DOI 10.22491/cmm.a031

A aplicação do método *Open Source Intelligence* nos estudos de Defesa

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

O imperativo de novos tempos pós-pandemia também é afeto à maneira pela qual se construirá o campo dos estudos de defesa e, dentro disso, das ciências militares. Alguns debates em franca expansão nos últimos anos podem ser apontados como definitivamente propulsores dessa nova era, onde os elementos informacionais ganham destaque. A informação é a variável constante nos processos tecnológicos que transformam estratégia e modelos operativos militares, mas também é atributo definidor de como as instituições se relacionarão nos anos que seguem.

Se de um lado nos dirigimos por um ambiente de dissipada quantidade de informação, de outro, as barreiras que interrompem fluxos indesejados de informação não estão postas de forma segura ou confiável. Portanto, há uma dissonância expressiva entre as necessidades pujantes de informação, para efeito de decisões assertivas, e os fluxos que trazem inseguranças variadas. Além dos elementos de insegurança críticos estarem dotados de grandes componentes informacionais – guerra eletrônica, ameaças transversais ou transnacionais, cybersegurança e cyberdefesa – os atributos de defesa de um Estado não são somente definidos pelas suas capacidades, posto que os componentes informacionais afetos são tanto internos quanto externos.

Desse modo, o contraste entre as necessidades informacionais e a incapacidade de instituições reagirem eficientemente a essas demandas parece ser central para o planejamento estratégico decorrente. A renovação dos modelos de inteligência, muito mais dirigidos ao tratamento das

informações do que à concepção obsoleta ligada aos modelos do século passado, pode ser a nova equação a ser resolvida pelos Estados.

Embora os regimes colaborativos estejam sob desconfiança, é notável que os protocolos que conduzem o comportamento de atores estatais continuam a manifestar interesse por algum grau de controle e submissão de comportamentos ao sistema internacional (KRAHMANN, 2003; AXELROD; HAMILTON, 1981). Desse modo, Estados não podem deixar de observar imperativos causados por atores terceiros, que somam-se àqueles de expressão estatal ou interestatal. Uma espécie de consenso sobreposto entre os vários tipos de representantes da arena informacional parece feito de alguns mínimos comuns possíveis que tocam a privacidade de dados, o controle de dados pessoais por corporações privadas e entes estatais, a mobilização de informações falseadas, e a existência de barreiras e universos paralelos na internet.

É exatamente por conta de ambientes paralelos que as inseguranças se expressam sobre sistemas de defesa, com alta repercussão em matéria de confiança e estabilidade. Portanto, prescinde tanto uma análise mais aprofundada, sistemática e acadêmica sobre essas variáveis quanto um aporte sobre políticas públicas, estratégias e doutrinas, proveniente dos trabalhos acadêmicos. A construção de metodologias e ferramentas apropriadas, alimenta a possibilidade de construir um campo de estudos híbrido com potencial crítico e manifestado ordinariamente sobre as instituições de estado afetas (MEDEIROS, 2016).

Nessa matéria, a possibilidade de uso da chamada OSINT (*Open Source Intelligence*) pode ampliar substancialmente as possibilidades de análise dentro e fora de instituições ligadas à defesa (GLASSMAN; KANG, 2012). A ideia central do uso de fontes abertas em benefício de sistemas de inteligência é voltada para a concepção de que quanto maior a capacidade de observar dados abertos, melhores as condições de visibilidade estratégica e operacional, uma vez que o mundo virtual proporciona um universo de informações não tratadas (BENES, 2013). Mesmo a OSINT não sendo caracterizada como método científico, como instrumento, ela permite qualificar a pesquisa com a possibilidade de análises qualitativas de grande montante, com alto impacto da ciência de dados no campo epistemológico amplo dos estudos de defesa (GONG; CHO; LEE, 2018).

Os desafios que tocam a coleta e análise de fontes e dados abertos demonstram que o paradigma da tecnologia, além de afetar os objetos dos estudos de defesa, orientam a maneira pela qual os agentes e pesquisadores devem estar capacitados para análise de sistemas de segurança (DAVIS; O'MAHONY, 2017). Somam-se a esses aqueles desafios de caráter ético, dado que a interface humana com a tecnologia exaspera pelos seus limites (HRIBAR; PODBREGAR; IVANUŠA, 2014). A chamada revolução das tecnologias de informação mobiliza também novas formas de interação humana e, por essa razão, os novos modelos de inteligência são dotados, além de dados abertos, da chamada *Crowdsourcing Intelligence* (WILLETT; HEER; AGRAWALA, 2012). Os elementos ligados a este modelo destacam não somente os meios e tipo de dados coletados, mas a capacidade dos sujeitos de interagir em benefício da obtenção de dados que ampliem a visibilidade de uma determinada matéria.

Nesse sentido, os temas ligados à segurança nacional, segurança internacional, segurança cooperativa, são transversais e merecem um aporte dos componentes informacionais envolvidos. Isso inclui a abordagem de temas como: fluxos migratórios a partir das redes de colaboração envolvidas; economia da defesa e a transferência informacional envolvida em acordos de variados termos colaborativos; o tráfico de ilícitos e humanos e as redes de conexão

submersas; e as novas formas de materializar acordos em zonas ausentes de soberania ou de soberania contestável.

Para complementar essa perspectiva acerca do uso de dados e da tecnologia informacional de forma colaborativa e confiável, uma série de métodos são adaptados e cruzados para que as bases de dados tenham uma mineração e a interpretação mais coerente e segura para ser transmitida pelos meios de comunicação, facilitando assim a divulgação do conhecimento no âmbito da defesa.

Ao analisar ferramentas de processo decisório, as bases de dados, os softwares para verificação de variáveis e análise de comportamento são utilizados no campo público e privado, por governos e corporações, para que sejam auxiliadas por meio da tecnologia acerca das decisões futuras que afetarão seus negócios e indivíduos. Em se tratando desse processo, há a responsabilidade quanto aos riscos e impactos dessas decisões analisadas com dados coletados de maneira individual e categorizados para a compreensão do coletivo, e ainda, do surgimento de fenômenos coletivos que afetem questões de segurança, defesa e desenvolvimento nacionais.

É com grande satisfação que apresentamos esta edição da Coleção Meira Mattos. Este número conta com cinco artigos de temáticas variadas, mas todos compartilham o fato de contribuírem substancialmente para o avanço das pesquisas em Ciências Militares. Além disso, destacamos que a variedade temática – ameaças cyber (QUEIROZ; KRISHNA-HENSEL, 2020), Guerra do Futuro (FONFRÍA, 2020), narcotráfico (ARIAS HENAO, 2020), logística militar (VIOLANTE et al., 2020) e geopolítica dos recursos (PEREZ, 2020) – presente nesta publicação representa bem a pluralidade de temas e agendas que compõem a área de defesa. Boa leitura!

Referências

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. Disponível em: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4205. Acesso em: 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. Disponível em: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3879. Acesso em: 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. Disponível em: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/4093. Acesso em: 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. Disponível em: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3677. Acesso em: 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. Disponível em: http://ebrevistas.eb.mil.br/index.php/RMM/article/view/3373. Acesso em: 11 ago. 2020.