

# Spies, Hackers, Social Media, AI, Oh My!

## CW3 Jason Coombs

Near-peer and state-sponsored adversaries are using social media, cyber operations, and traditional HUMINT tradecraft to target operations, Soldiers, and their families. Commanders must ensure their personnel understand that online behavior, OPSEC, and cybersecurity are not just personal matters, but battlefield vulnerabilities that can directly affect mission success.

### **The Battlefield Has Moved to Your Pocket**

Today's Army is operating more and more within the "gray zone" or below the threshold of war, where the operational lines can be blurry. Our adversaries do not always play by the same rules where there are Title 10 and Title 50 authorities. Our adversaries do not have to breach a wall, hack a classified system, or undertake extensive measures to recruit an insider threat. All they have to do is go online and appeal to one of Maslow's hierarchy of needs on LinkedIn, Instagram, Reddit, Discord, or any other social media platform to make a connection (Ceder, 2025; Lowe, 2025; Yoshida, 2025b). A quick look inside any Soldier's pocket reveals a smartphone that is now part of the operational environment. Every social media profile is a targeting package, and every friend is a line of operation (LOO), i.e., a target deck (Obis, 2025; Lt Col Lisenbee, 2024).

This threat is not theoretical. Senior Intelligence officials and leaders, the Government Accountability Office (GAO), and other Western intelligence services have all issued clear warnings that nation-state adversarial intelligence services like Russia and the People's Republic of China (PRC) are exploiting online platforms to assess, develop, and recruit Defense personnel to collect information on their behalf. These recruitments have occurred through elaborate ruses that include, but are not limited to, job offers, pay for seemingly meaningless tasks (e.g., write a white paper on your experiences in your unit), and sexual provocations (LTG Hale, 2025; GAO, 2025; D'Agati, 2019). The danger is not just what Soldiers post or how they portray themselves online, but how adversaries combine small pieces of seemingly harmless information into targetable intelligence.

If Commanders and Soldiers do not understand this threat in simple, practical terms, then the annual training requirements and Army policies will fail. Personnel must realize and understand that poor online practices can enable compromise across the human and technical domains, putting operations and even families at risk.

### **Adversaries Weaponizing Social Media**

With advancements in technology and the rise of social media applications, our adversaries and their foreign intelligence services (FIS) have adapted their offensive posture faster than the Department of War (DoW) can. Focusing on the path of least resistance, adversaries seek to develop an insider threat by exploiting human behavior. They are using social media and professional networking platforms like LinkedIn, Reddit, and Discord to collect resumes, unit affiliations, career and permanent change of station (PCS) timelines, and social networks to develop their targeting package (Ceder, 2025; Edwards, 2026; Lt Col Lisenbee, 2024; Lowe, 2025).

An Infantryman who has learned the most recent tactics and used new technology, the logistics Private who is doing all the ordering and processing of new gear and equipment, or the admin who knows

the ins and outs of the personnel in the unit – they all have information valuable to our adversaries. An important note that is not emphasized enough: Soldiers are not being targeted because they did something wrong; they are being targeted because they have value.

## **How Surfing Social Media Morphs Into Espionage**

Espionage cases no longer require secret meetings or specialized tradecraft; they can simply start with a message request. Recent news reporting highlights the threat and tactics of the People's Republic of China (PRC) on LinkedIn, where it poses as recruiters and consultants to identify and develop targets of interest (Edwards, 2026; Hui, 2026; Lt Col Lisenbee, 2024; Lowe, 2025). In November 2025, the Army's senior Intelligence Officer and former G-2, LTG Hale, issued a message to the force warning of threats facing Army personnel and their families, and of ongoing operations, and urging everyone to stay alert and aware. Hale pointed to seemingly harmless approaches, such as job offers or small payments to write papers about Soldiers' unit experiences, command climate, or how new technologies apply to current operations (LTG Hale, 2025; Lowe, 2025). These requests can then escalate to offers of money for unclassified Army publications or regulations, followed by sensitive but unclassified material, and ultimately - the coup de grâce - classified information. Once communication begins and any material is shared, it becomes a slippery slope; the hook is set (D'Agati, 2019; Polymeropoulos, 2026).

Foreign intelligence services understand human motivation. To highlight this, adversaries often use a matrix similar to the classic MICE framework that focuses on: money, ideology, compromise, and ego. Soldiers facing financial strains, work or career frustrations, loneliness, or a strong desire for recognition are especially vulnerable under MICE. Many of these feelings can be found and developed from an individual's online presence or profile, and are easily exploited. A simple picture of a pretty girl can capture a lonely Soldier's attention, or an offer of money for writing a simple paper about their weekly activities in exchange for money and accolades, allows an adversary to exploit these factors without the target ever realizing that they are being manipulated or doing something wrong (D'Agati, 2019; Polymeropoulos, 2026).

Several recent cases have demonstrated that these tactics are true, effective, and consistent. In a recent case, a U.S. Navy petty officer was approached through a social media chat group focused on stock trading. What began as a casual conversation turned into requests for sensitive military data, which he eventually provided in exchange for money (Yoshida M., 2025b). Another Sailor passed dozens of technical manuals to PRC intelligence officers after being recruited online, receiving relatively small payments that nonetheless resulted in a 16-year prison sentence (Fuentes, 2026). These two cases, among many, highlight a hard truth: adversaries only need opportunity, access, and patience.

## **The Setup – Fusing Social Media with Cyber Operations**

Espionage today is not exclusively about getting someone to talk or pass documents; it is also about compromising devices. As a follow-up to online targeting, adversaries are using social media to deliver malware or spyware, and with current advancements, it can be delivered without user interaction. Zero-click cyber exploitation is increasingly common, exploiting device vulnerabilities that allow compromise without the user clicking a link (Sharma, 2026; Sharma, 2026). Some of the more advanced tools, like NSO Group's Pegasus Project, used against government and military officials, dignitaries, and journalists, can collect nearly everything from their mobile devices (International, 2021). Less advanced spyware, such as "Hermit," which targets both iOS- and Android-based devices, allows attackers to collect messages, contacts, photos, and geolocation data (Townsend, 2022; Underhill, 2025). Malware and spyware are often delivered through social engineering via links. A common method is through job-advertisement links or posing as a female friend who sends their target a link to their OnlyFans page for

free content, which is actually a redirect to download spyware. With advancements in technology, cyber actors are embedding malicious code into messages and documents that execute automatically, using Artificial Intelligence (AI) to bypass basic security protocols (Sharma, 2026; Pearl, 2026).

The Army does a good job of emphasizing the importance of OPSEC but misses the mark on basic device security measures (AR 530-1, 2014; Flores-Wilkin, 2024; SM Guide, 2026; Flores-Wilkin, 2023). One could say that device security is covered in Cyber-Security training, but beyond not clicking on links from people you do not trust, what else is there? One of the easiest phone security measures is powering down your phone each night to thwart mobile threats. Most malware/spyware exploits do not persist through a device's power cycle (Whitney, 2025). Another threat mitigation is not scanning public QR codes, turning off location services, and asking, "Why does your calculator need access to your contact list? Check your applications and turn off unnecessary access to your phone's secrets. The big takeaway for a Soldier is simple: you do not have to be reckless or crazy online to be compromised; you just have to be predictable or lazy.

## **Why OPSEC Matters – Loose Lips Sink Ships**

Army Regulation (AR 530-1) defines Operational Security as the identification and protection of critical information from adversaries. That definition has not changed. What has changed is where that information resides. Seemingly harmless posts on social media – pictures of you on the compound in the warzone, complaints about the unit (morale), or even family updates can be pieced together like a puzzle that reveals a picture – unit readiness, timelines, vulnerabilities (Flores-Wilkin, 2024; Thorne, 2025; Yoshida M. , 2025). The Army's Social Media guidance warns Soldiers and families to assume adversaries are reading every post and painting the picture of access (AR 530-1, 2014; SM Guide, 2026).

The Army has programs in place and publishes articles of awareness, but are they read? Are they posted in locations where the new Infantryman arriving at his unit overseas can access them? This is definitely an area where we can improve. Most DoW components failed to provide proper OPSEC and CI training, often glossing over it, and many personnel were never trained on mobile device security (GAO, 2025; Flores-Wilkin, 2023). This is not a policy failure alone; it is a correctable leadership challenge.

## **Why Check-the-Box Training Is Not Enough**

Counterintelligence Threat Awareness and Reporting (TARP) is required annual training (AR 381-12, 2025) and while necessary, it does not change anyone's behavior. Unlike most Army online training, which usually consists of a kindergarten-style video, TARP is often delivered through in-person instruction. Soldiers often understand the rules in theory but underestimate in reality, how aggressively they are being targeted (Lt Col Lisenbee, 2024; LTG Hale, 2025). If Soldiers believe that espionage can only happen to someone else or that spyware only affects careless users, they will continue to overshare, accept unknown contacts, click links from unknown senders, and continue poor security practices.

## **The Commander's Role – Making it Real**

Command emphasis matters. Soldiers take cues from what leaders reinforce consistently, not just once a year. Commanders reinforce what is important. Therefore, Commanders must ensure Soldiers understand three simple truths (Flores-Wilkin, 2023):

- Every Soldier is a potential target, regardless of rank or MOS.

- Social media is an intelligence collection platform, not just entertainment.
- Small mistakes can have strategic consequences.

Hands-on leadership involvement includes attending training to understand the threat truly. Training should include real-world examples, personal examples when applicable, and current training, tactics, and procedures (TTPs) used by our adversaries, to have more impact than reading a slide of warnings. When leaders can acknowledge their own vulnerabilities and mistakes, it reinforces that these are share responsibilities, not a disciplinary trap or a simple yearly requirement.

## **OPSEC and Digital Discipline Is Combat Readiness**

Our adversaries are patient, professional, and persistent. They are not waiting for the next conflict to begin shaping the battlefield; they are doing it now, one friend request at a time (Lt Col Lisenbee, 2024). Ensuring Soldiers and their families understand the online threat environment is not about restricting freedom or discouraging technology use. It is about recognizing that OPSEC and digital discipline are now part of combat readiness (Flores-Wilkin, 2024). Similar to how we train Soldiers to secure weapons and sensitive equipment, we must train them to secure their personal information, online behavior, and devices.

The cost of complacency is no longer theoretical. It is measured in compromised operations, lives lost, endangered families, and ruined careers. Attention and focus from Commanders today can prevent tomorrow's clickbait headlines.

## **About the Author**

CW3 Jason Coombs is a Counterintelligence and TARP/OPSEC professional. CW3 Kristen Tritz, CW3 Michael Gabel, and CW3 Timothy Hornback peer-reviewed this article before submission.

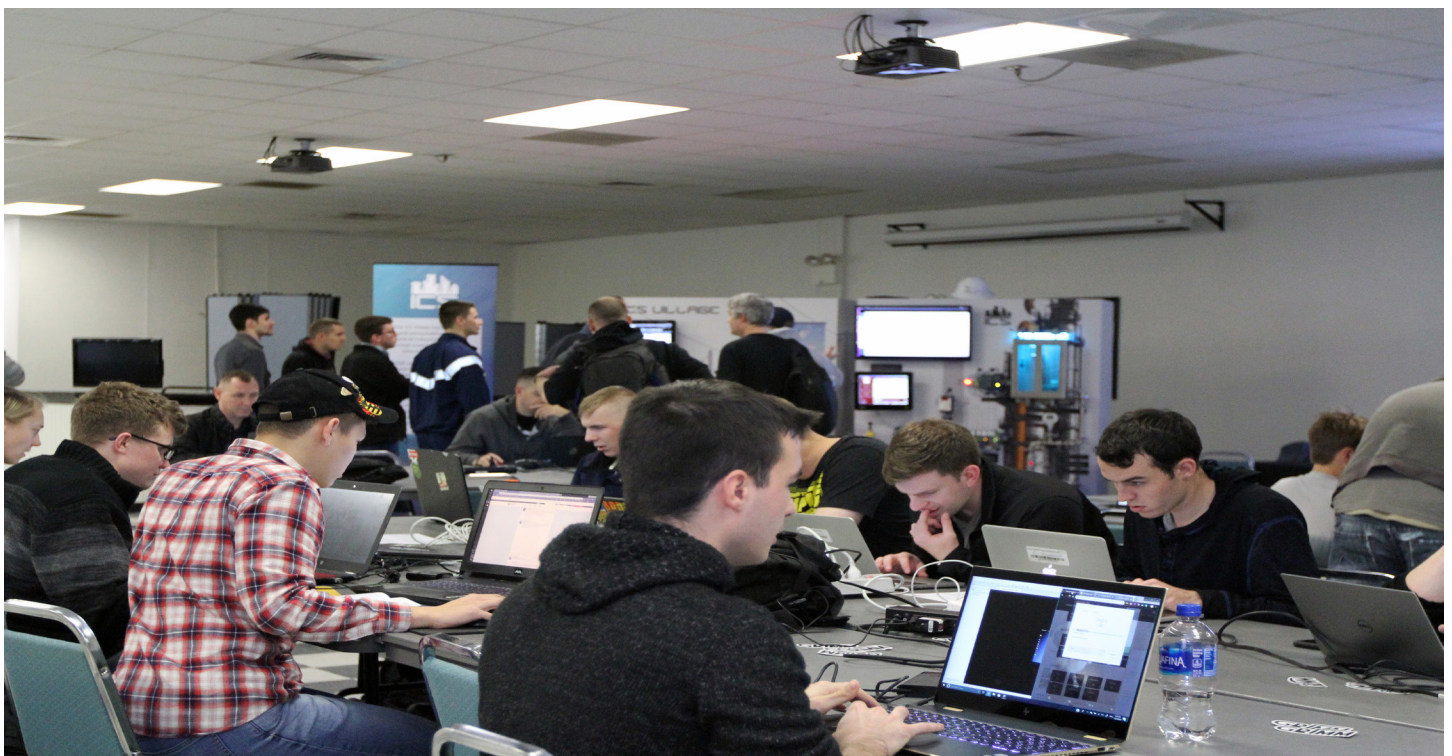


Photo: DVIDS 2018. FORT GEORGE G. MEADE, Md. – “Conquer the Flag” and “Howdy Neighbor IOT” (Internet of Things) capture the flag were two village events attendees could participate in at the third annual AvengerCo

## References

- Army Social Media Guide. (2026). Army social media guide. U.S. Army. <https://www.army.mil/socialmedia/>
- Ceder, R. (2025, October 16). Soldiers are being contacted by adversaries on LinkedIn, Reddit, the Army says. Defense News. <https://www.defensenews.com/news/your-army/2025/10/16/soldiers-being-contacted-by-adversaries-on-linkedin-reddit-army-says/>
- D'Agati, D. (2019, August 2). Want to fight insider threats? Just look for the MICE. ClearanceJobs. <https://news.clearancejobs.com/2019/08/02/want-to-fight-insider-threats-just-look-for-the-mice/>
- Edwards, C. (2026, January 20). Britain approves 'mega' Chinese embassy in London despite national security fears. CNN. <https://www.cnn.com/2026/01/20/uk/uk-china-mega-embassy-royal-mint-court-intl>
- Fuentes, G. (2026, January 13). Sailor to serve 16-year prison sentence for selling secrets to China. USNI News. <https://news.usni.org/2026/01/13/sailor-to-serve-16-year-prison-sentence-for-selling-secrets-to-china>
- Government Accountability Office. (2025). Information environment: DOD needs to address security risks of publicly accessible information (GAO-26-107492). <https://www.gao.gov/assets/gao-26-107492.pdf>
- Headquarters, Department of the Army. (2014). Operations security (AR 530-1). U.S. Army. Headquarters, Department of the Army. (2025). Counterintelligence awareness and reporting (AR 381-12). U.S. Army.
- Hale, A. (2025, November 24). Message to the force: Protecting the force against foreign intelligence threats. U.S. Army. <https://api.army.mil/e2/c/downloads/2025/11/24/10456559/message-to-the-force-protecting-the-force-against-foreign-intel-threats.pdf>
- Hui, S. (2026, January 20). UK approves a 'mega' Chinese embassy in London despite criticism of security risks. ABC News. <https://abcnews.go.com/International/wireStory/uk-approves-mega-chinese-embassy-london-despite-criticism-129374853>
- Lisenbee, C. (2024). Covert connections: The LinkedIn recruitment ruse targeting defense insiders. Journal of Indo-Pacific Affairs. <https://www.airuniversity.af.edu/JIPA/Display/Article/3768503/covert-connections-the-linkedin-recruitment-ruse-targeting-defense-insiders/>
- Lowe, A. (2025). Army's top spy warns of growing threat. U.S. Army. [https://www.army.mil/article/289201/armys\\_top\\_spy\\_warns\\_of\\_growing\\_threat](https://www.army.mil/article/289201/armys_top_spy_warns_of_growing_threat)
- Obis, A. (2025, November). DoD failing to address growing security threats posed by publicly available data. Federal News Network. <https://federalnewsnetwork.com/defense-news/2025/11/dod-failing-to-address-growing-security-threats-posed-by-publicly-available-data>
- Pearl, M. (2026). Did you get an Instagram password reset email recently? Gizmodo. <https://gizmodo.com/did-you-get-an-instagram-password-reset-email-recently-this-might-be-the-very-unpleasant-reason-2000708667>
- Polymeropoulos, M. (2026). The art of agent-running. Engelsberg Ideas. <https://engelsbergideas.com/notebook/the-art-of-agent-running/>

- Project Pegasus. (2021, July). Massive data leak reveals Israeli NSO Group's spyware used to target activists, journalists, and political leaders globally. Amnesty International. <https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/>
- Sharma, R. (2026). Radware uncovers ZombieAgent, a zero-click AI vulnerability in OpenAI agents. The Fast Mode. <https://www.thefastmode.com/technology-solutions/46638-radware-uncovers-zombieagent-a-zero-click-ai-vulnerability-in-openai-agents>
- Thorne, A. (2025). Learning to take OPSEC seriously protects everyone. U.S. Army. [https://www.army.mil/article/285690/learning\\_to\\_take\\_opsec\\_seriously\\_protects\\_everyone](https://www.army.mil/article/285690/learning_to_take_opsec_seriously_protects_everyone)
- Townsend, C. (2022). Google warns of 'Hermit spyware' infecting Android and iOS devices. Mashable. <https://mashable.com/article/google-warns-spyware-android-ios>
- Underhill, K. (2025). Android zero-click flaw lets hackers take over devices. eSecurity Planet. <https://www.esecurityplanet.com/threats/android-zero-click-flaw-lets-hackers-take-over-devices/>
- Whitney, L. (2025). Why you should power off your phone at least once a week, according to the NSA. ZDNET. <https://www.zdnet.com/article/why-you-should-power-off-your-phone-at-least-once-a-week-according-to-the-nsa/>
- Yoshida, M. (2025a). OPSEC awareness month: Avoid oversharing on social media, practice OPSEC. U.S. Army. [https://www.army.mil/article/285316/opsec\\_awareness\\_month\\_avoid\\_oversharing\\_on\\_social\\_media\\_practice\\_opsec](https://www.army.mil/article/285316/opsec_awareness_month_avoid_oversharing_on_social_media_practice_opsec)
- Yoshida, M. (2025b). AT awareness month: Online targeting, do not take the bait. U.S. Army. [https://www.army.mil/article/287786/at\\_awareness\\_month\\_online\\_targeting\\_dont\\_take\\_the\\_bait](https://www.army.mil/article/287786/at_awareness_month_online_targeting_dont_take_the_bait)