIn and the Office of Personnel Management (OPM) cyber hack in 2014, which compromised extensive data on over 22 million Americans with security clearances. China admitted the breach originated from within China but attributed it to criminal elements.[72] This highlights how an adversary's broader intelligence operations can facilitate more targeted approaches on LinkedIn. In 2018, following the significant 2017 breach of Equifax's data on Americans, US counterintelligence chief William Evanina cautioned about "super aggressive" actions by Beijing on the Microsoft-owned LinkedIn platform.[73]

In addition to fabricating fake identities, individuals engaging in human hacking also masquerade as major US corporations to enhance their credibility. For example, counterfeit LinkedIn accounts have "impersonated an HR manager from Collins Aerospace, a major US supplier of aerospace and defense products," as well as HR personnel from General Dynamics.[74] These tactics aim to establish various types of professional relationships, potentially luring experts in critical fields through false job opportunities.[75]

AI plays a crucial role in assisting intelligence officers in crafting sophisticated fake profiles by ensuring proper language usage in profiles and correspondence. While ethnic Chinese individuals in the West were previously more targeted,

---

[70] "LinkedIn Recruiter Lite," LinkedIn, n.d., https://business.linkedin.com/.

[71] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight"; and Ponniah, "How a Chinese Agent Used LinkedIn."

[72] Ponniah, "How a Chinese Agent Used LinkedIn"; Lowenthal, *Intelligence*, 502; and Rudd, *The Avoidable War*, 163.

[73] Ponniah, "How a Chinese Agent Used LinkedIn"; and Strobel and Landay, "Exclusive—U.S. Accuses China."

[74] Dominik Breitenbacher and Kaspars Osis, "Operation In(Ter)Ception: Targeted Attacks against European Aerospace and Military Companies" (white paper, ESET Research, June 2020,) 2, https://web-assets.esetstatic.com/.

[75] *Targeting U.S. Technologies*, 11.

virtual espionage aided by AI has expanded the scope of potential targets.[76] AI will further facilitate LinkedIn espionage on a larger scale, allowing for the continuous maintenance of fake profiles, despite LinkedIn's efforts to block and remove such accounts. The graph below, based on LinkedIn's transparency report data, illustrates the escalating trend of fake accounts being proactively restricted by platform administrators. This trend surged from 4.4 million at the close of 2021 to 15.1 million in the first half of 2023.

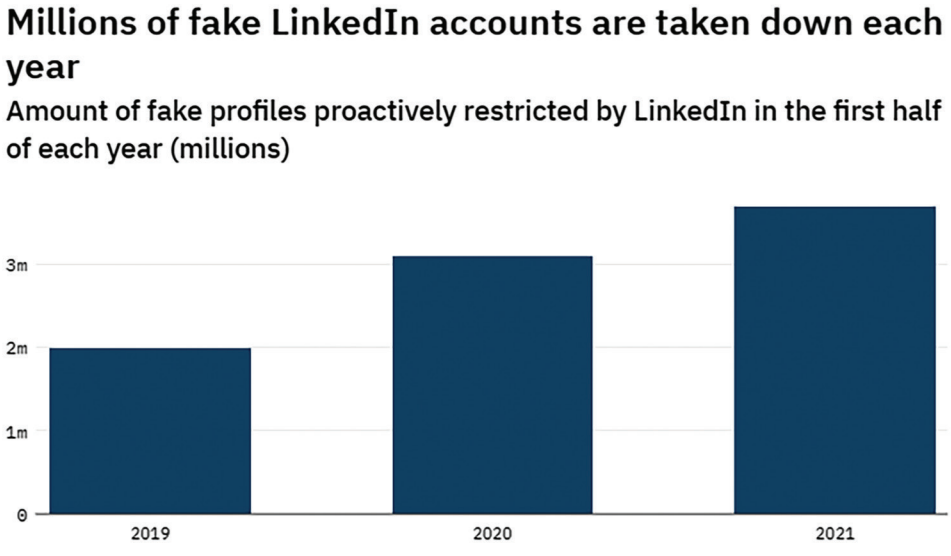

Figure 1. Millions of fake LinkedIn accounts are taken down each year

Moreover, the widespread use of smartphones and mobile capabilities has heightened LinkedIn's accessibility, increasing the likelihood of ensnaring a target. As one expert notes, "The leap into mobile technology, has had a tremendous influence on human behavior."[77] Adversaries exploit this by sending out numerous approaches simultaneously and patiently waiting for someone to take the lure.[78] Therefore, the question arises: How can this threat be effectively countered?

Defeating this Threat

Countering the threat posed by foreign adversaries attempting to recruit current and former DOD members via LinkedIn is both crucial and feasible. However,

[76] Aaltola, "Geostrategically Motivated Co-Option of Social Media," 8.
[77] Biały, "Social Media," 86.
[78] Corfield, "Why LinkedIn Is a Snooper's Paradise."

there is currently a lack of focused training, education, and mainstream awareness regarding this threat. Numerous articles and examples highlighting the risk of virtual espionage on LinkedIn support the findings of a study indicating that "LinkedIn members have been found to be significantly more likely than Facebook users to allow public access to their professional and educational data."[79] Mr. Yeo recounted to the *Financial Times* that "several former military commanders and specialists at the Pentagon accepted his connection requests without thinking."[80] Despite these risks, LinkedIn's professional community policy fails to offer practical recommendations for safeguarding against exploitation by fake profiles or falling victim to deception.

This article's top recommendation for countering virtual espionage involves launching a focused campaign by the US government aimed at turning adversaries' efforts against them and inflicting significant costs. This campaign would involve incentivizing current and former DOD members to report any suspicious contacts or solicitations to law enforcement. In exchange for their assistance in thwarting the adversary's espionage attempts, these individuals would receive monetary compensation. Law enforcement authorities would then pass on these reports to US counterintelligence agencies, which would collaborate closely with the targets. Through this collaboration, US counterintelligence agencies would exploit the activities of foreign intelligence services, including causing financial losses to adversaries by enabling the targets to receive and retain the money offered by adversaries. This campaign directly addresses the motivation of money that adversaries exploit to compromise individuals.

Moreover, everyone should exercise extreme caution when receiving new connection requests, particularly if they appear overly appealing; chances are, they are deceptive. The process of manipulating individuals often begins with a connection request, making it imperative for the community of current and former defense professionals to adopt specific measures before accepting such invitations. Firstly, individuals they do not know seeking to connect should have a mutual contact who can facilitate an introduction. Secondly, this introduction should be accompanied by relevant context explaining the reason for the connection request. Implementing these measures would signify a positive shift in the professional network-

[79] Mohammed Khaled Alotaibi, "The Influence of Personal Characteristics and Other Factors on the Susceptibility of Public Sector Employees to Cyber-Social Engineering through LinkedIn: A Mixed-Methods Sequential Explanatory Study" (thesis, Trinity College Dublin. School of Computer Science & Statistics. Discipline of Computer Science, 2021), 4, http://www.tara.tcd.ie/.

[80] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

ing behavior and norms within the defense community, bolstering collective resilience against virtual espionage.

Unsolicited consulting offers may appear innocuous on the surface, but receiving them unexpectedly from unfamiliar entities should raise concerns. When suspicions are aroused, it is crucial to promptly reach out to the OSI or other relevant federal law enforcement agencies within the DOD, such as the FBI. It is advisable to notify authorities if further investigation into an unsolicited consulting contact reveals signs of a fabricated persona or an illegitimate consulting firm.

The 2023 *NCS* highlights the imperative to develop and deploy "enhanced digital identity solutions," building upon the ongoing digital identity research program led by the National Institute of Standards and Technology (NIST) to fortify digital credentials.[81] These initiatives represent significant strides by the government and will play a crucial role in alerting social media users to fraudulent or deceptive networking attempts. However, the *NCS* does not explicitly address the threat of virtual espionage, although it could be inferred from passages concerning social networks. It is essential to explicitly acknowledge the danger posed by virtual espionage in the NCS, particularly while technical solutions are being developed, with specific mention of platforms like LinkedIn where such activities are prevalent.

On the other hand, the 2023 DOD *Cyber Strategy Summary* acknowledges the threat of virtual espionage and includes a line of effort (LOE) titled "Build Enduring Advantages in Cyberspace." This LOE encompasses initiatives aimed at developing, securing funding for, and implementing educational curricula at various levels of professional military and civilian education, including courses for General Officers and Senior Executive Service (SES) personnel.[82] Despite this recognition, the current training efforts within the LOE do not explicitly address the active DOD force's susceptibility to outside solicitations, side employment, or post-DOD work, whether in consulting or other capacities. It is imperative that the training efforts under the LOE be expanded to encompass these aspects and adequately prepare personnel for such threats.

Research and discussions underscore the importance of addressing the threat of virtual espionage within the DOD, with the "DOD Annual Cyber Awareness" computer-based training being identified as the closest existing framework for such education. However, it is evident that the current training falls significantly short in this regard. While the DOD-wide cyber awareness training adequately

[81] *National Cybersecurity Strategy*, 26.

[82] *US Department of Defense Summary Cyber Strategy* (Washington: DOD, 2023), 13–14, https://media.defense.gov/.

covers topics such as protecting personally identifiable information (PII) and operational security (OPSEC), it lacks specific education on virtual espionage targeting members through platforms like LinkedIn.

There is an urgent need to enhance the DOD Annual Cyber Awareness training by incorporating a dedicated section on virtual espionage, along with relevant vignettes illustrating common tactics and scenarios encountered on professional networking sites. Additionally, current DOD members would benefit from periodic counterintelligence training stand-downs, which can enhance their awareness and ability to identify suspicious activities or patterns indicative of an attack. The more informed and vigilant personnel are, the better equipped investigators will be to detect and mitigate potential threats.[83]

It is imperative to improve the existing guidelines governing outside employment for both active-duty DOD members and former personnel, to bolster efforts to mitigate threats. Clarity and consistency regarding permissible and restricted activities should be readily accessible through a simple online search. However, during research for this article, it became apparent that this information was not readily available at the top of search results.

An immediate remedy is to prioritize the dissemination of standardized guidance to ensure that pertinent information appears prominently in search results. Additionally, active military members seeking supplementary employment should seek additional guidance from local legal offices, while their current supervisory chain is responsible for addressing any questions or concerns related to outside employment. However, it has become evident from discussions that there is a pressing need for standardized protocols across all sectors, including civilians and contractors. As outlined in the Joint Ethics Regulations (JER 2-303), "commanders can require any DoD employee to report outside employment … and a commanding officer or supervisor can prohibit any off-duty employment if he or she believes the proposed activity will detract from readiness or will pose a security risk."[84]

A standardized questionnaire form should be implemented to ensure thorough review and assessment by the First Sergeant or their designated representative, aimed at identifying any potential espionage concerns involving military personnel. This form must include a legal disclaimer and a reminder of the serious repercussions of neglecting to conduct comprehensive background research on the prospective employer. It should also emphasize the importance of promptly reporting any

[83] Mitnick and Simon, *The Art of Deception*, 305.

[84] Department of Defense Standards of Conducts Office, "Joint Ethics Regulation on Outside Activities," November 2013, 4, https://dodsoco.ogc.osd.mil/; and Joint Base San Antonio Legal Assistance Office, "Off-Duty Employment," 1.

attempted espionage. Similarly, local Civilian Personnel Offices should require and oversee a similar process for civilians, while contracting officer representatives should manage it for DOD contractors. Enhanced oversight of outside employment should be complemented by an annual review of the outside employment program, integrated into a commander's programs as part of the Management Internal Control Toolkit (MICT) USAF inspection system.

It is important to note that while reviewing guidance from the DOD Standards of Conduct Office and sampling guidance from various installations for separating or retiring military personnel, no specific instructions were found for former DOD members who separated from service before reaching retirement eligibility. These individuals must also be mindful of the legal ramifications of providing valuable insights to foreign entities, potentially aiding adversaries in their intelligence efforts. The legal landscape surrounding non-retirees and former civilian retirees of the DOD remains unclear, necessitating explicit codification of rules, laws, and associated consequences in this area.

An area of notable concern with "no search results" pertains to employment restrictions for current and former holders of top-secret clearances. To further mitigate the risk of espionage, it is imperative for lawmakers and DOD authorities to address guidelines and penalties concerning individuals who currently hold or previously held such clearances.

Consideration should be given to implementing a ban preventing current and former DOD members from publicly disclosing their clearance status. This measure would disrupt foreign intelligence officers' ability to exploit LinkedIn algorithms for searching or receiving suggested contacts based on users' security clearance information. However, job seekers would still be able to disclose their clearance status during formal resume submissions or interviews. Such a policy could significantly enhance security measures and safeguard against potential espionage threats.

Another essential recommendation in countering the threat is to ensure that TAP offices inform separating and retiring DOD members about the potential risks. This information should also be integrated into the procedures of Civilian Personnel Offices and CORs for individuals leaving DOD-affiliated employment. Additionally, a valuable tool is to include susceptibility tests for social engineering attacks as part of routine security assessments for DOD members.[85]

Members should be informed to anticipate these evaluations periodically, fostering heightened awareness and sensitivity to potential vulnerabilities. This proactive

[85] Mitnick and Simon, *The Art of Intrusion*, 238; Mitnick and Simon, *The Art of Deception*, 262.

approach will contribute to a stronger defense against such threats, as individuals will be better prepared to identify and address potential weaknesses.

Another strategy to expose illicit actors involves drawing parallels with adversary offensive cyber operations. Foreign espionage officers may find it cumbersome to create and manage numerous fake personas or companies, leading them to reuse the same identities.[86] Identifying such indicators can be instrumental in identifying malicious activity and thwarting espionage attempts.

Encouraging progress has been made in addressing this issue. LinkedIn has engaged in discussions with US law enforcement agencies regarding Chinese espionage activities on the platform.[87] Additionally, there is a helpful app called "Think Before You Link" that is accessible to LinkedIn users. Sponsored by the United Kingdom's National Protective Security Authority, this app is designed to aid individuals in recognizing fake profiles on LinkedIn. It offers education on identifying indicators of fake profiles and includes a profile reviewer feature. This valuable tool is also available for use in the United States.[88]

Conclusion

In conclusion, LinkedIn espionage poses a significant threat to national security. Virtual espionage is characterized by its low cost and risk, as it bypasses traditional clandestine officer training requirements such as weapons training and specialized communication techniques. This is because LinkedIn provides a platform for attempting to recruit foreign nationals to steal secrets without the need for such training. Moreover, LinkedIn espionage eliminates the risk of these virtual intelligence officers being apprehended in foreign territory. The extent of this problem, as highlighted by US and other Western government officials, demands increased attention and action from policy makers, the DOD, and the defense industrial base to safeguard the resilience of both former and current DOD members.

The DOD continues to bolster its physical and increasingly sophisticated technical security measures, posing challenges to foreign spies seeking to acquire intelligence, defense plans, and technology. However, hackers targeting human vulnerabilities seek ways to bypass these robust defenses, recognizing that deceiving current or former DOD members can be a successful tactic.[89] Our adversar-

[86] Timo Steffens, *Attribution of Advanced Persistent Threats: How to Identify the Actors behind Cyber-Espionage* (Berlin: Springer Vieweg, 2020), 148.

[87] Ponniah, "How a Chinese Agent Used LinkedIn"; and Strobel and Landay, "Exclusive—U.S. Accuses China."

[88] Afiq Fitri, "MI5 and FBI Sound the Alarm on Online Espionage with LinkedIn a Prime Target," *New Media Statesman Group*, 19 May 2022, https://newstatesmanmedia.com/.

[89] Mitnick and Simon, *The Art of Deception*, 7.

ies rely on compromising US and Western defense professionals to commit treason, whether through unwitting cooperation or coercion. As Meeuwisse states, "Our nervous system contains many prewired mechanisms that operate in a certain way, whether or not we consciously approve of these actions."[90] This explains why individuals are often inclined to say yes to requests from people they like or to accept LinkedIn requests from individuals who appear credible and trustworthy, especially if endorsed by a mutual connection.[91] Psychology elucidates why individuals may be susceptible to requests from those who project trustworthiness, honesty, or attractiveness.

Some current and former DOD members inadvertently expose themselves by providing detailed information about their work history and clearance levels on LinkedIn, more so than they would on other online platforms.[92] As one observer noted, "In a bygone era, publicly advertising oneself as a holder of such clearances amounted to asking for it to be withdrawn."[93] When this information is coupled with the vast amounts of personal data held by commercial companies, it allows foreign intelligence services to develop a comprehensive psychographic profile of an individual.

Chinese intelligence targets individuals across the DOD spectrum, from high-clearance senior officials to lower-tier and early-career personnel. The ongoing exploitation of LinkedIn and the recent 2023 case involving two young Navy Sailors allegedly engaged in espionage highlight the statement made by Senator Mark Warner (D-VA), the top Democrat on the Senate Intelligence Committee, in 2018, underscoring "the length to which Chinese intelligence will go, and the 21st Century counter-intelligence challenges."[94]

Despite attempts by other countries like Russia, Iran, and North Korea, China poses the greatest threat for LinkedIn exploits.[95] China demonstrates a high level of comfort with espionage through various means, as evidenced by the numerous mass cyberattacks attributed to the country.[96] Intelligence agencies globally, particularly in the West, are concerned about China's "increasingly astute online espionage efforts," with LinkedIn being a prominent platform for such activities.[97]

---

[90] Meeuwisse, How to Hack a Human, 49.

[91] Mitnick and Simon, *The Art of Intrusion*, 236.

[92] Strobel and Landay, "Exclusive—U.S. Accuses China"; and Corfield, "Why LinkedIn Is a Snooper's Paradise."

[93] Corfield, "Why LinkedIn Is a Snooper's Paradise."

[94] Youssef and Strobel, "Navy Sailors Charged with Allegedly Spying for China"; and Strobel and Landay, "Exclusive—U.S. Accuses China."

[95] Ponniah, "How a Chinese Agent Used LinkedIn"; and Strobel and Landay, "Exclusive—U.S. Accuses China."

[96] Rudd, *The Avoidable War*, 292.

[97] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

US intelligence services are already cautioning their current and former officials about this threat.[98] The DOD must follow suit, with a specific focus on individuals' date range of separation, rank held, last position, overall assignments history, clearance status, and unique information exposure.

Potential counterarguments exist against concerns regarding foreign adversaries attempting to recruit current and former DOD members using LinkedIn. Some may argue that espionage over LinkedIn may be less of a concern than portrayed because most current and former defense professionals are likely to quickly identify and avoid such traps. Additionally, the DOD does not prohibit the use of LinkedIn and ensures that its personnel are trained in social media usage and obligated to protect sensitive defense information.[99] Moreover, sharing personal experiences in an unclassified context, such as on professional networking sites, is common and is not currently perceived as a significant threat.

Furthermore, concerns may not be warranted because LinkedIn actively identifies and removes fake accounts and collaborates with various government agencies worldwide to counter virtual espionage.[100] For these reasons, some individuals might believe that the danger posed by LinkedIn espionage is low.

Finally, it is worth noting that William Evanina, the former head of national counterintelligence for the United States from 2014 to 2021, was the first and last senior official to receive focused media attention in 2018 regarding espionage activity on LinkedIn targeting American military and government professionals. He publicly identified China as the perpetrator. However, it is essential for this issue to receive regular emphasis in the mainstream media, as it represents a significant threat to maintaining the US competitive stance in great-power competition. Evanina's media push occurred more than five years ago, highlighting the need for continuous attention to this matter. ✪

Lt Col Caleb S. Lisenbee II, USAF

Lieutenant Colonel Lisenbee is a cyberspace operations officer with a distinguished career in the US Air Force. Currently a student at Air War College, Air University, Maxwell AFB, Alabama, he previously served as the Deputy Division Chief for Current Operations at Headquarters 16th Air Force, Joint Base San Antonio-Lackland, Texas. In this role, he oversaw information warfare efforts across 49,000 Airmen, directing operations in support of 11 combatant commands and national priorities. Lisenbee began his Air Force journey in May 2004 after graduating from Fayetteville State University's ROTC program. Throughout his career, he has held various leadership positions, including squadron commander, and has served in multiple staff tours with organizations such as 17th Air Force, Air Force ISR Agency, US Indo-Pacific Command, and Pacific Air Forces. He has deployed numerous times in support of operations including Enduring Freedom, Iraqi Freedom, and Willing Spirit, accumulating 381 combat flying hours conducting ISR operations. Additionally, he played a direct role in Operation Odyssey Dawn.

[98] Strobel and Landay, "Exclusive—U.S. Accuses China."

[99] Manson, Murphy, and Shubber, "LinkedIn Spy Scandal Shines Spotlight."

[100] Corfield, "Why LinkedIn Is a Snooper's Paradise."