OPEN-SOURCE INTELLIGENCE: DEVELOPING ANALYTICAL CAPABILITY FOR THE AUSTRALIAN ARMY

By Warrant Officer Class 1 Greg Hopper, Australian Army

Army is responding to Accelerated Warfare as an Army in Motion–our teams are* ready now *and* future ready *for cooperation, competition and conflict.

—Lieutenant General Rick Burr, AO, DSC, MVO
Chief of Army, Australian Army

Introduction

The Australian Army is renewing its focus to meet the challenges of the current and future operating environments when working with joint, interagency, coalition, and whole of government task forces. It is also reviewing the impact and role of open-source intelligence (OSINT) in supplementing and supporting traditional military intelligence. The Australian Army, through the Land Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (LISREW) program in the Land Capability Division, Army Headquarters, has started the process to develop tactical and operational OSINT. The LISREW program aims to support commanders' decision making by improving situational awareness, which it achieves through a layered, multispectral network of sensors enabled by specialist intelligence.

The Australian Army is focusing on being future ready, and OSINT forms a key part of that requirement. LISREW has the authority to conduct OSINT analysis across the Army to inform the joint force. We are currently in discovery and undertaking trials to understand the workforce requirements, available systems, and software. The key challenges are individual intelligence analysis, collection management, and software support. This article will describe these challenges and will explain how we are identifying common problems and solutions.

As the Army OSINT workforce has grown, systems and commercially available software have been deconflicted with the Australian Defence Force, Joint Capability Group. This has allowed an economy of effort, increasing the capacity for the development of a Service OSINT capability while supporting joint needs. Until this point, some work had been done to meet specific capability requirements for supported commanders and units; however, this was by necessity rather than by design. This is now being addressed though significant engagement to develop baseline OSINT skills for analysts across the Army and the broader Australian Defence Force writ large.

The **Army Objective Force** seeks to optimize the Army for Accelerated Warfare. The Army Objective Force represents the next steps in the future design of the joint force—with an Army in Motion that will work more effectively across all domains and environments.

The **Joint Capability Group** was formed in July 2017 and has continued to evolve since its inception. The group provides a wide range of enabling capabilities to the Australian Defence Force services, including logistics support and services, health services, professional military education and training, and military legal services. The Joint Capability Group is also responsible for progressing leading-edge capabilities, such as cyberspace, data link, and satellite communications.

Forces Command's role is to prepare land forces in order to enable the joint force.

Special Operations Command's role is to provide ready and relevant forces to conduct special operations across the operational domain in a joint, combined, or interagency environment in support of Australia's national interests.

Joint Operations Command's role is to plan, control, and conduct operations, activities, and actions as directed to meet Australia's strategic objectives. Joint Operations Command is the critical node in applying defense capability at the operational level and conducts operations and exercises to meet government aims, deepen Australia's alliances and partnerships, and prepare the joint force for future contingencies.

Developing Open-Source Intelligence Analysts

The Australian Army has developed its OSINT training continuum through attendance at a range of military-partnered OSINT courses and commercial vendor training.[1] Feedback from the training indicated that commercial vendor training depended mostly on licensed software that was part of the vendor package, creating a reliance on the commercial software for OSINT research and analysis activities.

Although these types of applications are important in the context of OSINT capability development, intelligence analysts require the ability to conduct OSINT in a commercially agnostic environment in order to develop their critical thinking skills and generate comprehension of the operating environment's

magnitude and scope. Like learning to drive a car, once people are competent in basic skills, they can readily transfer those skills to larger, more complex vehicles without having to cover the fundamentals again.

This lesson has shaped the Australian Army's development of a customized OSINT training package for intelligence analysts, drawn from the breadth of training we attended. Focusing on individual analyst tradecraft skills was critical for the development of a generalist OSINT analyst. Regardless of an analyst's level of employment (tactical to strategic) within the Australian Army or the Australian Defence Force, the OSINT training package focuses more on individual appreciation of a range of tools and the process of OSINT rather than specific training and reliance on individual tools. This means that as the Australian Army develops its OSINT workforce for Service, partnered, or joint operations, capability development across the wider Australian Defence Force for the joint force integrator can occur using commercially available software for the breadth of OSINT activity required for information fusion and intelligence support.

Select Australian Army OSINT analysts now have the flexibility to apply their skills within the scope of a capability rather than training on individual tools. For example, this can be supporting tactical units for threat warning or situational awareness using limited tooling and online access, or operating in an intelligence fusion environment with significant commercial tooling support and defined reporting requirements.

In order to develop the breadth of skills for general OSINT analysts, we applied the following core fundamental OSINT skills to our training:

- **Australian and Australian Defence Force policy and legislation, including data management.** Describes the details required for a clear legal understanding of individual requirements and collective OSINT activities.
- **Operating in the open-source environment and the internet.** Teaches the pillars of open-source intelligence, digital domains, and key terms and concepts related to the internet and the web (surface web, deep web, and dark web).

Three Layers of the Web[2]

Surface Web

- ☐ Accessible.
- ☐ Indexed for search engines.
- ☐ Little illegal activity.
- ☐ Relatively small.

Deep Web

- ☐ Accessible by password, encryption, or through gateway software.
- ☐ Not indexed for search engines.
- ☐ Little illegal activity outside of dark web.
- ☐ Huge in size and growing exponentially.

Dark Web

- ☐ Restricted to special browsers.
- ☐ Not indexed for search engines.
- ☐ Large-scale illegal activity.
- ☐ Unmeasurable due to nature.

- **Search engines and web browsers.** Describes how to exploit search engines to conduct safe and secure initial website reconnaissance.
- **Open-source research opportunities and limitations.** Describes open-source intelligence, associated drivers, and risk management, including identifying and collecting information from news aggregators, multimedia, and other open resources.
- **Threats to open-source research and mitigation.** Focuses on operational security and communications security in an open-source context. Delivers practical security tradecraft relevant to open-source research and provides insight into adversary tradecraft implemented to mitigate compromise.
- **Online web resources and data extraction software.** Teaches how to use online tools to discover data from deep web sources and exploit online maps and tracking tools.
- **Source evaluation.** Teaches how to understand and explain source evaluation and content assessment techniques, including information corroboration, image and video verification, and the currency, relevance, authority, accuracy, and purpose method.

The Currency, Relevance, Authority, Accuracy, and Purpose Method[3]

Currency: The timeliness of the information.

Relevance: The importance of the information for your needs.

Authority: The source of the information.

Accuracy: The reliability, truthfulness, and correctness of the content.

Purpose: The reason the information exists.

- **Planning of open-source collection.** Describes the use of online tools to discover data from deep web sources and exploit online maps and tracking tools.
- **Open-source research and evaluation.** Introduces analysts to the ontology of various data, information, and resources that assist participants in managing open-source information collection tasks.
- **Research plans.** Highlights the importance of creating a research plan in the initial stage to produce better quality OSINT reports and briefings. Teaches analysts the value of using a research plan to navigate their OSINT process, as the plan will help them to understand the

information they are trying to produce, the audience they are producing it for, and ways to manage the information they require. Analysts learn how to identify resources and apply advanced use of search engines. They also learn how to track search trends and exploit search engines using Boolean functions before commencing their task.

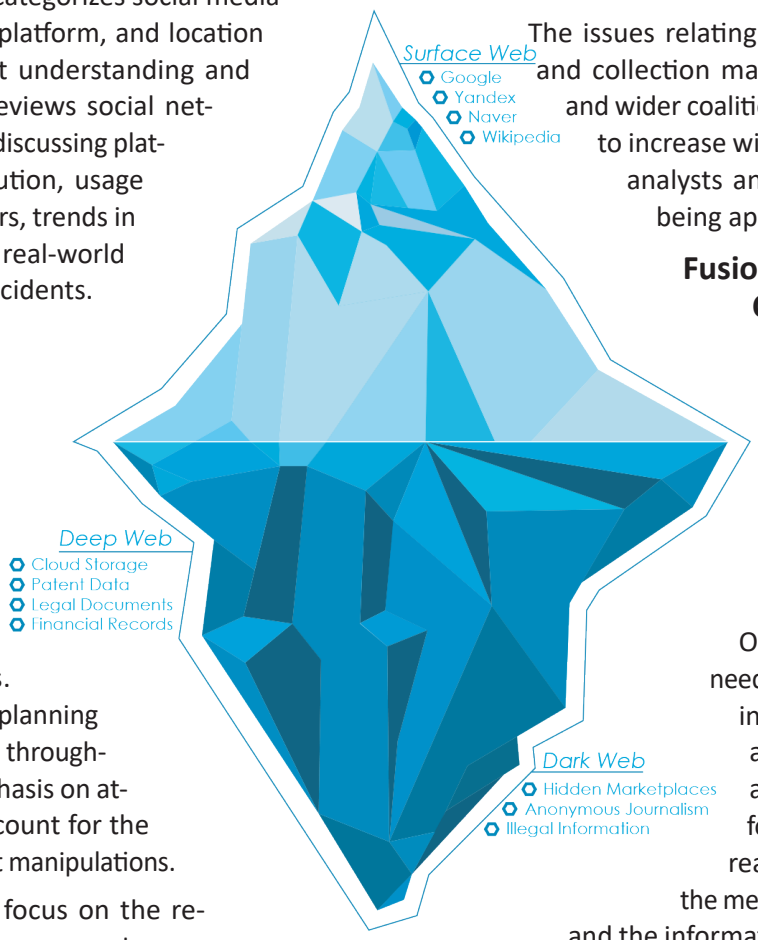
- **Use of social media.** Describes and outlines the social media landscape. Categorizes social media landscapes by theme, platform, and location to improve participant understanding and research tradecraft. Reviews social networking sites in depth, discussing platform history and evolution, usage by different threat actors, trends in activity and relation to real-world threats, and security incidents.

Collection Management Challenges

The key elements of the training provide analysts an understanding of the OSINT environment and introduce the capabilities and limitations that are imposed before, during, and after online activities. Moreover, the importance of planning and deconfliction is reinforced throughout the training, with an emphasis on attribution management to account for the environment and hostile threat manipulations.

These elements include a focus on the requirements and collection management process within the OSINT team environment. This process is manageable when individuals and teams are conducting activities; however, the complexity of deconfliction across the enterprise has yet to be addressed. This is compounded again within the joint or partnered environments with increased numbers of analysts conducting online activities. The ability to coordinate collection and conduct research is paramount within the OSINT environment when there are potentially hundreds of analysts pursuing information requirements online. Key challenges for requirements and collection management in an OSINT environment include—

- **Deconfliction of source information being applied to assessments.** This becomes more difficult when dozens of commercial software platforms are used or analysts are conducting individual tradecraft research across the organization. How do we mitigate single-source reporting from multiple analyst assessments?



- **Increase in OSINT analysts' online activities.** As the number of OSINT analysts' online activities increases, a single analyst's innocuous search may no longer be innocuous. The digital footprint to websites and data sources resulting from increased analyst research may provide hostile entities an understanding of our requirements and tactics, techniques, and procedures. This could give our adversary an opportunity to manipulate the environment or conduct targeted misinformation.

The issues relating to OSINT source validation and collection management across the Army and wider coalition environment will continue to increase with the expansion of qualified analysts and the varied software tools being applied.

Fusion and the Use of Commercial OSINT Software

As the Australian Army continues to develop its capability across the organization (Forces Command, Special Operations Command, and in support of Joint Operations Command), OSINT needs remain varied and challenging. Although individual skills are critical for intelligence analysts conducting research and for indicators and warning, the reality is that we must protect the members of our OSINT workforce and the information they are analyzing when operating online. We can achieve this protection with tools and systems that reduce their attribution, thereby retaining personal and organizational anonymity and protections.

The development of software and applications for the conduct of OSINT within the Australian Defence Force environment remains limited, with commercial sources being the most economical approach. As the Australian Army continues to develop the individual OSINT skills and knowledge of its people, we are pursuing systems and commercial software for the OSINT capability across the Australian Defence Force, alongside other Services. In doing so, the Army can support commercial software application trials and provide recommendations for differing levels of command and operational focus.

The breadth of capabilities from OSINT is extensive, with many commercial platforms for niche collection requirements;

however, when looking at commercial software, we need to consider more than just functionality. When selecting vendors, the Army, and more broadly the Australian Defence Force, should ask the following questions:

- Where did the software originate?
- What security measures are in place to support online user activities?
- Who can access the searches and research being conducted?
- Can the gathered information be easily packaged and transferred?
- What are the information export formats?
- Can search parameters be exported and integrated with competing OSINT software?

The selection of OSINT software remains a challenge to ensure applications provide the security and reduced attribution required for the conduct of intelligence operations research. The Army's ability to leverage multiple OSINT software applications in this area creates greater scope to develop and steer the support to end users within the Army and its commands.

Conclusion

The challenges that the Australian Army faces in developing its OSINT analytical capability require us to remain squarely focused on developing individual skills and knowledge across the workforce. The application and employment of the skills are the cornerstone to empowering a flexible resource for OSINT across the spectrum of operations at all levels of command. Through the development of the basics, a variety of commercial software, implemented via the Joint Capability Group as the joint force integrator, will ensure OSINT analysts have the ability to apply relevant and timely assessments. These assessments will support tactical units' threat warning and situational awareness as well as operations in an operational or strategic setting.

Epigraph

Australian Army, *Army in Motion Accelerated Warfare Statement by Lieutenant General Rick Burr, AO, DSC, MVO* (22 October 2020), 1, https://www.army.gov.au/our-work/army-motion/accelerated-warfare.

Endnotes

1. U.S. Department of the Army's Basic Open-Source Intelligence Courses 301 and 302; and commercial vendors such as SANS Institute, BlackHorse Solutions, Cyberspace Open Source Methods and Operations (COSMO), Janes, and OSINT Combine.

2. Andrew Quinney, "Surface web vs deep web vs dark web," Service Care Solutions, 27 June 2016, https://www.servicecare.org.uk/news/surface-web-vs-deep-web-vs-dark-web-61792715468.

3. "Evaluating Sources: The CRAAP Test," Benedictine University, accessed October 29, 2021, https://researchguides.ben.edu/source-evaluation.

WO1 Greg Hopper is a career intelligence professional with over 30 years' experience in a range of intelligence disciplines, including combat intelligence, special operations, psychological operations, and human intelligence. WO1 Hopper has operational experience from multiple deployments to the Middle East and the South West Pacific. He works in the Australian Army's Land Intelligence, Surveillance, Reconnaissance, and Electronic Warfare directorate at Army Headquarters, responsible for developing future intelligence capabilities.