Informática

O EMPREGO DA FONTE CIBERNÉTICA PARA A PRODUÇÃO DE CONHECIMENTOS DE INTELIGÊNCIA, NO NÍVEL ESTRATÉGICO

Alexandre Pinheiro[1]

Resumo. Com o surgimento da internet e a crescente utilização do espaço cibernético, impulsionado pela popularização das mídias sociais, a interconexão entre pessoas e organizações e a facilidade de acesso a informações modificaram o comportamento da sociedade. Apesar disso, no âmbito das operações militares, o conhecimento de inteligência continua tendo papel decisivo. Partindo dessas premissas, este trabalho de pesquisa teve por objetivo verificar a viabilidade de produzir inteligência a partir das fontes cibernéticas, principalmente para suprir as necessidades de planejamento no nível estratégico. Nesse contexto, produzir inteligência a partir de fontes disponíveis no espaço cibernético pode ser considerado um desafio, do ponto vista tecnológico, ou uma oportunidade de suprir os tomadores de decisão com conhecimentos confiáveis e no momento oportuno. Com essa preocupação em mente, buscou-se, por meio de pesquisas bibliográficas (busca e seleção de artigos publicados), encontrar exemplos bem-sucedidos de produção de inteligência ao redor do mundo, capazes de comprovar a viabilidade de produção de inteligência estratégica a partir das fontes cibernéticas, com ênfase nas mídias sociais. Como resultado desse trabalho, selecionou-se exemplos internacionais que comprovaram a relevância do trabalho de inteligência nas operações militares; verificou-se a validade do uso da fonte cibernética na produção de inteligência, exemplificando com os tipos de informações que podem ser obtidas e com ferramentas que podem ser aplicadas; demonstrou-se exemplos de operações de cunho militar realizadas em diversos países, cuja produção de inteligência nos níveis estratégico, operacional e tático são essenciais para o seu sucesso. Por fim, analisou-se os resultados apresentados pela pesquisa, a partir dos quais foi possível corroborar a capacidade de se empregar as fontes cibernéticas na produção de inteligência no nível estratégico.

Palavras-chave: Inteligência. Cibernética. Nível Estratégico. Mídias Sociais.

Abstract. With the Internet arise and the increasing of cyberspace use, it has driven by the social media popularization, the interconnection between people and organizations, and the ease information access, have changed the society behavior. Nevertheless, in the military operations scope, intelligence knowledge continues to play a decisive role. Based on these premises, this research aimed to verify the feasibility of producing intelligence from cybernetic sources, mainly to meet the planning needs at the strategic level. In this context, producing intelligence from available sources in the cyberspace can be considered a technological challenge or an opportunity to supply decision makers with reliable and timely knowledge. With this concern in mind, we have looked for through bibliographical researches (published papers search and selection), to find successful examples of intelligence production around the world, capable of proving the viability of strategic

[1]Capitão QCO Informática da turma de 2010. Mestre em Engenharia Elétrica pela Universidade de Brasília em 2016, Especialista em Gestão da Segurança da Informação pela Universidade de Brasília em 2014. Especialista em Criptografia e Segurança em Redes pela Universidade Federal Fluminense em 2012. Especialista em Aplicações Complementares às Ciências Militares pela EsAEx em 2010.

intelligence production from cybernetic sources, with emphasis on social media. As a result of this work, international examples were selected that proved the intelligence work relevance in military operations; we have verified the validity of the cybernetic source use in intelligence production, exemplifying with the information types which can be obtained, and the tools which can be applied; we have demonstrated examples of military operations carried out in a number of countries, whose production of strategic, operational and tactical intelligence, are essential for its success. Finally, we have analyzed the results presented by the research, from which it was possible to corroborate the ability to use cybernetic sources in the intelligence production at the strategic level.

Keywords: Intelligence. Cybernetic. Strategic Level. Social Media.

1 INTRODUÇÃO

O mundo virtual tem conquistado cada vez mais seguidores nas últimas décadas, criando uma nova gama de possibilidades que tornam a vida mais agradável devido à facilidade de acesso a informações e serviços. Como consequência do conforto oferecido pelo mundo virtual, uma parcela significante da população inseriu-se na sociedade da informação, tendo esta como seu ativo mais importante, o qual desempenha papel de extrema relevância na vida econômica, política e social das pessoas, organizações e nações (SANTOS, 2018).

Os sites de comércio eletrônico permitiram que as pessoas pudessem acessar e realizar transações comerciais de forma *online*. As plataformas de mídia social surgiram como uma importante ferramenta estratégica para as organizações por facilitar a comunicação com seus clientes e colaboradores.

No espaço cibernético são realizadas uma ampla variedade de atividades, como o envio de mensagens de texto, envio de e-mails, transações bancárias, acesso a notícias e interações por meio das mídias sociais. A capacidade de monitorar, coletar e analisar as informações que circulam no espaço cibernético torna-se fundamental para entender o ambiente operacional e moldar as operações militares, principalmente aquelas em que o teatro de operações abrange grandes áreas urbanas (COMMONS, 2018).

Segundo Commons (2018), a atividade de coletar, analisar e distribuir informações sobre as capacidades, atividades e prováveis linhas de ação de países estrangeiros ou de atores não estatais é denominada inteligência. No mesmo sentido, a inteligência cibernética é a inteligência produzida a partir de informações obtidas no espaço cibernético (BRASIL, 2015).

Inserido no domínio das atividades de inteligência encontra-se a inteligência estratégica, uma atividade específica de pesquisa que aborda as necessidades de conhecimento com nível de amplitude e detalhe suficiente para descrever ameaças, riscos e oportunidades. Na prática, a inteligência e a análise estratégica concentram-se na capacidade de raciocinar criativamente sobre as possíveis linhas de ação a serem adotadas através de questões de nível macro, mas sempre mantendo uma conexão pragmática com o

respectivo impacto sobre os resultados táticos e operacionais (McDOWEL, 2009).

Para a produção de inteligência, muitas das informações necessárias para entender os fatores físicos e humanos do ambiente operacional encontram-se disponíveis publicamente. Entretanto, para que os esforços de exploração de conteúdos públicos sejam eficazes, é necessário estabelecer procedimentos adequados de validação e verificação tanto das fontes como das informações obtidas (US ARMY, 2012).

A partir dessas considerações, realizou-se um estudo científico com o objetivo de confirmar a viabilidade da utilização das fontes de dados disponíveis no espaço cibernético para a produção de conhecimento de inteligência capaz de dar suporte às operações militares. Para isso, realizou-se uma pesquisa de natureza aplicada que buscou, utilizando uma abordagem qualitativa, por intermédio de uma pesquisa bibliográfica, selecionar relatos cujas evidências fossem capazes de determinar a relevância da inteligência nas operações militares, validar o uso das fontes cibernéticas na produção de inteligência e demonstrar o emprego das fontes cibernéticas em operações militares, com ênfase nas mídias sociais.

Finalizando o trabalho, realizou-se uma discussão sobre os resultados alcançados e a sua aplicabilidade na produção de inteligência destinada a subsidiar o planejamento em nível estratégico das operações militares.

2 REFERENCIAL TEÓRICO

Inicialmente, na sessão 2.1, abordou-se o conceito de conhecimento e a importância de sua gestão para as organizações modernas; na sessão 2.2, as múltiplas fontes de dados, que necessitam ser integradas, sendo o *Big Data* uma das ferramentas tecnológicas que viabiliza essa integração. Em seguida, na sessão 2.3, abordou-se o planejamento das operações militares; na sessão 2.4, a importância da inteligência militar na produção de conhecimento para a redução dos riscos e aumento dos índices de sucesso nas operações. Então, na sessão 2.5, tratou-se das fontes de informação de inteligência; na sessão 2.6, chegou-se ao conceito de inteligência de fontes abertas, suas características e vantagens; e por fim, na sessão 2.7, apresentou-se as informações de inteligência que podem ser obtidas a partir das mídias sociais, que é o foco desta pesquisa.

2.1 Conhecimento

O conhecimento é a informação combinada com a experiência, o contexto, a interpretação e a reflexão, sendo a fonte de vantagem competitiva característica das modernas economias. O conhecimento pode ser considerado uma entidade, que pode ser capturada, comunicada e acumulada; entretanto, o conhecimento pode ser visualizado

como um estoque e um fluxo, em virtude de sua natureza dinâmica e a maneira como é gerada, transmitida e incrementada (ARCHER-BROWN e KIETZMANN, 2018).

Nesse contexto, o conhecimento é um ativo que está em constante estado de fluxo, o qual requer a compreensão do modo pelo qual pode fluir entre diversos indivíduos, equipes e organizações. A obtenção de conhecimento e a sua gestão são processos críticos para as organizações (ARCHER-BROWN e KIETZMANN, 2018).

Segundo Archer-Brown e Kietzmann (2018), as questões chaves que determinam as características do conhecimento que geram implicações estratégicas críticas são:

a) Até que ponto o conhecimento pode ser transferido de forma a proporcionar vantagem competitiva?

b) Há capacidade, dentro de uma perspectiva social, de combinar conhecimentos?

c) Até que ponto o conhecimento pode ser apropriado de forma a gerar valor?

d) O nível de especialização do conhecimento pode gerar barreiras à sua replicação?

Em virtude dessas características, no contexto estratégico, a capacidade de gerenciar o conhecimento torna-se uma das mais importantes competências de uma organização. Gerenciar o conhecimento estratégico é buscar fazer algo útil do conhecimento, tornando-o uma fonte sustentável de vantagem competitiva, ou seja, permitir que a organização gere valor a partir de seus ativos de conhecimento, sejam eles explícitos ou tácitos (ARCHER-BROWN e KIETZMANN, 2018).

No âmbito das operações militares, devido a sua dinamicidade e complexidade, a chave para o sucesso não é apenas a força, mas a capacidade de coletar informações sobre a situação e transformá-las em conhecimento em tempo hábil para a tomada de decisões. Para isso, é necessário coletar e processar uma enorme quantidade de dados oriundas de equipamentos, veículos, estruturas, sistemas de comunicação, e tropas empregadas pelas forças amigas, assim como informações sobre o inimigo e seu movimento (MOHAMED e AL-JAROODI, 2014). Nesse sentido, percebe-se que a vantagem da decisão, conforme defendido por Symon e Tarapore (2015), depende da integração de variados conjuntos de dados, de inúmeras fontes, sendo o *Big Data* uma das alternativas para soluções de inteligência.

2.2 Big Data

Segundo Mohamed e Al-Jaroodi (2014), as grandes massas de dados, cuja análise, gerenciamento e armazenamento, em virtude do seu tamanho, são incompatíveis com os sistemas de gerenciamento de bancos de dados típicos, são denominados "*Big Data*". O tamanho dessas massas de dados varia de algumas dúzias de terabytes a vários petabytes, sobre os quais aplicações de *Big Data* extraem informações de inteligência e procuram por novos conhecimentos que resultem em vantagem competitiva.

Seguindo o mesmo princípio, Bartlett e Reynolds (2015) conceituaram *Big Data*

como o termo utilizado para definir as pesquisas que tratam da habilidade do ser humano de fazer medições sobre o mundo, registrar, armazenar e analisar tais medições em quantidades sem precedentes, possibilitando novos tipos de previsões. Essa análise preditiva traz junto uma ampla variedade de infraestruturas técnicas e intelectuais, a partir da modelagem e da aprendizagem de máquina para a estatística e a psicologia.

A expansão do acesso à internet, das mídias sociais e do uso de dispositivos móveis, somada aos mais diversos tipos de sensores instalados em veículos, rodovias, edifícios, fábricas, e outras instalações, produzem, a cada segundo, uma enorme quantidade de dados, nos mais diferentes formatos como mensagens, imagens e vídeos, os quais são adicionados a uma massa gigante de dados já existentes. Organizar, acessar e processar esses dados, na forma como eles foram coletados, de modo a serem incluídos nas tomadas de decisões de aplicações de tempo real é, normalmente, considerado um desafio técnico complexo. Em razão disso, o volume, a variedade e a velocidade são as características que diferenciam o *Big Data* das bases de dados tradicionais (MOHAMED e AL-JAROODI, 2014).

A realização de análises sobre essas grandes massas de dados possibilita identificar lacunas de conhecimento, correlações e associações até então inesperadas, além de anomalias e comportamentos irregulares. No âmbito do planejamento e execução de operações militares, os conhecimentos resultantes da análise de *Big Data* podem contribuir de maneira decisiva para o sucesso das mesmas. Tais análises podem ser aplicadas em diversas situações, como na identificação de padrões ou anomalias no padrão de vida de um possível alvo terrorista, no rastreamento automático de alvos militares em amplas áreas de vigilância, ou ainda, na identificação e priorização de áreas que necessitam de assistência humanitária e apoio na recuperação de desastres (SYMON e TARAPORE, 2015).

2.3 Planejamento das Operações Militares

A imprevisibilidade, a fluidez e a difusão dos conflitos atuais, que tendem a ser limitados, não declarados e de duração imprevisível, exigem que as Forças Armadas (FA) sejam flexíveis, versáteis e dotadas de mobilidade, capazes de possibilitar a sua atuação conjunta. Nesse sentido, a compatibilização dos procedimentos e a integração das ações das Forças Singulares tornam-se fundamentais para a eficiência das Operações Conjuntas (BRASIL, 2011).

Com o objetivo de assegurar a harmonia e o alinhamento dos procedimentos adotados no âmbito da Força Terrestre (F Ter) com os praticados nas Operações Conjuntas, o planejamento para o preparo e o emprego da F Ter segue o previsto na Sistemática de Planejamento de Emprego Conjunto das Forças Armadas (SisPECFA). O ciclo completo do SisPECFA contempla quatro níveis de planejamento não estanques, sendo eles os níveis político, estratégico, operacional e tático; os quais possibilitam a organização das ideias e dos trabalhos (BRASIL, 2014).

2.3.1 Nível Político

No nível político são definidos os objetivos políticos do planejamento, preparo e emprego conjunto das Forças Armadas (FA) nos conflitos, evidenciando as orientações e condicionantes aos planejamentos subsequentes, sendo de responsabilidade do Presidente da República. Neste nível, entre outras definições, são celebradas as alianças, formuladas as diretrizes para as ações estratégicas de cada expressão do poder nacional e definidas as limitações para o emprego dos meios militares e para o uso do espaço geográfico (BRASIL, 2011).

2.3.2 Nível Estratégico

No nível estratégico são transformadas as condicionantes e diretrizes políticas em ações estratégicas a serem desenvolvidas pelos diversos ministérios, de forma coordenada com as ações militares. Neste nível, mediante a adequação, flexibilização ou cancelamento de objetivos, as diretrizes e recursos podem ser reavaliados e ajustados (BRASIL, 2011).

O Planejamento Estratégico Militar (PEM) objetiva a construção de uma capacidade de defesa que garanta a segurança do País frente às ameaças externas e internas, focado no emprego conjunto das FA de forma articulada com as demais expressões do poder nacional. O PEM é dividido em três etapas: avaliação da conjuntura e elaboração de cenários; exame da situação e planejamento; e controle das operações militares (BRASIL, 2011).

Na etapa de avaliação da conjuntura e elaboração de cenários são identificadas as ameaças e oportunidades que possam implicar no emprego das FA, as quais são traduzidas em Hipóteses de Emprego (HE). A avaliação da conjuntura é o processo pelo qual se toma conhecimento dos fatos passados e presentes nos contextos nacional e internacional; já a elaboração dos cenários prospectivos considera a sequência dos acontecimentos e dos conhecimentos que traduzem a evolução desses fatos para uma situação vindoura, como resultado do trabalho especializado e permanente de inteligência (BRASIL, 2011).

Na etapa de exame da situação e planejamento, para cada HE identificado na etapa anterior, será elaborado um Plano Estratégico de Emprego Conjunto das Forças Armadas (PEECFA), que servirá de base para os planejamentos operacional e tático. O PEECFA identificará os objetivos estratégicos, os centros de gravidade (do ponto de vista estratégico), o Estado Final Desejado (EFD), a estrutura militar e os meios, as áreas de responsabilidade, as principais ações estratégicas das demais expressões do poder nacional, entre outras (BRASIL, 2011).

A etapa de controle das operações militares compreende as ações adotadas para o acompanhamento e avaliação das operações conduzidas pelos Comandos Operacionais Ativados, visando a verificar se a evolução da situação efetivamente conduzirá ao EFD.

Mudanças de situação, assim como uma evolução indesejada, poderão conduzir a mudanças no planejamento estratégico que, entre outras medidas, poderá alterar os objetivos políticos do conflito, alterar os limites das áreas de responsabilidade, além de adjudicar novos meios aos comandos operacionais ativados (BRASIL, 2011).

2.3.3 Nível Operacional

No nível operacional é elaborado o planejamento militar da campanha, observando os principais conceitos estratégicos, os objetivos e o EFD definidos no PEECFA. Neste planejamento são definidos os objetivos operacionais e as missões das forças componentes (BRASIL, 2011).

Neste nível é executado o Exame de Situação Operacional, a partir do qual é verificada a necessidade de alteração dos limites das áreas de responsabilidade, bem como a necessidade de adequação dos meios adjudicados. Para elaboração do planejamento no nível operacional são fundamentais as informações oriundas das atividades da inteligência, assim como a atualização dos dados sobre o Teatro de Operações (BRASIL, 2011).

2.3.4 Nível Tático

No nível tático é elaborado o planejamento das Forças Componentes, e este ocorre de forma paralela e simultânea ao planejamento operacional, de forma a proporcionar a realização de ajustes no Plano Operacional baseados nos resultados dos exames de situação táticos. No planejamento, a análise pormenorizada dos atores e da área de responsabilidade recebe destaque, voltando-se atenção especial ao levantamento das possibilidades do inimigo e o acompanhamento de suas ações, de seus centros de gravidade e de suas vulnerabilidades críticas (BRASIL, 2011).

A partir dessa perspectiva, percebe-se a relevância das informações sobre o inimigo para o planejamento das operações militares. Nesse sentido, Handel (1990) ressalta essa relação ao tratar da inteligência militar como o fator de redução de riscos durante o planejamento das operações militares. O autor reforça essa ligação, destacando a importância de se considerar apenas as informações relevantes sobre o inimigo em relação ao que as próprias forças estão realizando ou planejando.

2.4 Inteligência Militar

No âmbito militar, a inteligência pode ser definida como o produto resultante da coleção, processamento, integração, avaliação, análise e interpretação de informações disponíveis a respeito de nações estrangeiras, de forças ou elementos hostis ou potencialmente hostis, e de áreas de operações atuais ou potenciais (RICHELSON, 2018).

Segundo Wilson et al (2018), a Inteligência Militar (IM) é a resultante do processamento de informações específicas para uma área de operações real ou potencial, diferindo do processo de construção da informação, pois exige, além do processamento para prover um significado aos dados, uma análise relativa às suas implicações nas operações militares. A IM verifica e combina dados de múltiplas fontes, de forma a incrementar o nível de confiabilidade dos produtos de inteligência produzidos.

A IM busca a redução do grau de incerteza existente nos diversos ambientes operacionais com base na análise e integração dos dados obtidos pelos diversos sensores, identificando ameaças e oportunidades. Para o planejamento e a condução das operações, desde o nível tático até o estratégico, é fundamental a compreensão do ambiente operacional; assim sendo, é responsabilidade da IM a análise das condições, das circunstâncias e das influências que podem vir a afetar a execução das ações requeridas para cumprir a missão (BRASIL, 2015).

Ainda assim, o valor da inteligência depende de como o tomador de decisão escolhe usar a informação que lhe foi provida. Mesmo que a coleta e análise dos dados de inteligência possam ser totalmente precisas, e os resultados encontrados sejam efetivamente comunicados, a decisão final ainda cabe à autoridade competente, a qual pode ser totalmente desconexa dos resultados de inteligência (KOSAL, 2018).

Para atender às demandas de conhecimento durante as operações, a IM deve produzir uma combinação precisa e adequada dos conhecimentos, independente do escalão em que foram originados. Nesse contexto, a IM deve empregar meios para suprir, de forma adequada e direcionada, as necessidades de inteligência oriundas dos comandantes nos níveis estratégico, operacional e tático (BRASIL, 2015).

2.4.1 Inteligência no Nível Estratégico

No nível estratégico, a IM busca prioritariamente suprir os tomadores de decisão de conhecimentos sobre as expressões do poder do inimigo, além de elaborar avaliações estratégicas e os planejamentos relativos à segurança e a defesa nacional. O foco da IM, neste nível, é a produção e a salvaguarda dos conhecimentos necessários para a formulação de avaliações estratégicas para a produção de políticas e planos militares de alto nível, voltados para o alcance dos objetivos nacionais (BRASIL, 2015).

O trabalho de inteligência no nível estratégico é um processo permanente de levantamento de informações sobre nações de interesse e áreas de tensão internas, as quais são utilizadas na elaboração de diretrizes e de planos militares de âmbito nacional e internacional. No planejamento das operações, os conhecimentos oriundos da IM são

fundamentais na definição dos objetivos estratégicos, das ameaças, dos riscos, da logística e das missões; no dimensionamento, organização e desdobramento das forças componentes; na delimitação do teatro de operações; e na percepção da opinião pública (BRASIL, 2015).

2.4.2 Inteligência no Nível Operacional

No nível operacional, a IM busca produzir e salvaguardar os conhecimentos de inteligência necessários para o planejamento, condução e sustentação das operações militares no contexto da área de atuação de um comando operacional ativado[2]. As atividades da IM neste nível são exercidas de forma permanente, tanto na situação de paz para a elaboração e aplicação de planos operacionais, como na situação de conflito para a condução das operações militares (BRASIL, 2015).

As ações e atividades da IM no nível operacional abrangem todos os fatores que determinam como serão empregados de forma conjunta os meios terrestres, navais e aéreos, gerando produtos de natureza estimativa que permitam a análise da importância, intensidade e magnitude de uma ameaça. Além disso, a IM deve contribuir na concepção, no planejamento e na condução das campanhas militares; e obter o conhecimento sobre o ambiente de operações e as possíveis forças hostis (BRASIL, 2015).

2.4.3 Inteligência no Nível Tático

No nível tático, a prioridade da IM está direcionada aos objetivos essenciais da campanha, de forma a identificar vulnerabilidades no inimigo, sobre as quais possam ser desencadeadas ações decisivas. As atividades da IM neste nível buscam o conhecimento sobre o ambiente operacional e as ameaças nele presentes de forma a prover a consciência situacional ao comandante operativo (BRASIL, 2015).

Neste nível, os conhecimentos produzidos e salvaguardados pela IM são limitados e de curto alcance no tempo em virtude da volatilidade do ambiente de batalha, razão pela qual cresce de importância o princípio da oportunidade, de forma a proporcionar ao comandante a capacidade de frequentemente reavaliar a situação militar (BRASIL, 2015).

O sucesso das operações militares tem como fator determinante a oportunidade e a acurácia da inteligência produzida em todos os níveis (US ARMY, 2012), qualidades estas que estão diretamente relacionadas com a disponibilidade e a confiabilidade das fontes de

[2]O Comando Operacional é "o comando organizado de acordo com a Diretriz para o Estabelecimento da Estrutura Militar de Defesa, ao qual cabe a responsabilidade de execução da campanha militar e demais ações militares, segundo diretrizes de planejamento específicas", o qual é ativado pelo Presidente da República de forma permanente ou pelo tempo necessário à execução de uma determinada campanha militar (BRASIL, 2009).

informação.

2.5 Fontes de Informação

Qualquer pessoa, objeto ou atividade a partir do qual é possível obter dados e informações a respeito das forças inimigas, do terreno, das condições meteorológicas, ou sobre quaisquer outros atores presentes no teatro de operações, é denominada "fonte" ou "fonte de informação" (BRASIL, 2015). Uma importante fonte para a construção do conhecimento de inteligência é o espaço cibernético, um domínio global, dentro do ambiente informacional, que consiste de uma rede interdependente de infraestruturas de tecnologia da informação, que inclui a internet, as redes de telecomunicações, assim como quaisquer outros sistemas computacionais capazes de armazenar ou transmitir informações (US ARMY, 2012).

A fonte cibernética é o recurso que possibilita a obtenção de dados, protegidos ou não, oriundos do espaço cibernético, por meio de ações realizadas utilizando ferramentas computacionais. A integração dos dados e informações obtidos a partir da fonte cibernética, com aqueles oriundos de fontes humanas e de fontes abertas, bem como da análise de imagens, da exploração de informações geográficas, da análise do espectro eletromagnético, entre outros, possibilita a produção do conhecimento de inteligência (BRASIL, 2017).

As fontes humanas são as pessoas a partir das quais se obtém informações, podendo estas serem amigas, neutras ou hostis (BRASIL, 2015). Já as fontes abertas são quaisquer meios por intermédio dos quais são disponibilizados ou transmitidos, legalmente para o consumo do público em geral, fatos, instruções ou outros materiais, sem qualquer expectativa de privacidade (US ARMY, 2012).

Dentre os principais veículos de divulgação de informações oriundas de fontes abertas estão a mídia global, os blogs web, os relatórios governamentais, as imagens de satélite (ex. *Google Maps*), os artigos acadêmicos, o *Youtube*, o *Facebook* e outros grandes sites publicados na internet. Em razão do crescimento exponencial das informações publicadas, a expectativa é de que em 2020 a internet chegará a um volume de dados de 44 ZB (zettabytes), dobrando de tamanho a cada dois anos (QUICK e CHOO, 2018).

Segundo Bartlett e Reynolds (2015), a informação de fonte aberta pode ser definida como "a informação que está publicamente disponível e pode ser legalmente acessada por intermédio de pedido, compra ou observação". Peças publicitárias, notícias sobre aquisições e negócios, opiniões de especialistas, e publicações científicas produzidas tanto pelo setor privado como por agências governamentais e instituições acadêmicas são exemplos de informações de fontes abertas.

Apesar de a internet ser um excelente meio para a coleta de informações de fontes abertas, os dados coletados devem sofrer um processo rigoroso de avaliação para determinar a confiabilidade de sua origem. Além disso, no ambiente cibernético, nem todo o

dado está disponível, sendo necessário, em alguns casos e de acordo com a necessidade de conhecimento, a aplicação de técnicas de inteligência para sua obtenção.

2.6 Open-source Intelligence

A partir da coleta sistemática, do processamento e da análise de informações relevantes publicamente disponíveis (fontes abertas), e que não estão sob o controle direto do governo, é produzida a inteligência de fontes abertas, em inglês denominada *Open-Source Intelligence* (OSINT) (US ARMY, 2012).

Na produção de OSINT, cuidados devem ser tomados com informações oriundas de domínios públicos, pois estas não necessariamente são verificadas e podem ser tendenciosas e imprecisas. A identificação de fontes de informação é um processo contínuo à medida que os diferentes meios de comunicação passam por um ciclo de popularidade (QUICK e CHOO, 2018).

Apesar disso, Gibson (2004) destaca como os principais benefícios da OSINT sua flexibilidade, dinamicidade, baixo custo e velocidade de produção. A OSINT permite ainda: identificar riscos e estratégias nos níveis estratégicos, operacional e tático; abranger desde uma avaliação rápida até uma análise mais profunda em todos os níveis de planejamento; e contextualizar os requisitos de inteligência tanto históricos como os atuais.

Em razão dessas características, no nível das decisões políticas, tanto nas de cunho nacional como internacional, a OSINT tem como papel principal a geração de resiliência e de vantagem competitiva. Além disso, outro fator importante é que, em virtude de ser produzida a partir informações de fontes abertas, a OSINT pode ser compartilhada com outros órgãos de inteligência, assim como as inteligências de outras nações, incrementando reciprocamente os respectivos graus de confiança entre os envolvidos (QUICK e CHOO, 2018).

Atualmente, informações oriundas de plataformas de mídias sociais, como o *Facebook,* têm alcançado um grande destaque na produção de inteligência; entretanto nem toda informação inserida nessas plataformas se enquadram como informação de fonte aberta. Em função disso, somada a relevância que a inteligência produzida a partir das mídias sociais vem obtendo nos últimos anos, mesmo compartilhando o mesmo ciclo de produção da OSINT (coleta, processamento e análise, e disseminação), a mesma é tratada como um tipo específico de inteligência (OMAND, BARTLETT e MILLER, 2012).

2.7 Social Media Intelligence

A partir da explosão das mídias sociais, as atividades sociais, culturais e

intelectuais passaram a ser capturadas na forma digital e compartilhadas nessas plataformas, tornando a vida social registrável e mensurável (BARTLETT e REYNOLDS, 2015). Com isso, esses meios de compartilhamento constituíram-se em fontes para obtenção de informações de inteligência, dando origem a *Social Media Intelligence* (SOCMINT), que é a inteligência derivada das mídias sociais.

Nesse sentido, para Rajamäki, Sarlio-Siintola e Simola (2018), a SOCMINT pode ser definida como a exploração analítica das informações disponíveis nas mídias sociais. É também, segundo os autores, a habilidade de monitorar milhões de contas e *hashtags* em tempo real, e então analisar e armazenar esses dados, com baixo custo e, na maioria das vezes, com pouco impacto sobre a privacidade das pessoas.

A mídia social é um conjunto de tecnologias não estáticas, cuja infraestrutura tende a mudar no decorrer do tempo. Em razão disso, a SOCMINT cobre uma ampla variedade de aplicações, técnicas e capacidades, destinadas à coleta e ao uso dos dados de mídias sociais para a produção de conhecimentos de inteligência (BARTLETT e REYNOLDS, 2015).

Dentre as técnicas de acesso e processamento de grandes conjuntos de dados, diretamente a partir das plataformas de mídias sociais, destaca-se o uso de *Application Programming Interfaces* (API). Entretanto, os termos de uso, o formato e a utilidade dos dados variam muito de plataforma para plataforma. Apesar disso, devido ao crescimento da importância e do valor atribuído à análise de *Big Data*, a disponibilidade de API para coleta de dados nas diversas plataformas está se tornando cada vez mais comum (BARTLETT e REYNOLDS, 2015).

Assim como na OSINT, a SOCMINT requer a validação das fontes e a interpretação das informações obtidas. Além disso, outro ponto fundamental na produção da SOCMINT, considerando a possibilidade de compartilhamento da inteligência produzida, é distinguir informações de fonte aberta daquelas que possuem algum nível de restrição de acesso (BARTLETT e REYNOLDS, 2015).

As contas e grupos do *Facebook*, por exemplo, frequentemente tem variados graus de restrição de acesso e, além disso, diferentes plataformas frequentemente tem termos, condições e normas de uso completamente diversas, não existindo, portanto, uma definição clara do que pode ser considerada informação privada. Em função disso, a inteligência produzida baseada exclusivamente em informações de fontes abertas, obtidas nas mídias sociais, recebe a denominação específica de "*Open* SOCMINT" (BARTLETT e REYNOLDS, 2015).

3 METODOLOGIA

Este trabalho caracteriza-se como uma pesquisa de natureza aplicada e abordagem qualitativa, uma vez que os dados coletados são provenientes da própria bibliografia (TOZONI-REIS, 2009), com objetivo exploratório, no intuito de propiciar um melhor entendimento do assunto, onde a análise bibliográfica foi o principal processo técnico aplicado, pois as informações necessárias foram obtidas a partir de livros, artigos científicos e revistas. Para tal, realizou-se inicialmente um levantamento seguido da seleção de referências bibliográficas, a partir das quais apresentou-se os principais conceitos necessários ao entendimento da pesquisa.

Em uma segunda fase, realizou-se uma pesquisa histórico/bibliográfica, a partir da qual foi confirmada a **relevância da inteligência para as operações militares com base em fatos históricos sobre operações militares de outras nações que obtiveram êxito graças às informações geradas pela inteligência. Na sequência, realizou-se pesquisa bibliográfica com o objetivo de identificar exemplos de uso das *fontes cibernéticas na produção de inteligência nas diversas áreas do conhecimento e comprovar a possibilidade de sua aplicação na produção de inteligência militar. Concluindo essa fase, demonstrou-se o uso da fonte cibernética nas operações militares.***

***Na fase final,* realizou-se uma discussão dos resultados obtidos na segunda fase, onde, por meio da análise dos principais aspectos apresentados, verificou-se o alcance dos objetivos propostos para o trabalho.** Por fim, apresentou-se a conclusão deste trabalho com um resumo dos passos realizados.

4 RESULTADOS OBTIDOS

Durante a pesquisa bibliográfica buscou-se relatos de sucesso que evidenciassem o emprego da inteligência militar em situações de conflito, validassem o uso de fontes cibernéticas para a produção de inteligência militar e que demonstrassem o uso dessas fontes em proveito das operações militares. Os resultados são apresentados a seguir.

4.1 Relevância da inteligência nas operações militares

Sobre a relevância da inteligência para as operações militares foram escolhidas três operações ocorridas em conflitos recentes, com características completamente distintas, ocorridas em diferentes regiões do mundo e envolvendo contingentes militares de diferentes países, os quais são apresentados a seguir.

4.1.1 A segunda guerra entre Líbano e Israel, ocorrida de 12 de julho a 14 de agosto de 2006

Nesse caso, o conhecimento produzido pela inteligência militar israelense, principalmente no nível estratégico, por meio de informações obtidas durante o período pré-conflito, das quais se destacaram aquelas coletadas a partir de fontes abertas (transmissões em TV aberta e outros meios de comunicação), foram decisivas para o sucesso militar de Israel naquele conflito. Em razão do conhecimento de inteligência produzido, foi possível prever a possibilidade iminente de ataques, os principais alvos, o modo de operação (sequestro de soldados israelenses), o poder de fogo do oponente (o *Hezbollah*), e a localização e, principalmente, a destruição de arsenais (BAR-JOSEPH, 2007).

Entretanto, o resultado do trabalho de inteligência realizado no nível tático deixou a desejar, em virtude da classificação inadequada do conhecimento produzido, fato este que impediu que os líderes militares, responsáveis pela execução das operações, recebessem informações oportunas para a produção de uma consciência situacional adequada do teatro de operações. Outro ponto negativo, foi a dificuldade da inteligência israelense de identificar os sistemas de comando e controle inimigo, assim como a incapacidade de localizar e neutralizar seus líderes, principalmente em função do excelente trabalho de contrainteligência realizado pelo *Hezbollah* (BAR-JOSEPH, 2007).

4.1.2 A participação do contingente brasileiro (BRABAT), no âmbito da Missão das Nações Unidas para estabilização do Haiti (MINUSTAH), no período de dezembro de 2006 a março de 2017

Nesse episódio, após algumas tentativas frustradas de promover a paz no Haiti, que enfrentava no final de 2006 uma grave crise humanitária e de segurança, estando boa parte do seu território sob domínio de gangues, a MINUSTAH recebeu o sinal verde do governo haitiano para intervir militarmente e com força total. Devido aos insucessos anteriores, priorizou-se as ações de inteligência, a partir das quais foram coletadas e processadas informações em grande quantidade, com o objetivo de determinar a localização, o poder de fogo e as atividades das gangues e de seus líderes, preparar o ambiente e o espaço de batalha, minimizar os riscos para a tropa, e evitar fatalidades entre os cidadãos haitianos inocentes (DORN, 2009).

Com base nos conhecimentos de inteligência produzidos e da consciência situacional obtida em função destes, as operações foram guiadas pelo uso de grande quantidade de força direcionada de forma a obter vantagem psicológica e o rápido desengajamento do combate por parte das forças oponentes. Além disso, o uso de operações noturnas, o princípio da surpresa, a mobilidade e a aplicação de táticas para criar confusão entre os integrantes das gangues minimizaram os danos colaterais (DORN, 2009).

Outra estratégia adotada com sucesso foi a identificação e a conquista de modo cirúrgico de locais estratégicos, utilizados originalmente pelas gangues, os quais foram

denominados “pontos fortes”. A conquista desses pontos, além de possibilitar o patrulhamento de áreas antes “proibidas” em virtude do domínio das gangues, serviam para, deliberadamente, atrair o fogo dos bandidos que atacavam em retaliação à tomada do território, permitindo que as tropas respondessem com fogo a partir de posições relativamente seguras (DORN, 2009).

Como resultado dessas operações, mais de 800 integrantes de gangues foram presos, com um baixo número de fatalidades ocorridas, sendo oficialmente reportadas, durante todo o período das operações, apenas 11 (onze) óbitos, dentre os quais 7 (sete) de reconhecidos integrantes de gangues. Ainda, como resultado dos trabalhos de inteligência, Evens Jeune, um dos mais temidos líderes de gangue, que havia escapado durante o ataque a sua “fortaleza”, foi preso no sul da comuna haitiana de Les Cayes, a partir de informações obtidas junto à população local (DORN, 2009).

4.1.3 Campanha de contra insurgência na província de Kandahar, no Afeganistão, realizada pelas forças canadenses, no período de janeiro de 2008 até dezembro 2010

Nas operações realizadas nessa campanha, destacou-se o uso de fontes humanas (informantes Talibãs e/ou população civil local), a partir das quais eram coletadas ou confirmadas informações que permitiram capturar inúmeros suspeitos posteriormente confirmados como insurgentes, localizar e neutralizar uma rede Talibã de produção de artefatos explosivos improvisados (IED), além de prender seus líderes e financiadores. A qualidade e o volume de dados coletados, processados e selecionados pelo serviço de inteligência canadense possibilitaram que mais de 60% dos IED instalados em Kandahar fossem encontrados e desarmados (CHARTERS, 2012).

O entendimento da complexidade da população afegã e dos demais atores domésticos e internacionais, bem como de suas interações, foi fundamental para se construir uma consciência situacional sobre o ambiente e a sociedade nas quais as forças canadenses estavam operando. A presença constante dessas forças nas ruas resultou em um aumento da confiança e uma consequente cooperação da população local, que, por sua vez, tinha melhores condições de identificar os insurgentes, bem como localizar e notificar a presença de IED, o que contribuiu significativamente para a eficácia das operações em Kandahar (CHARTERS, 2012).

4.2 A fonte cibernética na produção de inteligência militar

Sobre a validação do uso de fontes cibernéticas na produção de inteligência militar analisou-se diversas referências bibliográficas, a partir das quais apresentaram-se as razões que tornaram a fonte cibernética uma fonte adequada, senão indispensável, para a produção de inteligência militar nos tempos atuais.

A Estratégia de Segurança Nacional da Grã-Bretanha reconhece que o trabalho de segurança e inteligência é geralmente baseado não apenas no consentimento e no entendimento do público, mas também na ativa parceria e participação de pessoas e comunidades. Danos graves à segurança ocorrem quando os esforços do estado não são aceitos ou confiáveis (CAMERON e CLEGG, 2010).

Por esse motivo, medir e compreender o ponto de vista de milhões de pessoas por meio do que elas estão digitalmente discutindo, falando, brincando, condenando e aplaudindo é de amplo interesse e de enorme valor para as mais diversas áreas do conhecimento, governos e demais organizações. Organizações utilizam ferramentas denominadas "*Social Media Analytics*" para rastrear nas mídias sociais as atitudes de seus clientes em relação às suas marcas, produtos e serviços, de forma a monitorar a sua reputação; assim como governos ao redor do mundo utilizam as mesmas ferramentas para mapear o conhecimento popular a fim de planejar soluções para situações de emergência (OMAND, BARTLETT e MILLER, 2012).

Além disso, com a facilidade de acesso às mídias sociais, os espectadores até então passivos puderam se tornar "jornalistas" ativos, fornecendo e transmitindo informações na hora e local onde estão ocorrendo os fatos. Em virtude da escala e dinamismo dessas informações, as ações das autoridades se tornaram muito mais efetivas no socorro às vítimas de catástrofes, como no terremoto no Haiti, em virtude dos inúmeros testemunhos reportados nas mídias sociais (OMAND, BARTLETT e MILLER, 2012).

Novos *softwares* e ferramentas de análise das mídias sociais possibilitaram, de longe, o maior nível de vigilância jamais visto anteriormente, trazendo consigo concomitantemente riscos e oportunidades. Em razão disso, nos últimos anos, ocorreu um crescimento significante nos estudos acadêmicos dos denominados "*Social Big Data*", os quais combinaram ciências sociais e computação, para juntas coletar, agrupar e entender quantidades muito grandes de dados sociais extraídos das mídias sociais (BARTLETT e REYNOLDS, 2015).

Os conteúdos multimídia como áudios, fotos e vídeos, inseridos nas plataformas de mídia social, podem adicionar informações úteis na caracterização dos mais diversos tipos de eventos. Entretanto, em virtude da variedade de formatos e das características específicas de cada tipo de conteúdo multimídia, diferentemente do que ocorre com os conteúdos textuais, combiná-los para entender as causas e efeitos dos eventos é um desafio.

Para enfrentar esse desafio, realizaram-se diversos estudos científicos, dos quais pode-se destacar o de Becker, Naaman e Gravano (2010), que propôs um *framework* que, baseado em uma abordagem de aprendizagem que faz uso de métricas de similaridade e técnicas de agrupamento/classificação, permite correlacionar conteúdos multimídia de diferentes plataformas de mídias sociais agrupando aqueles pertencentes ao mesmo evento. Segundo a proposta dos autores, para a classificação de similaridade, são considerados, além do próprio conteúdo, o contexto de sua publicação, como informações textuais aos quais está vinculado, como título e *hashtags,* a data e a hora em que foram publicados e a

localização geográfica de origem.

A soma do resultado de diversos estudos serviram de base para o desenvolvimento de ferramentas como o SUPER (*Social sensors for security assessments and proactive emergencies management*), um sistema de gerenciamento de emergências e incidentes de segurança, baseado na extração de informações das mídias sociais, desenvolvido no âmbito da Comissão Europeia, com a participação de diversas universidades. O sistema tem por finalidade explorar uma estrutura holística integrada, desenvolvida para rastrear e avaliar as reações das vítimas, dos voluntários e dos demais cidadãos em relação às situações de emergência, a partir de suas publicações nas mídias sociais, e, ao mesmo tempo, capacitar as forças de segurança e as agências de proteção civil para tirar o máximo de vantagem do conhecimento produzido para suas operações (MCCREADIE et al, 2015).

4.3 O uso da fonte cibernética em operações militares

Sobre a demonstração do uso de fontes cibernéticas em proveito das operações militares, foram escolhidos três exemplos de projetos/operações de cunho militar, de diferentes níveis e em diferentes países, onde a produção de conhecimento de inteligência, usando como fonte principal as mídias sociais, tornou-se fundamental para o sucesso das mesmas. Os resultados são apresentados a seguir.

4.3.1 Monitoramento de células terroristas pelas agências de inteligência dos Estados Unidos da América

As inteligências de órgãos como CIA, NSA, e Marine Corps mapeiam, a partir das mídias sociais, entre outros alvos, as atividades, as intenções e a logística, a nível global, de grupos com viés terrorista como os jihadistas e o Estado Islâmico. Para isso, utilizam uma variedade de *softwares* de análise/métricas como o *Visible: Socializing the Enterprise; o Geofeedia (ferramenta de reconhecimento facial); o CIA's Open Source Indicators; o DoD's Information Volume and Velocity; o Recorded Future; e o Palantir* (LIM, 2016).

Mesmo com o apoio dessas ferramentas, e de sua eficácia quando se trata de fins específicos, no âmbito da inteligência estratégica, a capacidade das agências de coletar informações supera em muito a capacidade de analisá-las. Apesar do poder dessas plataformas, e mesmo considerando que todos os dados obtidos sejam temporais e geoespacialmente marcados, há ainda a necessidade de atuação do analista, que dever saber especificamente o que procurar (LIM, 2016).

4.3.2 Monitoramento de extremistas pela Polícia de Londres

No Reino Unido, em razão do crescimento do uso das mídias sociais para organização e mobilização de massas, a Polícia Londrina tem empregado desde 2012 a SOCMINT para obter a consciência situacional e elaborar estratégias para conter desordens

e o extremismo no âmbito doméstico, particularmente nas manifestações e protestos. Além disso, a SOCMINT também é usada para monitorar tensões relacionadas ao trabalho policial, assim como menções hostis que possam repercutir na reputação da instituição policial (DENCIK, HINTZ e CAREY, 2018).

Para execução do trabalho de coleta e análise de informações oriundas das mídias sociais, a Polícia de Londres comprou ferramentas comerciais de diversos fornecedores, como os programas *TweetDeck* e o *Hootsuite*, os quais necessitaram ser adaptados às características do trabalho policial. Os principais tipos de análise realizados pelas ferramentas são: a busca por palavras chaves que permitam encontrar potenciais ameaças, a avaliação de riscos e recursos, e a identificação dos organizadores/influenciadores, todos apoiados por algoritmos capazes de filtrar ruídos e possibilitar o trabalho de análise apenas sobre os dados relevantes (DENCIK, HINTZ e CAREY, 2018).

4.3.3 Projeto de Vigilância Marítima Integrada da Guarda Costeira Holandesa

O objetivo do Projeto *Maritime Integrated Surveillance Awareness (*MARISA) é fortalecer a segurança marítima da Holanda e incrementar a inteligência da Guarda Costeira Holandesa (GCH) em termos de precisão, confiabilidade e redundância. Para isso, a GCH utiliza ferramentas matemáticas e conceitos pertencentes à teoria de grafos para analisar as redes de organizações criminosas nas mídias sociais, determinando a força e a direção das conexões entre os atores (KALDEN, 2018).

No planejamento de uma ação terrorista é esperado que ocorra um aumento de tráfego nas mídias sociais dos seus participantes, por meio dos quais, dependendo do nível de experiências dos envolvidos, pode-se obter diversas informações, como, por exemplo, sua localização. A partir dos dados coletados, são utilizados cálculos de centralidade para estimar os objetivos futuros das organizações criminosas e os papéis, atuais e futuros, de cada um dos atores identificados (KALDEN, 2018).

5 DISCUSSÃO DOS RESULTADOS

O papel da inteligência é prover ao tomador de decisão informações independentes e imparciais, que sejam oportunas, precisas, relevantes, verificáveis, que respondam às questões e que possibilitem que a tomada de decisão seja realizada de maneira proativa (QUICK e CHOO, 2018). Habituar o tomador de decisão aos riscos pode reduzir seus medos e sua impotência para tomar decisões no momento oportuno (GIBSON, 2004).

Em função das premissas acima e dos resultados apresentados na seção 4.1, é possível inferir que os conhecimentos produzidos pelo trabalho de inteligência continuam sendo um diferencial no planejamento e execução das operações militares, apesar das

mudanças nos formatos dos conflitos atuais. Outra característica importante observada na análise dos três exemplos selecionados é que, independentemente do tipo de conflito, das especificidades do teatro de operações ou do nível de organização das forças oponentes, o conhecimento produzido pela inteligência foi fundamental para a redução dos efeitos colaterais, da baixa de civis e do tempo necessário para se atingir os respectivos objetivos militares.

A redução dos riscos, em função do trabalho de inteligência, fica evidenciada no conflito entre Líbano e Israel, onde, por intermédio das ações preventivas realizadas pelas forças de Israel, evitou-se que o *Hezbollah* obtivesse sucesso nos planos de sequestrar soldados israelenses. Além disso, é claramente exemplificada o uso das fontes abertas quando da análise dos discursos de líderes do *Hezbollah* transmitidos em TV aberta, os quais serviram de alerta para a necessidade de produção de conhecimento de inteligência no intuito de antecipar-se a ataques, proteger alvos em potencial e viabilizar um contra-ataque rápido e eficaz.

No âmbito da MINUSTAH, mais uma vez a inteligência se mostrou eficaz, com destaque para o nível estratégico, pois, fazendo uso de fontes humanas, os conhecimentos de inteligência produzidos possibilitaram um planejamento preciso, que por sua vez resultou na execução conjunta de ações de resgate da confiança da população e de ataques rápidos e pontuais, praticamente sem baixas, mas com efeito determinante no desmantelamento das gangues e prisão dos seus líderes. De forma semelhante, a inteligência oriunda de fontes humanas, desta vez no nível tático, foi decisiva nas operações militares canadenses na província de Kandahar, no Afeganistão, onde a localização e o desarme de artefatos explosivos, produzidos e instalados na região pelo Talibã poupou inúmeras vidas inocentes.

Na seção 4.2, os estudos selecionados apresentam os diversos tipos de dados disponíveis no ambiente cibernético e a sua aplicabilidade na produção de conhecimento de inteligência. Demonstram, ainda, as razões que as tornam um diferencial na busca pelo sucesso, tanto nas operações militares, como no mercado corporativo.

A explosão do uso das mídias sociais, destacado por Bartlett e Reynolds (2015), em conjunto com a evolução das técnicas e ferramentas para a coleta, classificação e processamento das informações oriundas das fontes cibernéticas, corroboram a viabilidade do seu uso na produção, eficiente e eficaz, de conhecimento de inteligência compatível com as necessidades militares. Destaca-se, nesse sentido, o estudo realizado por Omand, Barlett e Miller (2012), que demonstra que, após a popularização das redes sociais, surgiu de maneira espontânea um novo tipo de jornalismo, oriundo de pessoas comuns, que, a partir de seus próprios dispositivos móveis, registram por meio de vídeos, fotos e mensagens de textos os acontecimentos em tempo real, e disponibilizam esse conhecimento imediatamente para qualquer pessoa que tiver interesse, em qualquer lugar do mundo.

Um exemplo prático desse tipo de jornalismo pôde ser observado na tentativa de

assassinato do Deputado Federal Jair Messias Bolsonaro, ocorrida durante ato de campanha à presidência da república do Brasil, que se realizava no município de Juiz de Fora – MG, em 6 de setembro de 2018. A notícia desse fato foi divulgada instantaneamente nas mídias sociais, com textos, imagens e vídeos dos mais diversos ângulos, os quais, além de tornar público o ocorrido, contribuiu de maneira decisiva com as autoridades policiais, não deixando quaisquer dúvidas quanto à autoria do ato perante a opinião pública.

Outro ponto que cabe ser destacado é a rápida evolução das ferramentas de tecnologia da informação (TI) utilizadas no trabalho de processamento e análise das grandes massas de dados disponíveis nas mídias sociais. Tal evolução torna-se mais evidente ao se comparar o estudo realizado por Becker, Naaman e Gravano (2010) com o realizado por McCreadie et al (2015); neste último estudo, fica claro que o problema mais geral de correlacionamento de conteúdo, descrito no primeiro estudo, já foi superado, e que o foco deste foi otimizar a aplicação das técnicas de análise em *Big Data* para um domínio específico.

Encerrando a discussão dos resultados, verifica-se que os exemplos selecionados e apresentados na seção 4.3 representam propostas viáveis de uso de conhecimento de inteligência produzido a partir das mídias sociais em proveito de operações de cunho militar. Verificou-se, ainda, que apesar de haver muitos estudos demonstrando o potencial do uso das fontes cibernéticas para a produção de inteligência, em especial das mídias sociais, existem poucos trabalhos científicos publicados que relatam os resultados práticos de sua utilização.

Devido à reduzida fonte de pesquisa, optou-se por selecionar três exemplos de operações de cunho militar, realizadas em três diferentes países, e que demonstram o uso de inteligência nos seus três níveis: o estratégico, o operacional e o tático. Todos os três exemplos têm a mídia social como sua principal fonte para produção de inteligência, entretanto, utilizam diferentes ferramentas e métodos para sua coleta, classificação e processamento.

No primeiro exemplo, o norte-americano, cujo foco é o monitoramento de células terroristas ao redor do mundo, o objetivo principal é produzir inteligência no nível estratégico, identificando para cada célula a sua capacidade militar (poder de fogo) e o nível de ameaça que representa. Em função dos conhecimentos de inteligência produzidos, tornam-se possíveis os planejamentos necessários, no âmbito de todas as suas forças, para garantir a segurança do seu território, bem como de suas tropas quando em operações em outros países.

Já no segundo exemplo, o holandês, cujo foco é a proteção das suas águas costeiras, o objetivo principal é produzir inteligência de nível operacional, que permita o mapeamento geoespacial de riscos, antecipando a probabilidade de determinados eventos ocorrerem em determinados lugares. Tudo isso visando a produzir uma consciência situacional da área de operações da Guarda Costeira Holandesa suficiente para o planejamento e o emprego dos

seus escassos recursos marítimos.

Da mesma forma, no último exemplo, o britânico, cujo o foco principal é a segurança interna da cidade de Londres durante protestos e manifestações, o objetivo é produzir inteligência para o nível tático, identificando, previamente e durante as manifestações, os líderes dos movimentos, demais participantes que apresentam sinais de comportamento extremista e os prováveis pontos de encontro desses participantes. Tudo isso com a finalidade de realizar o planejamento prévio da atuação policial durante as manifestações e, também, possibilitar uma resposta eficiente, eficaz e efetiva da Polícia de Londres a qualquer ato hostil/extremista iminente ou em execução.

Em função do exposto nessa discussão dos resultados, é possível afirmar que o uso da fonte cibernética e as tecnologias a ela relacionadas estão maduras o suficiente para o seu emprego na produção de inteligência no nível estratégico. Pode-se ainda inferir que em pouco anos a produção de inteligência a partir das fontes cibernéticas, principalmente das mídias sociais, deixará de ser um diferencial para o sucesso das operações militares, tornando-se um pré-requisito, de forma que a sua negligência resultará inevitavelmente no insucesso.

6 CONCLUSÃO

Iniciou-se este artigo descrevendo diversos conceitos relevantes para a pesquisa, dos quais pode-se destacar o conceito de conhecimento, com o seu valor e a importância do seu gerenciamento e aplicação nas tomadas de decisões; o conceito de *Big Data*, suas características, formas de exploração e possibilidades de aplicação nas operações militares; o conceito do planejamento das operações militares, destacando suas características nos níveis político, estratégico, operacional e tático; o conceito de inteligência militar, sua aplicação, limitações, e as suas características, de acordo com o nível em que será aplicada; o conceito de fontes de informação, seus principais veículos, características e limitações; finalizando com os conceitos sobre as inteligências de fonte aberta (*open-source*) e das mídias sociais (*social media*), descrevendo suas características e vantagens.

Demonstrou-se, assim, a relevância da produção e aplicação do conhecimento de inteligência na solução de conflitos por intermédio de operações militares. Para isso, analisou-se três conflitos recentes ocorridos em diferentes continentes e com características distintas, sendo que em todos os casos o uso de inteligência teve papel decisivo na eficácia das operações e na redução de baixas, tanto civis quanto militares.

Na sequência, validou-se o uso das fontes cibernéticas na produção de inteligência militar, apresentando as razões que tornam os dados oriundos destas fontes, principalmente aqueles disponíveis nas mídias sociais, fundamentais para a produção de inteligência nos dias atuais. Além disso, expôs-se a evolução das ferramentas e técnicas para a coleta, classificação, análise e produção eficiente de inteligência a partir de grandes massas de dados (*Big Data*).

Em seguida, para demonstrar o uso das fontes cibernéticas em operações militares, selecionou-se três exemplos de uso da inteligência nos níveis estratégico, operacional e tático, com finalidades de apoiar diferentes tipos de operações de cunho militar, em diferentes países, produzidas a partir das mídias sociais, utilizando diferentes técnicas e ferramentas. Tais exemplos não só confirmaram a possibilidade de utilização das fontes cibernéticas em operações militares, como também a de perceber que, independentemente do nível da inteligência a ser produzida, sem os dados oriundos das mídias sociais os resultados obtidos nas execuções de cada uma das missões elencadas seriam seriamente comprometidos, senão inviabilizados.

Para encerrar este estudo, realizou-se uma análise dos resultados obtidos com a pesquisa, por meio da qual foi possível concluir que as técnicas e ferramentas para a produção de conhecimento a partir de "*Big Data*", oriundas das fontes cibernéticas, já atingiram um nível de maturidade capaz de atender demandas de inteligência no nível estratégico. Outro fato importante que pode ser destacado é a velocidade com que as ferramentas evoluem, tornando-as cada vez mais especializadas na produção de inteligência específica para determinados fins.

Durante a realização desta pesquisa, o principal óbice encontrado foi a pouca quantidade de artigos científicos publicados com exemplos de aplicação prática da inteligência, provavelmente em função do assunto ser tratado de forma restrita dentro dos órgãos de inteligências de cada país. Outro fator importante a ser considerado foi o pouco tempo disponível para realização do trabalho, fato esse que restringiu a pesquisa, em sua grande parte, às publicações em periódicos científicos internacionais disponíveis on-line.

Em razão do exposto, sugere-se como trabalho futuro realizar um comparativo dos resultados aqui obtidos com a produção de inteligência no nível nacional. Sugere-se, ainda, a seleção de um conjunto de ferramentas dentre as aqui citadas, para a sua integração e aplicação em um exemplo prático para produção de inteligência no nível estratégico, considerando como o "teatro de operações" as áreas onde ocorrem ações militares em virtude da intervenção na segurança pública no estado do Rio de Janeiro.

REFERÊNCIAS

ARCHER-BROWN, Chris; KIETZMANN, Jan. Strategic knowledge management and enterprise social media. **Journal of Knowledge Management**, Emerald Publishing Limited, 2018.

BAR-JOSEPH, Uri. Israel's military intelligence performance in the Second Lebanon War. **International Journal of Intelligence and Counterintelligence**, v. 20, n. 4, p. 583-601, 2007.

BARTLETT, Jamie; REYNOLDS, Louis. **The State of the Art 2015:** a literature review of social media intelligence capabilities for counter-terrorism. London: Demos, 2015.

BECKER, Hila; NAAMAN, Mor; GRAVANO, Luis. Learning similarity metrics for event identification in social media. In: **Proceedings of the third ACM international conference on Web search and data mining**. ACM, 2010. p. 291-300.

BRASIL. Estado-Maior do Exército. **Manual de Campanha**: Glossário de Termos e Expressões para uso no Exército, 4ª Ed., 2009.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas**: Doutrina de Operações Conjuntas, 1ª ed., 2011.

BRASIL. Estado-Maior do Exército. **Manual de Fundamentos**: Doutrina Militar Terrestre, 1ª Ed., 2014.

BRASIL. Estado-Maior do Exército. **Manual de Fundamentos**: Inteligência Militar Terrestre, 2ª Ed., 2015.

BRASIL. Comando de Operações Terrestres. **Manual de Campanha**: Guerra Cibernética, 1ª Ed., 2017.

CAMERON, David; CLEGG, Deputy Prime Minister Nick. **A strong Britain in an age of uncertainty:** the national security strategy. London, v. 3, 2010.

CHARTERS, David A. Canadian military intelligence in Afghanistan. **International journal of intelligence and counterintelligence**, v. 25, n. 3, p. 470-507, 2012.

COMMONS, Austin G. A cibernética é o novo domínio aéreo: a superioridade nos domínios em megacidades. **Military Review**, p. 66-77, 2º Trimestre 2018. Disponível em: <https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese /a-cibernetica-e-o-novo-dominio-aereo-a-superioridade-nos-dominios-em-megacidades.pdf>. Acesso em: 10 jul. 2018.

DENCIK, Lina; HINTZ, Arne; CAREY, Zoe. Prediction, pre-emption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. new media & society. **New Media & Society**, v. 20, n. 4, p. 1433-1450, 2018.

DORN, A. Walter. Intelligence-led peacekeeping: the United Nations stabilization mission in Haiti (MINUSTAH), 2006–07. **Intelligence and National Security**, v. 24, n. 6, p. 805-835, 2009.

GIBSON, Stevyn. Open source intelligence: an intelligence lifeline. **The RUSI Journal**, v. 149, n. 1, p. 16-22, 2004.

HANDEL, Michael, L. **Intelligency and Military Operations**. Routledge, 1990.

KALDEN, J. P. H. Data Analysis Within the Netherlands Coastguard: Risk Mapping, Social Network Analysis and Anomaly Detection. In: **NL ARMS Netherlands Annual Review of Military Studies 2018**. TMC Asser Press, 2018. p. 193-200.

KOSAL, Margaret E. **Technology and the Intelligence Community: c**hallenges and advances for the 21st century. Gewerbestrasse: Springer, 2018.

LIM, Kevjn. Big data and strategic intelligence. **Intelligence and National Security**, v. 31, n. 4, p. 619-635, 2016.

MCCREADIE, Richard et al. SUPER: Towards the use of social sensors for security assessments and proactive management of emergencies. In: **Proceedings of the 24th International Conference on World Wide Web**. ACM, 2015. p. 1217-1220.

MCDOWEL, Dom. **Strategic Intelligence: a** handbook for practitioners, managers, and users. Toronto, The Scarecrow Press, Inc., 2009.

MOHAMED, Nader; AL-JAROODI, Jameela. Real-time big data analytics: applications and challenges.. In: **High Performance Computing & Simulation (HPCS), 2014 International Conference on**. IEEE, 2014. p. 305-310.

OMAND, David; BARTLETT, Jamie; MILLER, Carl. Introducing social media intelligence (SOCMINT). **Intelligence and National Security**, v. 27, n. 6, p. 801-823, 2012.

QUICK, Darren; CHOO, Kim-Kwang Raymond. Digital forensic intelligence: data subsets and open source intelligence (DFINT+ OSINT): a timely and cohesive mix. **Future Generation Computer Systems**, v. 78, p. 558-567, 2018.

RAJAMÄKI, Jyri; SARLIO-SIINTOLA, Sari; SIMOLA, Jussi. The ethics of open source intelligence applied by Maritime Law Enforcement Authorities. In: **ECCWS 2018 17th European Conference on Cyber Warfare and Security**. Academic Conferences and publishing limited, 2018. p. 424.

RICHELSON, Jeffrey T. **The US intelligence community**. Routledge, 2018.

SANTOS, Luiz Paulo Lopes dos. O comportamento humano. **O Comunicante**, [S.l.], v. 8, n. 1, p. 43-49, jan. 2018. Disponível em: <http://ebrevistas.eb.mil.br/index.php/OC/article/view/1115>. Acesso em: 10 jul. 2018.

SYMON, Paul B.; TARAPORE, Arzan. Defense intelligence analysis in the age of big data. **Joint Forces Quarterly—JFQ**, v. 79, p. 4-11, 2015.

TOZONI-REIS, Marília F. C. **Metodologia de Pesquisa**. Curitiba: IESDE Brasil, 2009.

US ARMY. **Open-Source Intelligence**, July 2012. Disponível em: <https://fas.org /irp/doddir/army/atp2-22-9.pdf>. Acesso em: 10 jul. 2018.

WILSON, Lauren E. et al. The forensic intelligence continuum in the military context. **Australian Journal of Forensic Sciences**, p. 1-13, 2018.

YEBOAH-OFORI, Abel; BRIMICOMBE, Allan. Intelligence & OSINT: developing mitigation techniques against cybercrime threats on social media. A Systematic Review. July, 2017. **International Journal of Cyber-Security and Digital Forensics**. v.7, n.1, p. 87-99, 2018.