 DOI 10.22491/cmm.a031

La aplicación del método *Open Source Intelligence* en los estudios sobre Defensa

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

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

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

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

Los nuevos tiempos pospandemia también ejercen su influencia en la forma en que se construirá el campo de los estudios sobre defensa y, entre ellos, de las ciencias militares. Se puede apuntar que algunos debates en desarrollo en los últimos años son propulsores de esta nueva era, en la que se destacan los elementos informativos. La información es la variable constante en los procesos tecnológicos que transforman la estrategia y los modelos operativos militares, pero también es un atributo definitorio de cómo se relacionarán las instituciones en los próximos años.

Por un lado, tenemos un entorno con una gran cantidad de información difundida, por el otro, las barreras que interrumpen los flujos de información indeseados no son seguras o fiables. Esto resulta en una expresiva disonancia entre las necesidades de información, a efectos de decisiones asertivas, y los flujos que traen variadas inseguridades. Además de que los elementos críticos de inseguridad cuentan con importantes componentes informativos –guerra electrónica, amenazas transversales o transnacionales, ciberseguridad y ciberdefensa–, los atributos de defensa de un Estado no solo se definen por sus capacidades, ya que los componentes informativos afectados son tanto internos como externos.

Así, el contraste entre las necesidades de informaciones y la incapacidad de las instituciones para responder eficientemente a estas demandas parece ser central para la planificación estratégica. La renovación de los modelos de inteligencia, más dirigidos al tratamiento de las informaciones que

a la concepción obsoleta vinculada a los modelos del siglo pasado, puede ser la nueva ecuación que resolver por los Estados.

Si bien los regímenes colaborativos están bajo desconfianza, se nota que los protocolos que impulsan el comportamiento de los actores estatales continúan interesados en algún grado de control y sometimiento de los comportamientos al sistema internacional (KRAHMANN, 2003; AXELROD; HAMILTON, 1981). De esta manera, los Estados no pueden dejar de observar imperativos provocados por terceros, que se suman a los de nivel estatal o interestatal. Una especie de consenso yuxtapuesto entre los distintos tipos de representantes del ámbito informativo parece constituirse de algunos mínimos comunes posibles relacionados a la privacidad de los datos, el control de los datos personales por parte de corporaciones privadas y entidades estatales, la movilización de informaciones falsificadas y la existencia de barreras y universos paralelos en Internet.

Debido a estos entornos paralelos, las inseguridades se manifiestan sobre los sistemas de defensa, lo cual repercute en confianza y estabilidad. Por tanto, se requiere tanto un análisis más profundo, sistemático y académico de estas variables como los aportes de políticas públicas, estrategias y doctrinas provenientes de trabajos académicos. La construcción de metodologías y herramientas adecuadas fomenta la posibilidad de construir un campo de estudios híbrido con potencial crítico y que se manifiesta de forma ordinaria sobre las instituciones estatales relacionadas (MEDEIROS, 2016).

En este sentido, la posibilidad de utilizar la llamada OSINT (*Open Source Intelligence*) puede ampliar de manera sustancial las posibilidades de análisis dentro y fuera de las instituciones vinculadas a la defensa (GLASSMAN; KANG, 2012). La idea central de utilizar fuentes abiertas en beneficio de los sistemas de inteligencia se vincula a la concepción de que la mayor capacidad de observación de datos abiertos resulta en mejores condiciones para la visibilidad estratégica y operativa, ya que el mundo virtual brinda un universo de informaciones sin tratamientos (BENES, 2013). La OSINT no se caracteriza como método científico, sino como instrumento, que permite calificar la investigación con posibilidad de análisis cualitativos a gran escala, con un alto impacto de la ciencia de datos en el vasto campo epistemológico de los estudios sobre defensa (GONG; CHO; LEE, 2018).

Los desafíos relacionados a la recolección y análisis de fuentes y datos abiertos demuestran que el paradigma tecnológico, además de afectar los objetos de estudios sobre defensa, orienta la forma en que los agentes e investigadores deben capacitarse para analizar los sistemas de seguridad (DAVIS; O'MAHONY, 2017). A esto se suman los desafíos de naturaleza ética, dado que la interfaz humana con la tecnología se intensifica por sus límites (HRIBAR; PODBREGAR; IVANUŠA, 2014). La llamada revolución de las tecnologías de la información también moviliza nuevas formas de interacción humana y, por ello, los nuevos modelos de inteligencia cuentan con, además de los datos abiertos, la llamada *Crowdsourcing Intelligence* (WILLETT; HEER; AGRAWALA, 2012). Los elementos vinculados a este modelo destacan no solo los medios y el tipo de datos recopilados, sino la capacidad de los sujetos para interactuar en beneficio de la obtención de datos que aumenten la visibilidad de un tema determinado.

En este sentido, los temas relacionados con la seguridad nacional, la seguridad internacional y la seguridad cooperativa son transversales y merecen el aporte de los componentes informativos involucrados. Esto incluye el enfoque en los siguientes temas: flujos migratorios desde las redes de colaboración involucradas; economía de defensa y transferencia de información involucrada en acuerdos de diversos términos colaborativos; tráfico de ilícitos y de personas y redes de conexión

sumergidas; y nuevas formas de materializar acuerdos en áreas que carecen de soberanía o de soberanía cuestionable.

Para complementar esta perspectiva sobre el uso de datos y tecnologías de la información de forma colaborativa y confiable, una serie de métodos se adaptan y se cruzan para que las bases de datos tengan una exploración y la interpretación más coherente y segura para ser transmitida por los medios de comunicación, lo que facilita la difusión del conocimiento en el ámbito de la defensa.

Para analizar las herramientas de la toma de decisiones, se utilizan bases de datos, softwares de verificación de variables y análisis de comportamiento en los ámbitos público y privado, por parte de gobiernos y corporaciones, para que cuenten con la asistencia de la tecnología sobre las decisiones futuras que afectarán sus emprendimientos y personas. En este proceso, existe la responsabilidad sobre los riesgos e impactos de estas decisiones analizadas con datos recolectados de manera individual y categorizados para el entendimiento del colectivo, y también sobre el surgimiento de fenómenos colectivos que afectan temas de seguridad nacional, defensa y desarrollo.

Con gran satisfacción presentamos esta edición de la Coleção Meira Mattos. Este número cuenta con cinco artículos de variadas temáticas, sin embargo comparten el hecho de que contribuyen sustancialmente al avance de las investigaciones en Ciencias Militares. Además, destacamos que esta variedad temática –ciberamenazas (QUEIROZ; KRISHNA-HENSEL, 2020), los conflictos del futuro (FONFRÍA, 2020), narcotráfico (ARIAS HENAO, 2020), logística militar (VIOLANTE et al., 2020) y geopolítica de los recursos (PEREZ, 2020)– presente en la edición representa la pluralidad de temas y agendas que componen el área de la defensa. ¡Buena lectura!

Referencias

ARIAS HENAO, D. P. Una mirada antinarcótica a la Colombia en posconflicto. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 305-330, 2020. DOI: https://doi.org/10.22491/cmm.a035. Disponible en: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4205. Accedido en: 11 ago. 2020.

AXELROD, R.; HAMILTON, W. D. The evolution of cooperation. **Science**, [*S.l.*], 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**, [*S.l.*], v. 6, n. 3, p. 22-37, 2013.

DAVIS, P. K.; 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**, [*S.l.*], v. 14, n. 1, p. 57-78, 2017.

FONFRÍA, A. Los conflictos del futuro: nuevo escenario para la industria de defensa. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 235-249, 2020. DOI: https://doi.org/10.22491/cmm.a032. Disponible en: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3879. Accedido en: 11 ago. 2020.

GLASSMAN, M.; KANG, M. J. Intelligence in the internet age: the emergence and evolution of Open Source Intelligence (OSINT). **Computers in Human Behavior**, [*S.l.*], 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**, [*S.l.*], v. 14, n. 12, p. 5428-5435, 2018.

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

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

MEDEIROS, S. E. Da Epistemologia dos Estudos de Defesa e os seus Campos Híbridos. **Revista Brasileira de Estudos de Defesa**, Niterói, RJ, v. 2, n. 2, 2016.

PEREZ, J. G. El conflicto de las Malvinas a través del prisma de la Geopolítica de Recursos Naturales. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 331-356, 2020. DOI: https://doi.org/10.22491/cmm.a036. Disponible en: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4093. Accedido en: 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. Disponible en: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3677. Accedido en: 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. Interoperabilidade na região amazônica: aplicação do método SAPEVO-M na seleção do melhor equipamento logístico a ser utilizado pelas Forças Armadas brasileiras. **Coleção Meira Mattos**, Rio de Janeiro, v. 14, n. 51, p. 251-277, 2020. DOI: https://doi.org/10.22491/cmm.a033. Disponible en: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3373. Accedido en: 11 ago. 2020.