Open-Source Intelligence Research Assignment:

The Significant Evolution of Open-Source Intelligence

Anthony J. Toledo

McAfee Institute

C|OSINT: Certified Open-Source Intelligence

Tim Matthews

August 3, 2024

Open-source information is nothing new and has always been available to the public. With the increasing rise of technological advances the methodology of gathering, reviewing, disseminating, and validating information has come with its challenges. The amount of data that is readily available is far greater now than it has ever been in human recorded history. While human intelligence remains valuable and effective, this may be a time where that might not be the most popular method of gathering intelligence, as it once was. While hackers have been more successful than before conducting identify theft and related criminal activity, legal authorities and enforcement agencies have met this challenge by increasing their effective implementation of technological investigative procedures. Cybersecurity professional careers are on the rise in the U.S. and U.K. and artificial intelligence is transforming the career field, while government entities have implemented many initiatives to keep up with the changes (Dimitriadis, 2024).

Understanding the significance and challenges faced with intelligence gathering is essential for any analyst or researcher. According to an article written by Ries (2023), a law firm Cybersecurity professional, "Most investigations should be iterative so that adjustments can be made as they progress" (para. 2). Flexibility and willing to learn new tricks of the trade are essential and critically important when it comes to gathering any data, especially information that is available to the public. Intelligence, information, and analysis are parallel but differentiated in their own right, "An OSINT analysis starts with a subject, such as an individual, company, event, or location, and uses manual search, automated tools, or both to find additional information, sometimes very comprehensive information" (Ries, 2023). The more comprehensive the information is, the more comprehensive and scrupulous must the efforts be to make that information valid and useful.

The challenges faced today are also some of the benefits as well. In correctional facilities and prisons, open-source intelligence has aided correctional staff by identifying patterns and relationships with inmates and criminal associates by way of processing massive amounts of data with algorithmic artificial intelligence (Wasson, 2024). While adversaries sometimes have the upper hand with technological sources, law enforcement and government agencies have also advanced their tactics, techniques, and procedures with this advancement.

Facing the challenges and rising above reproach remain the only outcome if any validated form of open-source intelligence program is to stay relevant. As Ries (2023) stated, “It is important to use OSINT appropriately, in compliance with applicable legal and ethical requirements” (para. 29). Once the information has been through the proper phases of the intelligence cycle (planning and directing, collection, processing and exploitation, analysis and production, dissemination, and evaluation and feedback), all parties involved must follow the appropriate ethical use of it. In the intelligence community, ethical standards should be above reproach, as to maintain a chain of custody of the utmost ethical standards. If responsible parties do not maintain the highest form of principles in their intelligence handling, whether it be government, private, or the industrial complex, then the challenges for acceptable standards will only become a hinderance rather than a virtue.

The outlook for the next decade of OSINT is one full of challenges and hope. As adversaries increase their attacks, the industrial complex and private industry will step in to assist legal and government authorities in protecting, detecting, deterring, and delaying enemy threats. As international criminal activity adapts, so does the opposition. The greater the threat, the greater the security, and as long as all parties understand the increasing trends, the critical function of well-trained intelligence professionals shall remain vigilant and on guard.

References

Dimitriadis, C. (2024, July 4). *Council post: The future of the Cybersecurity profession with the rise of ai*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2024/07/03/the-future-of-the-cybersecurity-profession-with-the-rise-of-ai/

Ries, D. G. (2023). Open-Source Intelligence (OSINT): An Important Investigative Tool for Attorneys. *GPSolo*, *40*(5), 59–64.

Wasson, M. (2024). Overcoming critical staffing shortages with OSINT. Corrections Today, 86(1), 22–24.