 DOI 10.22491/cmm.a031

The application of the Open Source Intelligence method in Defense studies

Sabrina Evangelista Medeiros
Marinha do Brasil, Escola de Guerra Naval.
Rio de Janeiro, RJ, Brazil.
sabrina.medeiros@marinha.mil.br

Ana Luiza Bravo e Paiva
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército.
Rio de Janeiro, RJ, Brazil.
albepaiva@ppgcm.eceme.eb.mil.br

Cintiene Sandes Monfredo Mendes
Escola Superior de Guerra Instituto Cordeiro de Farias.
Rio de Janeiro, RJ, Brazil.
csandes2@yahoo.com.br

ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

The new post-pandemic times is also affected by the way in which the field of defense studies and, within that, military sciences will be built. Some debates can propel this new era, where informational elements are highlighted. Information is the constant variable in technological processes that transform strategy and military operating models, but it is also a defining attribute of how institutions will relate in the years to come.

If, on the one hand, we move through an amount of dissipated information, on the other, the barriers that interrupt unwanted flows of information are not placed in a safe or reliable way. Therefore, there is an expressive dissonance between the powerful information needs, for the purpose of assertive decisions, and the flows that bring varied insecurities. In addition to the elements of critical insecurity being endowed with major informational components – electronic warfare, cross-cutting or transnational threats, cybersecurity and cyberdefense – the defense attributes of a State are not only defined by its capabilities, since the informational components affected are both internal and external.

Thus, the contrast between information needs and the inability of institutions to respond efficiently to these demands seems to be central to the resulting strategic planning. The renewal of intelligence models, which are much more focused on the treatment

of information than on the obsolete conception linked to the models of the last century, may be the new equation to be solved by States.

Although collaborative regimes are under suspicion, the protocols that drive the behavior of state actors continue to express interest in some degree of control and submission of behaviors to the international system (KRAHMANN, 2003; AXELROD; HAMILTON, 1981). Thus, States cannot fail to observe imperatives caused by third parties, which are added to those of state or interstate expression. A kind of overlapping consensus among the various types of representatives of the informational arena seems to be composed of some possible common minimums that touch on data privacy, the control of personal data by private corporations and state entities, the mobilization of falsified information, and the existence of barriers and parallel universes on the internet.

It is precisely because of parallel environments that insecurities are expressed about defense systems, with high repercussions in terms of trust and stability. Therefore, it does not require both a more in-depth, systematic and academic analysis of these variables, as well as an input on public policies, strategies and doctrines, coming from academic research. The construction of appropriate methodologies and tools fuels the possibility of building a hybrid field of studies with critical potential and manifested ordinarily over the state institutions affected (MEDEIROS, 2016).

In this regard, the possibility of using the so-called OSINT (Open Source Intelligence) can substantially expand the possibilities of analysis inside and outside defense institutions (GLASSMAN; KANG, 2012). The central idea of using open sources for the benefit of intelligence systems aims at the conception that the greater the ability to observe open data, the better the conditions for strategic and operational visibility, since the virtual world provides a universe of untreated information (BENES, 2013). Even though OSINT is not characterized as a scientific method, as an instrument, it qualifies research with the possibility of large-scale qualitative analyses, with a high impact of data science in the broad epistemological field of defense studies (GONG; CHO; LEE, 2018).

The challenges that affect the collection and analysis of open sources and data show that the technology paradigm, in addition to affecting the objects of defense studies, guides the way in which agents and researchers must be trained to analyze security systems (DAVIS; O'MAHONY, 2017). Added to these are ethical challenges, given that the human interface with technology exasperates by its limits (HRIBAR; PODBREGAR; IVANUŠA, 2014). The so-called information technology revolution also mobilizes new forms of human interaction and, for this reason, the new intelligence models are endowed, in addition to open data, with the so-called Crowdsourcing Intelligence (WILLETT; HEER; AGRAWALA, 2012). The elements linked to this model highlight not only the means and type of data collected, but the subjects' ability to interact for the benefit of obtaining data that increases the visibility of a given subject.

In this sense, the themes related to national security, international security, cooperative security, are cross-sectional and deserve an input from the informational components involved. This includes addressing issues such as: migratory flows from the collaboration networks involved; defense economics and information transfer involved in agreements of various collaborative terms; illicit and human trafficking and submerged

connection networks; and new ways of materializing agreements in areas lacking sovereignty or contestable sovereignty.

To complement this perspective on the use of data and information technology in a collaborative and reliable way, a series of methods are adapted and crossed so that the databases have a mining and the most coherent and secure interpretation to be transmitted by the media, thus facilitating the dissemination of knowledge in the field of defense.

When analyzing decision-making tools, databases, software for checking variables and analyzing behavior are used in the public and private fields, by governments and corporations, so they are assisted by technology about future decisions that will affect their businesses and individuals. In the case of this process, there is responsibility for the risks and impacts of these decisions analyzed with data collected individually and categorized for collective understanding and also for the emergence of collective phenomena that affect national security, defense and development issues.

It is with great satisfaction that we present this edition of Coleção Meira Mattos. This issue has five articles with varied themes, but all contribute substantially to the advancement of research in Military Sciences. In addition, we highlight that the thematic variety – cyber threats (QUEIROZ; KRISHNA-HENSEL, 2020), conflicts of the future (FONFRÍA, 2020), drug trafficking (ARIAS HENAO, 2020), military logistics (VIOLANTE et al., 2020), and geopolitics resources (PEREZ, 2020) – present in this publication represents well the plurality of themes and agendas that compose the defense area. Enjoy!

References

ARIAS HENAO, D. P. An anti-narcotics look at Colombia in post-conflict. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 305-330, 2020. DOI: https://doi.org/10.22491/cmm.a035. Available at: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4205. Access on: 11 ago. 2020.

AXELROD, R.; HAMILTON, WD. The evolution of cooperation. **Science**, [*Sl*], v. 211, n. 4489, p. 1390-1396, 1981.

BENES, L.. OSINT, new technologies, education: expanding opportunities and threats. A new paradigm. **Journal of Strategic Security**, [*Sl*], v. 6, n. 3, p. 22-37, 2013.

DAVIS, PK; O'MAHONY, A. Representing qualitative social science in computational models to aid reasoning under uncertainty: national security examples. **The Journal of Defense Modeling and Simulation**, [*Sl*], v. 14, n. 1, p. 57-78, 2017.

FONFRÍA, A. The conflicts of the future: a new scenario for the defense industry. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 235-249, 2020. DOI: https://doi.org/10.22491/cmm. a032. Available at: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3879. Access on:11 ago. 2020.

GLASSMAN, M .; KANG, MJ Intelligence in the internet age: the emergence and evolution of Open Source Intelligence (OSINT). **Computers in Human Behavior**, [*Sl*], v. 28, n. 2, p. 673-682, 2012.

GONG, S .; CHO, J .; LEE, C. A reliability comparison method for OSINT validity analysis**. IEEE Transactions on Industrial Informatics**, [*Sl*], v. 14, n. 12, p. 5428-5435, 2018.

HRIBAR, G.; PODBREGAR, I.; IVANUŠA, T. OSINT: the "gray zone"? '. **International Journal of Intelligence and CounterIntelligence**, [*Sl*], v. 27, n. 3, p. 529-549, 2014.

KRAHMANN, E. Conceptualizing security governance. **Cooperation and conflict**, [*Sl*], v. 38, n. 1, p. 5-26, 2003.

MEDEIROS, SE Of the Epistemology of Defense Studies and its Hybrid Fields. **Brazilian Journal of Defense Studies**, Niterói, RJ, v. 2, n. 2, 2016.

PEREZ, J. G. The Falklands/Malvinas conflict from the perspective of the Geopolitics of Natural Resources. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 331-356, 2020. DOI: https://doi.org/10.22491/cmm.a036. Available at: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4093. Access on: 20 ago. 2020..

QUEIROZ, F. de; KRISHNA-HENSEL, S. F. An assessment of cyber threats and migration as challenges to the European Union Pluralistic Security Community in the World Order 2.0. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 279-303, 2020. DOI: https://doi. org/10.22491/cmm.a034. Available at: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3677. Access on: 11 ago. 2020

WILLETT, W .; HEER, J .; AGRAWALA, M. Strategies for crowdsourcing social data analysis. *In* : SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS. 12., 2012, Austin, TX. **Proceedings**... Austin, TX: SIGCHI, May 2012. p. 227-236.

VIOLANTE, R. V.; CARVALHO, Y. M. de; SANTOS, M. dos; SILVA, P. A. L. da. Interoperability in the Amazon region: application of the SAPEVO-M method to select logistical equipment to be used by the Armed Forces. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 251-277, 2020. DOI: https://doi.org/10.22491/cmm.a033. Available at: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3373. Access on: 11 ago. 2020.