New! [Haag - Week 6](https://edge.apus.edu/portal/site/406241/tool/855949ad-3075-4284-8ded-13aab73f8995/discussionForum/message/dfViewThread" \o " Haag - Week 6)

Jeremiah Haag (Jun 10, 2019 8:39 AM) - Read by: 3

[Mark as Read](javascript:void(0);) [Reply](https://edge.apus.edu/portal/site/406241/tool/855949ad-3075-4284-8ded-13aab73f8995/discussionForum/message/dfViewThread)

Good morning Class, Dr. Burch;

The week six forum question focused on the power of social media and the information gleaned from Open Source Intelligence (OSINT) being prodigious and powerful enough to change the course of human events. We were asked to provide examples that might benefit from Social Network intelligence employing cyber intelligence techniques.

Open source intelligence is actually a big part of my current assignment. The Army has hundreds of public facing websites and it is the mission of my team to conduct vulnerability assessments, operational security (OPSEC) and compliance reviews as well as scan for personally identifiable information (PII) violations. My team scans upwards of 100 URLs per week containing more than 25,000 files at a time to ensure that the Army community is not inadvertently sharing information in an open source environment that shouldn’t be visible to the general public. That’s not to say that there aren’t other sites that Soldiers can’t divulge information as my team is only authorized to scan public facing .mil domains. We cannot look at social media platforms such as Facebook, Twitter, and Instagram etc. where Soldiers are placing information every day as well. Additionally, the team is not authorized to conduct penetration testing or red team style missions on these sites.

Back in 2015, ISIS released a hit list with 100 names on it, and was asking for sleeper members of their organization to track down and murder the individuals named on their list. The list matched pretty closely with service member’s names that had been released in various news articles and sources available to the open public referencing air strikes that were taking place during that time. ISIS issued an even larger hit list the following year with close to 700 names on it. The official word from the Pentagon is that these names were retrieved via publically accessible sources, but many question whether or not it was the result of a hacking operation on a government site.

Since the inception of social media, adversarial organizations have been scanning these sites and in certain instances, service member’s family members have been targeted via these platforms. Also in 2015, ISIS was able to hack a military spouse Twitter account and was posting threatening messages divulging the spouses full legal names and informing them that ISIS “knew everything about them” (Hoffman, 2015). An FBI investigation was launched into the validity of the threats as a result.

It’s not just terrorists that are using social media and open source intelligence capabilities. Nation States, even the United States uses dual persona capabilities to infiltrate adversary’s social media platforms for intelligence gathering purposes as well as a method to spread pro-American propaganda. One of the offensive cyber operations techniques is to suppress negative messages with positive messages. It is one of those low-hanging fruit opportunities that doesn’t require any specific skill set, but can be effective if the adversary is posting negative messages and those are immediately suppressed with positive messages. The information operations mission includes many techniques such as this one.

Hoffman, M. (2015) Military Spouses Threatened by ISIS Affiliate on Twitter, Facebook. Retrieved from: <https://www.military.com/daily-news/2015/02/10/military-spouses-threatened-by-isis-affiliate-on-twitter-facebo.html>

Jarvis, J. (2011) Revealed: US spy operation that manipulates social media. Retrieved from: <https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>