OPINIÃO

http://dx.doi.org/10.22480/rev.unifa.v30n2.426

O papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação no Brasil: comparação com Estados Unidos, Reino Unido, Alemanha e Rússia

The role of technological innovation and the joint management of the cybernetics sector in the integration of Information Operations in Brazil: comparison with the United States, United Kingdom, Germany and Russia

El papel de la innovación tecnológica y de la gestión conjunta del sector cibernético en la integración de las Operaciones de Información en Brasil: comparación con Estados Unidos, Reino Unido, Alemania y Rusia

Márcio Saldanha Walker[I]

RESUMO

O objetivo do estudo é verificar o papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação no Brasil. O advento das inovações tecnológicas modificou a visão das forças armas mundiais com relação à organização do setor cibernético e à integração das Operações de Informação. No Brasil, as propostas político-estratégicas do Ministério da Defesa resultaram em iniciativas no setor cibernético nas três Forças Armadas, impactando a gestão organizacional das Operações de Informação conjuntas. Por problema evidenciou-se foi que as três Forças Armadas brasileiras estruturaram diferentes sistemas cibernéticos e de informação, de forma divergente à tendência mundial quanto à interoperabilidade em Operações Conjuntas. No método, foi utilizada a comparação da visão político-estratégica organizacional e das estruturas cibernéticas conjuntas nas Operações de Informação dos Estados Unidos, Reino Unido, Alemanha e Rússia, com a visão político-estratégica e as estruturas cibernéticas e de Operações de Informação do Brasil. Assim, verificou-se que, embora parcialmente divergentes, os países comparados com o Brasil apresentam uma visão comum quanto à proposta político-estratégica e estrutura cibernética conjunta, diferentemente do modelo de gestão da informação cibernética do Brasil que não possui a visão conjunta organizacional. Como conclusão, o estudo sugere a integração pela inovação da Gestão da Informação, com a unificação da estrutura cibernética no nível estratégico e operacional conjunto das Forças Armadas, de forma a aumentar a interoperabilidade das Operações de Informação.

Palavras-chave: Operações de informação. Defesa cibernética. Guerra cibernética. Operações conjuntas.

ABSTRACT

This study is intended to verify the role of technological innovation and the joint management of the cybernetics sector in the integration of Information Operations in Brazil. The advent of technological innovations has modified the vision of forces of the world with regard to the organization of the cybernetics sector and the integration of Information Operations. In Brazil, the political-strategic proposals of the Ministry of Defense resulted in initiatives in the cybernetics sector in the three Armed Forces, impacting the organizational management of the Joint Information Operations. The problem was evidenced by the fact that the three Brazilian Armed Forces structured different cybernetic and information systems, divergent from the global trend in terms of interoperability in Joint Operations. The comparison between the of organizational political-strategic vision and the joint cybernetic structures

I. Comando de Operações Terrestres (COTER) – Brasília/DF – Brasil. Tenente-Coronel do Exército Brasileiro (EB). Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército (ECEME). E-mail: walker22ms@yahoo.com.br
Recebido: 21/07/2016 Aceito: 07/12/2017

was used in the Information Operations in the United States, United Kingdom, Germany and Russia, with the political-strategic vision and the cybernetic and Information Operations structures in Brazil. Thus, it has been verified that, although partially divergent, compared to Brazil, the countries present a common vision regarding the political-strategic proposal and the joint cybernetic structure, unlike Brazil's cybernetic information management model that does not have the joint organizational view. As a conclusion, the study suggests the integration by the Information Management innovation, with the unification of the cybernetic structure at the joint strategic and operational level of the Armed Forces, in order to increase the Interoperability of Information Operations .

Keywords: *Information operations. Cybernetic defense. Cybernetic warfare. Joint operations.*

RESUMEN

El objetivo de este estudio es verificar el papel de la innovación tecnológica y de la gestión conjunta del sector cibernético en la integración de las Operaciones de Información en Brasil. El advenimiento de las innovaciones tecnológicas modificó la visión de las fuerzas armadas mundiales con relación a la organización del sector cibernético y a la integración de las Operaciones de Información. En Brasil, las propuestas político-estratégicas del Ministerio de Defensa resultaron en iniciativas en el sector cibernético en las tres Fuerzas Armadas, afectando la gestión organizacional de las Operaciones de Información conjuntas. Se evidenció que las tres Fuerzas Armadas brasileñas han estructurado diferentes sistemas cibernéticos y de información, de forma divergente a la tendencia mundial en cuanto a la interoperabilidad en Operaciones Conjuntas. En el método, se utilizó la comparación de la visión político-estratégica organizacional y de las estructuras cibernéticas conjuntas en las Operaciones de Información de Estados Unidos, Reino Unido, Alemania y Rusia, con la visión político-estratégica y las estructuras cibernéticas y de Operaciones de Información de Brasil. Así, se verificó que, aunque parcialmente divergentes, los países comparados con Brasil presentan una visión común en cuanto a la propuesta político-estratégica y estructura cibernética conjunta, a diferencia del modelo de gestión de la información cibernética de Brasil que no posee la visión conjunta organizacional. Como conclusión, el estudio sugiere la integración por la innovación de la Gestión de la Información, con la unificación de la estructura cibernética al nivel estratégico y operacional conjunto de las Fuerzas Armadas, para aumentar la interoperabilidad de las Operaciones de Información.

Palabras clave: *Operaciones de información. Defensa cibernética. Guerra cibernética. Operaciones conjuntas.*

1 INTRODUÇÃO

A cultura organizacional, como a das Forças Armadas, é extremamente significativa considerando o seu funcionamento. As inovações não serão susceptíveis ao sucesso se a cultura organizacional em torno não for favorável (BRASIL, 2013).

O objetivo do estudo é verificar o papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação. O problema elencado para o presente estudo está no fato de que as três Forças Armadas brasileiras têm buscado inovar com diferentes sistemas cibernéticos e de informação, de forma divergente à tendência mundial quanto à interoperabilidade em Operações de Informação (Op Info) conjuntas. No método, foi utilizada a comparação da organização das Forças Armadas do Brasil com as Forças Armadas dos Estados Unidos, Reino Unido, Alemanha e Rússia, quanto à abordagem na capacidade de inovação no setor cibernético e nas Operações de Informação.

Considera-se pertinente a esse problema o fato de que a tomada da decisão no nível operacional do Comandante do Comando Conjunto depende da visão holística do cenário militar e civil, que, segundo Araujo (2013, p. 23), diante dos conflitos de Amplo Espectro, engloba o esforço conjunto das diferentes capacidades de informação e a demanda da inter-relação com as dessemelhantes agências militares e civis.

As Operações de Informação estão no campo de estudo das Ciências Militares que tratam de assuntos de Defesa e das expressões do Poder Nacional sob tutela da grande área do conhecimento de Ciência Política, com a concentração em Defesa Nacional (BRASIL, 2010). No Brasil, segundo o manual EB20-MC-10.213 (BRASIL, 2014c, p. 3-1), definem-se Operações de Informação pela

> Atuação metodologicamente integrada de capacidades relacionadas à informação (CRI), em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso.

As Capacidades Relacionadas à Informação apoiam-se nas estruturas físicas das especialidades militares já constantes nos quadros de material e pessoal das organizações militares da Marinha, Exército e Força Aérea, sendo elas "a Comunicação Social (Com Soc), as Operações Psicológicas (Op Psc), Guerra Eletrônica (GE), Guerra Cibernética e Inteligência" (BRASIL, 2014c, p. 3-1).

Sob tutela desse estudo estarão, ainda, os termos definidos para a capacidade cibernética pelo MD 35-G-01 (BRASIL, 2016), que contam com iniciativas inovadoras

das Forças Armadas, envolvendo considerações civis e militares, a fim de atender as expressões do Poder Nacional. Além disso, a ameaça cibernética coloca em risco a integridade de infraestruturas sensíveis, essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional. A proteção do espaço cibernético compreende a capacidade de atuação em rede e possui elementos intra e interorganizacionais (BRASIL 2012a, p. 71).

A seguir, será abordado o impacto da inovação tecnológica na gestão das Operações de Informação. Em seguida, serão apresentadas as opções para a gestão político-estratégica e as alternativas operacionais aos comandantes dos elementos das Força Armadas quanto às Operações de Informação, para então verificar-se a questão tecnológica ligada ao advento das Op Info e os efeitos da inovação na Guerra Cibernética. Por fim, será comparada a gestão da capacidade militar cibernética do Brasil com as iniciativas das Forças Armadas dos Estados Unidos, Reino Unido, Alemanha e Rússia, a fim de concluir-se sobre o impacto na integração das Operações de Informação.

2 A INOVAÇÃO TECNOLÓGICA E O IMPACTO NA GESTÃO DAS OPERAÇÕES DE INFORMAÇÃO

A Doutrina Militar, como um dos principais vetores do Processo de Transformação das Forças Armadas na Era do Conhecimento, busca a efetividade que se baseia na permanente atualização, em função da evolução da natureza dos conflitos, e da inovação, resultado das mudanças da sociedade e da evolução tecnológica aplicada aos assuntos de Defesa. A inovação tem papel importante, particularmente no interesse em estruturar as Operações de Informação, por agir na gestão, nas organizações e na tomada de decisão.

O Manual de Oslo, da Organização para a Cooperação e Desenvolvimento Económico (ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO, 1997), define quatro tipos de inovações que encerram um amplo conjunto de mudanças nas atividades das organizações: inovações de produto, inovações de processo, inovações organizacionais e inovações de marketing. Com relação à Inovação Organizacional esta é a implementação de um novo método organizacional nas práticas da organização e em suas relações externas. De acordo com a Fang (2005), a inovação pode ser dividida em duas categorias: inovações radicais e inovações incrementais, sendo que as radicais significam melhorias constantes que são adicionadas a determinados procedimentos, enquanto a incremental está relacionada a contínuas modificações para a melhoria desses processos. Segundo Fuck e Vilha (2012), as inovações tecnológicas incrementais podem ser entendidas como aperfeiçoamentos contínuos e graduais de produtos, serviços ou processos já existentes e correspondem à maior parte das inovações geradas. Já as inovações radicais correspondem à introdução de produtos, serviços ou processos totalmente novos no mercado e estão fortemente relacionadas às atividades de P&D.

Cromer, Dibrell e Craig (2011, p. 28) diz que, no sistema schumpeteriano, organizações empreendedoras incluem pessoas que são atribuídas à responsabilidade da introdução de novos processos. Martins e Tarblanche (2003) definem a inovação como a implementação de uma ideia nova, prática ou material para resolução de problemas. As inovações de processos são extremamente importantes para uma empresa porque apoiam as demais inovações de produtos e serviços (MÄNTYNEVA, 2012, p. 42-43; SOLATIE; MÄKELÄINEN, 2009, p. 35). As novas práticas aderem-se às inovações tecnológicas, tal como obtenção de conhecimento pela análise de dados com a inteligência tecnológica, a ser utilizada na análise dos sistemas de informação nas organizações (NEMUTANZHELA; IYAMU, 2011).

Segundo Rogers (2003), o processo de inovação voltada à decisão ocorre a partir da perspectiva da teoria da Difusão da Informação (DoI) que pode ser empregada na análise dos dados. O processo de inovação-decisão envolve cinco etapas: conhecimento, persuasão, decisão, implementação e confirmação, ou seja, o conhecimento ocorre quando os indivíduos, no caso deste estudo as Forças Armadas, estão conscientes da Inovação e conseguem a compreensão das suas funções. A persuasão ocorre quando os indivíduos ou unidades de tomada de decisões apresentam um comportamento favorável ou desfavorável para a inovação. A decisão indica quando o indivíduo ou unidade decide aprovar ou rejeitar a inovação. A implementação ocorre quando o indivíduo ou unidade decide usar a inovação. Por fim, a confirmação ocorre quando os tomadores de decisão, no caso das três forças singulares, confirmam a decisão de adotar a inovação.

Portanto pode-se inferir que a efetividade da gestão da informação pela inovação, como a implementação de uma ideia nova, prática ou material para resolução de problemas, baseia-se na permanente atualização de tomadores de decisão, em função do impacto da inovação tecnológica na gestão e na evolução da natureza dos conflitos. A tecnologia aplicada à gestão pode favorecer a análise dos dados dos assuntos de Defesa, contribuindo para a otimização das organizações e para a tomada de decisão, particularmente no interesse referente à estrutura do setor cibernético e das Operações de Informação.

3 AS OPERAÇÕES DE INFORMAÇÃO E SUA GESTÃO

A Dimensão Humana do ambiente operacional complexo remete os planejadores e decisores da estratégia militar à questão da legitimidade. Como salienta o EB20-MC-10.213 em relação à importância do tema para a solução dos conflitos

> As Operações de Informação (Op Info) envolvem o controle da narrativa (percepções) e a produção de reflexos no nível de aceitação das sociedades, quanto à necessidade da ação militar para a solução de conflitos. (BRASIL, 2014c, p.13).

Em uma visão mais ampla das três Forças, o conceito segundo o MD 35-G-01, as Operações de Informação são

> Ações coordenadas que concorrem para a consecução de objetivos políticos e militares. Executadas com o propósito de influenciar um oponente real ou potencial, diminuindo sua combatividade, coesão interna e externa e capacidade de tomada de decisão. Atuam sobre os campos cognitivo, informacional e físico da informação do oponente, e, também, sobre os processos e os sistemas nos quais elas trafegam, ao mesmo tempo em que procuram proteger forças amigas e os respectivos processos e sistemas de tomada de decisão. (BRASIL, 2016, p. 196).

A dimensão informacional do ambiente operacional é cada vez mais influenciada pela percepção estabelecida como válida nas mentes de um ou mais públicos-alvo – a narrativa dominante (senso comum) – que pode ser considerada um ponto decisivo nas operações militares contemporâneas e o terreno informacional, que passa a ser tão importante quanto o físico e o humano (BRASIL, 2014c, p. 2-3).

As Op Info fornecem opções estratégicas no nível político e nas alternativas operacionais aos comandantes dos elementos das Força Armadas de um Teatro de Operações/Área de Operações (TO/A Op). Contribuem, ainda, para a obtenção da Superioridade de Informações e para a Consciência Situacional. Porém a necessidade de integração conjunta entre as três Forças Armadas é colocada em condição, ou sob parâmetros, como regras, normas ou outros instrumentos de canalização do processo interno de cada visão especializada. As Op Info têm o foco na integração de ações ofensivas e defensivas, com ações tangíveis e intangíveis, em sintonia com outras Capacidades Relacionadas à Informação, coordenadas entre as várias Linhas de Operação e as Linhas de Esforço da Concepção Operacional.

Segundo Varvakis, Vital e Floriani (2010, p. 85), a gestão da informação requer o estabelecimento de processos, etapas ou fluxos sistematizados e estruturados, associado às pessoas responsáveis por sua condução, para que se obtenham os resultados almejados. McGee e Prusak (1994, p. 5) acrescentam que o valor da informação é determinado pelo usuário, o que implica a sua possível reutilização. Pode-se dizer, então, que a informação para ser útil depende da análise realizada pelo usuário conforme sua necessidade e circunstâncias de aplicabilidade. Perucchi e Ferreira (2010) afirmam que entre os maiores problemas enfrentados pelas organizações está a tarefa de saber lidar com a informação, visto que, se bem gerida, transforma-se em um ponto forte caracterizado como vantagem estratégica e competitiva. Para sistematizar-se a informação, deve-se seguir um modelo que atenda a realidade informacional do ambiente em que a informação esteja inserida, permitindo adequar-se aos objetivos finais das organizações (PERUCCHI; FERREIRA, 2010).

Em resumo, as opções para a gestão político-estratégica e as alternativas operacionais das Operações de Informação dependem de uma inovação de gestão com a visão conjunta das Forças Armadas. Requer o estabelecimento de processos, etapas ou fluxos sistematizados e estruturados, conforme sua necessidade e circunstâncias de aplicabilidade, para transformar-se em um ponto forte caracterizado como vantagem estratégica e competitiva para as Operações de Informação. Essa visão não pode ser divergente dentro das Forças Armadas, porque a integração é condição para as organizações. A gestão irá estabelecer regras, normas ou outros instrumentos de canalização, dependendo do processo interno de visão de cada Força Armada.

4 QUESTÃO TECNOLÓGICA LIGADA AO ADVENTO DAS OP INFO - EFEITOS DA INOVAÇÃO NA GUERRA CIBERNÉTICA

Segundo Bellais (2013), potências emergentes como China, Índia e Brasil precisam fortalecer sua estrutura de Defesa e estão envidando esforços para dedicar uma parte de seus orçamentos de defesa para P & D. A velocidade da inovação exige uma tendência da persistência de uma estrutura de Defesa centrada na tecnologia, principalmente quando se busca desenvolver o setor cibernético. Nesse sentido, a Tecnologia pode ser considerada como o condutor e indutor, *spill over*, da transformação das capacidades militares.

Saunders et al. (1995) acrescentam que se torna imperativo evitar surpresas tecnológicas, pois estas podem ameaçar ou pôr em risco a segurança nacional. Cowan e Foray (1995, p. 865) também contribuem dizendo que o investimento em P & D ajudam a manter

a tecnologia em nível exploratório, pois pode continuar com testes e experimentos de suas técnicas, processos e produtos por muito mais tempo depois de um mercado ter concebido uma tecnologia.

Nesse cenário, McKenzie (2001) identifica seis potenciais ameaças assimétricas: operações nucleares, químicos, biológicos, informações, conceitos operacionais e terrorismo. Em vista disso, a superioridade tecnológica continua a ser o núcleo de contratos de defesa e gerir a incerteza pode ser possível por meio da tecnologia. Donald Rumsfeld, então secretário de Defesa dos EUA, ressaltou, "nosso desafio neste novo século é difícil: para defender a nossa nação contra o desconhecido, o incerto, o invisível, e o inesperado" (RUMSFELD, 2002, p. 23).

Mesmo assim, em tempo de Paz, é um momento difícil para aquisições de armas, em virtude de ameaças assimétricas e a falta de um inimigo claramente identificável. Os planejadores e decisores da defesa não têm a dimensão do tipo de riscos que têm de evitar ou combater. Portanto os princípios de aquisição de defesa atual se tornam obsoletos quando vistos de forma singular, pois não visam elaborar uma lista de ameaças assimétricas e complexas. Serfati (1995) alerta que existe uma tendência em P & D de Defesa de concentrar o esforço em inovações incrementais, agregando tecnologia de forma contínua, que são, por definição, muito mais difíceis de alcançar de forma singular, pois tornam-se cada vez um investimento mais caro. A Tabela 1 demonstra o investimento anual em alguns dos países que estão à frente no investimento e na qualificação de pessoal em Guerra Cibernética.

Tabela 1 - Investimento anual na estrutura cibernética das Forças Armadas.

País	Financiamento anual em milhões de dólares	Número de tropas cibernéticas
Estados Unidos	7000	9000
Reino Unido	450	2000
Rússia	300	1000
Alemanha	250	1000

Fonte: Litovkin (2017).

Portanto, se o investimento de um país em uma determinada tecnologia é limitado e não pode manter o ritmo para o estado da arte, necessita-se de inovação direcionada aos fins do setor cibernético. Além disso, o esforço deve ser conjunto, uma vez que todos os elementos das Forças Armadas são responsáveis pela segurança nacional.

5 AS OPERAÇÕES DE INFORMAÇÃO NOS ESTADOS UNIDOS E A CAPACIDADE CIBERNÉTICA

5.1 Visão Político-Estratégica

As Operações Cibernéticas (*Cyberspace Operations*) nas Forças Armadas dos Estados Unidos da América (EUA) compreendem o domínio global do ambiente de informações, considerando a interdependência dos dados, seja na internet, redes de comunicações, sistemas computacionais, processadores e controladores. Essa capacidade está focada em ações ofensivas e defensivas, sendo integradas em múltiplas linhas de esforço para afetar adversários e potenciais tomadores de decisão (UNITED STATES, 2014, p. II-9).

Em relação às Operações de Informação, conforme o JP 3-13-1 (UNITED STATES, 2014, p. IX), os instrumentos do poder nacional (diplomático, informacional, militar e econômico) fornecem aos líderes dos EUA os meios para lidar com crises ao redor do mundo. Empregar esses meios no ambiente de informações requer a capacidade de transmitir com segurança, receber, armazenar e processar informações em tempo quase real.

O FM 3-0 (UNITED STATES, 2008, p. 12) salienta a importância da colaboração e do diálogo, da informação, entre os comandantes militares e as lideranças civis, considerando ser esse o enlace fundamental para o desenvolvimento da confiança mútua e de entendimento, de forma a estruturar organizações capazes de agir rapidamente às ameaças complexas.

Recentemente o governo dos EUA instituiu uma nova perspectiva de Estratégia de Segurança Nacional com a visão de que é necessária a integração entre todos os órgãos do governo: *whole of government approach*. Nessa mesma linha, segundo Perkis (2014), General e Comandante do U.S. *Army Training and Doctrine Command* (TRADOC), a doutrina Norte-americana busca adaptar-se a nova filosofia do emprego militar para **vencer em mundo complexo**.

5.2 Integração

Os Estados Unidos possuem um Centro Conjunto de Guerra de Operações de Informação (*Joint Information Operations Warfare Center* – JIOWC), que é responsável desde o tempo de paz em coordenar o desenvolvimento tecnológico e ações estruturais conjuntas das capacidades relacionadas à informação, incluindo o setor cibernético. Sob a direção do *United States Strategic Command* (USSTRATCOM), os

United States Cyber Command (USCYBERCOM), são responsáveis pela sincronização e coordenação das operações transregionais, bem como em coordenação com os comandos combatentes, *Joint Staff* (JS) e *Office of Secretary of Defense* (OSD) ligam-se com os demais departamentos (ministérios), agências e membros da base industrial de defesa dos *United States Government* (USG), tudo em conjunto com o *Department of Homeland Security* (DHS) (UNITED STATES, 2013, p. IX).

Cada força singular pode estabelecer um sistema de integração das Operações de Informação. O Exército dos Estados Unidos possui o 1º Comando de Operações de Informação (*1st Information Operations Command*), elemento de apoio a distância que fornece suporte ao planejamento operações de informação, operações do ciberespaço e análise de inteligência. Mas todas as iniciativas são integradas pelo USCYBERCOM, que é um comando combatente unificado, coordenando, integrando, sincronizando e conduzindo as atividades para proteger as redes de informação do DoD (UNITED STATES, 2017).

6 OPERAÇÕES DE INFORMAÇÃO NA ALEMANHA E A CAPACIDADE CIBERNÉTICA

6.1 Visão Político-Estratégica

A Guerra Cibernética (*Cyber-Krieg*) nas Forças Armadas da Alemanha realiza, por meio de medidas de segurança de TI, medidas eletrônicas para a proteção de procedimentos humanos, materiais e de segurança organizacional, bem como outras medidas técnicas e não técnicas para proteger seus próprios sistemas de informação. Isso garantirá a liberdade operacional, apoiando a preservação da superioridade de informação e, assim, contribuindo para a liderança e superioridade de ação.

Em relação às Operações de Informação, todo ato ou omissão pode ser percebido como informação. A informação conjunta é a base para o processo de gestão em todos os níveis. O trabalho no ambiente de informação é orientado sobre a dimensão puramente militar, mas para além do estado final desejado (estado final político), por isso tem importância ministerial conjunta (SCHINDLER, 2015). A superioridade da informação é buscada com ações para a recuperação, controle, processamento, transmissão e segurança das informações. As Operações de Informação na Alemanha envolvem, particularmente, as seguintes capacidades: informações públicas, comunicações operacionais, guerra eletrônica, guerra cibernética e operações psicológicas.

6.2 Integração

A coordenação das atividades é um fator essencial em virtude da natureza do ambiente de informação e dos objetivos político-estratégicos. A ação conjunta das Forças Armadas permite enfraquecer ou evitar os efeitos da ação inimiga na informação e nos sistemas de informação, protegendo também os setores civis interconectados.

O objetivo da coordenação das atividades no ambiente de informação é controlar a difusão do conteúdo, no tempo e espaço, bem como coordenar as atividades de informação, sincronizando-as, de forma que um efeito global seja alcançado. A atuação no ambiente de informação só poderá ser bem-sucedida se o próprio comando operacional conjunto puder agir no controle do movimento das tropas, de forma a verificar se os efeitos pretendidos estão de acordo com as ações cinéticas. Se forem diferentes, a credibilidade da campanha será posta em dúvida e os efeitos pretendidos não serão alcançados.

A Alemanha está estabelecendo um comando cibernético de informações por meio da fusão de unidades cibernéticas da Forças Armadas (*Bundeswehr*). O Comando Cibernético e da Informação (*Kommando Cyber-und Informationsraum*) será o responsável por integrar os setores cibernéticos, a tecnologia da informação, a inteligência militar, a geoinformação e a comunicação operativa (IHS 360, 2016).

7 OPERAÇÕES DE INFORMAÇÃO NO REINO UNIDO E A CAPACIDADE CIBERNÉTICA

7.1 Visão Político-Estratégica

As Operações Cibernéticas (*Computer Network Operations* - CNO) nas Forças Armadas do Reino Unido podem executar ataques de redes, exploração de redes e defesa de redes, sendo um importante vetor de controle, disseminação ou negação de informação, JWP 3-80 (UNITED KINGDOM, 2002).

Em relação às Operações de Informação, o impacto da mídia internacional e o impacto da tecnologia são aspectos vitais para as operações. Segundo o JWP 3-80 (UNITED KINGDOM, 2002, p. 1.1), a campanha de informação é uma atividade transversal na esfera das demais expressões do poder não se restringindo ao campo militar. Dessa forma, pode ainda envolver ações junto à esfera econômica, agências humanitárias e organizações internacionais.

O Ministério da Defesa (*Ministry of Defence* - MOD) é responsável em emitir as diretrizes para todos os níveis das Operações de Informações e das Operações de Mídia, permitindo a sincronização das ações. Em 2016,

o MOD emitiu a Estratégia Nacional de Segurança Cibernética 2016 – 2021, com o objetivo de defender o Reino Unido contra a evolução das ameaças cibernéticas, dissuadir qualquer forma de agressão no ciberespaço, desenvolver a indústria de segurança cibernética de forma inovadora e em constante expansão, e, ainda, estimular a participação do Reino Unido em ações internacionais (UNITED KINGDOM, 2017a).

7.2 Integração

A coordenação da Campanha de Informação é executada no mais alto nível, o nível político, em um gabinete interministerial. O Ministério da Defesa é representado nesse grupo pelo Diretor de Operações de Informação (*Directorate of Targeting and Information Operation - DTIO),* sendo que as operações militares do MOD são orientadas pela diretriz do Chefe de Estado-Maior (*Chief o Defense Staff - CDS*) (UNITED KINGDOM, 2002, p. 1-3).

O Reino Unido possui o *Joint Forces Command* (JFC), que fornece a base e o quadro de apoio para operações serem bem-sucedidas, garantindo recursos conjuntos que são desenvolvidos e gerenciados, centralizando o treinamento, a inteligência, os sistemas de informação e operações cibernéticas (UNITED KINGDOM, 2017).

Na estrutura de Operações de Informação conjunta, o *Joint Information Activities Group* (JIAG), estabelecido em 2013, deve prover especialistas em informação para os demais órgãos. O JIAG tem como principais unidades o *Defence Media Operations Centre* (DMOC) e o *Joint Information Operations Training and Advisory Team* (JIOTAT) (UNITED KINGDOM, 2016). A estrutura cibernética, o *Defence Cyber Operations Group* (DCOG), é subordinada diretamente ao Comando Conjunto das Forças Armadas e conta com uma Unidade Cibernética Conjunta (GREEN, 2015, p. 26).

O JWP 3-80 (UNITED KINGDOM, 2002, p. 3.1) explica que a estrutura dos componentes físicos e humanos de Operações de Informação deve focar na capacidade de comandar e influenciar toda infraestrutura cibernética, bem como na capacidade de processar e controlar os meios de comunicação e inteligência (*Command, Control, Communications, Computers and Intelligence - C4I).*

8 OPERAÇÕES DE INFORMAÇÃO NA RÚSSIA E A CAPACIDADE CIBERNÉTICA

8.1 Visão Político-Estratégica

As Operações Cibernéticas (Кибер-Война) são conduzidas de forma conjunta pelas tropas de guerra cibernética essencial para atingir os objetivos militares e políticos russos. No nível tático, a doutrina não concebe que as ações cibernéticas atuem isoladamente, pois fazem parte de um complexo de influências (GILES, 2011, p. 46).

De acordo com Giles (2012, p. 46), em relação às Operações de Informação, a visão russa de Guerra da Informação (*informatsionnoye protivoborstvo, informatsionnaya bor'ba*, ou o nome que está se difundindo, informatsionnaya voyna) é mais um conceito holístico que uma tradução literal que compreende Operações Cibernéticas, Guerra Eletrônica, Operações Psicológicas e Comunicação Estratégica. Ainda, existem divergentes percepções conceituais e doutrinárias da Rússia em relação a como os países ocidentais vinham interpretando as Operações de Informação, o que dificultava a padronização de procedimentos no campo informacional. Como observa Giles (2012, p. 64), "a chave da divergência entre Rússia e o Ocidente para uma aproximação na área da segurança cibernética é a percepção do conceito de ameaça**".**

Outra questão é a soberania da internet. O sistema russo requer um controle governamental sobre o que entra no espectro cibernético, considerando-se as fronteiras físicas do país. Segundo este sistema, "cada estado membro pode estabelecer suas normas para preservar a soberania e a gestão do espaço informacional de acordo com suas leis nacionais" (GILES, 2012, p. 65). Essa doutrina de Operação de Informação está exposta na *Information Security Doctrine of the Russian Federation* (RUSSIA, 2000) e pode ser definida como

> Um conflito, entre dois ou mais estados no espaço de informação, com o objetivo de causar danos aos sistemas de informação, processos e recursos críticos e outras estruturas, subvertendo os sistemas políticos, econômicos e sociais, bem como à massa psicológica, influenciando a população para desestabilizar a sociedade e o estado, bem como coagindo o governo do lado oposto a tomar decisões a nós favoráveis (GILES, 2012, p. 68, tradução nossa).

8.2 Integração

A importância do controle cibernético para a integração das capacidades relacionadas à informação tornou-se evidente pela falta de controle sobre o espectro informacional. Essa percepção pode ser entendida nas palavras de Mshvidobadze (2011, p.3, tradução nossa)

> A Rússia vê ciber-capacidades como instrumentos de guerra de informação, que combina inteligência, contrainteligência, desinformação, guerra eletrônica, debilitação das comunicações, a degradação do suporte de navegação, pressão psicológica, e destruição das capacidades cibernéticas inimigas.

Com o propósito de unificar o esforço e dar resposta ao amplo espectro das informações, a Rússia criou o *Information Troops*. Tais elementos fazem parte de uma complexa estrutura composta de

> diplomatas, especialistas, jornalistas, escritores, publicitários, tradutores, operadores, pessoal de comunicação, web designers, hackers e outros ... Para construir as contramedidas de informação, é necessário desenvolver um centro para a determinação de criticamente importantes entidades de informação do inimigo, incluindo a forma de eliminá-los fisicamente, e como conduzir a guerra eletrônica, guerra psicológica, contrapropaganda sistêmica e o treinamento de hackers. (GILES, 2011, p. 52).

Ainda, com o objetivo de estender o controle para além das fronteiras, a Rússia estabeleceu acordos de integração de informações militares com países do *Collective Security Treaty Organisation* (CSTO), do *Commonwealth of Independent States* (CIS) e da *Shanghai Cooperation Organisation* (SCO) (RUSSIA, 2012).

9 A ESTRUTURA ORGANIZACIONAL DAS OPERAÇÕES DE INFORMAÇÃO E DO SETOR CIBERNÉTICO NAS FORÇAS ARMADAS DO BRASIL

No ambiente estratégico, o Estado-Maior Conjunto das Forças Armadas (EMCFA) é o principal responsável pelo planejamento das Operações de Informações, de acordo com as diretrizes estabelecidas pela Estratégia Nacional de Defesa (END) (BRASIL, 2014a, p.56). Segundo o manual de Doutrina de Operações Conjuntas, MD 30-M-01 (BRASIL, 2011, p. 55), as ações no espaço cibernético deverão ter as seguintes denominações, de acordo com o nível de planejamento: o Estado-Maior Conjunto da Forças Armadas é o responsável por estabelecer o Plano Estratégico de Operações de Informação (PEOI) – a cargo da Subchefia de Operações (SC3), consolidando aspectos da Comunicação Social, Operações Psicológicas, Guerra Eletrônica e Defesa Cibernética, do ponto de vista estratégico do MD 30-M-01 (BRASIL, 2011, p. 23).

Como o Estado-Maior Conjunto das Forças Armadas deixou de estabelecer uma sistemática de planejamento único, a gestão do desempenho no setor de Operações de Informação e cibernética ficou prejudicada. Como exemplo, tal como no manual de Doutrina de Operações Conjuntas (BRASIL, 2011), o encargo das atividades cibernéticas é parcialmente dividido com o oficial de Comando e Controle, cabendo aos oficiais especialistas efetuar a ligação com o oficial de Operações de Informação do Estado-Maior Conjunto. Essa estrutura gera duplicação de esforços, bem como redundância de responsabilidades.

Na estruturação física das três Forças Armadas, o MD estabeleceu a diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional, com o desafio de integrar as iniciativas cibernéticas, organizar e executar os projetos de defesa cibernética. A primeira iniciativa ocorreu quando a Diretriz Ministerial nº 014/2009 atribuiu ao Exército Brasileiro a responsabilidade pela coordenação e integração do setor cibernético do MD (CARVALHO, 2011, p. 11). Posteriormente, por intermédio da Portaria nº 3.405/MD, de 21 de dezembro de 2012, o MD atribuiu ao Centro de Defesa Cibernética (CDCiber), do Comando do Exército, a responsabilidade pela coordenação e integração das atividades de Defesa Cibernética, no âmbito do Ministério da Defesa (CAMELO; CARNEIRO, 2013, p. 1).

Por conseguinte, o Exército Brasileiro estabeleceu o Centro de Defesa Cibernética do Exército (CD Ciber) e ativou dois núcleos de Defesa Cibernética em 2016, o Núcleo do Comando de Defesa Cibernética (NuComDCiber) e o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), este último passando a contar com militares das três Forças Armadas, trabalhando no mesmo ambiente físico (DEFESANET, 2015a).

A Marinha do Brasil inova no setor, estabelecendo o Centro de Guerra Eletrônica da Marinha (CGEM), com projetos de desenvolvimento da Marinha do Brasil, como o programa Brigada Anfíbia (DEFESANET, 2015b). A Marinha está estruturando, ainda, a Política Cibernética de Defesa (PCD), que deve funcionar como subsistema da atividade de Comando e Controle (C^2), com as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos (BRASIL, 2012c).

A atividade de Comando e Controle aborda três diferentes sistemas, o Sistema Naval de Comando e Controle (SISNC2), o Sistema de Informações sobre o Tráfego Marítimo (SISTRAM), que tem como propósito o acompanhamento e monitoramento de embarcações, nacionais e estrangeiras, que navegam na área de busca e salvamento (*Search And Rescue* – SAR) brasileira, e o Sistema de Gerenciamento da Amazônia Azul (SisGAAz), um sistema de C^2 para monitoração, controle e proteção das águas adjacentes ao litoral brasileiro que compõem a Amazônia Azul (MANSO, 2013, p. 67).

A Força Aérea Brasileira inova em Operações de Informação, estabelecendo o Sistema Aéreo de Guerra Eletrônica, sendo que a Defesa Cibernética (Def Ciber) é de responsabilidade da Seção de Comando e Controle

da Subchefia de Operações (DEFESANET, 2015b). Entretanto, além da Def Ciber, essa Seção também é responsável pelos assuntos de Comando e Controle, Tecnologia da Informação (TI), Guerra Eletrônica, Controle do Espaço Aéreo, Sensoriamento Remoto e Sistemas Espaciais (VEIGA, 2016, p. 5).

Segundo a Doutrina Básica da FAB, a Def Ciber consiste em empregar Meios de Força Aérea para proteger os Sistema de Comunicações e Tecnologia da Informação para Comando e Controle (SCTIC2), para obter dados para a produção de conhecimento de Inteligência e para causar prejuízos aos sistemas similares do oponente (VEIGA, 2016, p. 7).

Do exposto, verifica-se que as três Forças Armadas estabeleceram diferentes iniciativas gerenciais para o setor cibernético e de Operações de Informação.

10 COMPARAÇÃO COM AS PROPOSTAS ESTRATÉGICAS CIBERNÉTICAS E DAS OPERAÇÕES DE INFORMAÇÃO ENTRE AS FORÇAS ARMADAS ESTRANGEIRAS E DO BRASIL

10.1 Quanto à visão político-estratégica

No Brasil, a END é um documento que firma o compromisso constitucional de garantir a obtenção e manutenção dos objetivos nacionais permanentes estabelecidos pela Política Nacional de Defesa. Semelhante ao observado nas iniciativas do nível político-estratégico dos Estados Unidos, Alemanha, Rússia e Reino Unido, a END (BRASIL, 2012b) estabeleceu um vínculo entre o conceito e a política de independência nacional no setor cibernético e de Operações de Informação.

10.2 Quanto às iniciativas nas Operações de Informação

Em que pese as diversas iniciativas de modernização tecnológica, tal como os macroprojetos estratégicos que, a curto, médio e longo prazos, possibilitarão ampliar o domínio da informação, verifica-se que diferentemente dos países estrangeiros comparados com o Brasil, as capacidades relacionadas à informação nas Operações de Informação do Estado-Maior Conjunto, sob comando do MD, ainda encontram dificuldades para estar efetivamente integradas.

10.3 Quanto à inovação de estruturas cibernéticas

O investimento em Defesa passou a desenvolver-se, lastreado na capacidade de monitorar e(ou) controlar o território nacional e seu entorno estratégico, com grande papel destinado às capacidades de informação. Pelo advento tecnológico, a linha de desenvolvimento das capacidades operacionais tem buscado fortalecer os três setores de importância estratégica: o espacial, o cibernético e o nuclear.

Diferentemente dos Estados Unidos, Alemanha, Rússia e Reino Unido, a estruturação de diversificadas iniciativas inovadoras por parte das Forças Armadas brasileiras não deixou a estrutura física sob comado de uma única estrutura capaz de ações de planejamento de Defesa Cibernética e Guerra Cibernética, nem mesmo de Operações de Informação.

10.4 Quanto à gestão da Informação

Quando o Estado-Maior Conjunto das Forças Armadas (EMCFA) do Brasil deixou de estabelecer uma sistemática de planejamento único, a gestão do desempenho no setor de Operações de Informação e cibernética ficou prejudicada. Diferentemente, como verificado nas Forças Armadas que serviram de comparação, tais atividades mencionadas estão diretamente ligadas ao escopo de atividades sob coordenação geral do oficial de Operações de Informação. Se ocorrer a reprodução dessas estruturas para os escalões menores, ficará ainda mais difícil coordenar ou sincronizar as ações de Operações de Informação com as atividades de Operações.

10.5 Quanto à interoperabilidade

Segundo o Glossário das Forças Armadas, o Amplo Espectro das operações engloba o esforço conjunto das diferentes capacidades de informação e a demanda da inter-relação com as dessemelhantes agências militares e civis (BRASIL, 2016). Como observado nas Forças Armadas comparadas com o Brasil, as iniciativas inovadoras daqueles países estão estruturando o setor cibernético de forma a estar ligado à mais alta esfera dos interesses políticos nacionais, pois exige a integração com os demais sistemas das organizações do setor civil.

Do exposto, verifica-se que a comparação das iniciativas inovadoras das gestões das Forças Armadas dos Estados Unidos, Alemanha, Reino Unido e Rússia no setor cibernético e Operações de Informação, são divergentes do esforço de inovação da gestão das Forças Armadas do Brasil. Portanto conclui-se que existe grande dessemelhança pela singularidade e complexidade das iniciativas voltadas às estruturas internas de cada força em sua gestão organizacional, o que dificulta a integração das operações de Informação do Estado-Maior Conjunto das Forças Armadas.

11 CONCLUSÃO

O objetivo do estudo foi verificar o papel da inovação tecnológica e da gestão conjunta do setor cibernético na integração das Operações de Informação. A comparação da organização das Forças Armadas do Brasil com as forças armadas Estados Unidos, Reino Unido, Alemanha e Rússia pode evidenciar a divergência de abordagem na capacidade de inovação no setor cibernético e nas Operações de Informação.

Em síntese, em que pese o parcial alinhamento do Brasil com a tendência internacional, o MD precisa ainda ajustar as estruturas singulares à proposta de transformação das Forças Armadas. O setor cibernético é um setor que requer constante investimento em inovação e tecnologia, de forma que o esforço conjunto é mais indicado para adequar as pretensões brasileiras à dificuldade orçamentária tradicional na área de Defesa.

Foi evidenciado, ainda, que o sucesso da gestão da informação pressupõe a carência de uma percepção única, com iniciativas de enlaces convergentes, que permita integrar os vetores de informações dentro dos componentes das Forças Armadas e, com base nesse nível, replicada verticalmente para as operações dos escalões mais baixos e horizontalmente refletir para os demais órgãos civis do Poder Nacional.

Além disso, mesmo que a expressão militar tenha forte influência das inovações tecnológicas, não é, por si só, capaz de restaurar ou manter a segurança das informações. Sugere-se que o esforço envolva a gestão do poder militar das três Forças (Marinha, Exército e Aeronáutica) com os demais componentes civis do Poder Nacional (político, econômico, psicossocial e científico-tecnológico), para permitir a eficiência conjunta no setor cibernético e nas Operações de Informação do Estado-Maior Conjunto das Forças Armadas.

REFERÊNCIAS

ARAUJO, M. L. A. Operações no amplo espectro: novo paradigma do espaço de batalha. In: **Doutrina Militar Terrestre em Revista**, Brasília, jan-mar. 2013.

BELLAIS, R. Technology and the defense industry: real threats, bad habits, or new (market) opportunities? **Journal of Innovation Economics & Management**, France: De Boeck Supérieur, v. 2, n.12, 2013. p. 59 –78.

BRASIL. Escola Superior de Guerra. **Manual Básico**, rev. e atual. Rio de Janeiro, 2014a 4 v.

_____. Ministério da Defesa. **Debates sobre Guerra Eletrônica e Defesa Cibernética na LAAD**. Brasília, 2015b. Disponível em: <http://www.defesanet.com.br/laad2015/noticia/18889/Debates-sobre-Guerra-Eletronica-e-Defesa-Cibernetica-na-LAAD/>. Acesso em: 05 jun. 2016.

_____. Ministério da Defesa. Decreto n. 7.276, de 25 de agosto de 2010. Aprova a Estrutura Militar de Defesa e dá outras providências.). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 2010. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7276.htm>. Acesso em: 6 jun. 2016.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Portaria nº 9/GAP/MD, de 13 de janeiro de 2016. Aprova das Forças Armadas (MD35-G-01). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, n.14, 21 jan. 2016.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Portaria nº 3010/MD, de 18 de novembro de 2014b. Aprova Doutrina Militar de Defesa Cibernética (MD31-M-07). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, n. 224, 19 nov. 2014.

_____. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. Portaria nº 3810/MD, de 8 de dezembro de 2011. Aprova Doutrina de Operações Conjuntas (MD30-M-01). **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, n. 236, 09 dez. 2011.

_____. Ministério da Defesa. Estado-Maior do Exército. Portaria nº 8/EME, de 29 de janeiro de 2014. Aprova o Manual de Campanha (EB20-MC-10.2013) Operações de Informações 2014. **Boletim do Exército**, Brasília, DF, n.05, 31 jan. 2014c.

_____. Ministério da Defesa. Estado-Maior do Exército. Portaria nº 004/EME, de 09 de janeiro de 2014. Aprova o Manual de Fundamentos (EB70-MF-10.103) Operações 2014. **Boletim do Exército**, Brasília, DF, n.05, 31 jan. 2014c.

_____. Ministério da Defesa. Exército Brasileiro. **Bases para a transformação da Doutrina Militar Terrestre**. Brasília, DF, 2013. Disponível em: <http://www.cdoutex.eb.mil.br>. Acesso em: 5 jun. 2016.

_____. Ministério da Defesa. Exército Brasileiro. **Defesa Cibernética entra em nova fase**. Brasília, 2015a. Disponível em: <http://www.defesanet.com.br/cyberwar/noticia/19849/EB---Defesa-Cibernetica-entra-em-nova-fase/>. Acesso em: 01 jun. 2016.

_____. Ministério da Defesa. **Livro Branco da Defesa**. Brasília: [S.n.], 2012a.

_____. Ministério da Defesa. **Política Nacional de Defesa (PND)**: Estratégia Nacional de Defesa (END). Brasília: [S.n.], 2012b.

_____. Ministério da Defesa. Portaria Normativa nº 2.777/MD de 27 de outubro de 2014e. Aprova Diretriz de implantação de medidas visando à potencialização da Defesa Cibernética Nacional. **Diário Oficial [da] República Federativa do Brasil** Brasília, DF, n. 208, 28 out. 2014.

_____. Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Aprova a Política Cibernética de Defesa (PCD) - MD31-P-02. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, n.249, 27 dez. 2012c.

CAMELO, J. R. S.; CARNEIRO J. M. E. **A atuação do Centro de Defesa Cibernética na Copa das Confederações Fifa/2013**. Brasília: [S.n.], 2013.

CARVALHO, P. S. M. O setor cibernético nas Forças Armadas Brasileiras. **Desafios estratégicos para a segurança e defesa cibernética** 1. ed. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

COWAN, R.; FORAY, D. Quandaries in the economics of dual technologies and spillovers from military to civilian research and development. **Research Policy**, n. 24, 1995. p. 851-868.

CROMER, C. T.; DIBRELL, C.; CRAIG, J. B. A Study of Schumpterian (Radical) vs. Kirznerian (Incremental) Innovations in Knowledge Intensive Industries. **Journal of Strategic Innovation and Sustainability** vol. 7, n.1, 2011 p. 28-42.

FANG, Z. Exploring the synergy between entrepreneurship and innovation. **International Journal of Entrepreneurial Behaviour & Research**, v. 11, n.1, 2005, p. 25-41. Disponível em: <www.emeraldinsight.com/1355-2554.htm> Acesso em: 20 ago. 2010.

FUCK, M. P.; VILHA, A. M. Inovação Tecnológica: da definição à ação. **Revista Contemporâneos**, São Paulo, n. 9, p. 1-21, nov. 2011 – abr. 2012.

GILES, K. Information Troops: a Russian Cyber Command? In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, n.3, 2011. **Proceedings of**…. Estonia, 2011, p. 45-60.

_____. Russia's Public Stance on Cyberspace Issues. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT, n.4, 2012. **Proceedings of**… Oxford, 2012, p. 63-75.

GREEN, J. A. **Cyber Warefare**: a multidisciplinary analysis. London: Routledge, 2015. 196 p.

IHS 360: Germany outlines plan to create Bundeswehr cyber command. Disponível em: <http://www.janes.com/article/59861/germany-outlines-plan-to-create-bundeswehr-cyber-command>. Acesso em: 22 jun. 2016.

LITOVKIN, Nikolai. Russia's cyber army hacks a spot in the Top 5. **RBTH Science & Tech**. Jan, 2017 Disponível em: <https://www.rbth.com/defence/2017/01/12/russias-cyber-army-hacks-a-spot-in-the-top-5_679221> Acesso em: 12 nov. 2017.

MANSO, R. C. **Sistemas cibernéticos na MB**: desafios e perspectivas. Rio de Janeiro: Escola de Guerra Naval, 2013.

MÄNTYNEVA, M. **Kasvua innovaatioista**. Helsinki: Kauppakamari, 2012.

MARTINS, E.; TERBLANCHE, F. Building organizational culture that stimulates creativity and innovation, **European Journal of Innovation Management**, n.6, v.1, p. 64-75, 2003.

McGEE, J.; PRUSAK, L. Informação e Concorrência. In: _____. **Gerenciamento Estratégico da Informação**: aumente a competitividade e a eficiência de sua empresa utilizando a informação como uma ferramenta estratégica, 9. ed., Rio de Janeiro: Campus, 1994. p. 3-170.

McKENZIE, K. The rise of asymmetric threats: priorities for defense planning. In: FLOURNOY, M. (ed.). **QDR 2001 Strategic-driven Choices for America Security**. Washington: National Defense University Press, 2001. p. 75-105.

MSHVIDOBADZE, K. **The Battlefield On Your Laptop**. 2011. Disponível em: <http://www.rferl.org/articleprintview/2345202.html>. Acesso em: 11 out. 17.

NEMUTANZHELA, P.; IYAMU, T. A Framework for enhancing the information systems innovation: using competitive inteligente. **The Electronic Jour Rogers**, New York: Free Press, 2011.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÓMICO. **Manual de Oslo**: diretrizes para coleta e interpretação de dados sobre inovação. 3 ed. Rio de Janeiro, 1997.

PERKINS, D. G. Army operating concept: delivering the future. **US Army Training and Doctrine Command, Army Magazine**, United States, v. 64, n. 10, p. 65, out. 2014.

PERUCCHI, V.; FERREIRA, T. L. R. **Gestão e o fluxo da informação nas organizações**: um ensaio a partir da percepção de autores contemporâneos. João Pessoa: IESP, 2010.

ROGERS, E. M. **Diffusion of innovations**. 5 e.d. New York: Free Press, 2003.

RUMSFELD, D. Transforming the militar. **Foreign Affairs**, v.3, n.81, p. 20-32, 2002.

RUSSIA. **Collective Security Treaty Organisation**, 2012. Disponível em: <http://www.odkb. gov.ru/start/index_aengl.htm> Acesso em: 21 abr. 2016.

_____**. Security Council of the Russian Federation**: Information Security Doctrine of the Russian Federation. 2000. Disponível em: <http://www.scrf.gov.ru/documents/6/5.html>. Acesso em: 22 abr. 2016.

SAUNDERS, K. et al. **Priority-setting and strategic sourcing, in the naval research,dev elopment, and technology infrastructure**. Santa Monica: RAND, 1995.

SCHINDLER, F. **As Operações de Informação na Alemanha**. Rio de Janeiro: ECE5ME, 2015.

SERFATI, C. **Production d'armes, croissance et innovation**. Paris: Economica, 1995.

SOLATIE, J.; MÄKELÄINEN, M. **Ideasta innovaatioksi**: Luovuus hyö-tykäyttöön. Helsinki: Talentum Media Oy, 2009.

UNITED KINGDOM. Her Majesty's Government. **National Cyber Security Strategy 2016-2021**. Disponível em: <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf>. Acesso em: 9 nov. 2017.

_____. **Joint Forces Command**. Disponível em: <https://www.gov.uk/government/organisations/joint-forces-command>. Acesso em: 11 nov. 2017a.

_____. Ministry of Defense. **JWP 3-80 Joint Warfare Publication**: Information Operations. United Kingdom, 2002.

_____. Ministry of Defense. **Military recruitment, training and operations**. Disponível em: <https://www.gov.uk/guidance/the-defence-media-operations-centre-dmoc> Acesso em: 20 jun. 2016.

UNITED STATES. US Joint Chief of Staff. Department of the Army. **FM 3-0**: Operations. Washington, DC: [S.n.], 2008.

_____. US Joint Chief of Staff. Department of Defense. **DoD Initiates Process to Elevate U.S: Cyber Command to Unified Combatant Command**. 2017. Disponível em: <https://www.defense.gov/News/Article/Article/1283326/dod-initiates-process-to-elevate-us-cyber-command-to-unified-combatant-command/> Acesso em: 11 nov. 2017.

_____. US Joint Chief of Staff. Department of Defense. **JP 3-12**: Cyberspace Operations. Washington, DC: [S.n.], 2013.

_____. US Joint Chief of Staff. Department of Defense. **JP 3-13-1**: Information Operations.. Washington, DC: [S.n.], 2014.

VARVAKIS, G.; VITAL, L. P.; FLORIANI, V. M. **Gerenciamento do fluxo de informação como suporte ao processo de tomada de decisão**. Londrina: [S.n] , jun./jul. 2010.

VEIGA, R. Q. A defesa cibernética (Def Ciber) na visão da força aérea brasileira (FAB). **Coleção Meira Mattos**: Revista das Ciências Militares, Rio de Janeiro. Disponível em: <https://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/download/215/181>. Acesso em: 12 jun. 2016.