

# **Revista da Escola de Guerra Naval**

Periódico Especializado em Estudos Estratégicos

v.22, n.2, maio / agosto de 2016

**COMUNIDAD E IDENTIDAD EN LA COOPERACIÓN REGIONAL  
EN DEFENSA**

Marina Gisela Vitelli

**ATAQUES CIBERNÉTICOS PATROCINADOS PELO ESTADO**

Marcelo Antonio Osler Malagutti

**PLANEJAMENTO OPERACIONAL**

José Claudio da Costa Oliveira  
Rodolfo Castelo Branco Wadovski

**PROPRIEDADE INTELECTUAL NAS FORÇAS ARMADAS  
BRASILEIRAS**

Rogéria Prado Dall'Agnol  
Gláucio José Couri Machado  
Leidiane Bispo Brito  
Igor Dall'Agnol

**POLÍTICA E GESTÃO DE OFFSETS EM AQUISIÇÕES DE  
DEFESA**

Felipe Augusto Rodolfo Madeiros  
William de Sousa Moreira

**O EXÉRCITO BRASILEIRO E A EMULAÇÃO DOS MODELOS  
FRANCÊS E ESTADUNIENSE NO SÉCULO XX**

Eduardo Munhoz Svartman

**A QUESTÃO DA SEGURANÇA E DEFESA DO ESPAÇO CIBERNÉTICO  
BRASILEIRO, E O ESFORÇO POLÍTICO - ADMINISTRATIVO DO ESTADO**

Eduardo André Araujo de Souza  
Nival Nunes de Almeida

**OPERAÇÃO DE MANUTENÇÃO DA PAZ NO MAR? ESTUDO DE CASO  
SOBRE A FORÇA TAREFA MARÍTIMA NO LIBANO**

Luiz Gustavo Aversa Franco

---

# Revista da Escola de Guerra Naval

---



Rio de Janeiro, v. 22, n.2, mai./ago. 2016





## ESCOLA DE GUERRA NAVAL

---

A Revista da Escola de Guerra Naval é um periódico especializado em Estudos Estratégicos que tem o propósito de disseminar e promover intercâmbio, em níveis nacional e internacional, de conhecimentos relativos à Defesa com ênfase na área de Ciência Política e Relações Internacionais. Desta forma, tem como objetivo proporcionar maior integração entre a Marinha do Brasil e a sociedade, publicando artigos científicos, comunicações e resenhas.

---

### COMANDANTE DA MARINHA:

Almirante de Esquadra Eduardo Bacellar Leal Ferreira

### CHEFE DO ESTADO-MAIOR DA ARMADA:

Almirante de Esquadra Luiz Guilherme Sá de Gusmão

### DIRETOR DA ESCOLA DE GUERRA NAVAL:

Contra-Almirante André Luiz Silva Lima de Santana Mendes

### PRESIDENTE DO CENTRO DE ESTUDOS POLÍTICO-ESTRATÉGICOS – MB

Almirante de Esquadra (FN) Alvaro Augusto Dias Monteiro

### SECRETÁRIO-EXECUTIVO DO CENTRO DE ESTUDOS POLÍTICO-ESTRATÉGICOS

Contra-Almirante Márcio Magno de Farias Franco e Silva

**ISSN 1809-3191**

**e-ISSN 2359-3075**

**maio/agosto de 2016, vol. 22, n. 2**

### CORRESPONDÊNCIA:

ESCOLA DE GUERRA NAVAL

CENTRO DE ESTUDOS POLÍTICO-ESTRATÉGICOS

Av. Pasteur, 480 - Praia Vermelha - Urca

CEP 22290-255 Rio de Janeiro/RJ - Brasil

(21) 2546-9394 revista@egn.mar.mil.br

Aos cuidados do Editor Executivo da Revista da Escola de Guerra Naval

---

Os trabalhos poderão ser apresentados em conformidade com as Instruções aos Autores, contidas na última página de cada volume, para o e-mail: revista@egn.mar.mil.br

A **Revista da Escola de Guerra Naval** é uma publicação quadrimestral, editada pelo Centro de Estudos Político-Estratégicos (CEPE) e vinculada ao Programa de Pós-Graduação em Estudos Marítimos (PPGEM), sem fins lucrativos, **que publica, prioritariamente, trabalhos originais e inéditos.**

A política editorial da Revista estabelece que os artigos devem apresentar uma reflexão inovadora e contribuir para o desenvolvimento de um pensamento estratégico autóctone em matéria de Defesa, particularmente, no que se refere ao Poder Marítimo.

Todos os artigos para publicação estão condicionados ao processo de avaliação por pares e a aprovação dos membros do Conselho Editorial ou do Conselho Consultivo.

**Os artigos publicados pela Revista são de exclusiva responsabilidade de seus autores, não expressando, necessariamente, o pensamento da Escola de Guerra Naval nem o da Marinha do Brasil.**

**Direitos desta edição reservados à EGN, podendo ser reproduzidos desde que citados a fonte e informado à Escola de Guerra Naval.**

#### CONSELHO EDITORIAL CIENTÍFICO

Afonso Barbosa (*EGN/CEPE, RJ, RJ, Brasil*)  
Alcides Costa Vaz (*UNB, DF, Brasil*)  
André Barata Nascimento (*U Beira Int., Beira, Portugal*)  
Angela da Rocha (*PUC-RJ, RJ, Brasil*)  
Antônio Celso Alves Pereira (*UERJ, RJ, RJ, Brasil*)  
Antônio Manuel F. da Silva Ribeiro (*Universidade Técnica de Lisboa, Lisboa, Portugal*)  
Antonio Ruy de Almeida Silva (*PUC-RJ, RJ, Brasil*)  
Eurico de Lima Figueiredo (*UFF, Niterói, RJ, Brasil*)  
Fernando Manoel Fontes Diégues (*EGN/CEPE, RJ, RJ, Brasil*)  
Francisco Carlos Teixeira da Silva (*UF RJ, RJ, RJ, Brasil*)  
Helena Carreiras (*Univ. Lisboa, Lisboa, Portugal*)  
José Miguel Arias Neto (*UEL, Londrina, PR, Brasil*)  
José Murilo de Carvalho (*UF RJ, RJ, RJ, Brasil*)  
Marcio Scalercio (*PUC-RJ, RJ, Brasil*)  
Mário Cesar Flores (*EGN/CEPE, RJ, RJ, Brasil*)  
Michael Pavkovic (*USNWC, Newport, RI, USA*)  
Mônica Herz (*PUC-RJ, RJ, Brasil*)  
Reginaldo Gomes Garcia dos Reis (*EGN/CEPE, RJ, RJ, Brasil*)  
Rodrigo Fernandes More (*UNIFESP, SP, SP, Brasil*)  
Vinicius Mariano de Carvalho (*KING'S COLLEGE LONDON, UK*)  
Williams Gonçalves (*UERJ, RJ, RJ, Brasil*)

#### EQUIPE EDITORIAL

**Editor Científico:**  
Nival Nunes de Almeida (*UERJ, RJ, RJ, Brasil*)

**Editor Executivo:**  
Walter Maurício Costa de Miranda (*EGN/CEPE, RJ, RJ, Brasil*)

**Editores Assistentes:**  
André Panno Beirão (*EGN/PPGEM, RJ, RJ, Brasil*)  
Francisco Eduardo Alves de Almeida (*IGHMB, RJ, RJ, Brasil*)  
Sabrina Evangelista Medeiros (*Inter-American Defense College, Washington, DC*)  
William de Sousa Moreira (*UFF, Niterói, RJ, Brasil*)

**Assessora da Revista:**  
Elaine Pires

**Revisor:**  
Geraldo Bassani  
Jansen Coli Calil (*EGN/CEPE, RJ*)

**Diagramação e Programação Visual:**  
Ricardo de Oliveira Borges

**Normalização:**  
Nathalice Bezerra Cardoso  
Simone Freire Pinheiro

**Auxiliar Técnico:**  
Augusto Davi Meirelles Neves

#### Indexado em:

**Qualis/CAPES** - Coordenação de Aperfeiçoamento de Pessoal de Nível Superior  
**LATINDEX** - Sistema regional de información para revistas científicas de América Latina, el Caribe, España y Portugal  
**ICAP** - Indexação Compartilhada de Artigos de Periódicos  
**SUMARIOS** - Sumários de Revistas Brasileiras

Revista da Escola de Guerra Naval. – v. 22, n. 2, (mai/ago. 2016). – Rio de Janeiro:  
Escola de Guerra Naval, 1968 – v. ; 22 cm.  
Semestral  
ISSN 1809-3191 e-ISSN 2359-3075

1. Brasil. Marinha – Periódicos. I. Brasil. Marinha. Escola de Guerra Naval. II. Título.

---

## PALAVRAS DO DIRETOR

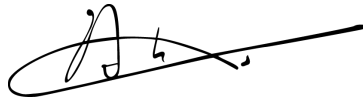
Em continuidade a uma trajetória iniciada em 1968, é com satisfação que apresento mais um número da Revista da Escola de Guerra Naval. Nesses 48 anos, nosso periódico vem sofrendo aprimoramentos constantes, sendo o último, a migração do site da revista para a plataforma SEER - Sistema Eletrônico de Editoração de Revistas, o que permite a completa automatização e o gerenciamento do processo de publicação de periódicos científicos eletrônicos.

Esse exemplar é aberto com o artigo intitulado “Comunidad e identidad en la cooperación regional en defensa: entendimientos en conflicto sobre pensamiento estratégico en el Consejo de Defensa Sudamericano (CDS)”, tema de grande atualidade, entre muitas razões, por ter sido do Brasil a proposta de criação do CDS. Assim, ao problematizar a construção de uma identidade estratégica sul-americana, o artigo ilumina a magnitude do desafio para se encontrar um pensamento estratégico comum em Defesa no nosso subcontinente.

Revestidos também dessa contemporaneidade, seguem-se temas como: guerra cibernética, propriedade intelectual e inovação tecnológica nas Forças Armadas, política de offset nas compras de defesa, operações de manutenção da paz no mar, e processos de emulação das missões francesa e estadunidense no Exército Brasileiro.

Finalizando, ressalto que a diversidade presente nas abordagens feitas pelos autores desta edição possibilita ao leitor refletir sobre a complexidade e a importância da pesquisa em temas stricto-sensu ligados à Defesa, que encontram em nossa Revista acolhimento preferencial.

Desejo a todos uma agradável leitura!



André Luiz Silva Lima de Santana Mendes  
Contra-Almirante  
Diretor

### ■ ARTIGOS

- COMUNIDAD E IDENTIDAD EN LA COOPERACIÓN REGIONAL EN DEFENSA: ENTENDIMIENTOS EN CONFLICTO SOBRE PENSAMIENTO ESTRATÉGICO EN EL CONSEJO DE DEFENSA SUDAMERICANO 233  
Marina Gisela Vitelli
- ATAQUES CIBERNÉTICOS PATROCINADOS PELO ESTADO 261  
Marcelo Antonio Osller Malagutti
- PLANEJAMENTO OPERACIONAL: O COMPONENTE CONCEITUAL DO PLANEJAMENTO COMO FUNDAMENTO PARA A CONSTRUÇÃO DE LINHAS DE AÇÃO 291  
José Claudio da Costa Oliveira  
Rodolfo Castelo Branco Wadovski
- PROPRIEDADE INTELECTUAL NAS FORÇAS ARMADAS BRASILEIRAS: UM PARALELO ENTRE A MARINHA, EXÉRCITO E AERONÁUTICA QUANTO AOS DEPÓSITOS DE PATENTES E AS POLÍTICAS DE CRIAÇÃO DOS NITs 309  
Rogéria Prado Dall’Agnol  
Gláucio José Couri Machado  
Leidiane Bispo Brito  
Igor Dall’Agnol
- POLÍTICA E GESTÃO DE OFFSETS EM AQUISIÇÕES DE DEFESA: CONTRIBUIÇÕES DA EXPERIÊNCIA INTERNACIONAL 327  
Felipe Augusto Rodolfo Medeiros  
William de Sousa Moreira

---

O EXÉRCITO BRASILEIRO E A EMULAÇÃO DOS MODELOS FRANCÊS E ESTADUNIDENSE NO SÉCULO XX Eduardo Munhoz Svartman	361
A QUESTÃO DA SEGURANÇA E DEFESA DO ESPAÇO CIBERNÉTICO BRASILEIRO, E O ESFORÇO POLÍTICO-ADMINISTRATIVO DO ESTADO Eduardo André Araujo de Souza Nival Nunes de Almeida	381
OPERAÇÃO DE MANUTENÇÃO DA PAZ NO MAR? ESTUDO DE CASO SOBRE FORÇA TAREFA MARÍTIMA NO LIBANO Luiz Gustavo Aversa Franco	411
■ <b>NORMAS PARA PUBLICAÇÃO</b>	441



### ARTICLES

- COMMUNITY AND IDENTITY IN REGIONAL DEFENSE COOPERATION: CONFLICTING VIEWS ABOUT STRATEGIC THINKING IN THE SOUTH AMERICAN DEFENSE COUNCIL  
Marina Gisela Vitelli 233
- STATE-SPONSORED CYBER-OFFENCES  
Marcelo Antonio Osller Malagutti 261
- OPERATIONAL PLANNING: THE CONCEPTUAL COMPONENT OF PLANNING AS A FOUNDATION FOR BUILDING LINES OF ACTION  
José Claudio da Costa Oliveira  
Rodolfo Castelo Branco Wadovski 291
- INTELLECTUAL PROPERTY IN ARMED FORCES  
Rogéria Prado Dall’Agnol  
Gláucio José Couri Machado  
Leidiane Bispo Brito  
Igor Dall’Agnol 309
- OFFSETS POLICIES AND MANAGEMENT IN DEFENCE ACQUISITIONS: CONTRIBUTIONS OF INTERNATIONAL BEST PRACTICES TO BRAZIL  
Felipe Augusto Rodolfo Medeiros  
William de Sousa Moreira 327

---

THE BRAZILIAN ARMY AND THE EMULATION OF FRENCH AND AMERICAN MODELS IN THE 20TH CENTURY Eduardo Munhoz Svartman	361
BRAZILIAN CYBERSPACE'S ISSUE ON SECURITY AND DEFENSE, AND THE POLITICAL-ADMINISTRATIVE EFFORT OF THE STATE Eduardo André Araujo de Souza Nival Nunes de Almeida	381
PEACEKEEPING AT SEA? A CASE STUDY OF THE MARITIME TASK FORCE IN LEBANON Luiz Gustavo Aversa Franco	411
<b>ARTICLES SUBMISSION GUIDELINES</b>	441

### **MARINA GISELA VITELLI**

Doutora em Relaciones Internacionales - Universidad Nacional de Rosario (2015). Atualmente Pós-doutoranda no Programa de Pós-Graduação em Relações Internacionais San Tiago Dantas, Bolsista FAPESP. Tem experiência na área de Ciência Política, com ênfase em Política Internacional, atuando principalmente nos seguintes temas: defesa, Brasil, Argentina, constructivismo e Consejo de Defensa Sudamericano.

### **MARCELO ANTONIO OSSLER MALAGUTTI**

Mestre em Estudos de Guerra no Kings College London, onde pesquisou Dissuasão Cibernética. Possui MBA em Estratégia Empresarial pela Fundação Getúlio Vargas. Diplomado pela Escola Superior de Guerra (ESG), tendo cursado o Curso de Altos Estudos em Política e Estratégia.

### **JOSE CLAUDIO DA COSTA OLIVEIRA**

Doutor em Ciências Navais pela Escola de Guerra Naval. Possui MBA em Gestão Internacional pela Universidade Federal do Rio de Janeiro (2004). Atualmente é professor da Área de Estratégia da Escola de Guerra Naval.

### **RODOLFO CASTELO BRANCO WADOVSKI**

Doutorando em Administração no COPPEAD-UFRJ. Mestre em Administração pelo COPPEAD/UFRJ (2015). Doutor em Ciências Navais pela Escola de Guerra Naval. Atualmente é professor da Área de Estratégia da Escola de Guerra Naval.

### **ROGÉRIA PRADO DALL'AGNOL**

Doutoranda e Mestre em Ciência da Propriedade Intelectual pela Universidade Federal de Sergipe. Possui especialização em Direito Público (2010). E é graduada em Gestão Pública pela Universidade Tiradentes (2007).

### **GLÁUCIO JOSÉ COURI MACHADO**

Doutor em Informática na Educação pela Universidade Federal do Rio Grande do Sul (2007), com Doutorado “sanduíche” na Universidade Aberta de Portugal. Professor adjunto da Universidade Federal de Sergipe (UFS), professor permanente do Programa de Pós-Graduação em Ciência da Propriedade Intelectual (PPGPI), professor colaborador do Programa de Pós-Graduação em Ensino Científico e Tecnológico (PPGeNT) da Universidade Regional Integrada do Alto Uruguai e das Missões (URI/RS).

**LEIDIANE BISPO BRITO**

Mestre em Ciência da Propriedade Intelectual pela Universidade Federal de Sergipe (2015). Atualmente é bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico. Atua principalmente nos seguintes temas: indicadores de c,t&i, desenvolvimento e inovação.

**IGOR DALL'AGNOL**

Graduado em Desenvolvimento de Aplicações para Web pela Faculdade de Administração e Negócios de Sergipe(2008) e em Física Médica pela Universidade Federal de Sergipe (2012). Possui especialização em Banco de dados pela Faculdade de Administração e Negócios de Sergipe(2014).

**FELIPE AUGUSTO RODOLFO MEDEIROS**

Mestre pelo Programa de pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN). Graduou-se em Relações Internacionais pela Universidade Federal Fluminense em 2013. Foi bolsista de Iniciação Científica com o projeto "A Base Industrial de Defesa Brasileira". Atualmente trabalha na Arcturus Advisors, empresa de consultoria que presta assistência a empresas norte-americanas de Defesa e Segurança.

**WILLIAM DE SOUSA MOREIRA**

Doutor em Ciência Política pela Universidade Federal Fluminense (UFF) (2013). CMG (RM1) Coordenador do Programa de Pós-Graduação em Estudos Marítimos (PPGEM-EGN). Pesquisador do Centro de Estudos Político-Estratégicos (CEPE-EGN) e do Núcleo de Estudos Estratégicos Avançados (NEA), do Instituto de Estudos Estratégicos (INEST) da UFF. Tem experiência na área de Defesa, com ênfase Estudos Estratégicos, Planejamento de Forças. Atualmente pesquisa as relações entre ciência, tecnologia, poder, com foco no uso da força em ambiente marinho, sistemas de inovação, aquisições de defesa e transferência de tecnologia.

**EDUARDO MUNHOZ SVARTMAN**

Doutor em Ciência Política pela Universidade Federal do Rio Grande do Sul (2006) com pós-doutorado na George Washington University (2016), é professor do Departamento de Ciência Política e dos Programas de Pós-Graduação em Ciência Política e em Estudos Estratégicos Internacionais desta Universidade. Foi professor visitante na Elliott School of International Affairs (EUA) e na Universidad Nacional de Rosario (Argentina), Diretor Acadêmico da Associação Brasileira de Estudos de Defesa (ABED) e editor executivo da Revista Brasileira de Estudos de Defesa. Atua principalmente nos seguintes temas: forças armadas, relações militares Brasil-Estados Unidos, políticas de defesa e política externa brasileira.

### **EDUARDO ANDRÉ ARAUJO DE SOUZA**

Mestrando do Programa de pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN). Possui MBA em Gerência de Projetos pela Universidade Federal Fluminense, com experiência nas indústrias de telecomunicações, petróleo e Sistemas Navais.

### **NIVAL NUNES DE ALMEIDA**

Doutor em Engenharia Elétrica pela Coordenação dos Programas de Pós-Graduação em Engenharia da Universidade Federal do Rio de Janeiro - COPPE/UFRJ (1997). Exerceu o cargo de Reitor da UERJ de 2004 a 2007. Atualmente é Professor Associado da Faculdade de Engenharia da UERJ e Professor Titular da Escola de Guerra Naval. Dedicar-se aos seguintes temas: ensino em engenharia; políticas públicas em ciência, tecnologia e inovação; sistemas inteligentes e automação; e gestão educacional.

### **LUIZ GUSTAVO AVERSA FRANCO**

Doutorando em Relações Internacionais pela Universidade de Brasília (UnB) e membro do Grupo de Estudos e de Pesquisa em Segurança Internacional (GEPsi) da mesma instituição. Atua principalmente nos seguintes temas: segurança internacional (foco em intervenções humanitárias e operações de paz) e defesa nacional (foco em base industrial de defesa).

## ARTIGOS

# COMUNIDAD E IDENTIDAD EN LA COOPERACIÓN REGIONAL EN DEFENSA: ENTENDIMIENTOS EN CONFLICTO SOBRE PENSAMIENTO ESTRATÉGICO EN EL CONSEJO DE DEFENSA SUDAMERICANO.

Marina Gisela Vitelli<sup>1</sup>

### RESUMEN<sup>2</sup>

El presente trabajo plantea la pregunta sobre cuál es el tipo de cooperación en defensa puesto en práctica por el Consejo de Defensa Sudamericano, como cuestión previa para indagar sobre sus logros y tareas inconclusas. Nuestro argumento es que la agenda de la seguridad cooperativa propia del concepto de la comunidad de seguridad registró algunos importantes avances. Contrariamente, la agenda de la construcción de una identidad estratégica encontró serios obstáculos que entorpecieron el logro de ese objetivo. Aún más preocupante, esos impedimentos se relacionan con la vigencia de una pregunta sin respuesta en la región: cuál debe ser el concepto estratégico y la misión de las fuerzas armadas en un contexto democrático y de fin del Guerra Fría. Para desarrollar nuestro argumento comenzamos por discutir los alcances dos conceptos: comunidad de seguridad y comunidad estratégica. Luego analizamos las acciones del CDS en función de las prácticas de la seguridad cooperativa y aquellas propias de la formulación de pensamiento estratégico, asociadas cada una a los tipos de comunidades mencionadas. Por último, discutimos los disensos existentes entre las visiones sobre la identidad estratégica y su relación con la tendencia a involucrar a las fuerzas armadas en misiones de seguridad pública (198p). **Palabras clave:** Comunidad de seguridad – Consejo de Defensa Sudamericano – Identidad estratégica – Misiones militares.

<sup>1</sup> Pos-doctoranda en el Programa de Pós Graduação em Relações Internacionais San Tiago Dantas (UNESP-UNICAMP-PUCSP). São Paulo, SP. E-mail: marinagvitelli@gmail.com

<sup>2</sup> El artículo reúne parte de los resultados del proyecto de investigación de post-doctorado financiado por la Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), n° de proceso 2015-13291-9

## INTRODUCCIÓN

En los últimos años, la actuación del Consejo de Defensa Sudamericano (CDS) – el organismo de la UNASUR encargado de la cooperación sobre asuntos de defensa – ha despertado cuestionamientos a respecto del nivel de convergencia –real y potencial– de las políticas de defensa de los países de la región. Parte importante de esa bibliografía ha intentado dar una respuesta a dicho interrogante analizando en qué medida el CDS constituye una comunidad de seguridad, (FLEMES; RADSECK, 2009; FLEMES, NOLTE; WEHNER, 2011; RIQUELME RIVERA, 2013; MEDEIROS FILHO, 2014; SAINT-PIERRE; SILVA, 2014; FUCCILLE, 2015; TEIXEIRA, 2013; TEIXEIRA JÚNIOR, 2015; OELSNER, 2015; RAMALHO DA ROCHA, 2015; RAMALHO DA ROCHA, 2016). Entre esos trabajos, nos resultan de particular interés aquellos análisis que se preguntaron sobre la relación entre ese término y las posibilidades reales de que este organismo cree –tal como reza en su estatuto– una identidad regional de defensa (MEDEIROS FILHO, 2013; LEITE, 2015).

De hecho, desde la creación del CDS estos dos conceptos propios del área de estudios de la defensa y la seguridad internacional -comunidades de seguridad e identidad estratégica regional- no sólo fueron utilizados el discurso académico, sino también en el político. Ahora bien ¿Qué quieren decir los países miembros del CDS cuando hablan de la construcción de una identidad estratégica regional? Creemos que responder a esta pregunta constituye un requisito fundamental para evaluar los avances y desafíos pendientes de la cooperación sudamericana sobre defensa. Si se tiene en cuenta que los documentos del CDS suelen incluir alguna fórmula que aclara que la construcción de una visión común sobre la defensa constituye una tarea gradual y que debe dar lugar a una perspectiva flexible, es sencillo ver que los países miembros de la UNASUR no se propusieron negociar una política regional de defensa común rigurosa, implementada por un organismo supranacional, que cuente con una fuerza operacional combinada bajo mandato de la organización. El objetivo, ciertamente, es mucho más modesto, pero no por eso menos innovador. A decir verdad, el proyecto de construir una identidad estratégica regional trae un elemento novedoso pero a la vez refiere a un desafío pendiente durante más de dos décadas para los estados de América del Sur: la definición el concepto

estratégico de las políticas de defensa y las misiones de las fuerzas armadas en el contexto de la democracia y el fin de la Guerra Fría.

En este contexto, el trabajo plantea la pregunta sobre cuál es el tipo de cooperación en defensa ensayado por el CDS, como pregunta previa para luego indagar sobre los logros del organismos y las tareas inconclusas, junto con las variables que explican esos retrasos. Un análisis de las actividades realizadas por el CDS desde su puesta en funcionamiento en 2009 y fines de 2015 muestra que, a grandes rasgos, hubo dos tipos de actividades: por un lado, aquellas que buscaron incrementar el diálogo y la interacción entre los ministerios de defensa y otros actores relevantes de las políticas de defensa, así como mejorar la confianza y la transparencia; y por otro, aquellas que tuvieron como propósito discutir, negociar y acordar definiciones comunes sobre la identidad estratégica regional. Nuestro argumento es que la agenda de la seguridad cooperativa propia del concepto de la comunidad de seguridad registró algunos importantes avances. Contrariamente, la agenda de la construcción de una identidad estratégica, propia del concepto de la comunidad estratégica que proponemos como más útil para describir el tipo de cooperación innovadora que el CDS se propone llevar adelante, encontró serios obstáculos que entorpecieron el logro de ese objetivo. Aún más preocupante, esos impedimentos se relacionan con la vigencia de una pregunta sin respuesta en la región: cuál debe ser el concepto estratégico y la misión de las fuerzas armadas en un contexto democrático y de fin del Guerra Fría.

Luego de una breve discusión sobre el concepto de comunidad de seguridad y comunidad estratégica, se analizan las actividades realizadas por el CDS segmentándolas en los dos tipos de agendas arriba mencionadas. Especial atención será colocada en el análisis del tipo de práctica de cooperación que asociamos con el concepto de comunidad estratégica. A seguir, se discutirán algunos entendimientos sobre la identidad estratégica que suscitaron controversias que remiten a la indefinición estratégica sobre las misiones que las fuerzas armadas deberían adoptar en el actual contexto. Fundamentalmente, abordaremos la tensión entre, por un lado, entendimientos que sostienen el concepto de cooperación disuasoria volcado hacia afuera y hacia actores estatales poderosos, y por otro, el concepto de seguridad multidimensional enfocado hacia amenazas domésticas de actores transnacionales.



## COMUNIDADES DE SEGURIDAD Y COMUNIDADES ESTRATÉGICAS

Si bien se considera que la obra de Karl Deutsch (1957) de fines de los años 50 constituyó el desarrollo pionero del concepto de comunidades de seguridad, fue el libro *Security Communities* editado por Emanuel Adler y Michael Barnett (1998, p. 7) la obra que se convirtió en referencia obligada de quienes analizan procesos y esquemas de cooperación regional en defensa orientados a garantizar las relaciones pacíficas entre sus miembros. El trabajo abordó un fenómeno anómalo para las relaciones internacionales, si se lo juzga desde la visión tradicional de la seguridad internacional anclada en la perspectiva realista: cómo explicar la existencia de regiones cuyos estados lograron tornar el recurso a la fuerza armada en un instrumento ilegítimo para resolver las disputas interestatales. La respuesta ensayada por los autores es que la dinámica positiva entre variables estructurales –el poder y las ideas- y los procesos de interacción entre distintos actores estatales y de la sociedad civil, generan confianza e identificación mutua entre los estados, la fuente del cambio pacífico.

Así, en una comunidad de seguridad los estados pasaron de una lógica de la rivalidad y la desconfianza hacia una dinámica marcada por expectativas mutuas de que el uso de la fuerza no es una opción para la resolución de los conflictos que pudieran surgir. La paz entre ellos descansa en la confianza y la identificación mutua. Lejos de implicar que desaparecen las diferencias de intereses o la competencia comercial, la clave de una comunidad de seguridad es que los miembros confían en que esas divergencias no serán resueltas de otra manera que no sea la negociación y la diplomacia. Ciertamente, no es una mera cuestión de fe, sino que “existen prohibiciones normativas –sean tácitas o formales- en contra del arreglo de las disputas por medio de medios militares” (ADLER; BARNETT, 1998, p. 35).

Hasta aquí cabe hacer el primer señalamiento: aquello que los autores entienden por seguridad está preponderantemente basado en la idea de ausencia de conflictos armados entre los miembros de esa comunidad, y en cierto punto en una noción de seguridad colectiva, esto es, en pensar la seguridad de uno de los miembros como equivalente a la seguridad del grupo bajo la lógica todos para uno y uno para todos. Se trata de estados que han llegado a consensuar una serie de cuestiones políticas amplias que hicieron que las consideraciones propias de la

política de poder ya no fueran las más aptas para garantizar sus intereses, porque las prácticas basadas en esa lógica irían en contra de un conjunto de coincidencias políticas que son más trascendentales en el mediano y el largo plazo.

Otra observación relevante es que, si una comunidad de seguridad designa a un grupo de estados que renuncia a hacer la guerra entre sí quiere decir que es un atributo de las relaciones mutuas entre esos estados y no de la institución que puedan (o no) crear para fomentar las relaciones pacíficas. Así, podríamos juzgar si América del Sur es una comunidad de seguridad y no si el CDS como organismo de cooperación tiene ese formato institucional. Para los mencionados autores, las instituciones de cooperación en defensa incentivan las relaciones pacíficas porque al aumentar las instancias de interacción y diálogo entre los actores de la defensa de los respectivos países multiplican las oportunidades de mutuo conocimiento y mejoran la confianza. No obstante este valor de las instituciones de cooperación, no deben tomarse como el fin de la cooperación, ellas son un medio entre otros para aumentar la confianza y la identificación mutua.

Sobre este último elemento surge otra imprecisión. Algunos trabajos entienden que un grupo de estados conforma una comunidad de seguridad madura sólo cuando adoptan una política de defensa común, equivalente a lo que los autores mencionan como identificación mutua. Pero se trata de una interpretación un tanto forzada del concepto que ocurre cuando se pierde de vista que el mismo sirve más para expresar la evolución que el concepto de seguridad europeo experimentó desde la *détente* hasta los años inmediatamente posteriores al fin de la Guerra Fría, que como manifestación de la expansión funcional y espacial por la cual pasó la Organización del Tratado del Atlántico Norte (OTAN) a partir de 1994. Nos referimos al proceso que comenzó a mediados de la década del setenta, que dio lugar al Acta de Helsinki y a la creación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), basado en la negociación de criterios comunes en materia de derechos humanos, democracia, cuidado del medio ambiente y otras definiciones amplias de políticas, conceptos clave de lo que más adelante se denominó como modelo de la seguridad cooperativa. Este plantea la indivisibilidad de la seguridad, entendiendo que las cuestiones de democracia, derechos humanos y bienestar de la población no pueden dissociarse de la noción de seguridad de corte militar (ADLER, 2008). Por tal motivo, la identidad colectiva implica que los estados lograron un importante nivel de consenso

en los temas apuntados y orientan sus políticas internas conforme esos principios, los cuales a su vez refuerzan percepciones de confianza e identificación mutua.

Si bien Adler y Barnett no operacionalizaron claramente qué entienden por identidad colectiva, realizando una interpretación de la obra y de sucesivos textos sobre la temática (ADLER, 2008; POULIOT, 2010) entendemos que los autores no se refieren a que los estados de la comunidad deban adoptar una Política de Defensa y Seguridad Común, una de las tareas más complejas de la Unión Europea, o un concepto estratégico unificado como el que la OTAN construyó en las últimas décadas. Esta organización sigue el modelo de una alianza militar con un tratado vinculante de defensa colectiva, que con los cambios operados en la seguridad internacional y la victoria de Occidente en el conflicto Este Oeste – y más aún luego del inicio de la Guerra contra el Terrorismo – modificó su concepto estratégico, ampliando su área de actuación tanto geográfica como funcional.

En suma, cuando los autores hablan de identidad y valores compartidos no se refieren a que la comunidad de seguridad adopte una política de defensa única y uniforme, con designación colectiva de las amenazas, precisamente la dirección que tomó la OTAN. De esta manera, mientras que las divergencias entre los países europeos que participaron en la coalición que invadió Irak en 2003 y quienes se opusieron constituyó una muestra de las dificultades de construir una política de defensa europea común, esto no debilitó la existencia de la comunidad de seguridad de esa región – e incluso en relación a sus socios del otro lado del Atlántico- ya que no implicó precarizar el compromiso de sus miembros con la seguridad cooperativa.

El uso que el CDS hizo del lenguaje identitario asociado a una potencial estrategia común puede haber confundido a algunos analistas que lo asociaron con el concepto de comunidades de seguridad. Algunos autores que escribieron sobre la seguridad y la defensa en América del Sur entendieron que la región no constituye una comunidad de seguridad porque no hay posibilidades de acordar entre los países cuál debe ser la estrategia de defensa regional, una divergencia similar a la que existiría en Europa (MEDEIROS FILHO, 2013). Junto con el desacuerdo sobre el rol de las fuerzas armadas en el combate de las “nuevas amenazas”, se ha llamado la atención sobre las discrepancias en lo relativo a la designación de una amenaza externa contra la región, en

un contexto en el cual algunos países sostienen una relación de fuerte tensión con Estados Unidos, otros en el extremo opuesto mantienen vínculos estrechos en materia de cooperación militar y un tercer grupo tiene una actitud doble de colaboración en algunas cuestiones y algunas desconfianzas en otras, como es el caso de Argentina y Brasil.

Intentando clarificar los conceptos proponemos aquí pensar que dentro del CDS existió hasta fines de 2015 una agenda basada en la seguridad cooperativa, propia del concepto de comunidades de seguridad, y otra agenda vinculada al concepto embrionario de “cooperación disuasoria” –la necesidad de cooperar al interior de la región para disuadir amenazas provenientes de países más poderosos- que no encuentra lugar dentro del planteo de Deutsch, Adler y Barnett. Es esta segunda agenda la que apela a una identidad regional de defensa en el sentido de consensos sobre misiones militares, sobre designación de amenazas y visiones sobre el entorno estratégico, una conceptualización de la identidad que se diferencia del concepto de identificación mutua planteado por la literatura de comunidades de seguridad.

Dada esta falta de adecuación entre el CDS y el concepto de comunidad de seguridad, proponemos pensar en el concepto de comunidades estratégicas, las cuales serían regiones que han llegado a desarrollar expectativas confiables de que resolverán sus conflictos de manera pacífica pero también desarrollarán una estrategia de defensa común basada en una identidad estratégica regional, en los términos planteados por Tibiletti (2014), que en otro trabajo transformamos en cuatro dimensiones de entendimientos: el entorno estratégico, los intereses regionales, las amenazas y riesgos y los instrumentos (VITELLI, 2015).

Comunidades de seguridad y comunidades estratégicas difieren también en relación al tipo de práctica que adopta la cooperación. Mientras que, tal como trabajó Adler (2008) una comunidad de seguridad se fortalece con la puesta en marcha de instancias de interacción y diálogo entre los actores de la defensa de los países miembros, así como el establecimiento de medidas de confianza y transparencia y por la construcción, una comunidad estratégica debe adicionar a las mencionadas otro tipo de práctica: aquellas que permiten la discusión, negociación y acuerdo de los elementos que componen una identidad estratégica regional, cristalizada en un concepto estratégico común. Cabe aclarar que ese concepto no implicaría una política uniforme con

un organismo ejecutor y una fuerza operativa, pero sí implicaría la adopción de una orientación general a respecto de las misiones de las fuerzas armadas y sobre los intereses a proteger y las amenazas a conjurar.

A continuación, exploraremos en detalle un tipo de actividad realizada por el CDS con el propósito de servir como momento de formulación de un pensamiento estratégico regional. Pero a pesar de poner de relieve que ese tipo de práctica constituyó una innovación del modelo de la cooperación regional en defensa propuesto por el CDS, apuntaremos que la ausencia de logros en dicha dimensión refleja que la definición de las misiones militares y las políticas de defensa en la democracia y contexto de pos Guerra Fría es aún una tarea pendiente.

## CONSENSOS EN TORNO A LA AGENDA DE LA SEGURIDAD COOPERATIVA

Si bien los países de América del Sur venían participando del proceso de diálogo y cooperación hemisférico sobre temas de seguridad y defensa desde la década del noventa, el CDS significó una multiplicación de las instancias de interacción y diálogo entre los actores de la defensa, esta vez acotando la membresía a la región sudamericana. Así, entre abril de 2009 y diciembre de 2015, el organismo realizó ocho Reuniones del Consejo de Ministros de Defensa; quince Reuniones de la Instancia Ejecutiva; dos Reuniones de Ministros de Relaciones Exteriores y de Defensa; treinta y dos talleres, seminarios, simposios y conferencias<sup>3</sup>; veintiséis Reuniones de Grupos de Trabajo<sup>4</sup>; y once ediciones de cursos<sup>5</sup>.

<sup>3</sup>Sobre las siguientes temáticas: Derechos Humanos y Derecho Humanitario, Inteligencia Estratégica Militar, CDS, Medicina Operacional, Política de Defensa, Control del Espacio Aéreo, Mujeres y Defensa, Movilización Nacional, Defensa y Recursos Naturales, Ciberdefensa, Industria y Tecnología de la Defensa, Planeamiento Estratégico, Enfoques conceptuales, Monitoreo de Áreas Especiales, Cooperación en Desastres Naturales, Medición de Gastos, Operaciones de Paz.

<sup>4</sup>Sobre las siguientes temáticas: análisis del documento Estrategia Global de Bases de Apoyo Libro Blanco del Comando de Movilidad Aérea, Lineamientos para un marco conceptual común, vehículo aéreo no tripulado, creación de un Atlas de Mapa de riesgo de Desastres, Diagnóstico para la cooperación en la defensa de Recursos Naturales, Crear comisión permanente de asesoramiento del CDS, Cooperación en Gestión de Desastres, Medidas de Confianza Mutua, Redacción del Reglamento del CDS, Países colaboradores con la MINUSTAH, amenazas cibernéticas, Inventario Militar, Protocolo de Paz, Lineamientos estratégicos para la Defensa, Industria y Tecnología para la defensa.

<sup>5</sup>Incluye las cuatro ediciones del CADSUL (también realizado en 2016); cuatro ediciones del Curso de Formación de Civiles en Defensa, dos ediciones del Curso en Derechos Humanos y Derecho Internacional Humanitario (también en 2016), y una edición del Curso de Capacitación para civiles en emergencias en operaciones de paz.

Independientemente de si esas actividades resultaron en compromisos vinculantes, normativa regional o creación de instituciones, no puede desconocerse que los actores de la defensa de la región vieron multiplicadas las oportunidades de encuentro y diálogo. Si bien es complejo medir el impacto de esas interacciones, la literatura sobre comunidades de seguridad, incluidos los trabajos de Deutsch, suponen que el incremento de las transacciones y las comunicaciones es un requisito de la construcción de la identificación mutua. Ciertamente, el fortalecimiento de la confianza fue identificado como uno de los desafíos pendientes a cuya solución el CDS debía contribuir. Así, las medidas de confianza mutua están mencionadas en los principios del CDS (d. fortalece el diálogo y el consenso en materia de defensa mediante el fomento de medidas de confianza y transparencia) y en los objetivos específicos (fortalecer la adopción de medidas de fomento de la confianza y difundir las lecciones aprendidas. El episodio del bombardeo de las fuerzas armadas colombianas al campamento de las Fuerzas Armadas Revolucionarias de Colombia (FARC) en territorio ecuatoriano tornó dramáticamente visible el déficit en materia de confianza y transparencia. A pesar de que dicha tensión trilateral no se resolvió en el seno de la UNASUR sino que fue llevada a la Organización de Estados Americanos (OEA) y al Grupo de Río, el siguiente episodio de conflicto logró reunir a los jefes de estado sudamericanos en Bariloche con el propósito de discutir los alcances de la renegociación del acuerdo de ayuda militar que Colombia mantiene con los Estados Unidos. Como resultado, la Declaración de Bariloche de agosto de 2009 planteó el objetivo de establecer un mecanismo de confianza mutua en materia de defensa y seguridad, instruyendo a los ministros de Relaciones Exteriores y de Defensa a celebrar una reunión extraordinaria – realizada días más tarde en Quito – que creara dicho sistema de manera complementaria a los que ya existen en la OEA, incluyendo mecanismos completos de implementación y garantías.

En cumplimiento, entre septiembre y diciembre de 2009, la Presidencia Pro Témpore desarrolló una propuesta de Procedimientos de Aplicación para las Medidas de Fomento de la Confianza y la Seguridad, finalmente aceptada por los ministros en mayo de 2010, luego a que previamente se realizase una Reunión de expertos sobre esa temática y una reunión del grupo de trabajo sobre medidas de confianza mutua. En noviembre de 2012 los ministros del CDS encargaron al Centro de Estudios

Estratégicos de Defensa (CEED) la sistematización, análisis y archivo de la información recibida sobre las medidas de fomento de la confianza a partir de los cual el CDS debía elaborar un Mecanismo de Seguimiento. La propuesta fue elaborada durante una reunión celebrada durante los días 4 y 5 de marzo de 2013 en Lima, y elevada a consideración de la instancia ejecutiva del CDS y se convino una reunión virtual para establecer la propuesta final<sup>6</sup>.

De hecho, a pesar de haber sido concebido para dedicarse al desarrollo de un pensamiento estratégico sudamericano, en sus inicios el CEED adoptó funciones relacionadas con la construcción de confianza y transparencia, tales como la creación del Registro Sudamericano de Gastos en Defensa y de Inventarios Militares. Otros trabajos, como el libro *La Institucionalidad de la Defensa*, cumplieron una función doble: al reunir la información relativa a los aspectos normativos, orgánicos y funcionales de los sistemas nacionales de defensa de cada país miembro funciona como un verdadero libro blanco de la defensa regional, incrementando la transparencia. Pero al mismo tiempo sirvió para alimentar la reflexión sobre la diversidad de políticas de defensa de los estados de la región, y los consecuentes desafíos de vincularlas a una identidad regional de defensa.

## NEGOCIANDO UN PENSAMIENTO ESTRATÉGICO REGIONAL

Ahora bien, teniendo en cuenta lo que sostuvimos más arriba con respecto a que una de las especificidades del CDS es plantear como uno de sus propósitos la construcción de una identidad regional en defensa, en este trabajo subrayamos un tipo de práctica que asociamos con ese elemento distintivo. En concreto, ponemos de relieve que los actores de la defensa de los países sudamericanos pusieron en marcha iniciativas durante las cuales buscaron discutir, acordar, e incluso señalar áreas de individualidad no negociables en el corto y mediano plazo, sobre un marco conceptual para la defensa. Asimismo, es posible distinguir dos

---

<sup>6</sup>Por cuestiones de espacio dejamos fuera de este trabajo el análisis de otras actividades de cooperación también asociadas a la seguridad cooperativa: el ejercicio UNASUR I y la creación del Atlas y Mapa de Desastres Naturales. Asimismo, es posible distinguir dos grandes dimensiones de ese marco conceptual. Por un lado, uno de los elementos más fundamentales de un proceso de cooperación regional en defensa es definir qué entendían los países miembros por “defensa” y por “seguridad”, y por otro lado, otros elementos fundamentales de una identidad estratégica regional: las amenazas y riesgos a conjurar.



grandes dimensiones de ese marco conceptual. Por un lado, uno de los elementos más fundamentales de un proceso de cooperación regional en defensa es definir qué entendían los países miembros por “defensa” y por “seguridad”, y por otro lado, otros elementos fundamentales de una identidad estratégica regional: las amenazas y riesgos a conjurar. Mientras que estos últimos elementos informan las primeras tres dimensiones de la identidad estratégica regional – entorno estratégico, interés regional y amenazas y riesgos - el primero se vincula con la última dimensión, la instrumental. Así, conociendo cuáles fueron los entendimientos discutidos en las primeras dimensiones podremos, para finalizar, entender la discusión sobre los conceptos de seguridad y defensa, esto es, la misión de las fuerzas armadas, como corazón del concepto estratégico.

El objetivo de dar lugar a un concepto estratégico regional fue incluido desde el primer plan de acción del organismo. El documento que planificó las actividades para el periodo 2009-2010 estableció en el eje n° 1 de Política de Defensa dos metas: propiciar la definición de enfoques conceptuales e identificar los factores de riesgo y amenazas que puedan afectar la paz regional y mundial. En el Plan de Acción siguiente (2010-2011) se unificaron en la actividad 1.c: Realizar un seminario para avanzar en la identificación de los factores de riesgo y amenazas que puedan afectar la paz regional y mundial, así como en la definición de enfoques conceptuales. En cumplimiento de ese mandato a partir de 2010 se inauguró una serie de Seminarios, todos ellos organizados en Caracas, destinados a debatir sobre las dos cuestiones señaladas: el marco conceptual sobre seguridad y defensa y las amenazas y riesgos enfrentados por la región. Otras dos actividades asociadas a la práctica de discusión de conceptos sobre la defensa regional fueron las reuniones de dos Grupos de Trabajo: aquel destinado a “Proponer y consolidar lineamientos estratégicos del CDS-UNASUR, para la construcción progresiva y flexible de una visión compartida de defensa regional”, y aquel destinado para “Desarrollar un marco conceptual común con el propósito de unificar conceptos empleados en el ámbito de la defensa de la región”.

Como mencionamos más arriba, otro espacio del cual se espera la participación en prácticas de pensamiento estratégico es el CEED, puesto que su principal misión es contribuir a los principios y objetivos del CDS a través de la investigación y la producción de conocimiento. El mencionado libro *La Institucionalidad de la Defensa* fue una medida de confianza mutua pero también fue un corolario de otra tarea que realizó el CEED,



más acorde al tipo de práctica que aquí ponemos de relieve: la discusión sobre qué implica la defensa para los países de la región. La definición de esta cuestión es el “ABC” de la cooperación en esta área, ya que si no todos entienden lo mismo por política de defensa, mal podrán cooperar, tal como exploraron Saint-Pierre y Lopes da Silva (2013). Tal la relevancia de zanjar la cuestión sobre qué implica hablar de defensa en la región que una de las primeras actividades que le fueron encomendadas al CEED por parte de los miembros del CDS fue la realización de un Informe sobre “los términos de referencia del concepto de seguridad y defensa”. Ese fue el mandato de los viceministros de defensa durante la IV Reunión de la Instancia Ejecutiva del CDS, celebrada los días 28 y 29 de abril de 2011 en la ciudad de Lima. En respuesta a la tarea encargada, el CEED incorporó la cuestión en su primer Plan de Acción y en diciembre de 2011 presentó a los ministros el Informe Preliminar del CEED al CDS acerca de los Términos de Referencia para los Conceptos Seguridad y Defensa en la Región Suramericana.

En el marco de las discusiones sobre qué factores relacionaban a la defensa de cada país de la región en una dimensión común, hacia el año 2012 tomó fuerza entre algunos estados la idea de que los estados miembros compartían un elemento de gran valor estratégico, que constituía a la vez una fortaleza y un potencial riesgo para la paz de la región: los recursos naturales estratégicos. Esta concepción sucedió en simultáneo con la agenda propuesta por Venezuela durante el período en el cual el ex canciller venezolano, Alí Rodríguez, se desempeñó como Secretario General de la UNASUR, para pensar a la integración regional en su conjunto como asociada a la realidad y al futuro de ese elemento común, los recursos naturales. La lógica discursiva proponía pensar que las posibilidades del desarrollo de América del Sur y de la autonomía de los países miembros era un destino atado a lo que se hiciera en materia de uso de los recursos naturales.

Es posible situar el inicio de esta agenda durante la VI Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la UNASUR, celebrada en Lima el 30 de noviembre de 2012, cuando el entonces Secretario General de la UNASUR, presentó el documento titulado “*Los recursos naturales como eje dinámico en la estrategia de integración y unidad de nuestros países*”. Al término de la reunión, los presidentes emitieron una Declaración en la que solicitaron a la Secretaría General la formulación de una Estrategia Continental y un Plan General para el aprovechamiento

de los recursos naturales de UNASUR. Asimismo, incluyeron varios párrafos avalando algunas de las propuestas del Secretario General, entre ellas la organización “a finales del primer trimestre de 2013 (de) un evento que congregue a expertos y autoridades de los Estados miembros de UNASUR, a fin de recabar insumos que contribuyan a la elaboración” de una estrategia de la UNASUR para su aprovechamiento”.

El evento mencionado tuvo lugar entre los días 27 y 30 de mayo de 2013 en Caracas, bajo el título *Conferencia de la UNASUR sobre Recursos Naturales para el Desarrollo Integral de la Región*. En virtud del enfoque integral que quiso dársele al tema, la conferencia involucró a todos los consejos ministeriales y de delegados de la UNASUR, en vistas de que el propósito era reflexionar sobre el rol de los recursos naturales para el potencial de la región, en términos económicos, sociales y estratégicos. En ese mismo año, el CDS creó el “Grupo de Trabajo para formular un diagnóstico para proponer mecanismos de cooperación en materia de protección y defensa de los recursos naturales y la biodiversidad con base en las legislaciones de los países miembros de UNASUR”, que se reunió en Caracas durante los días 22 y 23 de agosto de 2013. De igual manera, la cuarta edición del Seminario de Caracas continuó con la orientación hacia la reflexión sobre los recursos naturales y la defensa regional ya que, entre los días 5 y 7 de noviembre de 2013 se realizó el I Foro sobre “Políticas y Estrategias de Defensa Regional” y el IV Seminario “Enfoques Conceptuales de Defensa, Riesgo y Amenazas a la Región”.

En 2014 Argentina tomó la posta en la organización de eventos sobre recursos naturales, en las cuales también adquirió un rol relevante el propio CEED. Así, en junio se realizaron dos actividades en Buenos Aires: el día 9, tuvo lugar la *Conferencia sobre “Defensa y Recursos Naturales”*, y el día 10 se organizó un *Taller para realizar un Estudio sobre la Disponibilidad y Potencialidades de los Recursos Naturales Estratégicos de la Región*. Con el propósito de ofrecer insumos para el debate el Director del CEED, Alfredo Forti, formuló un documento titulado “La defensa y los recursos naturales en Suramérica. Aportes para una estrategia regional”. Si bien el texto expresó propuestas a título personal, Forti aclaró que el escrito recuperaba principios y objetivos ya consensuados por las delegaciones en el CDS, que serán analizados en detalle en el siguiente apartado (FORTI, 2014).

Mientras que la Conferencia fue un evento abierto al público,

el taller consistió en una reunión privada de los viceministros y jefes de delegación. Durante el encuentro, el Director del CEED expuso su visión sobre la vinculación entre la defensa y los recursos naturales y el Secretario General de la UNASUR presentó un Proyecto de resolución de un Segundo Protocolo Adicional al Tratado Constitutivo de UNASUR acerca del ejercicio de los derechos permanentes y soberanos de los estados de los pueblos sobre sus recursos naturales. Seguidamente, cada país planteó lineamientos a seguir en términos de defensa y protección de recursos estratégicos, debate que quedó plasmado en el anexo II del acta, al cual se denominó “Panel: Estrategias Nacionales sobre Recursos Naturales y Defensa”, así como un comunicado de consenso como anexo III. Este breve documento no planteó grandes medidas, sino que se limitó a solicitar la continuidad y profundización del “actual esquema regional cooperativo a través de nuevas iniciativas relativa a la protección de los recursos naturales, tales como la construcción de instrumentos jurídicos comunes y convergentes; desarrollos doctrinarios y conceptos compartidos; promoción de la formación y educación en las instancias regionales sudamericanas CEED y ESUDE”. También realizó el acostumbrado llamado a que las acciones cooperativas sigan los principios de gradualidad y flexibilidad.

Por la tarde se realizó un “Taller para realizar un inventario sobre los recursos naturales estratégicos que permitan elaborar un estudio sobre su disponibilidad y potencialidades en el ámbito de la defensa”. Entre otras cuestiones, se discutió sobre: cuáles son los recursos que cada país categoriza como estratégicos, qué constituye desde la perspectiva específica de la defensa un recurso estratégico y bajo qué criterios esos recursos son identificados y/o categorizados como estratégicos. Finalmente, en la última jornada tuvo lugar la II Reunión del Grupo de Trabajo “responsable de formular un diagnóstico para proponer mecanismos de cooperación en materia de protección y defensa de los recursos naturales y la biodiversidad, con base en las legislaciones de los países miembros de la UNASUR”.

El otro espacio de reflexión sobre la relación entre los recursos naturales y un potencial pensamiento estratégico sudamericano fue el CEED. El primer plan de trabajo de este centro de estudios incluyó el proyecto Estudio Prospectivo Suramérica 2025, una actividad de estudio e investigación con el propósito de dar lugar a “un estudio integral de activos estratégicos regionales y capacidades colectivas y su incidencia

para la sostenibilidad, seguridad y defensa estratégicas de la región y su posicionamiento en el Sistema Internacional de Seguridad". Así, durante el segundo semestre de 2015, el CEED publicó los resultados de la primera etapa de los trabajos, los tomos I y II del Estudio Prospectivo Sudamérica 2025. Una segunda fase se enfocará en la producción de análisis y elaboración de escenarios futuros tomando como referencia la proyección y efectos de la demanda de recursos estratégicos y como objeto de estudio el papel y las políticas de la defensa ante las oportunidades, desafíos, riesgos y amenazas que pudieran derivarse de los referidos escenarios prospectivos.

## **LAS AMENAZAS Y RIESGOS A LOS INTERESES REGIONALES EN EL ACTUAL CONTEXTO ESTRATÉGICO**

Durante las actividades arriba nombradas fueron discutidas un conjunto de temáticas que pueden ser analizadas a partir de las dimensiones de la identidad estratégica regional listadas en el apartado conceptual. En el caso de la dimensión contextual, esta reúne los entendimientos sostenidos por el grupo con respecto al sistema internacional y regional y la definición del entorno estratégico, en términos de conflicto y cooperación. Varios elementos de esta dimensión podrían ser analizados, pero aquí nos enfocaremos en uno que consideramos fundamental: en qué medida la presencia de Estados Unidos significa un elemento condicionante y desestabilizador de la seguridad sudamericana. El grado de cooperación o confrontación con este país en temas de seguridad constituye una variable altamente condicionante de las políticas de defensa, al punto que mal puede pensarse en una estrategia regional por más básica que sea que no acuerde un mínimo denominador sobre esta cuestión. Un disenso en este punto central genera tensiones que ponen a prueba no sólo las chances de éxito de un concepto estratégico propio sino también, en ocasiones, la misma comunidad de seguridad, tal como ocurrió con la renegociación del acuerdo militar entre Colombia y Estados Unidos por las bases militares en su territorio.

Precisamente en ocasión de dicha crisis, durante la Cumbre de Bariloche el ex presidente Hugo Chávez denunció la existencia del documento norteamericano Estrategia Global de Bases de Apoyo Libro Blanco del Comando de Movilidad Aérea. Si bien Venezuela no era la única delegación que pedía conocer la integridad del acuerdo

que Colombia negociaba con Estados Unidos, fue la alocución del líder venezolano la que más radicalmente planteó que las bases norteamericanas en Colombia formaban parte fundamental de la estrategia global de dominación militar de los Estados Unidos.

En la medida en que otros países miembros se sumaron a las preocupaciones esgrimidas por Chávez, acordaron en la Declaración de Bariloche que el documento norteamericano fuera analizado y se elevara un informe sobre sus contenidos. El tema fue tratado en la II Reunión de la Instancia Ejecutiva realizada en enero de 2010, en Manta, donde, en vista de no haber logrado el consenso para establecer un grupo de trabajo que realizara el mencionado análisis, los viceministros resolvieron encargar a la Presidencia Pro Tempore la elaboración de un informe sobre el citado debate (CDS, 2010). Luego se decidió la creación del grupo de trabajo, conformado por Argentina, Brasil, Venezuela y Ecuador. Este se reunió en Quito durante los días 3 y 4 de junio de 2010, elevando a la instancia ejecutiva una síntesis objetiva del documento y una propuesta firmada por Argentina y Venezuela. Si bien los documentos fueron remitidos al Consejo de Ministros del CDS, este tema no fue mencionado en el acta de la III reunión de dicho consejo y desapareció de la agenda.

A pesar de no haber redundado en una acción concreta del CDS, la narrativa sobre la excesiva presencia militar de los Estados Unidos en América del Sur dejó su marca y se reflejó en otras actividades del organismo, particularmente en los documentos que versan sobre una estrategia sudamericana de defensa de los recursos naturales, como será abordado a continuación. No obstante esto, es sencillo detectar que existió un grupo de países dentro del CDS que no adoptaron en ningún momento el discurso de alarma frente a la existencia del sistema de bases militares norteamericanas en la región, particularmente Chile, Perú y Colombia, marcando una clara división ideológica al interior del organismo en lo que hace a la principal definición identitaria: quiénes son los sudamericanos en relación al país más poderoso del sistema internacional, principal condicionante estratégico de la región.

La noción de interés regional – que en el marco de nuestro esquema analítico corresponde a la segunda dimensión de la identidad estratégica sudamericana – apareció reiteradamente en los documentos del CEED, inclusive en su estatuto. Específicamente, bien temprano este organismo comenzó a asociar la categoría de interés regional con la protección de los recursos naturales. Cabe aclarar, no obstante, que esta vinculación se

expresó más claramente en los escritos del director del CEED, realizados a título personal aunque expresando ideas que circulan entre actores civiles y militares de la defensa de los países miembros.

Por ejemplo, el documento que Forti presentó durante la Conferencia de junio de 2014 condensó ideas que ya había esbozado en otras oportunidades sobre la vinculación entre los recursos naturales y el concepto de la cooperación disuasoria como potencial norte de la cooperación sudamericana en defensa (FORTI, 2014). Luego de presentar datos que fundamentan el diagnóstico sobre la continuidad de la presión global sobre la explotación de los recursos naturales, el texto establece la siguiente relación: la escasez muy probablemente traerá disputas entre estados con mayores necesidades que capacidad de acceso a recursos, implicando un serio riesgo para quienes los posean en cantidad suficiente. En pocas palabras, según Forti, en términos estratégicos la abundancia es la otra cara de la escasez y de la apetencia de parte de potencias extra regionales: en un escenario de presión sobre los recursos quienes los tengan en abundancia, lejos de estar ajenos a las disputas serán probablemente el escenario de esos conflictos.

Según apuntaba Forti, no sólo son pensados en términos regionales porque tienen la misma relevancia para todos los estados, sino en virtud de su naturaleza y distribución: el hecho de que el agua, la biodiversidad, los minerales e hidrocarburos no respeten fronteras lleva a entender que los recursos estratégicos se caracterizan por su “regionalidad”, independientemente de la voluntad de los gobiernos de poner en práctica políticas cooperativas para garanticen el usufructo de los mismos. Frente al panorama de escases y apetencia, según Forti, los países de la región no han reaccionado aun en clave de pensar frente a tal escenario una estrategia regional que garantice “el control, acceso y usufructo endógeno de las mismas, condición del desarrollo sostenible de nuestras naciones y nuestra población”; algo que considera de extrema importancia (CENTRO DE ESTUDIOS ESTRATÉGICOS DE DEFENSA, 2015, p. 14).

En suma, si bien la estructura normativa y organizacional del CDS pone énfasis en que los estados conservan la capacidad soberana de determinar sus políticas de defensa, y que cualquier tipo de coordinación será gradual, el organismo tendría poco sentido si los países no intentaran identificar cuestiones en común, tales como conceptos de defensa y seguridad, entendimientos sobre riesgos y amenazas y bienes a defender de manera conjunta, aunque esto no signifique construir una fuerza armada

regional. De hecho, las actividades descritas en el apartado anterior pueden analizarse como la construcción de los recursos naturales como objeto de seguridad sobre los cuales los estados deben pensar estrategias comunes.

## **¿DEFENSA EXTERNA O SEGURIDAD INTERIOR? CONTINUIDAD DE LA INDEFINICIÓN DE LAS MISIONES MILITARES**

Para cerrar este breve análisis de los elementos de una identidad estratégica regional que fueron tratados durante las distintas actividades del CDS descritas aquí como formuladoras de pensamiento estratégico, pasamos a abordar las discusiones sobre la relación existente entre la defensa regional y las problemáticas de seguridad interna. Esta fundamental cuestión corresponde a la dimensión instrumental de la identidad estratégica, en tanto esta se pregunta sobre los medios que los países de la región están dispuestos a utilizar conjuntamente para conjurar las amenazas y enfrentar los riesgos previamente identificados.

Tal como hemos trabajado más extensamente en un trabajo previo, una de las primeras definiciones tomadas por el CDS fue dejar por fuera de su ámbito de acción aquellas cuestiones asociadas con la seguridad interna (VITELLI, 2016). Esto derivó incluso en la recomendación por parte del CEED de que se crearan sendos Consejos con atribuciones sobre la cooperación en materia de lucha contra el narcotráfico y en el área de crimen organizado y seguridad ciudadana. Tanto el Informe sobre los términos como el libro *La Institucionalidad de la Defensa*, reconocían que los países miembros empleaban a sus militares en misiones en seguridad pública, pero evaluaban que en general se trataba de funciones subsidiarias y que existían estructuras separadas para defensa y seguridad. Así, la decisión de circunscribir la actuación del CDS a los temas de defensa externa fue consensuada por los países miembros aún a pesar de que una cantidad creciente de ellos ha tendido a incrementar la participación de las fuerzas armadas en cuestiones de seguridad pública. Asimismo, comenzó a desarrollarse en el seno del CEED la propuesta de la cooperación disuasoria volcada hacia una misión militar tradicional – la protección de la soberanía y la integridad territorial – aunque veremos que se trató de una formulación sin una base real de consenso.

En este sentido, la formulación de Forti bajo el esquema de la



cooperación disuasoria establecía que hacia el interior de la región los países debían fortalecer la cooperación, es decir, aquellas iniciativas asociadas al modelo de seguridad cooperativa, como la construcción de confianza mutua y la coordinación de algunas políticas que no implicaran altos grados de integración. Esta cooperación resultaría crucial, no sólo para evitar conflictos armados entre los estados miembros, sino también para impedir el surgimiento de grietas políticas que pudieran ser aprovechadas por potencias extra regionales. Es en esta dimensión externa a la región donde entra el elemento disuasorio: “la categoría referida a la disuasión “hacia fuera”, implica que nuestras capacidades regionales en materia de defensa y militar deben concentrarse y fundirse en una sola cuando de lo que se trata es proteger al interés regional que representan los recursos naturales suramericanos frente al eventual accionar de terceros Estados” (FORTI, 2014, p. 19).

El director del CEED aclara que, en línea con la tradición pacífica de la región, se trata de una estrategia defensiva, que no contemplaba estrategias de proyección de poder. Se limita, por el contrario, a un conjunto de acciones que transmiten hacia el resto de los estados que los intentos por “lesionar la integridad territorial de un Estado particular del subcontinente –en este caso, los activos naturales que la conforman– constituye una acción dirigida hacia Suramérica en su conjunto”, replicando la noción de seguridad colectiva. Sobre la implementación efectiva de la disuasión hacia afuera, Forti propuso la creación de una “Fuerza Militar Suramericana”, cuya misión sería proteger los “factores comunes del interés regional suramericano”, de acuerdo a los criterios exclusivamente definidos de forma consensual por las autoridades políticas nacionales (FORTI, 2014, p. 19).

A pesar de la aparente coherencia de los enunciados de la cooperación disuasoria presente en los documentos firmados por Forti, debe apuntarse que su propuesta no reunió el consenso de un grupo importante de países, habiendo incluso algunos directamente contrarios a que se consagrara un concepto estratégico sobre la base de la defensa militar colectiva de los recursos naturales. Ciertamente, la negativa a adoptar esta perspectiva responde a diversos motivos, según de qué país se trate. Colombia y Perú están comprometidos con la lucha contra el crimen organizado por medios miliares dentro del esquema favorecido por Estados Unidos. En el otro extremo del espectro ideológico, Venezuela, Ecuador y Bolivia recurren a sus militares tanto para alguna forma de combate a la



criminalidad como para control de la protesta social. Argentina y Brasil han incrementado las misiones domésticas aun sosteniendo que no se trata una transformación radical de la política de defensa (DIAMINT, 2015).

Chile podría ubicarse en el primer grupo de países por afinidad ideológica pero es un caso diferente ya que no asigna misiones de seguridad pública a sus fuerzas armadas. A pesar de esto, este país sostuvo con mayor fuerza su oposición al concepto de cooperación disuasoria, basada en la división política existente entre los países que adoptan una perspectiva heterodoxa en materia económica y política, siendo Venezuela el ejemplo más radical, y aquellos defensores de la iniciativa privada –nacional y transnacional- con limitada intervención del estado. Así, en el acta de la I Reunión del Grupo de Trabajo sobre recursos naturales mencionada más arriba quedó registrada la intervención de este país, llamando a recordar que los países tienen el derecho a explotar sus recursos naturales conforme a sus propias políticas de medioambiente, desarrollo económico e inclusión social (CONSEJO DE DEFENSA SUDAMERICANO, 2014a). De similar manera, durante el Taller sobre recursos naturales organizado en Buenos Aires, en junio de 2014, este país intentó bajar las expectativas sobre un consenso alrededor de una estrategia disuasoria al destacar la importancia de que el CDS continúe basándose en el principio originario de cooperación defensiva por sobre el de seguridad colectiva que caracteriza a otros organismos (CDS, 2014b).

En suma, el CDS no produjo un documento definitivo y contundente sobre una visión común de la defensa anclada en su dimensión externa, asociada a la misión principal de las fuerzas armadas de garantizar la integridad territorial y la soberanía. Por el contrario, se limitó a aislar este tema tan controvertido creando dos consejos adicionales<sup>7</sup>, mientras individualmente los países miembros incrementaron la asignación de misiones domésticas para sus fuerzas armadas, inclusive aquellos como Argentina y Brasil, protagonistas de la doctrina hemisférica de la resistencia a la refuncionalización de los militares bajo la lógica de la seguridad multidimensional. Así, si bien el CDS no adoptó el concepto de seguridad multidimensional tampoco se posicionó claramente en favor de un concepto estratégico basado en la misión externa de las fuerzas armadas, el modelo disuasorio y la protección de los recursos naturales.

---

<sup>7</sup>Nos referimos al Consejo Sudamericano sobre el Problema Mundial de las Drogas y al Consejo Sudamericano en materia de Seguridad Ciudadana, Justicia y Coordinación de acciones contra la Delincuencia Organizada Transnacional.

## REFLEXIONES FINALES

Este artículo buscó atender a dos interrogantes, uno de orden conceptual y otro de tipo empírico. Así, en primer lugar, nos preguntamos qué implica la construcción de una identidad estratégica regional para los desarrollos conceptuales sobre cooperación en defensa, en particular para el concepto de comunidades de seguridad. En segundo lugar, buscamos analizar la labor del CDS desde su creación hasta la finalización de su plan de acción de 2015 en términos de ese objetivo innovador que el organismo se propuso, o puesto en otros términos: cómo se intentó crear esa identidad y qué resultados se obtuvieron.

La discusión conceptual resultó en la constatación de que la categoría de comunidad de seguridad no logra dar cuenta de la especificidad de la cooperación sudamericana en defensa, al menos del propósito que los miembros del CDS se plantearon en su creación. Retomando las formulaciones de Adler y Barnett sostuvimos que el concepto de comunidad de seguridad sirve más para analizar el déficit de confianza y la persistencia de la utilización de violencia limitada en la región que para reflexionar sobre la medida en la cual el CDS apunta a crear una identidad regional en defensa que se plantee como objetivo el logro de mayor autonomía estratégica, teniendo en cuenta que el organismo fue creado con ambas agendas. Ciertamente, resulta intuitivo pensar que sin confianza mutua y sin identificación común de misiones de las fuerzas armadas y amenazas comunes no puede existir una identidad estratégica regional, pero esos no son requisitos para la adopción de la regla de la seguridad colectiva y cooperativa, enfocada en la prevención de los conflictos internos y la defensa contra ataques armados externos. En contraste, cuando un conjunto de estados piensa en cooperar para impedir una penetración armada o lograr mayor autonomía estratégica de manera conjunta, el concepto de comunidad de seguridad muestra sus limitaciones.

Por lo tanto, el hecho de que los países de una región consigan o no dar lugar a una estrategia común de defensa con un concepto estratégico distintivo queda fuera del alcance del concepto comunidad de seguridad, entre otros motivos, porque el desarrollo de Adler y Barnett fue pensado para responder a lo que "seguridad" significaba para el área del Atlántico Norte en especial a mediados de los años noventa: la eliminación de guerras de alta y mediana escala y la estabilidad estratégico-militar del

sistema global, o sea, preocupaciones en torno al mantenimiento de cierto status quo. Por el contrario, si bien las preocupaciones que dieron lugar a la propuesta de creación del CDS incluían la necesidad de garantizar las relaciones pacíficas entre los países de la región, también figuraban otras inquietudes. En otras palabras, junto con el interés status quista de la paz regional, algunos países de la región piensan al CDS como una institución que se posiciona frente a otros dilemas, más propios del tipo de países que tiene una preocupación en torno de la autonomía estratégica.

Teniendo en consideración estos límites planteamos la necesidad de complementar el concepto con otros para poder dar cuenta de las especificidades del CDS, fundamentalmente los conceptos de identidad regional de defensa y comunidad estratégica. Ahora bien, el análisis de las actividades realizadas por el CDS y algunos de los entendimientos discutidos en el seno del organismo demostró que este no logró en sus primeros siete años consensuar los entendimientos fundantes de una identidad sudamericana de defensa. Desde nuestro punto de vista, esta agenda fue propuesta por aquellos países que compartían un interés por resistir la imposición de la agenda de seguridad hemisférica basada en la multidimensionalidad, pero estaba ausente una propuesta viable alternativa sobre cuál debía ser el concepto estratégico, un debate que aún no se ha resuelto ni siquiera al interior de los países. A nuestro entender, la utilización del lenguaje identitario fue contraproducente porque transmitió la idea de que se quería construir una cooperación más ambiciosa de lo que en realidad se está dispuesto a hacer. Sin embargo, no debe oscurecerse el hecho de que las actividades que se realizaron hasta el momento fueron inéditas en términos de cooperación regional en defensa, en particular, la puesta en funcionamiento de una mayor interacción entre los ministerios de defensa.

A grandes rasgos podemos identificar, entonces, que hubo dos agendas diferentes pero complementarias aunque no tuvieron el mismo respaldo político, por lo cual una acabó por avanzar más que la otra. La primera es la agenda de la seguridad cooperativa, que buscó generar mayores niveles de transparencia y de confianza entre los países miembros. Relacionado a ambas cuestiones se buscó también generar espacios de cooperación en temáticas no sensibles, tales como el mapeo de zonas de desastres naturales. Esta agenda tuvo el consentimiento de todos los países del CDS, independientemente de que, por diversos motivos, algunos tuvieron más participación que otros.

Del otro lado, hubo una agenda que dio especificidad al CDS, ya que a diferencia de las instituciones hemisféricas durante los años noventa y primeros años del 2000, en esta ocasión un grupo de países sostuvo el proyecto de que el CDS tratara un nuevo concepto estratégico con potencial autonomizante para la región, con implicancias sobre la concepción de la defensa y la correspondiente definición de las misiones militares. Países como Venezuela, Bolivia, Ecuador y Argentina, al igual que algunos sectores de Brasil, impulsaron la agenda de seguridad regional de la cooperación disuasoria. Esta se caracterizó por enfatizar la necesidad de que América del Sur definiera de manera autónoma sus intereses estratégicos y las estrategias para protegerlos. La fórmula se basó en tomar a los recursos naturales como objeto de seguridad amenazados por las estrategias de los países poderosos. Esta concepción no puede entenderse separada de lo que fue la oposición de algunos de estos países a que el concepto de seguridad multidimensional modificara las misiones militares desde la defensa externa –que debía ser delegada en las instituciones de seguridad internacional- hacia la seguridad pública.

Al mismo tiempo, debe tenerse en cuenta que esta oposición contrastó con la tendencia cada vez más marcada de algunas políticas domésticas de utilización de los militares en misiones internas, aunque se conservó como postura diplomática en los foros hemisféricos y en el marco del CDS. Esta contradicción expresa la ausencia de formulaciones estratégicas en los países de la región a respecto de escenarios de conflicto con actores estatales extra regionales, y la consecuente preferencia por misiones domésticas, inclusive en países como Argentina y Brasil, que tradicionalmente se opusieron a esa modificación doctrinaria.

# COMMUNITY AND IDENTITY IN REGIONAL DEFENSE COOPERATION: CONFLICTING VIEWS ABOUT STRATEGIC THINKING IN THE SOUTH AMERICAN DEFENSE COUNCIL.

## ABSTRACT

---

The article addresses the question of what type of defense cooperation did the South American Defense Council (SADC) put into practice, as a previous analysis to later evaluate the organism's both achievements and unfinished tasks. Our argument is that it had some successes regarding the cooperative security agenda, which is related to the security communities concept. On the contrary, the second agenda, based on the building of a strategic regional identity encountered serious obstacles. Even more concerning, those difficulties are connected to the persistence of an unresolved issue: which should be the strategic concept and the corresponding mission for the Latin American armed forces in a democratic and post cold war setting? In order to develop our argument we begin by discussing two concepts: security communities and strategic communities. Then, we analyze SADC activities in relation to cooperative security practices, as well as those that account for strategic thinking formulation, showing how they correspondingly relate to the two concepts. Finally, we discuss existing divergences of member countries' visions on the strategic regional identity in relation to the tendency to involve the armed forces in public security missions.

**Key words:** Security communities – South American Defense council – Strategic identity – Military missions

## REFERÊNCIAS

ADLER, Emanuel. The spread of security communities: communities of practice, self-restraint, and NATO's Post Cold War transformation. *European Journal of International Relations*, v. 14, n. 2, p. 95–230, 2008.

ADLER, Emanuel; BARNETT, Michael (Ed.) *Security Communities*. Cambridge: Cambridge University Press, 1998.

CONSEJO DE DEFENSA SUDAMERICANO (CDS). *Acta de la II Reunión Ordinaria de la Instancia Ejecutiva del CDS*. 2010. Disponible mediante requerimiento por email a basededadoscnds@gmail.com

CONSEJO DE DEFENSA SUDAMERICANO (CDS). *Acta de la I Reunión de la actividad 1.d Crear un Grupo de Trabajo para “proponer y consolidar Lineamientos estratégicos del CDS-UNASUR, para la construcción progresiva y flexible de una visión compartida de defensa regional*. 2014a. Disponible mediante requerimiento por email a basededadoscnds@gmail.com

CONSEJO DE DEFENSA SUDAMERICANO (CDS). *Acta de la II Reunión Grupo de Trabajo para formular un diagnóstico para proponer mecanismos de cooperación en materia de protección y defensa de los recursos naturales y la biodiversidad con base en las legislaciones de los países miembros de UNASUR*. 2014b. Disponible mediante requerimiento por email a basededadoscnds@gmail.com

CENTRO DE ESTUDIOS ESTRATÉGICOS DE DEFENSA (CEED). *Estudio Prospectivo Sudamerica 2025*. Primera Parte. Tomo I. Buenos Aires: CEED. 2015.

DEUTSCH, Karl. *Political Community and the North Atlantic Area*. Princeton: Princeton University Press, 1957.

DIAMINT, Rut. A New Militarism in Latin America. *Journal of Democracy*, v. 26, n. 4, p. 155-168, 2015.

FLEMES, Daniel; NOLTE, Detlef; WEHNER, Leslie. Una comunidad de seguridad regional en formación: la UNASUR y su Consejo de Defensa. *Revista de Estudios Internacionales*, v. 44, v. 17, p. 105-27, 2011.

FLEMES, Daniel; RADSECK, Michael. Creating Multilevel Security Governance in South America. *Working Paper 117*. GIGA Institute, 2009.

FORTI, Alfredo. *La Defensa y los Recursos Naturales en Suramérica Aportes para una Estrategia Regional*. 2014. Disponible em: <<http://www.ceedcds.org.ar/Espanol/09-Downloads/DEF-RRNN-ALFREDO-FORTI.pdf>>. Acceso en: 14 mar. 2015

FUCCILLE, Alexandre. Apontamentos para se pensar a segurança na América do Sul do século 21. In: CHAVES, Daniel; WINAND, Érica Cristina Alexandre; PINHEIRO, Lucas (Ed.). *Perspectivas e debates em Segurança, Defesa e Relações Internacionais*. Macapá: Editora da UNIFAP, 2015. p. 19-30.

LEITE, Lucas Amaral Batista. A América do Sul como comunidade de segurança: região autônoma e construção de identidade. *Brazilian Journal of International Relations*, v. 4, n.1, p. 92-110, 2015.

MEDEIROS FILHO, Oscar. Em busca de uma identidade regional de defesa: considerações sobre a estratégia de dissuasão extrarregional sul-mericana. *Revista Brasileira de Estudos Estratégicos*, v. 1, n. 3, p. 49-70, 2013.

\_\_\_\_\_. Breve panorama de segurança na América do Sul. In: NASSER, Reginaldo Mattar; MORAES, Rodrigo Fracalossi de. *O Brasil e a segurança em seu entorno estratégico*. Brasília: IPEA, 2014. p. 21-42.

OELSNER, Andrea. Pluralistic security communities in Latin America. In: MARES, David R.; KACOWICZ, Arie (Ed.). *Routledge Handbook of Latin American Security*. New York: Routledge, 2015. p. 84-173.

POULIOT, Vincent. *International Security in Practice: the politics of NATO-Russia diplomacy*. Cambridge: Cambridge University Press, 2010.

RAMALHO DA ROCHA, Antonio Jorge. Sudamérica en camino de formar una comunidad en seguridad: perspectivas de cooperación regional en defensa desde la visión brasileña. In: *Fortalecimiento de la cooperación en seguridad entre Bolivia, Brasil, Chile, Colombia, Ecuador y Perú: hacia una Comunidad en Seguridad*. Lima: IDEI-PUCP, 2015. p. 31-53.

\_\_\_\_\_. Tres pasos para avanzar en la construcción de una comunidad en seguridad en Suramérica. In: CANCELADO, Henry, et. al. *El proceso de construcción de una comunidad en seguridad entre Bolivia, Brasil, Chile, Colombia, Ecuador y Perú*: Red de Política de Seguridad. Lima: IDEI-PUCP, p. 30-101, 2016.

RIQUELME RIVERA, Jorge. La relación entre integración y seguridad en el MERCOSUR y sus proyecciones hacia Sudamérica. *Revista de Relaciones Internacionales, Estrategia y Seguridad*, v. 8, n. 1, p. 279-308, 2013.

SAINT-PIERRE, Héctor Luis; SILVA, Diego Lopes da. A Torre de Babel Sul-Americana: a importância da convergência conceitual para a cooperação em defesa. In: CARMO, Corival Alves do. *Relações Internacionais: olhares cruzados*. Brasília: FUNAG, 2013. p. 281-350.

SAINT-PIERRE, Héctor Luis; SILVA, Diego Lopes da. Percepções de Segurança Regional no âmbito da UNASUL: o Conselho de Defesa Sul-americano. In: AYERBE, Luis Fernando (Ed.). *Territorialidades e entrecruzamentos geopolíticos na América Latina*. São Paulo: Cultura Acadêmica, 2014. p. 43-220.

TEIXEIRA, Augusto Wagner Menezes. O Brasil e o Conselho de Defesa Sul-Americano: pensamento estratégico, comunidade de segurança e dissuasão regional. In: OLIVEIRA, Marco Aurelio Guedes de (Ed.). *Cultura de defesa Sul-americana*. Recife: Editora Universitária UFPE, 2013. p. 48-323.

TEIXEIRA JÚNIOR, Augusto Wagner Menezes. Contribuições do Conselho de Defesa Sul-Americano para a Cooperação Militar. *Revista Política Hoje*, v. 24, n. 1, p. 57-70, 2015.

TIBILETTI, Luis. Las distintas ofertas de identidades estratégicas en los países de UNASUR y su impacto en la búsqueda de una identidad de defensa suramericana. *Revista Brasileira de Estudos de Defesa*, v. 1, n. 1, p. 13-37, 2014.

VITELLI, Marina. Argentina, Brasil y la defensa en América del Sur: las identidades estratégicas y la seguridad regional. *Cuadernos de Política Externa*, n. 121, 2015.

\_\_\_\_\_. América del Sur: de la seguridad cooperativa a la cooperación disuasoria. *Foro Internacional*, v. 56, n. 225, p. 55-724, 2016.

Recebido em: 10/09/2016

Aceito em: 09/12/2016





# STATE-SPONSORED CYBER-OFFENCES

Marcelo A. O. Malagutti<sup>1</sup>

## ABSTRACT

---

In the post-industrial societies, computers are ubiquitous and pervasive. Besides, they are interconnected. As these characteristics give unprecedented productivity, they also present risks never faced before. Cyber offences pose the threat of powerful nations, both in the military and economic dimensions, being confronted by much weaker states, or even proto-states or terrorist groups. At the same time, *cyber superpowers* have the ability of remotely and surreptitiously coerce opponents without deploying troops in the field. This paper outlines the threats posed by state-sponsored cyber-offences and analyzes their characteristics, describing their applications in the light of some traditional military concepts, and also their motivations, the nature of their operations, the *warriors* and the *weapons* used.

**Keywords:** Cyber. Offences. Power Projection. Area Denial. Software Power.

---

<sup>1</sup>Master in Arts in War Studies candidate at the Department of War Studies of King's College London, London, United Kingdom. E-mail: marcelomalagutti@yahoo.com.br.

## INTRODUCTION

Cyber-offences' perpetrators, generically called *hackers*, have been divided into four different groups: cybercriminals (sometimes subdivided into individuals and organized as distinct groups), hacktivists, terrorists, and nation-states. Each of these groups has different motivations, scope of actions, targets, and resources, and thus deterrence and dissuasion options (MALAGUTTI, 2016b). Although clearly possible to concede that any of these groups could be state-sponsored, and used in an escalation strategy to destabilize an opponent state, this work will focus on the direct threats posed by nation-states to their peers, considering their motivations, the nature of their operations, the *warriors* and the *weapons* used so far.

## THE MOTIVATIONS

Nation-states have many motives to promote cyber-offences. The Snowden case revealed some. The first one has been political espionage, related to the personal communications of the Brazilian and Mexican Presidents, the German Chancellor, and some of their Ministers, amongst thousands of others. Outside the political realm, Snowden also revealed the espionage of Petrobras, the Brazilian state-owned oil company, that a couple of years before had announced the discovery of massive oil reserves in Brazilian waters (GREENWALD, 2014). A third real motivation connects to security and defence through surveillance, with bulk collection of metadata regarding phone calls, e-mails, messaging, file transfer and many more communication methods (GREENWALD, 2014; HIMR..., 2011; OPERATIONAL..., 2016). All of the above examples relate to *intelligence gathering*.

Besides the motives presented, related to "peacetime", there are also the traditional wartime military motivations of *projection of power* and *area denial* on the cyber domain. Cyber-offences perpetrated with existing technologies are unlikely to cause massive casualties directly (RID, 2012; RID; MCBURNEY, 2012). However, they could still serve as "effective means of political coercion or brute force" (LIFF, 2012). Influence and coercion of an opponent nation-state, by means of sabotage, if not an act of war, have been the aims of Stuxnet (DAVIS, 2015; FALLIERE; O'MURCHU; CHIEN, 2011; LANGNER, 2011; SANGER, 2012; ZETTER, 2011).

And then there is... financial profit! Until very recently this motivation had always been related to cybercriminals, and never to states. However, a series of attacks against the SWIFT network has been linked to North Korea (PERLROTH; CORKERY, 2016).

In the following pages, each of the above motivations is explored in larger detail.

## INTELLIGENCE GATHERING

For our purposes, we consider *intelligence gathering* as divided into two areas: *surveillance*, as the passive collection and analysis of information, and *espionage* as the active one.

### Surveillance

Communications Intelligence (often referred as COMINT) has always played a major role in security and defence matters. The Roman emperor Julius Caesar (100 BC to 44 BC) already used a transposition cypher algorithm, to avoid his enemies' understanding of captured messages (SINGH, 2000, p. 14-20).

A particular function of COMINT is *signals intelligence* (SIGINT). The Government Communications Headquarter (GCHQ), the agency responsible for SIGINT in the United Kingdom (UK), defines it as "intelligence derived from intercepted signals" (HIMR..., 2011, p. 9). It has become more and more relevant since the advent of the telegraph. GCHQ's website remarks the importance of the interception of the famous Zimmerman Telegram as one of the main reasons for the United States having entered WWI (OUR..., [201-?]). Radio communications made SIGINT even more important, and GCHQ's website also points the history of Bletchley Park, where Alan Turing and his team created Colossus, the first computer in history, that helped to decipher the German Enigma code, a valuable asset for winning WWII. The entire operational structure of Bletchley Park was based on "passive SIGINT", with the interception and transcription of every message sent by the Germans (bulk interception or collection), for subsequent analysis and deciphering. Thus, a surveillance operation.

History also shows that DARPA has sponsored the creation of the foundations of Internet. Moreover, the process of passive SIGINT based on the Internet nowadays is quite similar to that of WWII (HIMR..., 2011, p. 9-12).

In recent years, “the Internet is a major source of comparable intelligence power today” (OMAND, 2015). For the NSA it has become even easier, since

As the Internet developed, a large portion of the Internet backbone passed through the United States, meaning that many foreign-foreign communications could be accessed by surveillance done inside the US. Previously, foreign-foreign communications would have been accessed outside of the US, where the US Constitution and various laws are less strict than for access inside the US (SWIRE, 2015).

## Espionage

In the *cyber* context, however, intelligence gathering is not a passive task only. The UK Government has recently presented to the Parliament a case for keeping its bulk powers granted by Investigatory Powers Act 2000, not only for Bulk Interception but also for Bulk Interference (EQUIPMENT..., 2016). In its Code of Practice for Equipment Interference there is a list of activities allowed when there is “risk for the UK security” (OPERATIONAL, 2016, p. 7):

- a) obtain information from the equipment in pursuit of intelligence requirements;
- b) obtain information concerning the ownership, nature and use of the equipment in pursuit of intelligence requirements;
- c) locate and examine, remove, modify or substitute equipment hardware or software which is capable of yielding information of the type described in a) and b);
- d) enable and facilitate surveillance activity by means of the equipment.

It is important to observe that these activities do not need to be targeted to a particular computer, device, or even user. They can be conducted on sets of equipment, for instance in an entire building or village, anywhere in the world, if there is the suspicion of a “risk for the UK security” in that *area*.

Its counterpart, the U.S. NSA, has been granted the legal (by the American law) right to spy on 193 countries. The exception is their Five Eyes partners (Australia, Canada, New Zealand and the UK), considered “out of limits” by the Foreign Intelligence Surveillance Court under the Foreign Intelligence Surveillance Act of 1978 (KEDMEY, 2014).

Similarly, the U.S. Supreme Court has recently granted the

Federal Bureau of Investigations (FBI) the possibility of hacking computers worldwide, based only on warrants given by American judges. Until then, a judge in a U.S. state could only give orders limited to that state (KHANDELWAL, 2016; YADRON, 2016). One of FBI's missions is counter-intelligence. Thus, to defend the U.S. against espionage, FBI is legally authorized to hack computers outside the U.S.

What information is aimed by cyber espionage? It can be political, military or economic information from or about another government; or theft of trade secrets or intellectual property from private corporations or universities (CILLUFO; CARDASH; SALMOIRAGHI, 2012). Cyber theft of military technology from universities is not new, with a famous case having been reported already in 1989 by Clifford Stoll in his seminal *The Cuckoo's Egg* (STOLL, 1990). Indeed, in the early stages of the Internet.

The clear intent of economic espionage is "to increase the economic prosperity or viability of business concerns in a given state", and although state-directed, its "ultimate beneficiaries may be private or semi-private entities" (CILLUFO; CARDASH; SALMOIRAGHI, 2012).

The U.S. government frequently accuses China of "stealing" technical, military and economic information. American authors argue in the same direction, saying that "foreign intelligence services" engage in industrial espionage in support of private companies and that "an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress" is stolen every year "from networks maintained by U.S. businesses, universities, and government agencies" or that as national power is intimately connected with economic vitality, sustained intellectual property losses allegedly could erode U.S. power (LYNN, 2010).

Other recent cases show that the U.S. is not the only victim of this activity. The Norwegian intelligence service publicly accused the Chinese of stealing sensitive data and state military secrets from Norway-based firms (MURDOCK, 2016). The Swiss government has accused the Russians of being connected to the cyber espionage of the state-owned military supplier company RUAG (GOVCERT.CH, 2016). The Germans have accused the Russians of being behind attacks to the Bundestag (WAGSTYL, 2016a).

However, a European Parliament report released in 1999, and the facts revealed in the Snowden case in 2013, showed that the NSA is also engaged in economic espionage gaining "enormous advantage for American industry" (CAMPBELL, 1999; GREENWALD, 2014, p. 138).

Ultimate aims of espionage “include the desire to influence decisions, and affect the balance of power (regionally, internationally, and so on)” (CILLUFO; CARDASH; SALMOIRAGHI, 2012).

Indeed, during the recent U.S. presidential elections, the U.S. intelligence community has attributed to Russia the hacking of the e-mail accounts of members of the Democrat Party and the leaking of selected information in a way of favouring the Republican candidate, declaring the Russians intended to influence the results of the American presidential elections (PALETTA, 2016). The next day, President Obama stated the White House was studying ‘proportional’ responses, while the day after Mr. Sergei Lavrov, Russia’s Foreign Affairs Minister, said to CNN ‘we do not deny’, but ‘we have not seen a single fact’, a ‘single proof’. ‘If they decide to do something, let them do it’, said Mr. Lavrov (KREVER; SMITH-SPARK, 2016). The Republican candidate eventually won, although having more than one million votes less than the Democrat candidate. Just a week after the U.S. elections, the Chief of German Intelligence announced that Germany is worried about possible Russian influence in the German elections, to happen in 2017 (WAGSTYL, 2016b; GERMAN..., 2016).

## MILITARY AFFAIRS

In 1993, just after the end of the Cold War, Arquilla and Ronfeld declared “Cyber War Is Coming” (ARQUILLA; RONFELDT, 1993). Since then the debate about what would (or would not) constitute cyberwar, cyber weapons, cyber warfare, or cyber domain gained more and more space in the popular imagination, in the media, in policy making and the academia.

In this hype, there are considerations regarding the direct or indirect effects of a cyber attack in terms of lethality or physical harm to people, machinery or buildings, that could characterize the use of violence (CLARKE; KNAKE, 2010; MAHNKEN, 2011; RID, 2012; STONE, 2013). There are discussions regarding cyber as the fifth warfighting domain, after land, sea, air and space (ESTADOS UNIDOS, 2013; LIBICKI, 2012). The debate involves strategic and conceptual considerations, questioning if cyber would not be part of information or electronic warfare, or if it would not be considered just a force multiplier traversing all other domains ((KOPP, 2010; STONE, 2007; MAHNKEN, 2011; SHARMA, 2010; ESTADOS UNIDOS, 2013). There were also some more metaphysical considerations, as the fact of cyber being human-made while the four previous where God’s

creation, fortunately already grounded (DENNING, 2015; LIBICKI, 2009).

These discussions aside, the fact is the pervasiveness of information systems in modern armed forces has simultaneously “empowered and imperiled” military forces (ARQUILLA, 2011). To understand how, it is useful to analyse the role of cyber in some of the basic military functions.

### **Projection of Power and Area Denial**

In political science and military jargon *projection of power* consists in the ability to apply national power out of national boundaries. Military traditional examples include aircraft carriers and ballistic missiles. More recently *drones* have become a popular example.

It is reasonable to conceive that a CNA might be used by a state to project force without physically placing conventional military forces in the field, with lower costs and no risk of casualties (LIFF, 2012).

*Area denial* relates to denying the adversary the ability to bring into (or freely using within) the contested region its operational capabilities (RUSSELL, 2015). Traditional examples can be minefields, caltrops or the *dragon teeth* used on the famous Siegfried Line.

How to implement area denial in cyber? An immediate answer seems to be shutting down the Internet! As mentioned above, the creation of the Internet has been sponsored by DARPA. During the cold war, the U.S. military was worried about the risks of a nuclear first-strike from USSR to destroy the U.S. possibility of retaliation. Hence, the solution has been a development designed for resiliency.

While much of the physical infrastructure of cyberspace is relatively unprotected, located on beaches, along railways, and in buildings in densely populated areas, very little of that critical infrastructure is critical by itself. The nodes and cables may be relatively exposed and potentially vulnerable, none is singularly important to the entire system. The infrastructure consists of redundant cables and satellites for private sector communications and military operations. The logic programming of the data and telecommunications was designed to adapt to changing circumstance, to automatically route traffic through an alternate route when the first route is unavailable. This “self-healing” property of cyberspace makes it difficult to cause substantial damage without launching a full assault against the infrastructure (RUSSELL, 2015).



Thus, an attack aiming the destruction of the physical infrastructure of the cyberspace in a well-connected country is virtually impossible.

Besides, cyber power can be divided into two categories: *Software Power* and *Hardware Power* (MALAGUTTI, 2016b). As explained above, destroying the hardware could be ineffective for projecting power. Nevertheless, considering the *Software Power* perspective, it is not necessary to destroy hardware to achieve power projection or area denial.

A good example of *Software Power* capabilities is provided by Eligible Receiver, an exercise promoted by the U.S. Joint Chiefs of Staff in June of 1997 to test U.S. computer defences. The proposed scenario was that of a crisis that forced Washington to send troops and aircraft to South Korea quickly. Thirty-five specialists of the National Security Agency (NSA) composed the *red team*, simulating hackers in service of North Korea to subvert the American operation, using only publicly available equipment and information. In just two weeks, using only commercial computers and hacking programs downloaded from the Internet, they have been able to “simultaneously break into the power grids of nine American cities and crack their 911 emergency systems”. Established “civilian chaos and distracted Washington”, the *hackers* attacked the Pentagon’s computer networks and got access to 36 of them, becoming able to “roam freely across the networks, sowing destruction and distrust wherever they went”, for instance directing supplies to wrong destinations, possibly incapacitating last generation jet fighters due to the lack of fuel, replacement parts, or ammo (ADAMS, 2001).

Since the *hackers* have promoted their attacks remotely, without physical (or proximity) access to the targets, they have projected power. Moreover, since they have limited the operational capabilities of U.S. military forces, they have imposed area denial. Without physical destruction, since the networks were still there. However, they could not be trusted by the U.S. military.

## **Disruption and Force Multiplier**

There are two major concepts regarding the uses of military cyber capabilities. The first one relates to strategic cyber warfare, as the capacity of accomplishing huge effects in complete surprise. The second one relates to operational cyber warfare, used in support of conventional military in battle (ARQUILLA, 2011).

Operational cyber war has the potential to amplify physical operations, and it is relatively inexpensive, it is worth developing, although not only a question of technique but also requires the understanding of how potential opponents use information to wage war (LIBICKI, 2009, p. xx). As an example of operational cyber capabilities, allegedly the Chinese have an ingenious tactic for inserting computer viruses through the air into three models of reconnaissance and surveillance planes used by the U.S. Air Force. They wage the attack via electromagnetic waves targeting the onboard surveillance systems that emit a signal, what could disrupt the airplane's controls and cause its crash (HARRIS, 2014, p. 63).

Indeed, cyber attacks are unlikely to be decisive, and the damage (or disruption) caused by a successful cyber attack will probably be more ephemeral than a kinetic one since defenders may be able to recover the affected systems in short time. The greatest benefit of cyber warfare will probably come from its use in conjunction with, or as an enabler of, conventional kinetic military means, as Israel did in Operation Orchard in 2007 (LIFF, 2012; MAHNKEN, 2011; RID; MCBURNEY, 2012).

Command-and-Control (C2) for many non-cyber military capabilities is so heavily reliant on cyberspace that an opponent could be tempted to seek a crippling first-strike it (MORGAN, 2010). Perhaps the most significant effect of Eligible Receiver has been the fact that the *hackers* have also been able of paralyzing the human C2 system with high level of mistrust originated by fake orders from a commanding general, "bogus news reports on the crisis and instructions from the civilian command authorities".

As a result, nobody in the chain of command, from the president on down, could believe anything. This group of hackers using publicly available resources was able to prevent the United States from waging war effectively (ADAMS, 2001).

This process is usually referred as *decapitation*, intended to disrupt the internal cohesion of the adversary and that could potentially cripple the attacked state's defending military forces and increase the effectiveness of a subsequent kinetic attack (LIFF, 2012).

One way of avoiding decapitation of retaliatory cyber capabilities is decentralizing them, and both the Chinese and the American military, traditionally command-centric, seem to be working in the development of decentralized cyber capabilities. China is developing military cyber

capabilities in some of its militia units that compose the second level of reserves of their military forces, typically assigned to local civil defence tasks (AUSTIN, 2016b). The U.S. also plan to employ its second level of reserves, the National Guard, in cyber activities (AUSTIN, 2016b; SHALAL, 2016).

Cyber clearly offers a new set of resources to be used by military strategists for achieving political ends, either as force multipliers, incapacitating the enemy in preparation for kinetic strikes, or as strategic coercive tools to be used instead of kinetic strikes. Americans, Russians, and Chinese, among others, have published their defence strategies including cyber operations as part of their military capabilities and missions.

### **Coercion**

The anonymity provided by cyberspace also enables a flexible coercion strategy, allowing the compelling measure to be conducted privately and the victim to respond actions with “less concern about the influence of third parties or the demands of conclusive attribution” (HARE, 2012).

Coercion has been the purpose of Stuxnet, by means of sabotage, if not an act of war (FALLIERE; O’MURCHU; CHIEN, 2011; LANGNER, 2011; SANGER, 2012; ZETTER, 2011). For the first (known) time a software tool has been used by a nation-state to impose its political will onto another, using violence, as the physical destruction of machinery, and even direct lethality, as being used against a nation’s vital interest. Thus, in “Clausewitzian” terms, an act of war. Cyberwar. Stuxnet “succeeded in disrupting and delaying Iranian nuclear efforts, by some accounts to an extent rivalling the effects of a limited military strike” (KISSINGER, 2014, p. 345). Stuxnet might have been the U.S. option to avoid an Israeli air strike against the Iranian facilities at Natanz, similar to that of Operation Orchard, when Israeli jets bombed an alleged nuclear Syrian facility in the Deir ez-Zor area (SANGER; MAZZETTI, 2016).

Recently uncovered information shows that Stuxnet was the spearhead of a much larger operation named Nitro Zeus, “devised to disable Iran’s air defenses, communications systems and crucial parts of its power grid” (Ibid). Since Iran signed a nuclear control agreement, Nitro Zeus “has been shelved, at least for the foreseeable future” (Ibid). Had the compelling intent of Stuxnet not worked, a broader range of cyber attacks would have been triggered, in an escalation still in the cyber domain. This exemplifies a gradual shift

from tactical force multiplier to strategic warfare (SHARMA, 2010).

Not only the Americans have used cyber power for sabotage. In December of 2016 a power shortage in Ukraine has been caused by a series of cyber attacks attributed to Russia, that however not complex in structure have been well coordinated, leaving more than 80,000 people without energy (ZETTER, 2015).

## **Financial Profit**

Until very recently financial profit had always been considered an objective of cyber criminals, and not of states. A series of attacks on the SWIFT network, a Brussels-based banking consortium that runs what is considered the world's most secure payment messaging system, however, has been attributed to North Korea by the security firm Symantec. The attacks have been conducted thru banks in the Philippines, Vietnam, and Bangladesh. Even experienced security researchers declared never previously having seen attacks carried by a nation-state for stealing money (PERLROTH; CORKERY, 2016).

## **THE OPERATIONS**

The examples given characterize cyber operations. They are generically named Computer Network Operations (CNO) and can be divided into three subsets: Computer Network Exploitation (CNE), Computer Network Attack (CNA) and Computer Network Defence (CND) (EUROPEAN PARLIAMENT, 2011, p. 7). These types of CNO and its characteristics are detailed below. Intelligence gathering and spying CNO are often called CNE. A different kind of CNO is named CNA and aims to "destroy or otherwise incapacitate enemy networks" or the confidentiality, integrity and availability (the CIA triad) of information in the targeted networks (SCHNEIER, 2014). It is important to observe that the major difference between CNE and CNA regards their objective, since "technically speaking, CNA requires CNE to be effective. In other words, what may be preparations for cyber warfare can well be cyber espionage initially – or simply be disguised as such." (EUROPEAN PARLIAMENT, 2011, p. 7) Both CNE and CNA are offensive operations and consist, basically, of hacking opponent's computer networks (SCHNEIER, 2014). The last group of CNO, and the only defensive one, is named CND and

aims to defend computer networks from both CNE and CNA. Amongst the most frequently cited characteristics of CNOs are:

- Its asymmetry in comparison with conventional or nuclear weapons.
- The attribution difficulty and “plausible deniability”.
- The offensive advantage resulting from the difficulty of effective CND.
- The difficulty of deterring cyber attacks.

## THE WARRIORS

Freedman (2015, p. 228) posed the following question: “Might an army of software wizards use insidious electronic means to dislocate the support systems of modern societies, such as transport, banking and public health?”. Besides the importance of software power in this question, an interesting aspect of it is: who integrates this “army of software wizards”?

### Profile

As offensive operations are essentially hacking activities, the “software wizards” that perpetrate them are hackers.

The profile of a hacker fits that of the “ideology of violation” which “holds that things which it is possible to steal deserve to be stolen, and the security of things that are guarded ought to be tested to destruction by those with sufficient technical nous to do so” (BETZ; STEVENS, 2011, p. 34). They are classified according to the kind of hacking they practice. *White hats* (or *ethical hackers*) are non-malicious ones that “explore networks for their own enjoyment or testing its security on behalf of its owners”, who make their living “discovering holes in systems and then alerting the manufacturer or developer so that they can be patched”. *Black hats* (or *crackers*) are malicious hackers that “break into a system for some other purpose” (BETZ; STEVENS, 2011, p. 25; HARRIS, 2014, p. 67).

Progressively, hacking has become more objectively purposeful. [...] Criminals co-opted hackers for criminal purposes; governments co-opted them for purposes of state, including espionage and war; and hackers as human individuals have voluntarily attached themselves to all sorts of social movements and causes out of whim or conviction (BETZ; STEVENS, 2011, p. 33).

Hackers may “be off the government payroll but linked to a particular political faction or individual politicians (more likely in non-Western states)”. They may also be superpatriots with no formal connection with their government but “striking at adversaries in lieu of or in advance of where they are sure the government would go” or acting as proxies of their governments (LIBICKI, 2009, p. 46). However, cyber warriors are hackers in state employ, perhaps in uniform, acting “in the cause of specific policy objectives”, that can “be employed to create and operate malware, such as the Stuxnet worm” (BETZ; STEVENS, 2011, p. 26).

While private hackers are more likely “to use techniques that have been circulating throughout the hacker community”, “state hackers can tap a larger and more secretive research effort that can consolidate discoveries, tools, and techniques across their own organization”. They are also likely to be “disciplined in attacking certain targets for certain reasons and avoiding others that may look equally interesting but are not part of the plan” (LIBICKI, 2009, p. 47).

## Recruitment and Training

The recruitment of cyber warriors by U.S. armed forces and the NSA is very comprehensive. Each armed force branch has developed a set of aptitude tests “to determine whether someone might be suited to network maintenance and defence or shows promise for the rarer, more sophisticated offensive missions”. They have also inserted basic training in cyber security for all officers, while all “five military service academies now include cyber warfare as a field of study”. The best hackers of each one participate in a competition sponsored by the NSA, whose specialists act as a *red team* to test their skills. The final step in the “education of cyber warriors is on-the-job training” (HARRIS, 2014, p. 61).

The military have also “urged colleges and universities to teach cyber warfare”, and the NSA has worked together with some universities to help writing their curriculum. In some cases, candidate students have to pass a background check and get a security clearance, since “part of the coursework includes classified seminars at the NSA”, which in some cases even provide scholarships and monthly stipends for students of computer science that after graduation have to work for NSA. The undergraduate courses develop the basic and defence skills. The agency then complements the training for offensive operations (HARRIS, 2014, p. 66).

The recruitment happens even at undergraduate levels. A program

named CyberPatriot, a nationwide competition for middle and high school students, sponsored by the military and cosponsored by defence contractors, helps to identify young talents in the field. “NSA also recruits from the best computer science schools, including Stanford University and Carnegie Mellon. Additionally, it sends representatives to the most important annual hacker conventions, Black Hat and DefCon Las Vegas.” (HARRIS, 2014, p. 67)

The British GCHQ, by its side, works on the accreditation of Master (MSc) courses, having already 18 courses of 14 universities certified (OUR..., 2016).

## THE WEAPONS

The literature is plenty of different names for cyber threats: virus, worms, botnets, Trojans, malware, rogue code, logic bombs, and so on. However, all of them have two things in common: they consist of software (software power!), and they have to be somehow implanted in the targeted networks. An *implant* is a piece of software designed to activate or enable a subsequent action; in many cases, they allow the attacker to send (or load) attack code that the target system will run causing damage to its functions or integrity (LIBICKI, 2010). In this section we detail the main features of cyber-weapons.

### The Anatomy of Software Weapons (or the Cyber Kill Chain)

A typical modern Advanced Persistent Threat (APT) is a multi-phase attack software tool, for either CNA or CNE operations, usually based on the Intrusion Kill Chain (HUTCHINS; CLOPPERT; AMIN, 2010). Each phase relates to different functions performed at different times by the software for offensive actions. The seven original phases of the Intrusion Kill Chain have been rearranged in the thirteen steps of the Industrial Control Systems (ICS) Cyber Kill Chain, presented below (ASSANTE; LEE, 2015):

- *Reconnaissance*: consists in the examination, possibly with the support of human intelligence (HUMINT), of the target to find possible “weaknesses and identify information that supports attackers in their efforts to target, deliver and exploit elements of a system”.
- *Weaponization*: “includes modifying an otherwise harmless file”, such as



a PDF or MS Word document, “for the purpose of enabling the adversary’s next step”.

- *Targeting*: “is the process of analyzing and prioritizing targets and matching appropriate lethal and nonlethal actions to those targets to create specific desired effects”.

- *Delivery*: consists in the attacker finding a “method to interact with the defender’s network”, for instance, a phishing e-mail used to deliver a weaponized PDF.

- *Exploit*: “is the means the adversary uses to perform malicious actions”, for instance when the weaponized PDF is opened.

- *Install*: is the consequence of the well-succeeded exploitation, for instance when the opened weaponized PDF installs an implant or malware or connects a VPN.

- *Command and Control (C2)*: consists in establishing a connection to the previously installed capability (implant), for instance by abusing trusted communications such as the VPN, often by “hiding in normal outbound and inbound traffic, hijacking existing communications”.

- *Act*: can consist of many different actions; common activities include: discovery (and corruption) of new targets (application systems or data); “lateral movement around the network”; “installation and execution of additional capabilities”; data exfiltration; “anti-forensic techniques, such as cleaning traces of the attack activity”; and defending implant’s or attacker’s foothold when encountering defences or incident responders.

- *Attack Development and Tuning*: the attacker develops capabilities tailored to the specific target and for the aimed results.

- *Testing*: consists in testing the developed capabilities against a testing facility as similar as possible to the target environment, often based on information gathered in the previous steps.

- *Delivery*: consists in the delivery of the newly developed capabilities specific to the aimed target.

- *Installation*: is the installation (or modification) of the old software with new specific software capabilities.

- *Execution*: consists in running the software weapon to achieve the desired results.

The premise of this model is that “just one mitigation breaks the chain and thwarts the adversary. Therefore, any repetition by the adversary is a liability that defenders must recognize and leverage” (HUTCHINS; CLOPPERT; AMIN, 2010). APTs are usually well succeeded because defences are often based on pattern matching, and only able to



recognize events of some of the stages individually, but not the entire attack.

## Backdoors

Implants can be inserted into software as it is being developed, and can be used for creating remotely operated *kill switches* and *backdoors* written into the computer chips' firmware allowing outsiders to remotely manipulate the systems they run.

Already in 2001, U.S. intelligence officials believed "that certain hardware and software imported from Russia, China, Israel, India, and France" were infected with *devices* able to "read data or destroy systems", although the suspicion was hard to verify (ADAMS, 2001).

Recently, however, counterfeit hardware has been identified in systems procured by the U.S. DoD (LYNN, 2010). A U.S. House Permanent Select Committee on Intelligence report, in 2012, posed recommendations restricting the acquisition of networking equipment from Chinese companies Huawei and ZTE (BANACH, 2012). In December of 2015 Juniper Networks announced the discovery of a secret backdoor in the operating system of their firewalls (ZETTER, 2015). It has not become clear who did put that backdoor in the system.

## Intelligent Agents

APTs are perhaps the most sophisticated type of software weapons. The most famous one up to date is Stuxnet, which amongst many features it had is also "noteworthy for something it did not do": although an intelligent agent, it was not a *learning* agent. Machine-learning techniques are quickly developing, and a next generation agent could be able to *learn*. Indeed, as the "defence and intelligence establishments in the United States, Britain and Israel have traditionally been well ahead of general trends in computer science research", it "would be surprising if an intelligent coded weapon capable of learning had not been developed yet" (RID; MCBURNEY, 2012).

The same rationale on learning agents applies to defence systems. Back in 2009, the U.S. Department of Homeland Security published A Roadmap for Cybersecurity Research where it appointed the need for threat detection based on machine learning mechanisms to find outliers (ESTADOS UNIDOS, 2009, p. 39). This is usually called *active defence*.

## Asymmetry

The term *asymmetrical warfare* is sometimes used to characterize “countering an adversary’s strengths by focusing on its weaknesses” (ADAMS, 2001). It fits well in the idea of “no forced entry in cyberspace”, but simply the exploitation of the enemy’s vulnerabilities (LIBICKI, 2009, p. iii e xiv).

However, focusing on the adversary’s weaknesses would be wise in any conflict, not only in asymmetrical ones. The best definition, so, is that which considers *asymmetry* as the disparity between the powers of the opponents.

The costs of developing conventional or nuclear forces exert a dissuasion effect, by the futility of competing with the U.S. Navy in constructing carrier task forces and submarine fleets, for instance (NYE, 2012; RUMSFELD, 2002). The same idea applies to the development of missile defences. Besides the costs, there are the difficulties associated with the access to related technologies, as the seamless rocket tubes made of special alloys, needed for missile production, and the components required for the manufacture and operation of small nuclear reactors for carriers and submarines.

It is not difficult to imagine that a Stuxnet-like tool could be used to infect and disable missile defences of the U.S., Russia, China, India or Pakistan, for example. As Stuxnet has damaged the mechanical parts of the Iranian centrifuges, the same effect could be achieved in the steam turbines of nuclear subs. Alternatively, this worm could perhaps damage some mechanical component, preferably of difficult replacement, of missiles’ launching platforms. In these hypothetical ways, a tool whose cost would be in the tenths of millions would have disabled missile defences billions of dollars. Perhaps not even a worm would be necessary; just a backdoor could cripple the missile alert or launching systems for, say, half an hour.

This is the scenario usually associated with the concept of asymmetry related to Software Power, since “the barriers to entry in the cyber domain are so low that non-state actors and small states can play a significant role at low cost” (NYE, 2012).

The asymmetry is also created by the imbalance of attack space – larger, technologically dependent nations possess a larger network space with a greater number of weak spots vulnerable to attacks, while the smaller nation has a smaller network surface to protect (ARENG, 2014).

This turns into a situation where, even though great powers make larger investments in the development of cyber capabilities, small states still have more opportunity to compete in this domain than in traditional warfare, because “in modern warfare, ‘mass’ is no longer a decisive factor”, and “asymmetric warfare dilute the traditional power and dominance logic” (ARENG, 2014).

More to the point, it is precisely because others suffer inferiority in conventional conflict that they feel driven to emphasize cyberattacks as a way to even the score. Thus, the United States, for all its advantages, might suffer more than adversaries would if retaliation begets counterretaliation (LIBICKI, 2009, p. 32).

Software power, so, offers means for “Lilliputian States” (as also non-state actors) to develop their capabilities and face opponents that otherwise could not be confronted (ARENG, 2014). In defence terms, this has been captured by the World Economic Forum’s 2015 Network Readiness Index, which showed no G20 countries in the top five positions, occupied by Singapore, Finland, Sweden, Netherlands, and Norway respectively (AUSTIN, 2016a).

## Ephemeral Nature

The entire concept of cyber attack tools is based on the exploitation of vulnerabilities. It can be by means of the *weaponization* of an Adobe PDF or Microsoft Word file with malicious code, or possibly thru the exploitation of a backdoor installed in a network asset, like a router. However, when a vulnerability is reported to the software manufacturer, it releases *patches* to fix it. The same situation happens with Intrusion Detection Systems and anti-virus software. When the patch is applied that specific vulnerability becomes useless for that particular target, and another one needs to be found.

Clearly, an exploitation may have already occurred when the patch is applied, and an implant may have been already installed. However, supposing this implant has been designed to exfiltrate data by establishing a VPN, for instance, using privileges of a stolen user id and password, that password could be changed, ceasing the possibility of that implant to execute its mission.

Moreover, as long as long as this implant tries to use the now

invalid credentials, it would reveal itself to the defenders monitoring the network, allowing further attribution and its undesired effects. To avoid this situation, the implant may be intelligent enough to detect that the credentials are not valid and “commit suicide”, deleting itself to eliminate its traces and avoid forensics.

In any case, attacking tools are valid for a very specific scenario of vulnerabilities present in a particular combination of versions of the software: application, operating system, IDS and anti-virus, and their patches. An un-patched version of the operating system may be protected by the latest version of the anti-virus, and so on.

### **Unpredictable and Uncontrollable Propagation**

Cyber weapons are also integral to the globally interconnected cyberspace in which we are immersed. “The effects of attacks at one point can spread unpredictably, far beyond the target and even back to the attacker, given *the highly interdependent nature of cyberspace*.” (MORGAN, 2010)

One of the interesting aspects of Stuxnet is the fact that it infected an air-gapped network, or a system not connected to the Internet, indicating that it has possibly got its target thru a vast range of technical components, from an infected USB drive to off-the-shelf software or hardware components, as a plug-and-play driver or whatsoever (ARQUILLA, 2011).

The development of software weapons faces a tricky dilemma: should the aims be wide-and-shallow or narrow-and-deep? Essentially, achieving greater destructive potential will likely to significantly increase the development and deployment complexity, thus cost and time, while limiting potential targets, the risk of collateral damage and, hence, the political utility of the weapon (RID; MCBURNEY, 2012).

For some time it has been speculated that a programming error allowed Stuxnet to “escape” beyond the confines of its initial target’s networks. Currently, however, it is believed that its original mission, the destruction of the Iranian nuclear centrifuges, have been changed in a later version, allowing it to realize reconnaissance tasks, sending to its creators the IP addresses of machines infected by contractors working for the Iranians. The more “aggressive programming features” implemented in Stuxnet latest versions would have also increased the chances of it being discovered, as indeed it was in June 2010 by a small security company in Belarus (HARRIS, 2014, p. 46-47). “Escaped” or not it has

infected many information systems in more than 150 countries, and now it may be reengineered for other purposes (ARQUILLA, 2011). This is, indeed, an important “feature” of cyber weapons: its fast and uncontrolled proliferation. Langner even celebrated the fact that Stuxnet had been developed by the U.S.; the different levels of control implemented in it avoided a major strike on Industrial Control Systems using the same (or similar) targeted Siemens software worldwide (LANGNER, 2011).

### **U.S. Dominance (or the Software Superpower)**

During the Cold War, when the world was divided in two, Brodie defined the U.S. as a status quo nation: “determined to keep what it has, including existence in a world of which half or more is friendly or at least not sharply and perennially hostile” (BRODIE, 1959).

After the disintegration of the USSR, the U.S. has become an uncontested superpower in both conventional and nuclear force. Nowadays, it is still a status quo nation, but not with only a half of the world. Indeed,

[...] American leaders from both the Democratic and Republican parties have made it clear that they believe the United States, to quote Madeleine Albright, is the “indispensable nation” and therefore it has both the right and the responsibility to police the entire globe (MEARSHEIMER, 2010).

The U.S. software industry is the largest in the world, being a net exporter and concentrating many of the best code writers of the world; its universities’ computer science courses are top ranked, and the Pentagon is already working in public-private partnerships for creating superior military capabilities in the cyberspace (LIBICKI, 2009; LYNN, 2010; MORGAN, 2010; RID; MCBURNEY, 2012). Although there is considerable secrecy regarding U.S. attack capabilities, it is widely believed that U.S. cyber military capabilities are the best in the world.

The U.S. has just increased by 35% (\$19 billion dollars) its budget for cyber security policies, including \$3 billion for the creation of its new Cyber Reserve (AUSTIN, 2016a). It views supremacy in the “fifth domain” as essential to its mission, and has incorporated cyber attacks into conventional warfare. It has used them to disable infrastructure in other countries

in the same way they say to fear domestically (HARRIS, 2014, p. xxi).

Recently leaked Presidential Policy Directive 20 (PPD-20) “instructs the military to draw up a list of overseas targets “of national importance” where it would be easier or more effective for the United States to attack with a cyber weapon than a conventional one” (HARRIS, 2014, p. 54; ESTADOS UNIDOS, 2012). “On the spectrum of cyber hostilities, the United States sits at the aggressive end” (HARRIS, 2014, p. xxi). The best evidence is Stuxnet and Snowden cases.

## CONCLUSION

A thorough analysis of the available literature on cyber power and cyber deterrence, mostly written by authors from NATO partners, shows that it reflects an aggressive posture, based on the need of attacking tools that could both instil fear and impose dominance in the cyberspace. Moreover, the evidence presented by both Snowden and Stuxnet cases, as also Nitro Zeus, as that of the other cases analysed, support this perception.

So far, a few acts of coercion thru sabotage, but many reported cases of espionage, with the threat of influence on decision making. In other words, coercion. Dominant state actors so far are the members of the Five Eyes group (U.S., UK, Australia, Canada and New Zealand), and North Korea, India, Israel, Iran, and France, often cited in the active pole of cyber offences.

In the globalized economy of these days, every nation might have interests that conflict with at least one of the cited countries. Thus there is the need of protecting them accordingly. This requires long-term preparation, planning, and investments, typical on matters of national security and defence.

The good news is there are excellent commercial opportunities in the market of defence *Software Power* that can be explored by non-aggressive nations while they develop their defences.

# ATAQUES CIBERNÉTICOS PATROCINADOS PELO ESTADO

## RESUMO

---

Nas sociedades pós-industriais computadores são ubíquitos e pervasivos. Adicionalmente, são interconectados. Enquanto essas características atribuem produtividade sem precedentes, elas também apresentam riscos nunca antes enfrentados. Ofensas cibernéticas introduzem a ameaça de que nações poderosas, tanto na expressão militar quanto naquela econômica, sejam confrontadas por estados muito mais fracos, ou ainda por protoestados ou grupos terroristas. Ao mesmo tempo, superpotências cibernéticas desenvolvem a habilidade de remota e subrepticiamente coagir oponentes sem a necessidade de empregar tropas no teatro de operações tradicional. Este artigo delinea as ameaças postas por ofensas cibernéticas patrocinadas por estados e analisa suas características, descrevendo suas aplicações à luz de alguns conceitos militares tradicionais, bem como suas motivações, a natureza de suas operações, dos *guerreiros* e das *armas* usadas. **Palavras-chave:** Ciberespaço. Ofensas. Projeção de poder. Negação de área. Software Power.

## REFERENCES

ADAMS, J. Virtual Defense. *Foreign Affairs*, v. 80, n. 3, p. 98, 2001.

ARENG, Liina. *Lilliputian states in digital affairs and cyber security*. Tallin: CCDCOE, 2014. Tallin Paper, n.4. Disponível em: <[https://ccdcoe.org/sites/default/files/multimedia/pdf/TP\\_04.pdf](https://ccdcoe.org/sites/default/files/multimedia/pdf/TP_04.pdf)>. Acesso em: 16 fev. 2016.

ARQUILLA, John; RONFELDT, D. Cyberwar is coming! *Comparative Strategy*, v. 12, n. 2, p. 141–165, 1993.

ARQUILLA, John. From blitzkrieg to bitskrieg: the military encounter with computers. *Communications of the ACM*, v. 54, n. 10, p. 58-65, Oct. 2011.

ASSANTE, M. J.; LEE, R. M. *The industrial control system cyber kill chain*. [s.l.]: SANS Institute Reading Room, Oct. 2015. Disponível em: <<https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>>. Acesso em: 7 jun. 2016.

AUSTIN, G. Middle powers and cyber-enabled warfare: the imperative of collective security. In: ASIAN SECURITY CONFERENCE - SECURING CYBERSPACE: ASIAN AND INTERNATIONAL PERSPECTIVES, 18., 2016, New Delhi. *Anais...* New Delhi: IDSA, Feb. 2016a

\_\_\_\_\_. Strategic culture and cyberspace: Cyber militias in peacetime?. *The Diplomat Magazine*, Tokyo, 12 Feb. 2016b. Disponível em: <<http://the-diplomat.com/2016/02/strategic-culture-and-cyberspace-cyber-militias-in-peacetime/>>. Acesso em: 16 fev. 2016.

BANACH, W. *Investigative report on the U.S. National security issues posed by Chinese telecommunications companies Huawei and ZTE*. Washington: U.S. House of Representatives, 8 Oct. 2012. Disponível em: <[https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20\(FINAL\).pdf](https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf)>. Acesso em: 12 jun. 2016.

BETZ, D.; STEVENS, T. *Cyberspace and the state: towards a strategy for cyber-power*. London, U.K: Routledge for the International Institute for Strategic Studies (IISS), 2011.

BRODIE, B. The anatomy of deterrence. *World Politics*, v. 11, n. 02, p. 173-191, jan. 1959.

BUCHANAN, B. *The Cybersecurity dilemma: Hacking, trust and fear between nations*. United Kingdom: C Hurst & Co Publishers, 2017.

CAMPBELL, D. *Development of Surveillance Technology and Risk of Abuse of Economic Information Part 2/5*. Brussels: European Parliament, 1999. Disponível em: <[http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN\\_ET\(1999\)168184\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET(1999)168184_EN.pdf)>. Acesso em: 26 set. 2016.



CILLUFFO, F.; CARDASH, S.; SALMOIRAGHI, G. A blueprint for cyber deterrence: building stability through strenght. *Military and Strategic Affairs*, v. 4, n. 3, p. 3–23, 2012.

CLARKE, R. A.; KNAKE, R. K. *Cyber war: the next threat to national security and what to do about it*. New York: HarperCollins Publishers, 2010.

DAVIS, P. Deterrence, influence, cyber attack and cyberwar. *International Law and Politics*, v. 47, n. 327, p. 327–355, 2015.

DENNING, D. Rethinking the cyber domain and deterrence. *Joint Forces Quarterly*, v. 77, n. 2nd Quarter, p. 8–15, 2015.

EQUIPMENT interference code of practice: pursuant to section 71 of the regulation of Investigatory powers act 2000. London: TSO, 28 Jan. 2016. Disponível em: <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/496069/53693\\_CoP\\_Equipment\\_Interference\\_Accessible.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496069/53693_CoP_Equipment_Interference_Accessible.pdf)>. Acesso em: 6 jun. 2016.

ESTADOS UNIDOS. Department of Homeland Security. *A roadmap for cybersecurity research*. Washington: US Department of Homeland Security, Nov. 2009. Disponível em: <<https://www.dhs.gov/sites/default/files/publications/CSD-DHS-Cybersecurity-Roadmap.pdf>>. Acesso em: 8 dez. 2016.

ESTADOS UNIDOS. Joint Chiefs of Staff. *JP 3-12 (R) cyberspace operations*. Washington: Joint Chiefs of Staff, 2013. Disponível em: <[http://www.dtic.mil/doctrine/new\\_pubs/jp3\\_12R.pdf](http://www.dtic.mil/doctrine/new_pubs/jp3_12R.pdf)>. Acesso em: 16 fev. 2016.

ESTADOS UNIDOS. White House. *Presidential Policy Directive/PPD-20*. Oct. 2012. Disponível em: <<https://fas.org/irp/offdocs/ppd/ppd-20.pdf>>. Acesso em: 14 fev. 2016.

FALLIERE, N.; O MURCHU, L.; CHIEN, E. *W32.Stuxnet Dossier*. [s.l.]: Symantec, Feb. 2011. Version 1.4. Disponível em: <[https://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf)>. Acesso em: 7 dez. 2015.

FREEDMAN, L. *Strategy: a history*. United States: Oxford University Press, 2015.

GCHQ certifies six more masters' degrees in Cyber security. *GCHQ*, 23 May 2016.

GERMAN intelligence services 'alarmed' about potential Russian interference in elections. *DW.COM*, Deutsche Welle, 16 nov. 2016. Disponível em: <<http://www.dw.com/en/german-intelligence-services-alarmed-about-potential-russian-interference-in-elections/a-36413582>>. Acesso em: 17 nov. 2016.

GOVCERT.CH. *APT case RUAG*: technical report. [s.l.]: MELANI, 23 May 2016. Disponível em: <[https://www.melani.admin.ch/dam/melani/it/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report\\_Ruag-Espionage-Case.pdf](https://www.melani.admin.ch/dam/melani/it/dokumente/2016/technical%20report%20ruag.pdf.download.pdf/Report_Ruag-Espionage-Case.pdf)>. Acesso em: 6 jun. 2016.

GREENWALD, G. *No place to hide*: Edward Snowden, the NSA and the surveillance state. United Kingdom: Hamish Hamilton, 2014.

HARE, F. The significance of attribution to cyberspace coercion: a political perspective. INTERNATIONAL CONFERENCE ON CYBER CONFLICT (CYCON), 4., 2012. *Anais...* Tallin: IEEE, 5 jun. 2012.

HARRIS, S. *@War: the rise of the military-internet complex*. United States: Eamon Dolan/Houghton Mifflin Harcourt, 2014.

HIMR Data Mining Research Problem Book. [s.l.]: GCHQ, 20 Sept. 2011. Disponível em: <<https://fveydocs.org/document/hmr-data-mining/>>. Acesso em: 3 mar. 2016.

HUTCHINS, E. M.; CLOPPERT, M. J.; AMIN, R. M. *Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains*. Bethesda: Lockheed Martin Corporation, 2010. Disponível em: <<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf>>. Acesso em: 26 nov. 2015.

- KEDMEY, D. Report: NSA authorized to spy on 193 countries. *Time*, 1 July. 2014.
- KHANDELWAL, S. U.S. Supreme court allows the FBI to hack any computer in the world. *The Hacker News*, 28 Apr. 2016.
- KISSINGER, H. *World order*. United States: Penguin Group (USA), 2014.
- KOPP, C. The four strategies of information warfare and their applications. *IO Journal*, v. 1, n. 4, p. 28–33, Feb. 2010.
- KREVER, M.; SMITH-SPARK, L. Lavrov denies Russian influence over US election. CNN, 12 Oct. 2016.
- LANGNER, R. *Cracking Stuxnet, a 21st-century cyber weapon*. TED Talks, 29 Mar. 2011. Disponível em: <[https://www.ted.com/talks/ralph\\_langner\\_cracking\\_stuxnet\\_a\\_21st\\_century\\_cyberweapon?language=en](https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en)>. Acesso em: 12 set. 2015
- LIBICKI, M. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: Rand Corp, 2009.
- \_\_\_\_\_. Cyberspace is not a Warfighting Domain. *I/S: A Journal of Law and Policy for the Information Society*, v. 8, n. 2, p. 321–336, 2012.
- \_\_\_\_\_. Pulling Punches in Cyberspace. In: National Research Council (U.S.). Committee on Detering Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. *Proceedings of a workshop on deterring cyberattacks*, Washington, D.C: National Academies Press, 2010. p. 123–147.
- LIFF, A. P. Cyberwar: a new “absolute weapon”? the proliferation of cyberwarfare capabilities and interstate war. *Journal of Strategic Studies*, v. 35, n. 3, p. 401–428, June. 2012.
- LORD, Kristin M.; SHARP, Travis (Ed.). *America’s Cyber Future: Security and Prosperity in the Information Age*. Washington, D.C: CNAS, June, 2011. v. 1. Disponível em: <[http://www.cnas.org/sites/default/files/publications-pdf/CNAS\\_Cyber\\_Volume%20II\\_2.pdf](http://www.cnas.org/sites/default/files/publications-pdf/CNAS_Cyber_Volume%20II_2.pdf)>. Acesso em: 2 fev. 2016.

LYNN, W. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, v. 89, n. 5, Sept. 2010.

MALAGUTTI, M. *Cybersecurity in practice (part.I): software power*. Strife Blog, 2 Nov. 2016a. Disponível em: <<http://www.strifeblog.org/2016/11/02/cybersecurity-in-practice-part-i-software-power/>>. Acesso em: 2 nov. 2016.

\_\_\_\_\_. O papel da dissuasão no tocante a ofensas cibernéticas. *Doutrina Militar Terrestre em Revista*, v. 9, p. 18–27, July 2016b.

MEARSHEIMER, J. J. The gathering storm: China's challenge to US power in Asia. *The Chinese Journal of International Politics*, v. 3, n. 4, p. 381–396, 1 Dec. 2010.

MORGAN, P. M. Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm. In: National Research Council (U.S.). Committee on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. *Proceedings of a workshop on deterring cyberattacks*. Washington, D.C: National Academies Press, 2010. p. 55 – 76.

MURDOCK, J. Cyber-espionage: norway's intelligence chief accuses china of stealing military secrets. *Technology*, 1 Mar. 2016.

NYE, Joseph. *Cyber war and peace*. Project Syndicate, 10 Apr. 2012. Disponível em: <<http://www.project-syndicate.org/commentary/cyber-war-and-peace>>. Acesso em: 9 jan. 2016.

OMAND, David. *Understanding digital intelligence and the norms that might govern it*. Centre for International Governance Innovation and Chatham House, Canada, Mar. 2015. Paper Series, n. 8. Disponível em: <[https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no8.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no8.pdf)>. Acesso em: 10 mar. 2016.

OPERATIONAL case for bulk powers. GOV.UK, mar. 2016. Disponível em: <[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/504187/Operational\\_Case\\_for\\_Bulk\\_Powers.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf)>. Acesso em: 3 mar. 2016.

OUR history. GCHQ, [201-?]. Disponível em: <<http://www.gchq.gov.uk/history/Pages/index.aspx>>. Acesso em: 10 mar. 2016.

PALETTA, D. U.S. Blames Russia for recent hacks. *The Wall Street Journal*, 7 Oct. 2016.

PERLROTH, N.; CORKERY, M. North Korea linked to digital attacks on global banks. *The New York Times*, 27 May 2016.

RID, T. Cyber war will not take place. *Journal of Strategic Studies*, v. 35, n. 1, p. 5–32, Feb. 2012.

RID, T.; BUCHANAN, B. Attributing Cyber attacks. *Journal of Strategic Studies*, v. 38, n. 1-2, p. 4–37, 23 Dec. 2014.

RID, T.; MCBURNEY, P. Cyber-Weapons. *The RUSI Journal*, v. 157, n. 1, p. 6–13, Feb. 2012.

RUMSFELD, D. H. Transforming the military. *Foreign Affairs*, v. 81, n. 3, p. 20, 2002.

RUSSELL, A. Strategic anti-access/area denial in cyberspace. In: INTERNATIONAL CONFERENCE ON CYBER CONFLICT: ARCHITECTURES IN CYBERSPACE, 7., 2015. *Anais...* Tallinn: NATO/CCDCOE, 2015. Disponível em: <[https://ccdcoe.org/cycon/2015/proceedings/11\\_russell.pdf](https://ccdcoe.org/cycon/2015/proceedings/11_russell.pdf)>. Acesso em: 8 jun. 2016.

SANGER, D. E. Obama ordered wave of Cyberattacks against Iran. *Middle East*, 1 June. 2012.

SANGER, D. E.; MAZZETTI, M. U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. *Middle East*, 17 Feb. 2016.

SCHNEIER, B. Computer network exploitation vs. computer network attack. *Schneier on Security*, 10 Mar. 2014. Disponível em: <[https://www.schneier.com/blog/archives/2014/03/computer\\_networ.html](https://www.schneier.com/blog/archives/2014/03/computer_networ.html)>. Acesso em: 28 nov. 2015

SHALAL, A. U.S. National guard may join cyber offense against Islamic state: Carter. *Reuters*, 6 Mar. 2016.

SHARMA, A. Cyber wars: A paradigm shift from means to ends. *Strategic Analysis*, v. 34, n. 1, p. 62–73, 5 Feb. 2010.

SINGH, S. *The code book: the science of secrecy from ancient Egypt to quantum Cryptography*. United States: Knopf Doubleday Publishing Group, 2000.

STOLL, C. *The cuckoo's egg: tracking a spy through a maze of computer espionage*. London: The Bodley Head, London, 1990.

STONE, J. Cyber war will take place! *Journal of Strategic Studies*, v. 36, n. 1, p. 101–108, Feb. 2013.

\_\_\_\_\_. Technology and war: a trinitarian analysis. *Defense & Security Analysis*, v. 23, n. 1, p. 27–40, Mar. 2007.

SWIRE, P. *US surveillance law, safe harbor, and reforms since 2013*. [s.l.: s.n.]. 2015. Disponível em: <<https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf>>. Acesso em: 3 mar. 2016.

WAGSTYL, S. German security head warns of election interference from Russia. *Financial Times*, 16 Nov. 2016b.

\_\_\_\_\_. Germany points finger at Kremlin for cyber attack on the Bundestag. *Financial Times*, 13 May 2016a.

YADRON, D. Supreme court grants FBI massive expansion of powers to hack computers. *The Guardian*, 3 May 2016.

ZETTER, K. Everything We Know About Ukraine's Power Plant Hack. *WIRED*, 20 Jan. 2016.

\_\_\_\_\_. How digital detectives deciphered stuxnet, the most menacing malware in history. *WIRED*, 11 July 2011.

\_\_\_\_\_. Secret code found in juniper's firewalls shows risk of government backdoors. *WIRED*, 18 Dec. 2015.

Recebido em: 22/09/2016

Aceito em: 09/12/2016



# PLANEJAMENTO OPERACIONAL: O COMPONENTE CONCEITUAL DO PLANEJAMENTO COMO FUNDAMENTO PARA A CONSTRUÇÃO DE LINHAS DE AÇÃO

Rodolfo Castelo Branco Wadovski<sup>1</sup>

José Claudio da Costa Oliveira<sup>2</sup>

## RESUMO

---

O planejamento de Operações Conjuntas militares tem uma lógica em que o planejador foca seu esforço inicialmente na compreensão do problema e posteriormente na busca por soluções. Para o esforço inicial, os conceitos da Arte Operacional são utilizados em um processo denominado Abordagem Operacional. Este artigo trata da utilidade da Arte / Estratégia Operacional para lidar com os problemas complexos típicos das Operações Conjuntas, apresentando uma proposta de método para a condução da Abordagem Operacional, bem como apontando algumas correspondências de terminologia entre as doutrinas militares brasileira e estadunidense.

**Palavras-chave:** Arte Operacional, Estratégia Operacional, Abordagem Operacional, Operações Conjuntas, Planejamento, Problemas Complexos.

---

<sup>1</sup> Doutorando, Programa de Doutorado da Coppead, Rua Pascoal Lemme, 355, Rio de Janeiro, RJ. E-mail: rodolfo.wadovski@coppead.ufrj.br

<sup>2</sup> Doutor em Ciências Navais, Instrutor de Estratégia da Escola de Guerra Naval, Av. Pasteur, 480, Urca, Rio de Janeiro, RJ. E-mail: oliveira@egn.mar.mil.br



## INTRODUÇÃO

Apesar de os conflitos estarem sendo cada vez mais permeados por aspectos tecnológicos, são ainda os seres humanos que têm que compreender o problema e construir soluções apropriadas. Os embates entre os oponentes de um conflito ocorrem sob a influência da moral e das emoções humanas, com todas as suas complicações e inconsistências. Nesse contexto, a liderança é uma das causas primordiais do resultado final. A dimensão humana permanece fundamental, mas ao longo das últimas décadas a complexidade dos conflitos vem aumentando, particularmente pela necessidade de realizar operações envolvendo mais de uma força armada e outros atores não militares (USMC, 1997; BRASIL, 2011).

Em sintonia com esse entendimento, as Forças Armadas dos Estados Unidos da América (EUA) orientam que os comandantes de suas forças conjuntas e seus estados-maiores desenvolvam seus planos conjugando arte e ciência por meio da aplicação dos conceitos da *Operational Art* e do *Operational Design*. Essa filosofia auxilia a força conjunta a estruturar como seus meios serão empregados para alcançar o estado final desejado (UNITED STATES, 2012). Segundo o manual *Joint Operation Planning* (JP5) (2011b), a *Operational Art* é a abordagem cognitiva de um comandante e seu estado-maior para o desenvolvimento de estratégias, enquanto que o *Operational Design* é o processo de concepção e construção de uma estrutura que oriente um plano para uma operação de grande envergadura.

No mesmo sentido, a doutrina brasileira considera fundamental o amplo entendimento da situação pelo comandante e seu estado-maior, sendo fundamental “a determinação desses chefes militares para impor a vontade nacional sobre os eventos” (BRASIL, 2011, p. 73). A Arte Operacional, também denominada Estratégia Operacional (BRASIL, 2007), é entendida como “um conjunto de conceitos relacionados ao emprego de meios militares e não militares em um Teatro de Operações (TO) para conceber uma campanha ou simplesmente uma operação militar” (BRASIL, 2012, p. 1).

É possível conjecturar que a natureza humana aliada às características das operações militares, particularmente aquelas que envolvem mais de uma força, bem como outros atores civis, possui um

elevado grau de complexidade, tanto para seu entendimento quanto para sua solução. A Arte Operacional se propõe a lidar com essa complexidade, tentando reduzir as incertezas e ambiguidades do ambiente operacional. Cada vez mais a sua utilidade vem sendo reconhecida para conjugar arte e ciência para a compreensão de problemas complexos que envolvem atores heterogêneos. A utilização dos seus conceitos vem ganhando espaço nos últimos anos em Forças Armadas de diversos países. Entretanto, estes autores, ao longo de suas vivências na Escola de Guerra Naval, no Rio de Janeiro – RJ, Brasil, e na *Joint Forces Staff College*, em Norfolk – VA, EUA, têm observado que alguns conhecimentos demandam maior aprofundamento. Três pontos se destacam: a diferenciação entre o que é compreensão e o que é solução de um problema, a ausência de um método claro para o processo de compreensão de um problema e algumas dificuldades para a correta associação entre as nomenclaturas brasileira e norte-americana.

Este trabalho, fundamentado em pesquisa bibliográfica de natureza qualitativa, tem três propósitos. Primeiro, iluminar a utilidade da Arte Operacional para a compreensão e solução de problemas complexos relacionados às operações conjuntas, enfatizando a separação entre a compreensão e a solução do problema. Segundo, apresentar um método para a condução do processo de compreensão do problema. Terceiro, esclarecer algumas diferenças importantes de terminologia entre as doutrinas dos EUA e do Brasil.

Para atingir esses propósitos, primeiramente abordaremos as diferenças entre as naturezas dos problemas simples e complexos. Em seguida, visitaremos alguns conceitos da doutrina norte-americana e veremos o *Design* e o *Planning* como partes complementares para a resolução de problemas. Posteriormente, apresentaremos um método para o desenvolvimento do processo de *Design*. Por fim, à luz da visão brasileira comparada à norte-americana, esclareceremos alguns pontos referentes à nomenclatura.

## **PROBLEMAS SIMPLES E PROBLEMAS COMPLEXOS. NÍVEL TÁTICO E NÍVEL OPERACIONAL**

Conforme David Wagman (2006), as formas de solucionar problemas simples e complexos não são totalmente incompatíveis.

Entretanto, problemas simples possibilitam uma abordagem mais direta. Segundo Rittel e Webber (1973), podemos perceber que um problema é complexo quando ele possui algumas peculiaridades, tais como:

- Não existe uma forma padrão para formular um problema complexo. A cada passo em direção a uma solução, a percepção do problema muda.
- Não há solução “certa” ou “errada”. O que pode haver são resultados “bons” ou “ruins”.
- Chegar a um acordo entre todos os atores interessados de qual é o problema e qual seria uma solução adequada pode ser um grande desafio.
- Assim como um terremoto produz tremores secundários, a solução de um problema complexo pode trazer consequências imprevisíveis.
- Após a implementação de uma solução, provavelmente não será possível voltar atrás.
- São normalmente problemas únicos, que estão sendo analisado pela primeira vez.
- Normalmente as soluções de problemas complexos têm forte impacto na vida de pessoas.

Para exemplificar, imaginemos o reparo da pista do Aeroporto Santos Dumont, no Rio de Janeiro. Pode ser um problema difícil de resolver, por envolver uma série de atividades, como a interdição dos voos, o deslocamento de pessoal e material para realizar o reparo e a necessidade de atender exigências técnicas rigorosas do piso da pista. Mas essa dificuldade não pode ser confundida com complexidade.

Comparando com o reparo da pista, um problema bem mais complexo seria a construção de outra pista naquele aeroporto, que teria que responder a uma série de questões intrincadas, tais como: haveria aterro? Esse aterro influenciaria o fluxo de água na Baía da Guanabara, alterando o trânsito de navios? O aumento do fluxo de passageiros exigiria mudanças no tráfego no Centro da cidade? As rotas das aeronaves interfeririam com o Aeroporto Tom Jobim? Quais seriam os órgãos públicos envolvidos no planejamento?

Comparando-se os dois e destacando as questões que necessitam ser resolvidas, isto é, as exigências de um planejamento abrangente, a diversidade de atores envolvidos e as possibilidades de solução, pode-

se dizer que o reparo da pista é um problema simples em relação ao segundo caso, que seria um problema complexo. Note-se que não estamos analisando se o problema é fácil ou difícil.

De forma semelhante, podemos comparar um problema do Nível Tático<sup>3</sup> com um do Nível Operacional<sup>4</sup>. O problema tático (por mais difícil que seja) tende a ser mais simples que o operacional, pois este exige análise abrangente e participação de mais atores no planejamento do que um problema tático. Exemplificando, por mais difícil que seja o problema tático de realizar minagem em litoral hostil, a decisão de realizar ou não essa operação dentro do Teatro de Operações<sup>5</sup> exige uma compreensão mais ampla no Nível Operacional, havendo necessidade de considerar as implicações diplomáticas, interferências com outras forças e aspectos logísticos, dentre outros fatores. Relativizando, poderíamos dizer que o problema tático é simples e o problema operacional é complexo.

Ora, se o problema no Nível Operacional é, por natureza, complexo, a sua forma de planejamento exige uma abordagem mais ampla do que o problema tático. E é justamente nessa abordagem ampla que se evidencia a necessidade de dedicar-se de modo abrangente ao estudo do ambiente e do problema de modo a possibilitar ao comandante estabelecer as diretrizes gerais que orientarão seu estado-maior na busca por alternativas de solução apropriadas. Em outras palavras, a conclusão do estudo do comandante irá inspirar a confecção detalhada de Linhas de Ação (LA) em harmonia com a visão do comandante.

Fica evidente então a existência de duas grandes fases no planejamento operacional: a compreensão do problema e a construção de soluções para esse problema.

---

<sup>3</sup> Nível Tático: nível responsável pelo emprego de frações de forças militares, organizadas, segundo características e capacidades próprias, para conquistar objetivos operacionais ou para cumprir missões específicas (BRASIL, 2007).

<sup>4</sup> Nível Operacional: nível que compreende o planejamento militar e a condução das operações requeridas pela guerra, em conformidade com a linha estratégica estabelecida (BRASIL, 2007).

<sup>5</sup> Teatro de Operações: parte do teatro de guerra necessária à condução de operações militares de grande vulto, para o cumprimento de determinada missão e para o consequente apoio logístico (BRASIL, 2007).

## DESIGN E PLANNING: A VISÃO NORTE-AMERICANA

As publicações militares doutrinárias norte-americanas destacam que a resolução de um problema complexo passa por duas grandes “partes”: o *design* (compreensão) e o *planning* (solução). Esse entendimento pode ser resumido nas seguintes ideias:

- Compreensão e solução são qualitativamente diferentes, ainda que atividades inter-relacionadas essenciais para a resolução de problemas complexos (UNITED STATES, 2010).
- Apresentado um problema, o Estado-Maior (EM) frequentemente se apressa diretamente na busca de uma solução sem entender claramente o ambiente complexo da situação, o propósito do envolvimento militar e a abordagem requerida para resolver as questões centrais (UNITED STATES, 2010).
- Enquanto o *design* foca no entendimento sobre a natureza de um problema não familiar, o *planning* foca na geração de um plano (uma série de ações executáveis) (UNITED STATES, 2010).
- O comandante inicia o desenvolvimento de seu *design* ao receber a missão. Como resultado, o *design* foca na concepção do problema e não no desenvolvimento de Linhas de Ação (LA) (UNITED STATES, 2010).

Se para a resolução de problemas complexos, ou seja, se no planejamento no Nível Operacional foi identificada a necessidade de duas grandes “partes” (*design* e *planning*), o que faria a ligação entre as duas? Como o comandante poderia conduzir a sua concepção do problema (*design*) de modo a passar a seu EM o seu entendimento da situação? A partir de que base, de que orientação o EM iniciaria a construção de soluções (*planning*), isto é, de Linhas de Ação? O planejamento conjunto buscaria construir soluções com qual entendimento comum do problema?

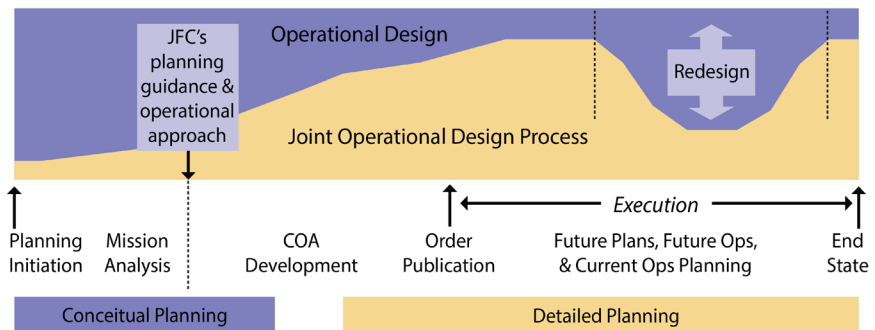
Uma resposta está no *Operational Design*, que procura fazer uma ponte entre o *design* e o *planning*, entre a compreensão do comandante e as possíveis soluções (Course of Actions - Linhas de Ação) a serem propostas pelo seu EM.

A doutrina norte-americana entende *Operational Design* como a concepção e construção de uma estrutura intelectual que sustenta o planejamento de uma campanha ou operação de grande vulto e sua subsequente execução, ampliando a visão da arte operacional por meio de um processo criativo que ajuda os comandantes e planejadores a definir objetivos, estratégias, meios e riscos (USA, 2011b; USA, 2011c; USA, 2012).

O *Operational Design* busca uma abordagem sistêmica do ambiente operacional para identificar nódulos, junções e pontos de interconexão que servirão de foco para as ações dentro das LA. Ações contra esses pontos são arranjadas para atingir efeitos desejados, que por sua vez visam objetivos que conduzem a um estado final desejado (USA, 2010; USA, 2011b; USA, 2011c).

Indo além, ao concluir o *Operational Design*, o Comandante permite que outros atores não militares (agências governamentais, organismos internacionais, ONG etc.) que participam da operação tenham uma compreensão comum do que deve ser resolvido e tenham condições de construir soluções convergentes (USA, 2011a).

Em que momento se desenvolve o *Operational Design*? Na verdade, o *design* não é algo a ser completado, mas um processo vivo. Entretanto, como pode ser observado na figura 1, o *design* predomina fortemente nas fases iniciais. No caso do processo de planejamento conjunto norte-americano (*Joint Operations Planning Process – JOPP*), que tem sete passos (*Planning Initiation, Mission Analysis, Course of Action (COA) Development, COA Analysis and Wargaming, COA Comparison, COA Approval and Plan or Order Development*), os dois primeiros passos são dedicados ao *design* e outros passos ao *planning* (USA, 2011c) (Fig. 2).



Adaptado pelos autores (2011)

Figura 1: o processo do *Operational Design* (USA, 2011c).

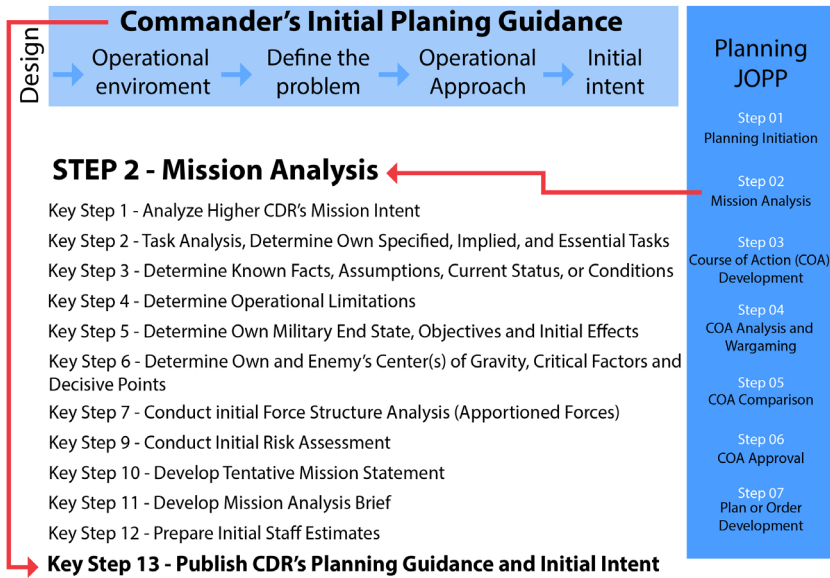


Figura adaptada pelos autores (2011)

Figura 2: o design e o planning no processo de planejamento conjunto dos EU

O *Operational Design* é um processo, cujo resultado final, na doutrina norte-americana, recebe a denominação de *Operational Approach*. É importante ter em mente que o *Operational Design* (processo) resulta no *Operational Approach* (produto), materializado no *Commander's Planning Guidance*. O *Operational Approach* pode ser representado em um desenho que apresenta de forma resumida os principais conceitos discutidos no processo, como Estado Final Desejado (EFD), Objetivos, Centro de Gravidade (CG), Pontos Decisivos (PD) e Linhas de Operação (LO). Essa representação gráfica do *Operational Approach* visa ajudar os planejadores a visualizar inter-relacionamentos que devem existir dentro da operação. A sua confecção pode agregar detalhes, tais como alvos ou outras tarefas que apoiem o alcance de PD.

Aqui já é importante frisar um aspecto fundamental: o *Operational Design* foi criado para fazer uma ligação entre o *design* e o *planning*. Ele é concluído (evidentemente poderá ir sendo atualizado posteriormente) após a *Mission Analysis*, antes das *Course of Action*.

## UM MÉTODO PARA O DESENVOLVIMENTO DO PROCESSO DE DESIGN

Então o *Operational Design* faz uma ponte entre a compreensão do problema e suas soluções (Linhas de Ação). Mas como fazer esse *Operational Design*? Nas publicações estadunidenses não está claramente definido como fazê-lo. Apresentaremos a seguir uma proposta para conduzir o processo do *Operational Design* elaborada por Keith D. Dickson, professor de Estudos Militares do Joint Forces Staff College (DICKSON, 2011). O processo sugerido é constituído de oito passos:

### 1 - Definir o Estado Final Desejado (EFD)

O *Operational Design* inicia-se com a Análise da Missão. Três produtos dessa análise: EFD, Objetivos e CG (próprio e do inimigo) são essenciais e devem ser completamente compreendidos porque proveem foco para os subsequentes esforços de planejamento.

### 2 - Definir os Objetivos<sup>6</sup> que conduzem ao EFD

Objetivos descrevem o que deve ser atingido para alcançar o EFD. Algumas vezes Objetivos tornam-se Pontos Decisivos (PD) no *Operational Design* porque eles são essenciais não somente para alcançar o EFD, mas críticos também para afetar o CG inimigo ou proteger o próprio CG. Em suma, enquanto Objetivos podem ser PD, PD não são sinônimos de Objetivos. Objetivos se referem ao EFD, enquanto PD se referem ao CG.

### 3 - Definir os Efeitos desejados que apoiem os Objetivos

Efeitos definem condições que devem existir na conquista dos Objetivos. Um Efeito é um estado físico ou comportamental de um sistema que resulta de uma ação ou outro efeito.

### 4 - Identificar os CG próprio e do inimigo

A identificação das Vulnerabilidades Críticas (VC) do CG inimigo permite a determinação de PD relacionados ao ataque a essas VC.

### 5 - Identificar os PD que permitam atingir o CG inimigo e proteger o CG próprio

PD originam-se da análise do EFD, Objetivos e CG. Em termos gerais, PD são algo pelo qual o comandante deverá lutar. Algumas vezes os PD estão relacionados com tarefas porque estas descrevem o que deve ser feito para o sucesso da missão. Tarefas específicas podem tornar-se PD.

<sup>6</sup>Na nossa doutrina seriam os Objetivos Operacionais, derivados dos Objetivos Estratégicos (BRASIL, 2011).



Há PD que são comumente definidos na maioria das operações, como por exemplo, localidades geográficas, situação aérea favorável, proteção de linhas de comunicação e C2 inimigo neutralizado. Há também aqueles PD que são únicos para cada circunstância, provenientes do exame dos CG próprio e do inimigo.

**6 – Identificar Linhas de Operação (LO) que descrevem como os PD estão relacionados entre si e como deverão ser alcançados, de modo a atingir o CG inimigo**

As LO devem derivar dos PD. A natureza dos PD relacionados a uma LO define a LO. Este é o porquê dos PD serem definidos antes das LO. A importância de bem definir e compreender as LO é básica para integrar PD, CG, Objetivos e EFD. Claramente definidas, as LO proveem clareza e racionalidade a todas as ações do comandante. As LO devem ser definidas em termos amplos para possibilitar um modo mais flexível de pensamento.

As LO podem ser de duas categorias: Física e Lógica (Tab. 1). LO podem ser também uma combinação de LO Física e LO Lógica.

*Tabela 1: LO Física e Lógica.*

LO Física	LO Lógica
<ul style="list-style-type: none"> <li>• Tipicamente utilizada para o <i>design</i> de operações de combate. Relacionadas com os requisitos ou os componentes do Comando Conjunto.</li> <li>• Orientação da Força no Tempo e no Espaço em relação ao inimigo.</li> <li>• Estruturam operações que geralmente consistem em uma série cíclica, de curto prazo e executadas dentro de uma moldura temporal finita.</li> </ul>	<ul style="list-style-type: none"> <li>• Particularmente útil para trabalhar no ambiente interagências e multinacional.</li> <li>• Coletivas e descritivas na sua natureza e referem-se a condições.</li> <li>• Posição relativa da Força em relação ao inimigo é menos relevante (operações de estabilização ou contra insurgência).</li> <li>• Foca na representação lógica do arranjo de tarefas, efeitos e/ou objetivos.</li> </ul>

Fonte: Elaborado pelo autor

7 - Identificar como os PD estão relacionados com as fases da operação a fim de identificar como as operações estão estruturadas no tempo, espaço e efeitos.

A partir deste passo, o planejador pode examinar como e onde certos PD apoiam mais de uma LO. O faseamento ajuda a sequenciar os eventos no tempo, espaço e efeitos e examinar eventos chave relacionados com PD e compreender a sequência das ações. Esse sequenciamento dos PD auxilia no delineamento das fases, que por sua vez possibilita ao Comandante estabelecer sua Intenção por fases.

8 - Completar a sincronização e integração detalhada das forças, requisitos (C2, Inteligência, apoio de fogo, movimento e manobra, proteção e sustentação)<sup>7</sup>, tarefas, alvos e efeitos centrados nos PD e fases para obter unidade de esforço.

Os PD devem ser examinados a fim de identificar alvos a eles relacionados e efeitos nesses alvos que conduzam ao alcance desses PD. Alvos são priorizados e designados às Forças Componentes, as quais devem coordenar ações para apoiar o alcance de cada PD.

Cada PD é relacionado aos outros PD para possibilitar uma visão completa do que está ocorrendo no ambiente operacional no espaço e no tempo. Isso permite a coordenação entre os elementos militares e não-militares da operação, bem como a definição de responsabilidades.

Uma vez que as fases são definidas em termos de PD, a Intenção do Comandante<sup>8</sup> por fases pode ser completada, esboçando claramente o que está acontecendo, definindo quem apoia e quem é apoiado e definindo prioridade de esforços.

Estes autores entendem que esse método pode ser adaptado ao Processo de Planejamento Conjunto (PPC), uma vez que a metodologia e os conceitos utilizados não conflitam com o entendimento geral encontrado na doutrina brasileira. O método é útil por estruturar em um processo sequencial a análise dos Elementos Operacionais<sup>9</sup>.

---

<sup>7</sup>No PPC, "os requisitos retratam, geralmente, aspectos ofensivos, defensivos, de apoio, de inteligência, de logística, de comando e controle e de adestramento, relacionados aos princípios de guerra, às diretrizes emanadas do escalão superior, às características da área de responsabilidade e aos próprios meios" (BRASIL, 2006, v. 2, p. 36).

<sup>8</sup>A Intenção do Comandante é estabelecida ao final da Fase 1 da Etapa 1, em que o comandante estabelece o enunciado da sua missão, bem como delinea a forma como ele visualiza para que suas forças sejam empregadas (BRASIL, 2011).

<sup>9</sup>Segundo a publicação Manual de Estratégia Operacional, Volume 1, Componentes da Estratégia Operacional (EGN-601), existe uma série de elementos utilizados na Arte/Estratégia Operacional, dentre eles: Teatro de Guerra e Teatro de Operações, Estado Final Desejado, Objetivos Operacionais, Esforços Operacionais, Base de Operações, Centro de Gravidade, Capacidades Críticas, Requisitos Críticos, Vulnerabilidades Críticas, Linhas de Operação, Pontos Decisivos, Alcance Operacional, Ponto Culminante, Pausa Operacional e Guerra de Manobra (BRASIL, 2012).

A figura 3 apresenta um exemplo hipotético de um esquema gráfico construído seguindo os passos desse método.

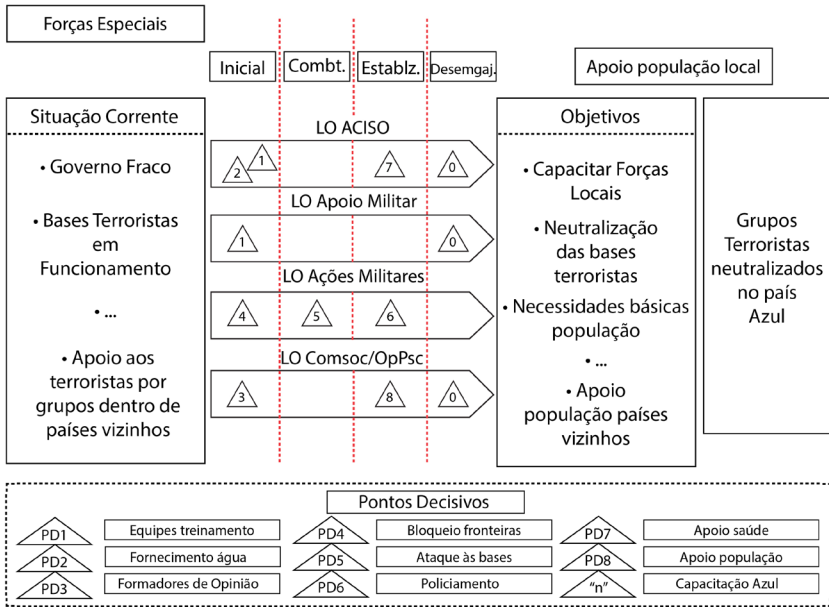


Figura elaborada pelos autores

Figura 3: exemplo hipotético de gráfico construído seguindo os passos do método do professor Dickson.

## DESIGN E PLANNING: A VISÃO BRASILEIRA

O que até agora foi tratado neste artigo sobre a visão norte-americana serve para entender a perspectiva brasileira. As doutrinas dos dois países, particularmente em relação à complexidade dos problemas no Nível Operacional e o enfoque no planejamento em duas “partes” (*design e planning*) seguem a mesma lógica. Veremos que as diferenças estão em boa parte relacionadas à nomenclatura.

No que tange à complexidade dos problemas, no caso brasileiro, podemos afirmar que, enquanto uma Força Naval atuando no Nível Tático pode utilizar o Processo de Planejamento Militar (PPM), uma Força Conjunta no Nível Operacional deve utilizar o Processo de Planejamento Conjunto (PPC). Em que pese o PPC ser muito semelhante ao PPM, o PPC

agrega os conceitos da Arte/Estratégia Operacional.

Em relação à divisão do planejamento em duas “partes”, o que se chama *design* e *planning* nos EUA equivale ao que no Brasil se denomina respectivamente por “Componente Conceitual do Planejamento Operacional” e “Componente Detalhado do Planejamento Operacional”. No caso do PPC brasileiro, o processo de *design* é forte na Fase 1 (Análise da missão e considerações preliminares) da Etapa 1 (Exame da Situação), resultando na Diretriz de Planejamento. A Fase 2 (A Situação e sua compreensão) da Etapa 1 também exerce uma forte influência no *Design*, o que demanda uma constante atualização na Diretriz de Planejamento.

Todo o processo de *design*, que a doutrina dos EUA chama de *Operational Design*, é denominado na doutrina brasileira de Abordagem Operacional. Já o produto do *Operational Design*, que a doutrina norte-americana denomina *Operational Approach*, materializado no *Commander's Planning Guidance*, a doutrina brasileira materializa na Diretriz da Planejamento. Assim como na doutrina dos EUA o resultado do *Operational Design*, isto é, o *Operational Approach*, normalmente é apresentado por meio de um esquema gráfico para auxiliar a visualização por todos da concepção do problema pelo Comandante, na doutrina brasileira o resultado do processo da Abordagem Operacional pode ser apresentado graficamente, em que a denominação desse esquema gráfico, no entendimento destes autores, deve ser nomeado “Representação Gráfica da Abordagem Operacional”.

Outro ponto essencial para a associação entre os conceitos da doutrina norte-americana e brasileira está na correta interpretação do item 3.1.1, do Anexo A, do Volume 1 do manual MD-30-M-01: “O Desenho Operacional é a representação gráfica da síntese das Linhas de Ação (LA) que o Comandante no nível operacional desenvolveu junto ao seu Estado-Maior Conjunto” (BRASIL, 2011, p. 79).

O que o manual MD-30-M-01 chama de Desenho Operacional é a representação gráfica da síntese da LA escolhida, tendo como eixo das abscissas o tempo. Não é o *Operational Design* da doutrina norte-americana. O Desenho Operacional mencionado nessa publicação militar brasileira é construído na Fase 3 (Possibilidades do inimigo, linhas de ação e confronto) da Etapa 1 do PPC e não deve ser confundido com o que denominamos de Representação Gráfica da Abordagem Operacional, que se refere às fases anteriores. Especificamente em relação à definição desse conceito, seria conveniente deixar explícito no texto do manual que esse

Desenho Operacional é fruto de um processo que se desenrolou durante a Abordagem Operacional e se consolidou após a elaboração da Linha de Ação. O esquema a seguir sintetiza as duas “partes” do planejamento de problemas no Nível Operacional, apontando as semelhanças e diferenças entre as doutrinas do Brasil e dos EUA (Fig. 4).

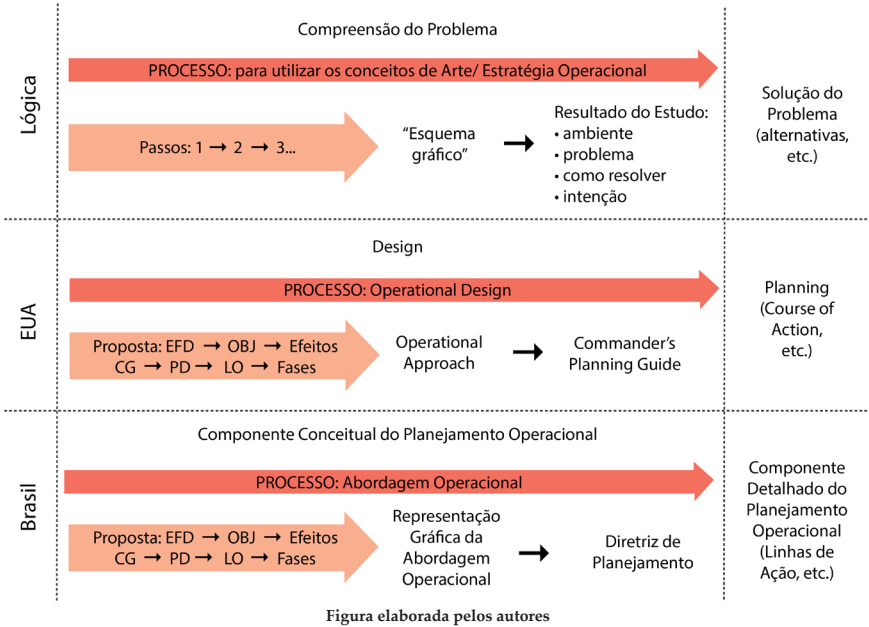


Figura 4. Esquema comparativo dos processos de planejamento.

## CONCLUSÃO

As operações no Nível Operacional são caracterizadas por um elevado grau de complexidade. A Arte/Estratégia Operacional, por meio do estudo conduzido durante o processo da Abordagem Operacional, auxilia na compreensão de problemas complexos e na realização de uma análise mais integradora das variadas questões e atores envolvidos. A percepção de que problemas complexos exigem um grande esforço inicial na sua compreensão, levou as doutrinas militares a visualizar o planejamento em duas grandes “partes”, conhecidas no Brasil por: “Componente Conceitual do Planejamento Operacional” e “Componente Detalhado do Planejamento Operacional”. Uma apropriada compreensão do problema permite o detalhamento de melhores soluções.

A Abordagem Operacional ajuda o comandante a definir sua visão estratégica, sendo útil como um guia geral para a operação por levar em conta as necessidades de atores militares e não-militares. Com a Abordagem Operacional, o comandante e seu EM podem criar diversas LA afinadas com a intenção do comandante e com o mesmo entendimento de EFD, CG, PD e LO. Não é demais frisar que o processo da Abordagem Operacional é anterior à confecção das LA: a Abordagem Operacional facilita a estruturação da análise do problema e sua compreensão, a qual irá inspirar a criação de LA condizentes com a situação em questão.

Para a condução do processo da Abordagem Operacional, é importante contar com um método que facilite a estruturação lógica dos conceitos da Arte Operacional. A definição sequencial do EFD, Objetivos, Efeitos, CG, PD, LO e a compreensão global de seus interrelacionamentos dentro da concepção geral do problema é fundamental. Estes autores julgam que o método de oito passos apresentado facilita a aplicação do intelecto e da imaginação dos planejadores para lidar com Elementos Operacionais dentro das complexidades do Nível Operacional.

Dentro do escopo da Arte Operacional, enquanto a lógica das doutrinas do Brasil e dos EUA são semelhantes, no que se refere à terminologia há que se ter alguns cuidados. Especial atenção deve ser prestada aos termos norte-americanos “*Design*”, “*Planning*”, “*Operational Design*” e “*Operational Approach*”, que na doutrina brasileira são respectivamente tratados por “Componente Conceitual do Planejamento Operacional”, “Componente Detalhado do Planejamento Operacional”, “Abordagem Operacional” e “Representação Gráfica da Abordagem Operacional”. Também crítico é não confundir o que a doutrina brasileira chama de “Desenho Operacional” com o “*Operational Design*” norte-americano.

A principal limitação desta pesquisa está associada ao pequeno número de trabalhos escritos sobre o tema, particularmente sobre as peculiaridades brasileiras. Muitas referências utilizadas aqui são manuais militares, que, em que pese seu valor para a disseminação do conhecimento e utilização prática por comandantes militares, não são estudos acadêmicos em sentido stricto. Uma oportunidade de pesquisa futura está no aprofundamento dos conceitos de cada um dos Elementos Operacionais, especialmente a integração de todos eles ao final do processo da Abordagem Operacional. Outra lacuna do conhecimento pode ser preenchida com um estudo a respeito da utilização efetiva dos resultados da Abordagem Operacional na confecção das Linhas de Ação.

# OPERATIONAL PLANNING: THE CONCEPTUAL COMPONENT OF PLANNING AS A FOUNDATION FOR BUILDING LINES OF ACTION

## ABSTRACT

---

The planning of a military Joint Operation has a logic where the planner focuses first on understanding the problem and then on searching for a solution. For the understanding part, the Operational Art's concepts are utilized through a process named Operational Design. This article deals with the usefulness of the Operational Art to address the complex problems of Joint Operations and presents a proposal of a method to conduct the Operational Design, as well as it points out some correspondences between the terminology of the Brazilian and North-American military doctrines.

**Keywords:** Operational Art, Operational Design, Joint Operations, planning, complex problems.

## REFERÊNCIAS

BRASIL. Ministério da Defesa. *Doutrina de Operações Conjuntas*: MD-30-M-01. Brasília, DF: MD, 2011. v.1 e v.2.

BRASIL. Ministério da Defesa. *Glossário das Forças Armadas*: MD35-G-01. Brasília, DF: MD, 2007.

BRASIL. Escola de Guerra Naval. *Manual de Estratégia Operacional*: EGN-601. Rio de Janeiro, RJ, 2012.

BRASIL. Estado-Maior da Armada. *Manual de planejamento operativo da Marinha* (EMA-331), Brasília, DF, 2006.

DICKSON, Keith. *Operational Design: A Methodology for Planners*, Norfolk, VA, 2011.

RITTEL, Horst; WEBBER, Melvin. Dilemmas in a General Theory of Planning. *Policy Science*, n. 4, p. 155-169, 1973.

UNITED STATES. JCS. *Joint Operations: JP-3.0*. Washington, DC, 2011.

UNITED STATES. JCS. *Joint Operation Planning: JP-5.0*. Washington, DC, 2011.

UNITED STATES. JCS. *Joint Planner's Handbook for Operational Design*. Suffolk, VA, 2011.

UNITED STATES. JFCS. *Operational Art and Campaigning, Primer AY 09-10*, Norfolk, VA, 2010.

UNITED STATES. *The Joint Staff Officer's Guide*, Norfolk, VA, 2012.

UNITED STATES. Marine Corps. *Warfighting: MCDP 1*. 1997.

WAGMAN, David C. Wicked Problems. *Power Engineering*. 01 may 2006.

Recebido em: 17/05/2016

Aceito em: 09/12/2016





# **A PROPRIEDADE INTELECTUAL NAS FORÇAS ARMADAS BRASILEIRAS: UM PARALELO ENTRE MARINHA, EXÉRCITO E AERONÁUTICA QUANTO AOS DEPÓSITOS DE PATENTES E AS POLÍTICAS DE CRIAÇÃO DOS NITs.**

Rogéria Prado Dall'Agnol<sup>1</sup>  
Gláucio José Couri Machado<sup>2</sup>  
Leidiane Bispo Brito<sup>3</sup>  
Igor Dall'Agnol<sup>4</sup>

## **RESUMO**

---

A Propriedade Intelectual tornou-se ferramenta fundamental e estratégica para o desenvolvimento econômico de um país. Desse modo, destaca-se a capacidade de instituições, como as Forças Armadas do Brasil, de fazer PD&I. Assim, o presente estudo faz um levantamento da proteção intelectual da Marinha, do Exército e da Aeronáutica por intermédio do número de depósitos de patentes e compara a situação de seus Núcleos de Inovação Tecnológica – NIT. Utilizou-se a

---

<sup>1</sup> Doutoranda em Ciência da Propriedade Intelectual pela Universidade Federal de Sergipe (UFS) São Cristóvão, SE. E-mail: rogeriavictoria@hotmail.com

<sup>2</sup> Doutor em Informática na Educação pela Universidade Federal do Rio Grande do Sul. Professor Adjunto da Universidade Federal de Sergipe (UFS) São Cristóvão, SE. E-mail: gcmachado@hotmail.com

<sup>3</sup> Mestre em Ciência da Propriedade Intelectual pela Universidade Federal de Sergipe (UFS) São Cristóvão, SE. E-mail: leidianebrito@gmail.com

<sup>4</sup> Graduado em Desenvolvimento de Aplicações Para Web pela Faculdade de Administração e Negócios de Sergipe (UFS) São Cristóvão, SE. E-mail: igordall@gmail.com

pesquisa bibliográfica e documental e a análise empírica dos números de depósitos de patentes por meio de buscas na base de patentes do Instituto Nacional de Propriedade Industrial (INPI), no período de 1976 a 2014. Notou-se que a Força Aérea do Brasil é o centro com maior número de pedidos de depósito e o Exército Brasileiro o que menos deposita. A atuação do NIT-DCT ainda é muito incipiente. **Palavras-Chave:** Forças Armadas, Inovação, Propriedade Intelectual.

## INTRODUÇÃO

As Forças Armadas do Brasil são compostas pela Marinha, pelo Exército e pela Força Área, configurando-se por instituições nacionais permanentes e regulares, tendo como missão constitucional zelar pela defesa da Pátria, garantir os poderes constitucionais e, por iniciativa destes, a lei e a ordem.

Cubero (2002) afirma que o crescimento militar tecnológico tornou-se algo muito grande, chegando a chamar tal desenvolvimento de uma revolução organizacional das forças armadas, e que, sendo assim, elas se transformaram num gigantesco complexo de engenharia. O desenvolvimento tecnológico de artigos militares pode tornar um país especialmente poderoso, tanto na questão de defesa nacional quanto na potencialidade econômica, uma vez que tais produtos podem ser vendidos ou fornecidos tecnologicamente.

Diante da importância e da amplitude que a Propriedade Intelectual abrange, hoje em dia, no Brasil, já existe legislação específica, por meio de diferentes leis que determinam e estabelecem os ditames acerca da Propriedade Intelectual em virtude das constantes alterações no desenvolvimento econômico e tecnológico do país.

Por essa razão, este trabalho foi elaborado com o objetivo principal de levantar a quantidade de depósitos de pedidos de patentes realizados pelas Forças Armadas, fazendo um paralelo entre elas; e, como objetivos específicos criar indicadores que viabilizem uma análise comparativa quanto ao número de depósitos efetuados por cada FA; e, levantar e analisar a literatura sobre a criação, instalação e funcionamento de Núcleos de Inovação Tecnológica (NIT) das Forças Armadas, identificando suas ICTs.

## METODOLOGIA OU ESCOPO

Para atender o objetivo de identificar a inserção da proteção intelectual na Marinha, Exército e Aeronáutica e atuação de seus Núcleos de Inovação Tecnológica – NIT, foram realizadas pesquisas bibliográficas e documentais, além de busca de patentes em banco de dados nacional. O procedimento inicial utilizado foi a pesquisa bibliográfica e teve-se o cuidado em selecionar trabalhos relevantes com informações fidedignas sobre o tema. A pesquisa documental foi o segundo passo realizado para a continuação da elaboração deste estudo. Este tipo de pesquisa segue os mesmos caminhos da bibliográfica, no entanto a diferença se dá pelo fato de a pesquisa documental ter fontes muito mais amplas, diversas e dispersas. Assim, Gil (2002) classifica os documentos como sendo de “primeira mão” e “segunda mão”, ao que ele define como sendo de primeira os que não receberam nenhum tratamento analítico como os documentos conservados em arquivos de órgãos públicos e instituições privadas, incluindo os vastos outros documentos como cartas pessoais, diários, fotografias, gravações, memorandos, regulamentos, ofícios, boletins dentre outros. O terceiro procedimento metodológico realizado foi o levantamento de dados relativos ao número de depósitos de patentes das três Forças Armadas Brasileiras. Para esta pesquisa alguns critérios para o detalhamento da estratégia e abrangência da busca foram realizados. Ressalte-se que por se tratar de uma análise sobre a quantidade de patentes no âmbito das forças armadas e não de uma prospecção tecnológica<sup>5</sup>, optou-se pela busca apenas no banco de patentes nacional. Além disso, a lei de patentes reza que todos os pedidos de depósitos de objetos que versem sobre defesa nacional não poderão ser depositados no exterior. Sendo, então, as Forças Armadas do Brasil, nosso objeto de estudo, não seria relevante uma busca em base internacional, uma vez que a maioria dos pedidos verse sobre defesa nacional.

Para a pesquisa do número de depósitos de patentes elaborou-se uma estratégia a um conjunto de palavras-chave<sup>6</sup> no campo depositante a fim de identificar os principais centros depositantes. Para essa busca, utilizou-se o banco de patentes do Instituto Nacional de Propriedade Industrial - INPI.

---

<sup>5</sup> De acordo com Kupfer e Tigre (2004), Prospecção Tecnológica pode ser definida como um meio sistemático de mapear desenvolvimentos científicos e tecnológicos futuros capazes de influenciar de forma significativa uma indústria, a economia ou a sociedade como um todo.

<sup>6</sup> As palavras-chave utilizadas foram um conjunto e combinações de palavras e/ou siglas em português, quais sejam: Marinha, Brasil, Força Aérea Brasileira, Aeronáutica, Exército Brasileiro, CTMSP, IEAPM, IPQM, IEAV, ITA, IAE, IME, CTEx.

O detalhamento dos critérios de análise e da estratégia da busca é apresentado na tabela 1.

*Tabela 1. Determinação de critérios de análise, estratégia e abrangência da busca.*

Critérios de Análise								
Base de dados utilizada	Estratégia de busca							
Base de Patentes (Instituto Nacional de Propriedade Industrial)	Palavras-Chave							
Tipo de monitoramento	Identificar							
Nacional	Evolução temporal							
Período								
1996 - 2014								
Estratégia de Busca								
	01	02	03	04	05	06	07	08
Centro Tecnológico da Marinha em São Paulo (CTMSP)	x							
Instituto de Estudos do Mar Almirante Paulo Moreira (IEAPM)		x						
Instituto de Pesquisas da Marinha (IPqM)			x					
Instituto de Estudos Avançados (IEAv)				x				
Instituto Tecnológico de Aeronáutica (ITA)					x			
Instituto de Aeronáutica e Espaço (IAE)						x		
Instituto Militar de Engenharia (IME)							x	
Centro Tecnológico do Exército (CTEx)								x
TOTAL	03	03	23	13	07	36	15	08

Fonte: Elaborado pelo autor (2014)

## RESULTADOS E DISCUSSÃO

O Brasil ainda possui tímidos investimentos em Pesquisa, Desenvolvimento e Inovação PD&I, e tais investimentos estão diretamente relacionados à capacidade de um Estado em desenvolver ativos protegíveis com os quais se possam ganhar vantagens financeiras, ou seja, baixos investimentos implicam em escassez em pesquisa, desenvolvimento e inovação, e, conseqüentemente em quantidade de patentes.

Ao analisar a tabela 2 abaixo, quis-se apenas comparar das três instituições qual possui o maior número de depósitos de patentes. Vale ressaltar que a quantidade de depósitos levou em consideração os pedidos em base nacional.

*Tabela 2: Patentes por ICT's*

NIT-MB			NIT-DCTA			NIT-DCT	
CTMSP	IEAPM	IPQM	IEAV	ITA	IAE	IME	CTEx
03	03	23	21	22	37	15	08

Fonte: Elaborado pelos autores (2014)

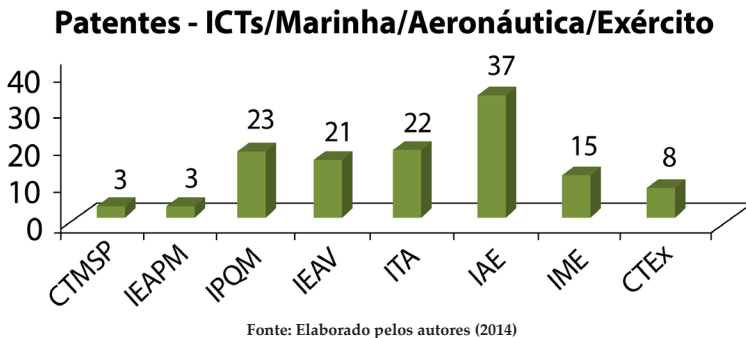
Partindo-se da pesquisa quantitativa, realizada no banco de patentes do INPI nota-se que as Instituições de Ciência e Tecnologia da Marinha do Brasil (NIT-MB), que fizeram depósito de pedido de patentes foram as seguintes: Centro Tecnológico da Marinha em São Paulo – CTMSP; Instituto de Estudos do Mar Almirante Paulo Moreira – IEAPM e o Instituto de Pesquisa da Marinha – IPQM. Já as ICTs da Força Aérea do Brasil (NIT-DCTA) que depositaram foram: Instituto de Estudos Avançados – IEAV; Instituto Tecnológico de Aeronáutica – ITA; e o Instituto de Aeronáutica e Espaço – IAE. As ICTs do Exército Brasileiro (NIT- DCT) que fizeram depósitos de pedido de PI foram: Instituto Militar de Engenharia – IME e o Centro Tecnológico do Exército – CTEx.

Nota-se que o Instituto de Aeronáutica e Espaço – IAE, Instituto de Pesquisa da Marinha – IPQM e Instituto Tecnológico de Aeronáutica – ITA são as três ICTs que mais depositaram respectivamente pedidos de patentes. É observável, que apesar de ser a mais nova das FAs, a Força Aérea se destaca quanto ao número de pedidos de patentes. Ao observar o número de depósitos de cada uma de suas organizações militares, seria razoável esperar um número maior de depósitos realizados pelo ITA. Tal instituição possui cursos de graduação, mestrado e doutorado acadêmicos e profissionais, alguns dos cursos possuem mais de 40 anos, e, apesar deste instituto ser referência em

formação de engenheiros no Brasil, além de possuir trabalhos voltados para desenvolvimento e pesquisa, não demonstrou depósitos de pedidos de patentes tão expressivos. A esse fenômeno não se quis, neste trabalho, os motivos que justifiquem o baixo desempenho quanto à quantidade de depósitos ora realizados. Do mesmo modo, o IME, apesar de seus tradicionais cursos de engenharia, demonstrou um número relativamente baixo, se levarmos em consideração o número de engenheiros formados e o número de cursos de mestrados e doutorados em diversas áreas de engenharias, como mecânica, defesa e nuclear. Sendo assim, foi constatado que o Exército Brasileiro foi o que menos depositou o que soa desconforme, já que a ideia natural seria pensar em um número bem maior de depósitos, deixando o Exército como um dos maiores depositantes de pedidos de patentes por ter, o EB, uma Organização Militar peculiar, histórica e tradicional como o IME.

A figura 1, abaixo, dispõe em um gráfico, para melhor compreensão, todas as ICTs que realizaram depósitos de pedidos de patentes, no âmbito das Forças Armadas brasileiras. Assim, em termos de quantidade, é possível fazer um paralelo entre as instituições militares. As quatro ICTs que mais depositaram foram, respectivamente, o Instituto de Aeronáutica e Espaço – IAE, o Instituto de Pesquisa da Marinha – IPQM, o Instituto Tecnológico de Aeronáutica – ITA e o Instituto de Estudos Avançados IEAv<sup>7</sup>.

Figura 1: comparação do número de depósitos entre as ICTs.



A figura 2, seguinte, faz uma demonstração das instituições que fizeram depósitos de pedidos de patentes apenas no âmbito da Força Aérea do Brasil, assim, é possível comparar qual a instituição que mais e menos depositou. Como anteriormente citado, o Instituto Tecnológico de Aeronáutica – ITA não obteve um número de depósitos expressivo,

<sup>7</sup> IEAv – É uma Organização Militar da Força Aérea Brasileira.

muito embora seja uma instituição voltada para o ensino e pesquisa com cursos de graduação e pós-graduação nas áreas de engenharias. Devido à tradição e histórico do ITA, fica difícil conceber que a instituição tenha apenas o total de vinte e dois pedidos de patentes. Por esse motivo é viável levar em consideração o sigilo de patentes de que trata a lei de patentes no seu artigo 75, que deixa claro que o objeto de interesse à defesa nacional não está sujeito à publicações ora previstas nesta lei.

O Instituto de Estudos Avançados – IEAv também uma organização militar que pertence à Força Aérea, com mais de 50 anos de existência e com atividades voltadas à P&D figura com o número de 21 depósitos de patentes. O IEAv possui grupos de Pesquisa junto ao CNPq que abordam aerotermodinâmica e hipersônica, tecnologia nuclear espacial, métodos computacionais em transporte de partículas, engenharia virtual, sistemas eletromagnéticos, efeitos da radiação ionizante em dispositivos e materiais de uso aeroespacial, óptica aplicada, sensores a fibra óptica, lasers e aplicações, fotônica em silício, sensoriamento remoto e termo-hidráulica.

O Instituto de Aeronáutica e Espaço – IAE, segundo a busca de patentes realizada até o final do ano de 2014, é a ICT com maior número de depósitos. Não é a que mais deposita apenas entre as ICTs da FAB<sup>8</sup>, mas a que mais deposita entre todas as ICTs no âmbito das Forças Armadas. O Instituto de Aeronáutica e Espaço – IAE tem sua origem na década de 50, com a criação, em 1º de janeiro de 1954, do Instituto de Pesquisas e Desenvolvimento – IPD no campus do então Centro Técnico de Aeronáutica – CTA. Contudo, o IAE foi estabelecido definitivamente em 17 de outubro de 1969. Um fato marcante na história do IAE foi o desenvolvimento de vários foguetes de sondagem, com a finalidade de colocar satélites na órbita da Terra, que deu ao Brasil o domínio das tecnologias para desenvolvimento do VLS – Veículo Lançador de Satélites.

“O IAE tem como missão ampliar o conhecimento e desenvolver soluções científico-tecnológicas para fortalecer o Poder Aeroespacial Brasileiro, por meio da Pesquisa, Desenvolvimento, Inovação, Operações de Lançamento e Serviços Tecnológicos em sistemas aeronáuticos, espaciais e de defesa e como visão ser reconhecido, no Brasil e no exterior, como uma instituição de excelência capaz de transformar Pesquisa e Desenvolvimento em Inovação na Área Aeroespacial” (IAE, 2015)<sup>9</sup>.

O IAE tem sua PD&I voltada para as tecnologias de defesa, sendo assim o número de pedidos de patentes pode ser superior ao demonstrado neste gráfico, além de levar em consideração o sigilo o qual decreta a Lei de Patentes.

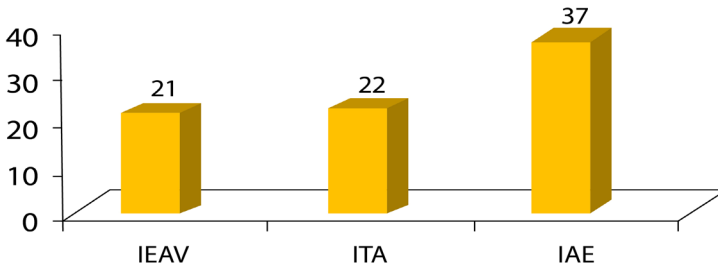
<sup>8</sup> FAB – Força Aérea Brasileira

<sup>9</sup> Disponível em: < <http://www.iae.cta.br> > Acesso em: 17 mar. 2015



Figura 2: comparação do número de depósitos entre as ICTs da Força Aérea do Brasil

### Pedido de Patentes - NITDCTA - Força Aérea Brasileira

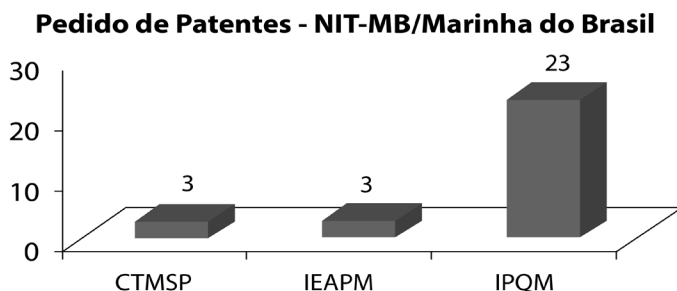


Fonte: Elaborado pelos autores (2014)

Com relação à Marinha do Brasil, a figura 3 traz as três ICTs que têm depositado pedidos. Percebe-se que o Instituto de Pesquisas da Marinha – IPQM é a instituição com maior número de depósitos. A instituição foi criada no ano de 1959 e o “local indicado para a instalação desta instituição foi a Ilha do Governador, Rio de Janeiro, não só pela disponibilidade de terrenos junto ao mar, como também pela proximidade de onde, posteriormente, viria se instalar a Universidade do Brasil, hoje UFRJ, o que facilitaria a desejada integração IPqM/Universidade” (IPQM). O IPQM possui projetos nas áreas de armas, guerra eletrônica, sonares e sistemas digitais. As outras duas ICTs que também depositam são: o Centro Tecnológico da Marinha em São Paulo – CTMSP e o Instituto de Estudo do Mar Almirante Paulo Moreira – IEAPM. Ambas as instituições aparecem no gráfico com o número de três depósitos de pedidos de patentes. A primeira foi criada em outubro de 1986. É uma ICT relativamente nova, localizada em São Paulo/Brasil e tem suas atividades de PD&I voltada especialmente para o desenvolvimento de programas nucleares aplicáveis à propulsão naval (CTMSP)<sup>10</sup>. A segunda foi criada em 1971, como consequência do Projeto Cabo Frio. Tal projeto tinha como escopo a criação de um núcleo destinado a apoiar e executar estudos do mar e de seus recursos oceanográficos.

<sup>10</sup> Disponível em: <<http://www.mar.mil.br>> Acesso em: 17 março 2015

Figura 3: comparação do número de depósitos entre as ICTs da Marinha do Brasil.



Fonte: Elaborado pelos autores (2014)

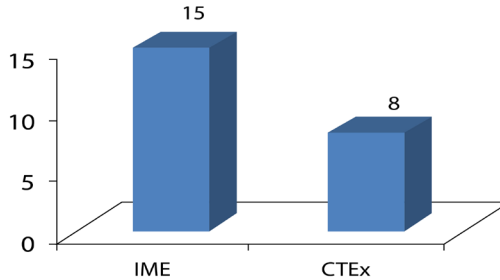
A figura 4 traz as duas ICTs que têm depositado pedidos de patentes no âmbito do Exército Brasileiro. O Instituto Militar de Engenharia – IME, até final de 2014, tinha depositado quinze pedidos de patentes. O IME nasceu da fusão da Escola Técnica do Exército com o Instituto Militar de Tecnologia, em 1959. Ao todo vem formando engenheiros a mais de 200 anos. Esta OM<sup>11</sup> é uma escola de engenharia nas áreas de construção, eletrônica, elétrica, mecânica, química, cartografia, nuclear, defesa, dentre outras. Possui cursos de graduação, mestrado e doutorado e é uma das instituições de ensino mais renomadas do país. O quantitativo de depósitos encontrado é um tanto inquietante, haja vista as atividades peculiares ao desenvolvimento de inovações tecnológicas. No entanto, vale considerar o sigilo das patentes, como bem assim diz a Lei nº 9.279. É provável que, de algum modo, isso explique o baixo número de pedidos.

O Centro Tecnológico do Exército – CTEEx, foi criado em 1946, e, sua atividade fim é Pesquisa e Desenvolvimento. O Centro desenvolve de forma independente ou em conjunto com outras instituições, diversos projetos com apoio financeiro da FINEP – Financiadora de Estudos e Projetos, vinculada ao Ministério da Ciência e Tecnologia. Atualmente, existem mais de vinte projetos financiados pela FINEP. A maioria dos projetos ora financiados versam sobre defesa, e, nesse caso é provável que haja outros tantos pedidos de patentes sob sigilo, assim, não contabilizados no banco de patentes do INPI.

<sup>11</sup> OM – Organização Militar

Figura 4: comparação do número de depósitos entre as ICTs do Exército Brasileiro.

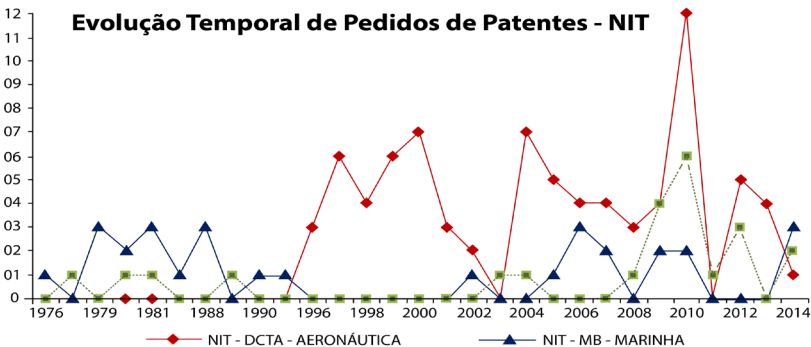
### Pedido de Patentes - NIT-DCT - Exército Brasileiro



Fonte: Elaborado pelos autores (2014)

A figura 5 mostra a evolução temporal dos números de depósitos realizados pelas Forças Armadas no intervalo de tempo entre 1976 e 2014. Percebe-se nitidamente que a Força Aérea (NIT-DCTA) tem um número de depósito superior as outras duas FAs. Nesse aspecto, não se consegue saber o motivo por que a Força Aérea deposite mais. Poderia haver diversos fatores, desde um maior investimento financeiro repassados às ICTs do NIT-DCTA, incentivo à pesquisa, até a gestão de Propriedade Intelectual. Ainda, analisando a figura em comento, percebe-se que a Marinha (NIT-MB) diminuiu os depósitos depois de ter passado um período de oito anos sem fazer nenhum pedido de patentes, tornando a depositar somente em 2004. Aquele ano de 2004 coincide com a publicação da Lei nº 10.173 de 02 de dezembro de 2004, a conhecida lei de Inovação. Tal Lei estabelece medidas de incentivo à inovação e à pesquisa científica e tecnológica no ambiente produtivo, com vistas à capacitação, ao alcance da autonomia tecnológica e ao desenvolvimento industrial do País.

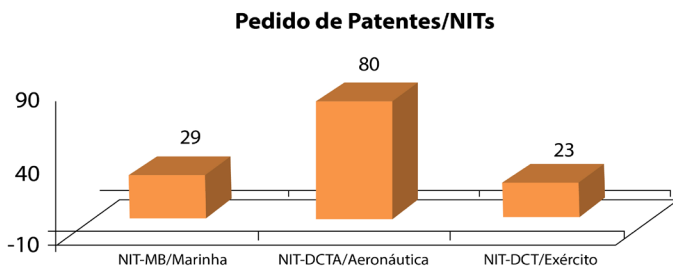
Figura 5: Evolução temporal do número de depósitos realizados pelas ICTs das FAs.



Fonte: Elaborado pelos autores (2014)

A figura 6 traz o quantitativo de depósitos realizados por cada uma das Forças Armadas Brasileiras. Assim, é possível fazer, de forma clara e precisa, a comparação entre elas. A Força Aérea aparece com oitenta depósitos de pedidos de patentes, sendo ela a FA<sup>12</sup> que mais tem depositado. Em seguida, a Marinha com vinte e nove pedidos e por último, com vinte e três pedidos o Exército Brasileiro.

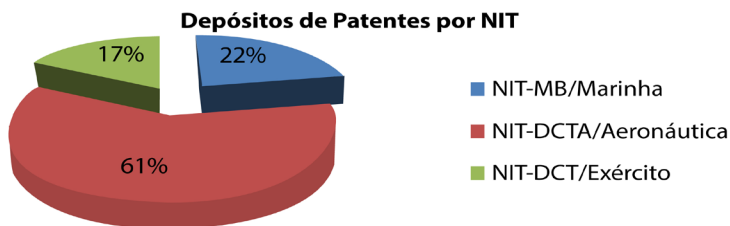
Figura 6: Quantidade de depósito de pedidos de patentes por FA.



Fonte: Elaborado pelos autores (2014)

Na figura 7, foram colocados em gráfico para melhor compreensão, os valores em percentuais dos depósitos de patentes por NIT. Assim, observa-se claramente o panorama geral do quantitativo encontrado por meio da pesquisa ora realizada. Veja-se que, com 17% de todos os pedidos efetuados, está o NIT-DCT, o qual pertence ao Exército Brasileiro. Um número relativamente pequeno, levando-se em consideração aspectos institucionais de tal Força Armada, citados anteriormente. Logo em seguida, temos o NIT-MB, da Marinha Brasileira, com o percentual de 22% e finalmente, com 61% dos pedidos realizados, o NIT-DCTA, da Força Aérea do Brasil, ficando como o Centro com maior número de depósitos.

Figura 7: Quantidade de depósito de pedidos de patentes por NIT.



Fonte: Elaborado pelos autores (2015)

<sup>12</sup> FA – Força Armada

O quadro 1, explana de forma esquematizada e resumida, a situação dos NITs das Forças Armadas trazendo uma melhor visualização do que já foi dito anteriormente a respeito. O presente quadro traz uma comparação entre os Núcleos de Inovação Tecnológica quanto à data de criação, efetivo atual, estágio de implementação e número de ICTs. Sendo assim, os NITs da Marinha e do Exército foram criados no ano de 2009, sendo, portanto, mais recentes que o NIT da Aeronáutica, o que talvez explique o fato de ser o NIT com maior nível de maturidade. Essa Força Armada é que possui o maior número de efetivo e a que possui o Núcleo de Inovação Tecnológica implementado. A Marinha está com seu NIT ainda em fase de implementação, e com um efetivo de 5 pessoas. O NIT do Exército se mostra ainda muito incipiente, com NIT não implementado e com efetivo de apenas dois profissionais. Em relação aos números de ICTs, a Marinha possui um total de oito<sup>13</sup> ICTs, e o Exército e Aeronáutica possuem ambos um total de dez cada uma.

*Quadro 1 - Análise Comparativa entre os NITs quanto a data de criação, efetivo, estágio de implementação e número de ICTS.*

NIT	Criação	Efetivo	Estágio de implementação	Nº de ICTS
Marinha	2009	05	Implementação	08
Exército	2009	02	Não implementado	10
Aeronáutica	2006	06	Implementado	10

Fonte: Elaborado pelos autores (2015)

## CONCLUSÃO

Considerando alguns aspectos como a visão panorâmica da Propriedade Intelectual no mundo; o Brasil como país emergente e almejando ocupar patamar de potência mundial; a importância da PI para competitividade e crescimento econômico; e o grau de importância das Forças Armadas para um país como aliadas na geração de riqueza, é possível afirmar, com base neste estudo, o baixo quantitativo de pedidos de depósitos de patentes realizados pelas FAs brasileiras, levando em

<sup>13</sup> Atualmente a Marinha do Brasil (MB) possui o número de 10 (dez) ICTs, de acordo com a Portaria nº 109 do Estado-Maior da Armada, datada de 29 de maio de 2015.

consideração o período de 1976 até 2014. Ainda, mesmo datada de 2004, a lei de Inovação, os NITs das Forças Armadas não demonstram um grau de maturidade desejável, haja vista, por exemplo, quadros de pessoal diretamente envolvidos com PI muito reduzidos, em que pese também, o NIT do Exército Brasileiro ainda se encontrar em fase de implementação.

Como resultado pode-se verificar que há sim uma preocupação com o tema em questão, e que projetos têm sido realizados com sucesso, mas ficou demonstrado por meio da exposição dos gráficos e informações colhidas que os resultados ficaram aquém do ideal se considerarmos os aspectos inicialmente citados. Ainda vale ressaltar que a Força Armada com menor depósito de pedidos de patentes é justamente a que possui uma das organizações mais antigas e tradicionais no âmbito das FAs com potencial para gerar inovação tecnológica, a saber, o Instituto Militar de Engenharia IME. Nesse caso, temos um paradoxo já que o pensamento comum levaria a uma ideia diferente da do resultado obtido neste trabalho. Além do baixo número de depósitos realizados pelo EB, este possui o NIT mais incipiente, o qual não possui ainda sequer um organograma. Isso não quer dizer que esforços não estejam sendo realizados, mas mostra um ponto fraco em relação à PI no âmbito do Exército, o que torna a gestão fragilizada, necessitando, então, planejamentos e decisões mais determinísticas e pragmáticas.

O Brasil, como candidato ao título de potência mundial, tem procurado inserir-se no contexto competitivo mundial, valendo-se de várias ferramentas, dentre elas a propriedade intelectual, que se tem mostrado instrumento de grande valia para desenvolvimento econômico. Contudo, os processos que envolvem a promoção da PI mostram-se ainda incipientes, quiçá estivesse no ritmo ideal, mas isso ainda não pode ser afirmado, haja vista necessite-se ainda de muito mais investimentos em PD&I e de uma gestão em PI mais pragmática e solidificada. Este trabalho limitou-se em quantificar a quantidade de patentes depositadas pelas forças armadas brasileiras e em verificar a situação atual de seus NITs. Assim, como todo trabalho científico, foi limitado, mas tomando como base os resultados desta produção, pode-se comprovar a incipiência do Brasil nos assuntos voltados a PI e a gestão desta.

Não se pode olvidar de algumas variáveis que podem ter influenciado os resultados deste trabalho. Como exemplo, saliente-se o caráter sigiloso das patentes quando o assunto versar sobre defesa nacional.

O art. 75 da Lei de patentes reza que o pedido de patente originário do Brasil cujo objeto interesse à defesa nacional será processado em caráter sigiloso e não estará sujeito às publicações previstas nessa mesma lei. Devido a tal sigilo, é possível conceber que os números de depósitos de patentes encontrados, por meio de busca realizada em plataforma nacional do Instituto Nacional de Propriedade Industrial INPI, estejam distantes dos números reais, e, assim sendo, os resultados obtidos neste trabalho, especificamente quanto aos números de patentes fiquem comprometidos em relação aos reais valores. Em sendo assim, o sigilo possa até justificar os baixos números ora encontrados nos resultados apresentados. Além do caráter sigiloso dos pedidos que versem sobre defesa nacional, há poucos trabalhos voltados especificamente sobre as Forças Armadas e suas propriedades intelectuais, o que tornou esta pesquisa lenta e limitada.

Vale ressaltar, ainda, que durante a realização desta pesquisa, foram realizadas inúmeras ligações e trocas de mensagens por meio de correio eletrônico, além de conversas e trocas de informações com oficiais superiores e intermediários pessoalmente. Muitas informações foram colhidas de maneira informal, uma vez que não se poderia divulgar o conteúdo delas. Saliente-se, ainda, que foi elaborado um questionário e enviando às três Forças Armadas com inúmeras perguntas, as quais foram respondidas sob a condição de não serem divulgadas. As informações colhidas do resultado dos questionários e demais informações colhidas via ligação telefônica e correio eletrônico, serviram apenas para confrontação com outros dados oficiais das próprias FAs e de outras fontes. Ressalte-se, ainda, a dificuldade de entrar em contato com o pessoal do NIT de ambas as Forças Armadas, bem assim como a dificuldade e demora em obter informações consistentes a respeito dos pedidos das patentes por meio dos próprios NITs.

Foram quatro as hipóteses levantadas neste trabalho, as quais foram sendo confirmadas no transcurso desta pesquisa, as quais estão listadas na página 12 deste trabalho. Assim, a preocupação com a Propriedade Intelectual no âmbito das Forças Armadas se mostra, ainda muito incipiente, e as políticas de PI não estão sendo feitas de maneira progressiva e no mesmo ritmo com o que se produzem novas tecnologias e, por isso mesmo, existe uma necessidade latente de que exista uma preocupação maior acerca das políticas de PI nas Forças Armadas, uma vez que o Brasil esteja se destacando no cenário econômico internacional.

Ficou claro também que é primordial manifestar e desenvolver ações estratégicas que tenham a finalidade de promover a Propriedade Intelectual em todas as Organizações Militares e que essas ações sejam manifestadas inicialmente pelos NITs, além de ter ficado evidente, a necessidade de fomentar ações voltadas à disseminar o conhecimento sobre a Propriedade Intelectual nas Forças Armadas, com o intuito de auxiliar os Comandos Militares no desenvolvimento de políticas específicas.

Dessa forma, o sentimento que se tem é que faltam articulação e organização na gestão de PI por parte dos NITs, demonstrando, de fato, um caminho longo a percorrer para que tais núcleos se transformem naquilo para os quais foram criados.

Assim, este estudo e a metodologia aqui aplicada se apresentam como um relevante instrumento com utilidade para os comandos das Forças Armadas, gestores dos NITs, gestores das próprias ICTs e pesquisadores sobre temas afins, com o intuito de avaliar a produção e a gestão da Propriedade Intelectual nas Forças Armadas Brasileiras.



# INTELLECTUAL PROPERTY IN ARMED FORCES

## ABSTRACT

---

Intellectual property has become fundamental and strategic tool for economic development of a country. Thus, there is the capacity of institutions such as the armed forces of Brazil , to make RD & I . The present study is a survey of the Navy intellectual protection, Army and Air Force through the number of patent deposits and compares the situation of its Technological Innovation Centers - NIT . We used the bibliographical and documentary research and empirical analysis of the numbers of patent applications by searching in the National Institute of patents based Industrial Property (INPI) , from 1976 to 2014. It was noted that the Air Force Brazil is the center with more filing of applications and the Brazilian Army the least deposits . The performance of NIT- DCT has hardly begun .

Key words: Armed Forces , Innovation, Intellectual Property.

## REFERÊNCIAS

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA. *Revista Brasileira de Inteligência*. Brasília: Abin, 2005.

BRASIL. Exército. Separata ao BE N° 6/2014. *Boletim do Exército*, Brasília, 7 fev. 2014.

BRASIL. Ministério da Ciência, Tecnologia e Inovação. Secretaria de Desenvolvimento Tecnológico e Inovação. *Política de propriedade intelectual das instituições científicas e tecnológicas do Brasil: relatório Formict 2012*. Brasília: Ministério da Ciência, Tecnologia e Inovação, 2013.

BRASIL. Secretaria da Ciência Tecnologia e Inovação da Marinha. Tecnologia a bordo. *Pesquisa Naval: Informativo de Ciência, Tecnologia e Inovação da Marinha do Brasil*, v. 1, n.1, mar. 2010.

CUBERO, Jaime. Antimilitarismo e anarquismo. *Revista Verve*, 2002.

GIL, Antônio Carlos. *Como elaborar projetos de pesquisa*. 3.ed. São Paulo: Atlas, 2002.

\_\_\_\_\_. *Como elaborar projetos de pesquisa*. 4 ed. São Paulo: Atlas, 2002.

Recebido em: 11/09/2016

Aceito em: 09/12/2016



# POLÍTICA E GESTÃO DE “OFFSETS” EM AQUISIÇÕES DE DEFESA: CONTRIBUIÇÕES DA EXPERIÊNCIA INTERNACIONAL PARA O BRASIL

Felipe Augusto Rodolfo Medeiros<sup>1</sup>  
William de Sousa Moreira<sup>2</sup>

## RESUMO

---

O presente artigo explora as características dos acordos de compensação comercial, industrial e tecnológica, conhecidos como “offsets”<sup>3</sup>, praticados internacionalmente. A partir da construção de uma base teórica e conceitual, o trabalho busca depreender da experiência internacional contribuições para o aprimoramento da gestão de offsets no Brasil. Desenvolvido com base em pesquisa de mestrado pelo primeiro autor, sob orientação do segundo, o presente artigo sintetiza subsídios que podem informar a reflexão de atores envolvidos na formulação de normas atinentes às práticas de offset.

**Palavras-chaves:** Aquisições de defesa. Compensação industrial e tecnológica. Offset. Transferência de Tecnologia.

---

<sup>1</sup> Mestre pelo Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN) e pesquisador do Núcleo de Avaliação de Conjuntura do Centro de Estudos Político-Estratégicos da Escola de Guerra Naval (NAC/CEPE-EGN), Rio de Janeiro, RJ, Brasil. E-mail: felipe.a.medeiros@hotmail.com.

<sup>2</sup> Doutor em Ciência Política. Professor do PPGEM-EGN, Rio de Janeiro, RJ, Brasil. E-mail: williamsm2k@gmail.com.

<sup>3</sup> Neste trabalho, offset é entendido como “acordo de compensação de natureza comercial, tecnológica e/ou industrial que um comprador demanda como pré-condição para realização de uma aquisição”. “Offset direto” são os acordos de compensação que envolvem bens e serviços diretamente relacionados ao objeto do contrato original (por exemplo, coprodução de componentes de um caça). “Offset indireto” são os acordos de compensação que envolvem bens e serviços não diretamente relacionados ao objeto do contrato original (por exemplo, a compra de produtos agrícolas ou a composição de uma joint-venture para fabricação de medicamentos).

## INTRODUÇÃO

Acordos de compensação industrial, comercial e tecnológica – usualmente conhecidos como “offsets” – tornaram-se parte integrante dos processos de aquisições de defesa. Nem sempre bem compreendidos, mas muito citados, entraram nos discursos, políticas públicas e contratos mundo afora.

Poucos são os governos que não os exigem de empresas estrangeiras quando adquirem produtos de emprego militar. De transferência de tecnologia contracompra de produtos agrícolas, passando por acordos de coprodução, composição de “joint ventures” e investimento em áreas outras que não a de defesa, a complexidade dos “offsets” começa pela linguagem associada. Como contratos, podem assumir formas diversas, limitadas apenas pela criatividade dos negociadores no governo e na indústria.

O Brasil não está alheio à essa tendência global e demanda offsets nas compras que realiza junto a empresas não nacionais. Talvez o caso mais recente em que tal demanda reverberou junto à opinião pública foi quando da aquisição dos caças Gripen, no Projeto FX-2. Ênfase foi dada ao fato de que o governo brasileiro exigiu transferência de tecnologia que pretensamente alavancaria o grau de desenvolvimento tecnológico da base industrial de defesa.

A formação do senso comum relativo a esses empreendimentos se alimenta de notícias de mídia, algumas divulgadas por periódicos prestigiados e ligados às áreas de pesquisa e desenvolvimento, que reproduzem frases simplificadoras. Como por exemplo a de que “[c]om transferência total de tecnologia, caça Gripen NG será propulsor de salto no setor aeroespacial brasileiro”.<sup>4</sup> As altas instâncias políticas também contribuem nessa formação, como quando da afirmação da Presidente da República, em outubro de 2015, de que “[t]ransferir tecnologia é tão importante quanto os novos aviões”.<sup>5</sup>

Ainda que a um ritmo aquém do ideal, o Estado brasileiro vem dispendendo considerável volume de recursos com sistemas de

---

<sup>4</sup> Informações Disponíveis em: <<http://www.inovacao.unicamp.br/reportagem/com-transferencia-total-de-tecnologia-caca-gripen-ng-sera-propulsor-de-salto-no-setor-aeroespacial-brasileiro/>>. Acesso em: 20 jun. 2016.

<sup>5</sup> Informações Disponíveis em: <<http://blog.planalto.gov.br/transferir-tecnologia-e-tao-importante-quanto-comprar-novos-avioes-afirma-dilma-em-visita-a-saab/>> Acesso: em 04 mar.2016.

defesa – US\$ 5,4 bilhões apenas no caso supracitado. Uma vez que esses gastos estão condicionados à transferência de tecnologia e à promoção de políticas de conteúdo local, ambas expressas na forma de acordos de compensação. Os contratos de offset em defesa são internacionais e tendem a envolver consideráveis somas de recursos, notadamente nas grandes aquisições de defesa, podendo mesmo alcançar o valor do contrato original. Cabe acrescentar que novas demandas de controle social requerem crescente grau de transparência e acompanhamento. No caso brasileiro, o Tribunal de Contas vem se qualificando para auditoria de grandes projetos de defesa.

Convém, pois, que os diversos atores e entidades partícipes das aquisições de defesa ampliem o entendimento sobre as características dos acordos de compensação praticados no exterior; as políticas (“policy” e “politics”) que os consubstanciam e a base teórica que os informa e molda. Eis o mister deste artigo que, com base em pesquisa de mestrado realizada pelo primeiro autor, sob orientação do segundo, busca perscrutar na experiência internacional sugestões para o aprimoramento da gestão de offsets no Brasil. Além desta seção introdutória, ele conta com uma destinada a apresentar subsídios para elaboração de uma política de gestão de acordos de offset, derivados do estudo de documentos e das políticas públicas de governos estrangeiros. A seção seguinte traz considerações sobre o arcabouço político-jurídico brasileiro sobre acordos de compensação. A elas se seguirão algumas considerações finais.

## **SUBSÍDIOS PARA ELABORAÇÃO DE UMA POLÍTICA DE GESTÃO DE OFFSETS**

Um dos riscos a ser evitado ao se buscar “lições” para políticas públicas a partir da experiência internacional é a assimilação acrítica de padrões forâneos. Assim, não é uma tarefa trivial identificar subsídios potencialmente úteis a serem adotados no sentido de se aferir resultado positivo, pois, aquilo que funcionou para um determinado país pode não funcionar de maneira semelhante para outro. Mesmo políticas que deram certo no passado podem não render os mesmos resultados se executadas em outro momento histórico. Seria, por isso, temerário dizer que o estudo dos documentos de gestão de offset de governos estrangeiros pode prover necessariamente ensinamentos ao Brasil.

Com esse entendimento, foram examinadas fontes bibliográficas e documentais inerentes às práticas de offsets em seis diferentes países,

que compuseram uma amostra da experiência internacional considerada pelos autores como suficiente para os propósitos da pesquisa, a saber: Índia, Coreia do Sul, Canadá, Israel, Emirados Árabes Unidos e Arábia Saudita. Os critérios que levaram a essas escolhas foram, principalmente: o posicionamento no mercado internacional de defesa como compradores; o potencial de possibilitar algum tipo de analogia com o caso brasileiro; a acessibilidade a documentos e políticas públicas formais; e a explicitação ou não de posturas governamentais relativas às práticas de compensações.

O resultado da pesquisa pode ser melhor apresentado sob a forma de questões que uma política de gestão de acordos de compensação deve – ou deveria – considerar. Em função de sua inerente complexidade, foram elaboradas respostas baseadas nas boas práticas internacionais, extraídas dos documentos analisados. Elas permitem expor elementos úteis para formuladores de políticas e normas voltadas à gestão de compensações. Desse modo, as questões formuladas e respostas elaboradas servem de instrumento de análise e permitem, ainda, desvelar outros questionamentos.

Evidentemente, não se pretende a partir delas prescrever ou recomendar formulações, mas, alternativamente, informar a reflexão. As opções, por exemplo, por colocar maior risco financeiro sobre as empresas estrangeiras (exigindo títulos de performance) ou por delimitar modalidades de offset representam escolhas por maior ou menor flexibilidade administrativa e negocial. Cada Estado deve fazê-las à luz de seus objetivos políticos e econômicos e dos riscos de comportamento oportunista que antecipa de seus burocratas e de empresários nacionais e estrangeiros.

Faz-se mister observar, ademais, a adequação das questões listadas ao regime jurídico de cada país. É possível, por exemplo, que as leis que governam compras públicas impeçam a adoção de uma das opções de resposta fornecida (por exemplo, proibindo flexibilização do valor das aquisições a partir do qual offsets são exigidos), não podendo, portanto, ser contrariadas por um ato normativo, como um manual das forças armadas sobre offsets.

Na busca e seleção de documentos para análise, foram encontrados, por exemplo: sa “Defence Offset Guidelines”, da Índia, que é parte do “Defence Procurement Procedure” (DPP); na Coreia do Sul, as “Offset Program Guidelines”; no Canadá, as “Industrial and Regional Benefits Bidders Instructions, Terms and Conditions e Evaluation Plan”; em Israel, as “Guidelines for Industrial Cooperation”, nos Emirados Árabes Unidos, as “Tawazun Economic Program Guidelines”; e na Arábia Saudita, as

“Saudi Arabia Offsets Guidelines”.

Observou-se, assim, que não há padrão internacional para nomear os documentos que governam acordos de compensação. Parece haver, todavia, uma tendência para que uma “Política de Offsets” (“Offset Policy”) seja um documento amplo, que apenas estabelece objetivos gerais, ao passo que uma “Política para Gestão de Offsets” (“Offset Guidelines”, “Offset Guidelines Paper” ou outro termo semelhante) seja efetivamente um manual ou documento de diretrizes para orientar os negociadores governamentais.

Entre os temas relativos a offsets, direta ou indiretamente abordados nesses documentos específicos e também na literatura associada, merecem atenção: modelo de gestão; valor mínimo para exigência de compensação; formulação de propostas, avaliações e contratos; especificidade e detalhamento de políticas; mecanismos de fomento; fatores multiplicadores e valoração da transferência de tecnologia; prioridades tecnológicas justificadoras; direitos de propriedade intelectual; execução cruzada de créditos; prazos e metas para execução; sistema de penalidades para descumprimento e/ou atraso; exigências de garantias; sistema de banco de créditos; relações entre governos, empresas e conteúdo estrangeiro; programas derivados de aquisições emergenciais; “offset brokerage”; e avaliação do programa executado, entre outros.

Para racionalizar a abordagem desse amplo leque temático a partir de um modelo que estimule a reflexão, bem como a apresentação e discussão de aspectos relevantes para a elaboração de uma política, foram elaboradas as questões expostas no quadro 1 abaixo, que abrangem e ampliam os temas acima mencionados. Nesse sentido, passa-se a abordá-las, discutindo-as individualmente.

*Quadro 1 – Questões relevantes para uma “Política de Gestão de Acordos de Compensação”*

1. Qual o modelo de gestão de offsets?
2. Qual o piso a partir do qual offsets são exigidos e qual seu percentual?
3. A proposta de offsets afeta o contrato principal?
4. Como o comprador avalia as propostas de offset?
5. O país comprador definirá de maneira mais restrita as modalidades de offset que optará por uma linguagem mais ampla e inespecífica?



6. Há “cotas” mínimas para tipos específicos de offset?
7. Há algum mecanismo de fomento específico a pequenas e médias empresas? (SMEs)
8. Há algum mecanismo de fomento com foco regional/geográfico?
9. Qual a política quanto a fatores multiplicadores?
10. Como será feita a valorização de offsets de transferência de tecnologia?
11. Serão listadas as tecnologias que se deseja obter com offsets?
12. Como se lida com questões de licenças e direitos de uso de propriedade intelectual?
13. Será permitida a execução cruzada de créditos de offset?
14. Qual será o prazo para execução do programa de compensação?
15. Qual o sistema de penalidade no caso de descumprimento e/ou atraso?
16. São exigidos os títulos de performance (ou no caso brasileiro, Seguro Garantia e Fiança Bancária, entre outras formas previstas na legislação)?
17. O governo comprador terá um sistema de bancos de créditos de offset?
18. Haverá dispositivos especiais nos casos em que a venda do produto de defesa e intermediada pelo governo estrangeiro, mas o contrato de offset é assinado diretamente com a empresa fabricante?
19. Serão exigidos offsets de empresas locais que utilizem, em seus produtos e soluções, grande percentual de conteúdo estrangeiro?
20. Há dispositivos, nos documentos do país importador, para quando suas empresas estiverem exportando e forem, portanto, credoras de offset?
21. Há dispositivos que versem sobre programas de offset derivados de aquisições feitas em situações emergenciais?
22. Há alguma restrição ao serviço de “offset brokerage”?
23. Como o órgão gestor dos offsets avalia programas executados?

Figura elaborada pelos autores

## 1 – Qual o modelo de gestão de offsets?

Deve-se determinar em que instância os offsets serão geridos, se no nível do Ministério da Defesa ou das forças singulares. É preciso estabelecer se haverá um órgão permanente – uma diretoria, departamento, secretaria – para gerir offsets (como fazem os indianos) ou se eles serão administrados em uma comissão. Esta pode, de sua própria feita, ser permanente ou temporária. Esses modelos não são mutuamente excludentes. Como o caso coreano ilustra, é possível que haja um órgão permanentemente dedicado à gestão de offsets (o que presumivelmente facilitaria a formação de capital humano e transmissão de conhecimento) que compõe *ad hoc* uma comissão para a feitura do planejamento, negociação e implementação de um programa de compensação.

Deve-se decidir, também, se será admitida a participação de entes externos aos militares/Ministério da Defesa. Outros ministérios e agências ligados às áreas de desenvolvimento industrial, científico e tecnológico; e fomento a micro e pequenas empresas são as escolhas mais intuitivas e internacionalmente recorrentes. Eles não são, todavia, os únicos. É possível conceber também a participação de órgãos de controladoria e auditoria. Por fim, cabe decidir sobre a participação de civis externos ao governo na gestão dos offsets. Eles podem advir da academia, empresas, associações e federações industriais, terceiro setor, entre outros. A participação desses últimos não precisa ser onerosa ao Estado. Alternativamente, seus préstimos podem ser considerados serviço público e não incorrer em custos extras ao Executivo.

## 2 – Qual o piso a partir do qual offsets são exigidos e qual seu percentual?

Um documento de diretrizes deve estabelecer o valor mínimo a partir do qual offsets serão exigidos de empresas estrangeiras e estipular qual será seu percentual. Ele deve também estipular se há a possibilidade de isentar as companhias estrangeiras de fornecer compensações e, alternativamente, prever se há a possibilidade de exigi-las mesmo que contrato seja de um valor abaixo do piso estipulado.

Cabe também considerar se haverá percentuais de offset diferenciados para contratos de maior monta (isto é, percentuais mais altos para contratos a partir de um valor “x”), ou se as essas exigências serão reduzidas em licitações para as quais haja apenas somente um fornecedor (por exemplo, metade do percentual padrão). É possível que a lei que governa as compras públicas e as exigências de offset de um

determinado país não permita tal flexibilidade. Todavia, em havendo discricionariedade sobre essas questões, é recomendável que o documento de diretrizes estabeleça quem é o agente responsável por decidi-las (por exemplo, o presidente da hipotética comissão de compensação).

### 3 – A proposta de offsets afeta o contrato principal?

É preciso determinar se o projeto de compensação é apenas eliminatório ou se ele será, também, classificatório. Isto é, deve estar claro se é necessário apenas apresentar uma proposta de offsets que obedeça a um mínimo de requerimentos estabelecidos pelo gestor ou, alternativamente, determinar se essa proposta afetará o resultado do contrato principal. Como afirmado anteriormente, uma opção não é necessariamente melhor do que a outra. Elas representam escolhas de política pública diferentes.

A opção por offsets classificatórios fornece estímulos para que os fabricantes estrangeiros busquem diferenciar-se da concorrência oferecendo os melhores pacotes de compensação possíveis. Porém, ela incorre no risco de que se desvie o foco da capacidade operacional do sistema para os benefícios econômicos, tecnológicos e laborais que se espera obter com os offsets. Ademais, offsets classificatórios podem implicar em um aumento generalizado dos preços das propostas, postos que os fabricantes buscarão fornecer extensos pacotes de compensação tentando diferenciar-se e antevendo que seus concorrentes farão o mesmo. A opção por offsets apenas classificatórios estimularia os fornecedores estrangeiros a compensar somente o “mínimo necessário” para evitar sua desclassificação. Por outro lado, ela mitiga as possibilidades de prejuízo à capacidade operacional e aumento de preços. Justen Filho (2014, p. 121) propõe, especificamente sobre o caso brasileiro, que compensações podem ser apenas condição eliminatória. Do contrário, ele argumenta, elas feririam o princípio da isonomia. Já Gamell (2015, p.02) defende que offsets podem ser também classificatórios sem ferir o princípio da isonomia, conquanto sua avaliação obedeça a “critérios adequadamente estabelecidos no edital”. O que enseja a pergunta seguinte.

### 4 – Como o comprador avalia as propostas de offset?

Seja para eliminá-las, seja para classifica-las, o órgão gestor deve avaliar as propostas de offset que recebe dos fabricantes estrangeiros. É desejável que em seu manual sobre gestão de acordos de compensação, o Estado estipule uma metodologia para a pontuação de propostas. O caso canadense é ilustrativo, pois relaciona em uma fórmula a qualidade projeto

de compensação vis-à-vis os objetivos estabelecidos para o programa de offset e o risco envolvido em sua consecução (CANADÁ, 2013a, p. 08). É improvável que se elimine totalmente as discricionariedades de uma equação como essa, seja porque a atribuição de uma pontuação numérica ainda dependerá de avaliações qualitativas e subjetivas, seja pela inclusão de outros elementos à equação. É possível que fórmulas desse gênero sejam disponibilizadas nos editais (podendo mudar de um para outro) e não estejam presentes nos documentos de diretrizes. Do ponto de vista da transparência e padronização, todavia, o mais indicado seria disponibilizar essas fórmulas no “manual de offsets”.

Novamente, não é possível dizer que um desses três cursos de ação – (1) não ter uma equação, avaliando propostas de maneira exclusivamente qualitativa; (2) disponibilizar uma fórmula no documento de diretrizes; (3) disponibilizar uma fórmula apenas nos editais – é necessariamente melhor que o outro. São opções diferentes, com implicações diferentes. A escolha por uma em detrimento das outras deve, entretanto, refletir opções administrativas conscientes.

5 – O país comprador definirá de maneira mais restrita as modalidades de offset que aceita ou optará por uma linguagem mais ampla e inespecífica?

A literatura oferece definições amplas daquilo que pode ser considerado um offset. Ele pode consistir de coprodução, subcontratação, produção licenciada, transferência de tecnologia, contracompra, “barter”, fornecimento de linhas de crédito, composição de “joint-ventures”, investimento externo direto, “buyback”, transferência de equipamento, entre outras formas.<sup>6</sup> Um manual de gestão de acordos de compensação

<sup>6</sup> *Barter, ou troca* – Troca direta de bens e serviços, concluída de forma quase simultânea, substituindo total ou parcialmente o pagamento em dinheiro. No contexto de offsets, é uma maneira de desmonetizar uma transação. *Buyback* – Acordo em que um exportador de máquinas e equipamentos se compromete a comprar de volta no futuro parte da produção derivada dessas exportações, como pagamento total ou parcial. *Coprodução* – Transações baseados em acordos de governo a governo autorizando a transferência de tecnologia para permitir que empresas estrangeiras fabriquem total ou parcialmente artigos de defesa. Normalmente dependem de Memorandos de Entendimento e/ou de Cartas de Oferta e Aceite. *Counterpurchase, ou contracompra* – Acordo em que o fornecedor estrangeiro se compromete a comprar uma porcentagem do contrato em produtos do país importador e revendê-los a terceiros. *Produção sob licença* – Produção total ou parcial de um artigo de defesa baseada na transferência de informações técnicas entre o fabricante estrangeiro e um governo ou produtor local. Está acompanhada de uma licença de produção e/ou comercialização. *Subcontratação* – Acordo de compensação para que a exportadora contrate empresas no país importador para produzir partes do bem negociado, substituindo fornecedores de outras partes do mundo. Não costuma envolver transferência tecnológica e se beneficia de competências já existentes.

deve estabelecer se aceitará offsets nessa linguagem mais ampla e inespecífica (como fazem canadenses e israelenses), ou se delimitará um número menor de modalidades elegíveis (como Índia, Coreia do Sul e Emirados Árabes Unidos).

A primeira opção dá ampla flexibilidade para os negociadores do governo comprador adaptarem suas exigências e buscarem maximizar os ganhos advindos do offset. A segunda opção traz o ônus de retirar parte dessa flexibilidade. Porém, ela torna o processo mais previsível e ajuda a direcionar a política de compensação para um número mais restrito de objetivos (possivelmente gerando ganhos de escala e escopo no investimento feito pelas empresas estrangeiras). As duas opções não são inteira e/ou mutuamente excludentes, como ilustra o manual coreano. É possível estipular um número limitado de modalidades elegíveis de compensação, abrindo, porém, uma categoria de “outras formas não previstas anteriormente”, a qual possibilitaria aos negociadores maximizar os ganhos para o erário em uma conjuntura específica (por exemplo, caso a companhia que fornece o offset possua uma tecnologia de interesse nacional cujo fornecimento não seria possível pelas modalidades restritas). Se o Estado optar por essa “terceira via” – categorias limitadas, porém com a opção de “outros” –, é desejável que o documento de diretrizes estipule a quem compete autorizar o recebimento de offsets fora das categorias padrão (por exemplo, o presidente da hipotética comissão de compensação).

#### 6 – Há “cotas” mínimas para tipos específicos de offset?

Não é incomum que os manuais de offsets postulem que uma parte das compensações devidas seja fornecida de uma forma específica; algo nos moldes de “ao menos 30% das obrigações totais devem ser exercidas na forma de offsets indiretos”. Canadenses, sauditas e indianos, por exemplo, o fazem. Essa diferenciação não ocorre apenas entre offsets diretos e indiretos. Há ocorrências, por exemplo, de países que estabelecem que um determinado percentual de offsets (“no mínimo 50%”, por exemplo) ocorra na forma de transferência de tecnologia ou contracompra de produtos constantes em uma lista elaborada pelo Ministério da Defesa. Quando um governo faz a opção por listar um número limitado de modalidades de offset elegíveis, conforme discutido na questão anterior, é possível que ele estabeleça também que um percentual mínimo do total de créditos devidos seja exercido em uma das modalidades designadas. A opção por

definir ou não cotas mínimas implica em um “trade-off” entre flexibilidade administrativa por maior foco e direcionamento da política de compensação.

7 – Há algum mecanismo de fomento específico a pequenas e médias empresas (SMEs)?

É possível que o gestor dos offsets decida utilizá-los para fomentar o desenvolvimento das pequenas e médias empresas do parque industrial local. Há variadas maneiras de fazê-lo. Ele pode: exigir que um percentual mínimo de offsets seja executado com companhias desse porte (conforme discutido na questão anterior); estabelecer modalidades de offset específicas exclusivas para SMEs; ou oferecer multiplicadores maiores para projetos executados em parceria com elas. Esta última forma tende a gerar menos distorções de mercado, pois a empresa estrangeira mantém a opção de não colaborar com companhias de menor porte e só o fará se calcular que essa parceria será eficiente e eficaz. Uma cota mínima, por ser mandatória, pode eventualmente “forçar” parcerias ineficientes e com exíguas chances de sobrevivência no médio e longo prazos.

Mecanismos de fomento a SMEs surgem da percepção de que – sem a oferta de estímulos adicionais – há a tendência de que conglomerados estrangeiros concentrem seus offsets em empresas locais de maior porte (presumivelmente pouco numerosas em países em desenvolvimento), já que elas tendem a possuir maior capacidade técnica e implicarem em menor risco. Os militares e gestores civis podem preferir concentrar acordos de compensação em indústrias de defesa já estabelecidas – para torná-las ainda mais robustas – a espriá-los por companhias menores e financeiramente mais frágeis. Direcionar offsets para empresas de pequeno e médio pode ajudá-las a desenvolver novas capacidades e integrar-se às cadeias de suprimento global. Tal êxito não é, entretanto, garantido. A opção por uma ou outra via envolve gerenciar o risco de interrupção do fluxo orçamentário (que afeta principalmente as SMEs) com os objetivos política e economicamente estabelecidos (que tendem ao estímulo ao desenvolvimento de indústrias de pequeno e médio porte).

8 – Há algum mecanismo de fomento com foco regional/geográfico?

Aqueles dedicados a pensar a gestão da inovação vêm elaborando modelos teóricos e organizacionais para criar ambientes propícios à pesquisa, desenvolvimento e inovação industrial. Surgem, assim, parques tecnológicos, “clusters”, ecossistemas de inovação, sistemas setoriais de

inovação, Arranjos Produtivos Locais (APLs), entre outros. Nem todos esses modelos pressupõem uma concentração geográfica de atores, já outros (como “clusters” e APLs) estão inerentemente baseados nela. Um documento de diretrizes de offset pode estabelecer – de maneira análoga ao que faz para pequenas e médias empresas – mecanismos que concentrem regionalmente as compensações ofertadas pela parte estrangeira. Eles podem servir tanto para apoiar clusters e parques tecnológicos já existentes quanto para promover o surgimento e/ou fortalecimento de novos, dinamizando as economias de regiões desassistidas. Uma política de offsets com um foco regional traz a vantagem de poder gerar sinergias com agências de desenvolvimento dos gover’nos estaduais e municipais, parceiras recorrentes de clusters e APLs.

### 9 – Qual a política quanto a fatores multiplicadores?

Um manual de diretrizes de offset, idealmente, estipula se fatores multiplicadores serão ou não aceitos. Caso seja feita a opção por aceitá-los, deve ficar claro se os valores desses multiplicadores serão estabelecidos no próprio documento de diretrizes ou se sua determinação dependerá exclusivamente da discricionariedade dos gestores do programa de compensação. Quando se opta por determinar em documento quais serão os multiplicadores, a “melhor prática internacional” parece ser determinar um valor limite para cada modalidade de offset aceita. Estabelece-se, por exemplo, “um multiplicador de até 3 para offsets de coprodução, se as partes fabricadas no país comprador forem consideradas de alto valor agregado” ou “um multiplicador de até 1,5 para offsets de contracompra, conquanto os produtos sejam adquiridos de pequenas e médias empresas cadastradas pelo Ministério da Defesa”. Observe-se que a praxe é estabelecer um valor limite, e não um valor único de referência. Podem ser garantidos multiplicadores aquém do teto permitido, a depender do juízo dos gestores do programa de compensação. Assim, nunca é totalmente eliminado o poder de discricionariedade dos avaliadores governamentais (e nem é desejável que ele o seja).

A desvantagem de se estipular em um manual os valores máximos dos multiplicadores é a perda de flexibilidade nas negociações com as empresas estrangeiras. Assim, caso uma companhia multinacional esteja disposta a oferecer como offset uma tecnologia particularmente sensível, os gestores nacionais ficam impedidos de “premiá-la” com um multiplicador mais alto. Sem esse estímulo, é possível que a empresa desista de tal arranjo. Por outro lado, regras claras sobre multiplicadores dão mais previsibilidade à gestão

dos contratos de offset e auxiliam a companhia estrangeira a calcular com maior precisão quanto deverá dispendar para cumprir suas obrigações de compensação. Com esse cálculo mais objetivo, o risco financeiro se reduz, incorrendo (ou assim se presume) em um menor repasse de custos ao preço final do contrato principal. Finalmente, convém que o documento de diretrizes postule se há também um piso para multiplicadores e se (e em quais circunstâncias) poderão ser garantidos multiplicadores menores que 1.

10 – Como será feita a valoração de offsets de transferência de tecnologia?

Há diferentes maneiras de delimitar o que constitui uma “transferência de tecnologia”. É possível até mesmo questionar o caráter de transferibilidade da tecnologia dado ser ela um bem imaterial.<sup>7</sup> Assim, os manuais de gestão de offset costumam demarcar o que entendem constituir uma operação de ToT. Embora variem, os elementos que costumam ser citados são: a cessão de documentação especializada; a assistência técnica direta de especialistas estrangeiros (tanto no ambiente fabril quanto no laboratorial); e o fornecimento de programas de treinamento e qualificação de mão de obra. Um documento de diretrizes sobre compensações pode optar por estipular critérios quantitativos para o cálculo dos valores de documentação técnica, assistência e treinamento. É o que fazem os coreanos ao determinar os valores máximos de crédito de offset que aceitam conceder pela documentação especializada (até US\$ 150/página), pela assistência técnica direta (entre US\$ 7.000 – 15.000/mês/instrutor ou especialista estrangeiro) e pelo material usado nos programas de treinamento (até US\$ 5.000/indivíduo treinado). Esses valores não precisam ser estanques (não faz sentido que o sejam), e podem ser atualizados periodicamente. Embora se mantenha o caráter qualitativo da valoração desses offsets de ToT (por exemplo, ao se determinar quanto o vale o trabalho de um engenheiro da empresa estrangeira), a opção pela atribuição de critérios quantitativos dá mais transparência sobre um aspecto tão controverso do domínio dos offsets. Adicionalmente, ele mitiga os riscos de comportamento oportunista e corrupção. A desvantagem, como em casos anteriores, é a perda de flexibilidade administrativa e negocial.

---

<sup>7</sup> A caracterização da tecnologia como bem imaterial deriva da conceituação empregada por Longo (2007, p. 113), que a define como “o conjunto organizado de todos os conhecimentos científicos, empíricos ou intuitivos empregados na produção e comercialização de bens e serviços”.



### 11 – Serão listadas as tecnologias que se deseja obter com offsets?

Parece emergir uma tendência global em política de offset sobre essa questão. Observa-se a existência de países que listam, em seus manuais de compensação, quais as tecnologias que pretendem obter por meio desses acordos. É o caso, por exemplo, de Índia e Canadá. Tais tecnologias – especialmente quando selecionadas por serem portadoras de futuro – podem eventualmente distanciar-se daquelas encontradas em um sistema de C4IRS, navio de escolta ou caça fabricados no presente. Como selecionar quais tecnologias comporão tal lista e que ênfase será dada a ela (em oposição às demandas surgidas de negociações ad hoc feitas com empresas locais) são questões as quais os manuais encontrados não tratam. Convém um maior debate sobre o tópico.

### 12 – Como se lida com questões de licenças e direitos de uso de propriedade intelectual?

Projetos de cooperação industrial e tecnológica não raras vezes envolvem produtos (componentes, subsistemas, “softwares”, etc.) que estão segurados pelo regime internacional de proteção à propriedade intelectual. Para completar projetos de compensação nessas áreas, é possível que seja necessária a cessão desses direitos, mormente na forma de licenças. Entretanto, parece haver uma tendência global entre os grandes importadores de não aquiescer com o pagamento dessas licenças e/ou não contabilizá-las para efeito do cálculo do crédito de offset obtido. Se fazê-lo é eficaz e eficiente para o comprador, não é possível dizer. Não foram encontrados estudos dedicados especificamente a esse aspecto. Porém, dado que parece haver quase um consenso entre grandes importadores a respeito, convém a um manual de administração de offsets marcar posição clara sobre o tópico (isto é, afirmar diretamente se aceita ou não pagar/ contabilizar licenças e direitos de uso de propriedade intelectual, quando relacionados a programas de compensação).

### 13 – Será permitida a execução cruzada de créditos de offset?

O termo “execução cruzada de offsets” foi cunhado neste trabalho por conta da ausência, na literatura, de uma expressão melhor.

Essa execução ocorre de duas formas: a primeira, quando uma empresa executa com uma força singular (por exemplo, a Marinha) a obrigação de compensação que contraiu por conta de um contrato celebrado com outra (por exemplo, o Exército). Considere-se que essa hipotética empresa estrangeira já vem desenvolvendo projetos de offset com a Marinha e ganhou seu primeiro contrato com o Exército. É possível que haja mais ganhos de um investimento continuado com a força naval do que haveria caso se começasse “do zero” um programa de cooperação com o Exército ou empresas a ele relacionadas. Em havendo tal possibilidade, convém que seja facultado aos gestores exercê-la. Autorizar textualmente execuções cruzadas desse tipo, todavia, faz sentido apenas em países como o Brasil, nos quais cada força gere individualmente seus offsets. Se eles são administrados no nível do Ministério da Defesa, não haveria impedimentos *a priori* para “cruzamentos” dessa modalidade.

A outra forma de execução cruzada ocorre quando uma empresa estrangeira cumpre as obrigações devidas por outra. A lógica que orienta a decisão de um ente privado de fazer offsets em prol de outro é similar à descrita no parágrafo anterior. Considerem-se, hipoteticamente, duas empresas: “D” e “T”; ambas francesas, da área de defesa, que não competem entre si e a segunda é fornecedora usual da primeira. Assuma-se que “T” ganha um contrato em um país “A”, com o qual “D” já tem um histórico de cooperação e já possui programas de compensação em execução. É factível que haja mais ganhos adicionando o valor dos offsets devidos por “T” aos programas que “D” vem executando do que haveria se “T” começasse uma iniciativa inteiramente nova. É possível que o Estado comprador esteja particularmente interessado nos offsets que “T” (um fabricante de radares e sistemas C4IRS) pode oferecer, que “D” (uma empresa de construção naval) não pode. Todavia, em não sendo esse o caso e considerando-se os possíveis ganhos maiores em investimentos acumulados, convém que o documento de diretrizes sobre gestão de offsets estabeleça se autoriza ou não tais execuções cruzadas.

Caso a execução cruzada seja permitida, o manual de gestão de compensações deve também estabelecer em que condições ela é autorizada. Os indianos, por exemplo, só a autorizam quando uma das companhias estrangeiras é fornecedora ou subcontratada da outra. Já os coreanos, *a priori*, permitem arranjos de qualquer tipo que duas ou mais empresas internacionais proponham, sujeito apenas à aprovação do Presidente

do Conselho de Compensação. Parece haver consenso, todavia, de que, independentemente do fabricante que esteja cumprindo as obrigações de offset, a responsabilidade pelo seu sucesso continua recaindo sobre a empresa que ganhou o contrato principal.

#### 14 – Qual será o prazo para execução do programa de compensação?

Embora pareça secundária, a questão do prazo de execução do programa de compensação tem relevância, pois se relaciona diretamente à questão do sistema de penalidades em casos de atraso e descumprimento (tema da próxima questão). O estudo documental revela que há três maneiras mais comuns de estabelecer esse prazo: ou ele coincide com o de execução do contrato principal; ou ele será esse prazo acrescido de um período “x” de anos; ou ele será negociado individualmente. O tempo adicional “x” também fica estabelecido no manual de administração de offsets. Os governos que postulam que o prazo de execução será avaliado caso a caso costumam recomendar, porém, que ele coincida com o do contrato principal. Caso se opte por esse modelo de prazo flexível, convém que o documento de diretrizes estabeleça a quem cabe a decisão sobre essa definição (por exemplo, o presidente de uma hipotética comissão de compensação)

A única “quase exceção” encontrada na pesquisa documental (o que não exclui a possibilidade de que haja outras) ocorre na Índia. O governo indiano considera o prazo de execução do programa de compensação como o período do contrato principal acrescido de até dois anos. Todavia, para eles, o tempo de execução do contrato principal inclui a garantia fornecida pelo vendedor. Essa opção fornece estímulos para que o fabricante estrangeiro estipule uma garantia mais longa para o produto fornecido, particularmente se os offsets forem complexos e ele estimar que as possíveis penalidades derivadas de atrasos serão maiores do que aquilo que se gastaria nos primeiros anos da manutenção do produto. Este seria o período, a lógica orienta, em que os custos de manter o sistema seriam menores (particularmente se comparados com aqueles do fim de sua vida útil). Ainda assim, há a possibilidade de ganho mútuo. A desvantagem do modelo indiano é a de que ele tende a atrasar o momento em que o comprador passa a aproveitar os benefícios dos offsets, posto seus prazos se tonarem mais elásticos.

## 15 – Qual o sistema de penalidade no caso de descumprimento e/ou atraso?

Sobre esse tópico, um manual de gestão de offsets deve primeiro definir se há um sistema de penalidades para descumprimento do cronograma dos acordos de compensação. Nem todos os países preveem punições. Os israelenses, por exemplo, afirmam não estipular sanções de qualquer ordem. A única exceção seria nos casos de esgotamento das opções de renegociação, a partir do que – e apenas após consultas com outros ministérios envolvidos – a empresa estrangeira poderia ser proibida de contratar com o governo por um período não superior a cinco anos<sup>8</sup>. Mitra (2009, p. 62) observa que um programa de compensação será bem-sucedido apenas se as duas partes – a que fornece offsets e a que os recebe – tiverem um interesse real em seu sucesso. A estipulação de punições rígidas por não conformidade, segundo o autor, “pode ser contraproducente”, uma vez que contrariaria o princípio da boa-fé entre parceiros. Caso se escolha estabelecer um sistema de penalidades, deve-se decidir se elas serão aplicadas de maneira escalonada – seguindo um cronograma com marcos temporais (semestrais, anuais...) pré-acordados –, ou se as sanções serão aplicadas apenas ao final do período previsto para execução dos offsets. O documento de diretrizes pode também postular quais serão essas punições. Elas podem ser: pagamento de multas e rescisões; desconto no montante a ser pago pelo contrato principal; suspensão dos pagamentos do contrato principal; recuperação (parcial ou total) de um título de performance (ou outra forma de seguro); entre outras. Não é incomum que os documentos de diretrizes ofereçam alguma condescendência às empresas estrangeiras e estabeleçam um limite da obrigação não cumprida a ser penalizada nesses moldes. Assim, termina-se com uma redação nos moldes de “essas penalidades serão cobradas até o limite de 20% (ou outro valor) da obrigação total de offset”. Há governos que estabelecem esse limite, porém postulando-o válido apenas para atrasos no cronograma parcial do projeto de compensação. Se houver descumprimentos após o fim do período total de execução do contrato de offset, as penalidades passam a ser aplicadas sem um limite percentual.

---

<sup>8</sup> Informações Disponíveis em: <<http://www.moital.gov.il/NR/exeres/85C96324-328D-40FC-9E8A-78B6CC5F6E7E.htm>>. Acesso em: 20 fev. 2016.

Assim, há quatro decisões a se tomar no que tange a punições: se elas serão aplicadas, ou não; quais serão as formas de penalização; em havendo mais de uma, a quem compete estabelecer qual delas será aplicada; se há um limite nas penalizações (expresso em percentual do valor total do programa de offset); e, em havendo esse limite, se ele é válido para atrasos no cronograma parcial ou se será estendido também para descumprimentos do prazo final de execução do programa de compensação.

16 – São exigidos títulos de performance (ou, no caso brasileiro, Seguro Garantia e Fiança Bancária, entre outras formas previstas na legislação)?

Títulos de performance são, grosso modo, seguros emitidos por bancos e outras instituições financeiras. Eles podem tanto ser exigidos como um pré-requisito anterior sequer ao início da execução do programa de compensação, quanto ser demandados apenas em caso de atrasos ou descumprimentos (ocasião em que funcionam como penalidade). Tomada a decisão de exigir títulos de performance, deve-se decidir qual será seu valor. Quando os gestores optam por demandá-los antes da execução do programa, parece ser comum exigir a emissão de um título no valor integral a ser compensado. Quando eles funcionam como penalidade, é mais recorrente que eles sejam exigidos como uma fração da obrigação não compensada (por exemplo, 50% da obrigação de offset que não foi cumprida após o primeiro marco temporal do contrato). Por fim, convém que o manual de gestão defina qual o valor do título a ser resgatado em caso de descumprimentos. A pesquisa documental revelou não ser tão recorrente o resgate do valor integral do título. Normalmente ele é resgatado parcialmente (por exemplo, 20% de seu valor de face a cada seis meses de atraso). Embora a exigência por tais títulos tenha sido recorrente nos documentos estudados, não houve um padrão predominante na maneira, periodicidade e valores exigidos.

Títulos de performance representam um risco extra e um custo adicional para a empresa estrangeira. Risco e custo que serão tanto maiores quanto mais altos forem os valores dos títulos exigidos pelo órgão gestor do offset. A decisão de quanto desse risco colocar sobre a parte estrangeira (ao exigir percentuais maiores ou menores) – incluindo a opção de não colocar risco ao não exigir tais seguros – é uma que deve ser tomada observando

o retrospecto recente dos acordos celebrados. Porque embora sejam um risco, esses títulos funcionam também como um estímulo às companhias estrangeiras, a fim de que executem tempestivamente os *offsets* com os quais concordem. Portanto, pensando no caso brasileiro, optar por exigilos e como fazê-lo depende de responder a seguinte pergunta: atrasos e descumprimentos vêm sendo recorrentes por parte de parceiros estrangeiros, a ponto de gerar a necessidade de que se os estimule a serem mais diligentes na execução dos acordos de compensação? É possível que esses retardamentos não sejam comuns, o que dispensa a necessidade de exigir títulos de desempenho. Alternativamente, é possível que apenas um fornecedor em particular tenha sido particularmente displicente no passado recente, de tal maneira que é possível que valha à pena refletir sobre uma regra que estabeleça a cobrança de títulos de *performance* apenas se um fornecedor tiver atrasado a execução de suas obrigações com o governo comprador (neste caso, o Estado brasileiro) em um determinado período de tempo (por exemplo, nos últimos dez anos). Essa opção se coloca como alternativa à regra de exigir títulos de *performance* de todas as companhias que fornecerão *offsets*.

#### 17 – O governo comprador terá um sistema de banco de créditos de *offset*?

É possível que, no decurso de um programa de compensação, a empresa estrangeira tenha um desempenho acima do originalmente estimado e obtenha créditos de *offset* além do necessário. O que fazer, então, com o excedente? A maioria dos documentos de diretrizes estudados ao longo da pesquisa postula a existência de um sistema de banco de créditos de *offset*.

Decidindo-se pela implementação de um banco de crédito de compensação, cabe estabelecer se esses créditos terão um prazo de validade. O padrão internacional parece oscilar entre três e seis anos, a partir da data em que a autoridade governamental os certifica. Após esse período, se não forem utilizados, os créditos expiram. Outro ponto que cabe ao manual de gestão de *offsets* disciplinar é o percentual de créditos acumulados que podem ser utilizados no cumprimento de obrigações futuras. A tendência internacional parece ser estabelecer que no máximo 50% do valor das novas obrigações possa ser satisfeito utilizando créditos acumulados. Esse percentual pode variar, todavia. O Canadá não permite que a companhia estrangeira “fracione” os créditos que têm reservados. Ela deve utilizar a

totalidade de que dispõe, ainda observando o teto estabelecido (também de 50%). Hipoteticamente, então, uma empresa “A” que deva compensar o governo em 60 milhões de dólares pode fazê-lo com até US\$ 30 milhões em créditos acumulados. Caso ela disponha de US\$ 40 milhões no banco de créditos de offset, deverá utilizar integralmente esse valor, e não apenas o máximo permitido. Pelo que se constata, então, que US\$ 10 milhões em créditos de compensação acumulados serão perdidos. O governo canadense, todavia, foi o único encontrado na pesquisa que impôs tal limitação. As diretrizes dos outros países não impõem restrições semelhantes.

O último ponto que convém ao manual disciplinar é o da transferibilidade entre empresas de créditos acumulados. Ele deve estabelecer se permite, ou não, essa transferência. Caso permita, ele deve postular se ela será irrestrita ou se algum tipo de limitação será imposta, isto é, a transferência apenas será autorizada entre empresas com relação produtiva e/ou acionária entre elas (quando fornecem componentes uma para a outra e/ou quando uma é proprietária/propriedade da outra). Para observar o princípio da transparência, é desejável que o documento aponte a autoridade responsável por autorizar essas transferências (se tal autorização for requerida).

18 – Haverá dispositivos especiais nos casos em que a venda do produto de defesa é intermediada pelo governo estrangeiro, mas o contrato de offset é assinado diretamente com a empresa fabricante?

O caso mais tradicional – embora não o único – de venda de produtos de defesa intermediada por um governo estrangeiro é o do programa “Foreign Military Sales (FMS)” dos Estados Unidos. Todavia, o governo dos EUA não assume responsabilidade ou promove intermediação na celebração de acordos de compensação. Em aquisições feitas via FMS, o governo comprador está adquirindo os produtos de defesa diretamente do governo americano (via “Defense Security Cooperation Agency”), mas acordando os offsets com o fabricante original do equipamento, uma empresa privada. Para criar uma relação direta entre o provedor das compensações e o comprador, é possível que o segundo tome precauções extras. Os indianos, por exemplo, exigem a emissão de título de performance no valor de 5% do total de offsets devidos.

Em vendas intermediadas pelos governos – particularmente

quando estes absorvem das empresas o risco de inadimplência, como ocorre no FMS – é possível que falte às companhias privadas o estímulo necessário para o cumprimento diligente de suas obrigações de compensação. Parece razoável, portanto, refletir sobre os possíveis mecanismos que o governo comprador pode estipular para gerar tal estímulo. Demandar a emissão de um título é uma maneira possível. Como em outras questões expostas anteriormente, não há um curso de ação necessariamente correto. O que há são opções político-administrativas. Refletindo sobre o caso brasileiro: se em casos de vendas intermediadas por seus governos, as empresas estrangeiras não geraram problemas na execução de offsets, é possível dispensar salvaguardas adicionais.

19 – Serão exigidos offsets de empresas locais que utilizem, em seus produtos e soluções, grande percentual de conteúdo estrangeiro?

Cobrar offsets de empresas locais pode parecer um contrassenso. Por definição, compensações seriam cobradas exclusivamente de companhias estrangeiras. Behera (2015, p. 74-75) argumenta, todavia, que a cobrança de offsets a empresas locais visa a estimular o desenvolvimento efetivo de uma base industrial de defesa e impedir que conglomerados internacionais utilizem empresas nacionais apenas como fachada (“front organization”), sem agregar conhecimento ou valor real à produção local. Se o documento de diretrizes optar por cobrar compensações de empresas nacionais, convém que ele estabeleça se haverá um percentual de conteúdo estrangeiro até o qual elas estarão isentas da necessidade de fornecer offsets. Por exemplo, “se até 50% (em valor) do produto for composto de componentes estrangeiros, a empresa nacional não precisará fornecer compensações”. O valor de 50% nesse caso é meramente hipotético. O manual de gestão pode estabelecer um número diferente. Esse documento deve fazer outra diferenciação importante. Se o conteúdo estrangeiro exceder o limite de isenção, os offsets serão cobrados sobre o todo o valor do conteúdo não nacional ou apenas sobre a faixa que exceda aquele limite? Retornando à hipótese anterior, se o limite de isenção for de 50% e o conteúdo estrangeiro no produto local for 60%, serão cobrados offsets sobre todo o valor de 60% ou apenas sobre os 10% que excedem o teto permitido? Questões desse gênero precisam ser esclarecidas.



Uma vez mais, não há opção correta ou errada. A escolha por cobrar, ou não, offsets de empresas locais reflete o quão isoladas ou integradas às cadeias globais de suprimento o governo local quer que suas indústrias estejam. Penalizar com a exigência de compensações as companhias que utilizem muitos subsistemas estrangeiros pode estimulá-las a nacionalizar conteúdo, mas também podem ter consequências deletérias sobre sua competitividade (refletida no preço pago pelo erário) e sobre sua capacidade de se tornar fornecedora de grandes empresas globais.

20 – Há dispositivos, nos documentos do país importador, para quando suas empresas estiverem exportando e forem, portanto, credoras de offset?

Usualmente, documentos de diretrizes de países importadores se limitam a governar os offsets que lhe são devidos. Todavia, eventualmente surge de um Estado tradicionalmente importador uma empresa com capacidade e competitividade para exportar. Os gestores de offset devem decidir, então, se o seu documento de diretrizes estabelecerá alguma providência para apoiar essas empresas. Idealmente, ele versaria sobre o que o governo, e particularmente o Ministério da Defesa, pode e não pode fazer para dar suporte a essas empresas. Ele contemplaria (ou proibiria) as possibilidades de “swaps” ou isenções de offsets, isto é, anular obrigações mútuas de offset entre dois países quando o fluxo comercial de produtos de defesa é bilateral, e não apenas unilateral. O documento de diretrizes pode também esclarecer se haverá diferenciação entre o apoio fornecido pelo governo a empresas privadas e estatais.

Considerações dessa natureza devem ser particularmente cuidadosas na observação da legislação existente. O país “A” não cobrar offsets de uma empresa de um país “B”, porque uma indústria privada do primeiro está vendendo produtos para o governo do segundo pode ser tomado como uma confusão indevida entre a coisa pública e a esfera privada. Em tese, o Estado está deixando de se beneficiar (nesse caso específico, de offsets) para prestar auxílio a uma companhia privada. Operações dessa natureza podem ser ilegais, dependendo do arcabouço legislativo nacional, e chamar a atenção dos órgãos de auditoria e controladoria.

21 – Há dispositivos que versem sobre programas de offset derivados de aquisições feitas em situações emergenciais?

É da natureza das forças armadas serem empregadas em situações de crise. A deflagração de guerras, a participação em operações de defesa civil decorrentes de grandes desastres naturais ou um engajamento em operações de paz da ONU podem gerar a necessidade de equipar tempestivamente os militares. Todo o processo de negociação de acordos de offset pode alongar o período entre o surgimento da necessidade e a efetiva entrega do equipamento, prejudicando as operações como um todo. Por isso, é recomendável que o documento de diretrizes verse sobre programas de offset derivados de aquisições feitas em situações emergenciais. Ele pode, por exemplo, considerar a possibilidade de adiamento dos processos de negociação e execução dos acordos de compensação até que a crise esteja dirimida, ou mesmo admitir a possibilidade de não exigir offsets de nenhuma ordem (se, além do prazo, os custos se tornarem uma variável particularmente sensível).

## 22 – Há alguma restrição ao serviço de “offset brokerage”?

Os “brokers” (“corretores”, ou “intermediários”) de offsets são profissionais privados dedicados a fazer a intermediação entre empresas estrangeiras e governos compradores, articulando acordos e localizando e conectando parceiros comerciais e industriais. A atuação desses indivíduos, embora a priori legal, por vezes está associada à corrupção e ao beneficiamento indevido de grupos de interesse. O manual de gestão de offsets pode considerar estabelecer restrições – uma vez que criminalizar é atribuição do Legislativo – à livre atuação de “brokers”. O governo canadense demanda que as empresas estrangeiras se comprometam a não efetuar, a profissionais privados, pagamentos que sejam contingentes ao aceite de projetos de compensação nos quais aqueles tenham participado. O Canadá foi, contudo, o único Estado pesquisado a estabelecer limitações dessa natureza. Uma vez mais, a questão é ajustar a política à resolução de problemas reais. Se a atuação de “brokers” começar a ser frequentemente associada a práticas corruptoras ou antiéticas, pode-se considerar que o documento de diretrizes limite sua capacidade de agência ao pressionar, por mecanismos variados, empresas estrangeiras a não contratarem seus serviços. Do contrário, disposições nesse sentido podem ser desnecessárias. É recomendável, todavia, que o governo exija da parte estrangeira a notificação do emprego dos serviços desses profissionais. Facilitando, assim, eventuais trabalhos posteriores de auditoria e investigação.

### 23 – Como o órgão gestor dos offsets avalia programas executados?

Uma das “boas práticas” da administração pública é avaliar os resultados das políticas implementadas. É esse processo de avaliação que permite identificar méritos e falhas, recomendando aperfeiçoamentos e, eventualmente, a descontinuidade das políticas públicas executadas. A aferição do êxito de políticas de offset esbarra frequentemente na indisponibilidade de dados empíricos, que são protegidos tanto pelas empresas quanto pelos governos compradores. O não acesso às fontes primárias é um problema que parece afligir muitos autores (MITRA, 2009; KIRSCHWEHM, 2014; BEHERA, 2015). Brauer e Dunne (2004, p. 01) afirmam ser comum que os próprios governos que cobram os offsets não se mostrem dispostos a avaliar os ganhos econômicos de seus programas de compensação.

Ainda assim, um documento de diretrizes pode estipular maneiras de avaliar o sucesso dos programas de offset conduzidos. O governo sul-coreano prevê uma fórmula (COREIA DO SUL, 2014, p.16) que correlaciona, entre outros elementos, o montante do contrato principal, o percentual exigido de offsets, o valor das operações de compensação realizadas, o prazo de execução e um elemento arbitrário (o valor de “classes de offset”, estipulado a partir da complexidade das tecnologias ofertadas pela parte estrangeira). O governo canadense correlaciona o valor do investimento feito, sua qualidade em relação aos objetivos do programa de compensação e o risco envolvido na transação, associado a outros elementos (a divisão da pontuação total pelo valor a ser compensado, seguido pela multiplicação desse número por 100, estabelecendo um valor mínimo para aprovação) (CANADÁ, 2013a, p. 11). Não se pretende aqui sugerir um transplante das fórmulas coreana ou canadense para os documentos dos militares brasileiros. É preciso, todavia, reconhecer que o esforço de elaborar uma equação que oriente avaliações *a posteriori* do programa de compensação se coaduna com as boas práticas da administração da coisa pública. Cabe, portanto, chamar atenção para a necessidade de se estipular uma fórmula que garanta maior grau de objetividade e transparência à avaliação de programas de offset, sem desrespeitar leis razoáveis de proteção a informações sigilosas.

Como fica evidente, as perguntas acima listadas se relacionam ao processo de elaboração de um manual de gestão de acordos de offset em seu

aspecto “formal”. A tradução da “forma” de um documento de diretrizes para a prática tende a ser um processo intrincado, mesmo quando o país que fornece os offsets e aquele que os recebe tenham atingido razoável grau de entendimento político<sup>9</sup>. Sem os dados empíricos, é virtualmente impossível identificar quais são os efetivos problemas enfrentados por um país na execução de seus programas. Por isso, refletindo sobre o caso brasileiro, estes autores optaram por elaborar os tópicos supracitados na forma de perguntas, e não de afirmações ou respostas.

## CONSIDERAÇÕES SOBRE O ARCABOUÇO LEGAL BRASILEIRO

O primeiro elemento do arcabouço legal brasileiro (em ordem de precedência, não necessariamente cronológica) a versar especificamente sobre offsets é o Decreto nº 7.546 da Casa Civil, que estabelece a Comissão Interministerial de Compras Públicas (BRASIL, 2011). A ele se segue a Portaria Normativa nº 764 do Ministério da Defesa, que aprova a “Política e as Diretrizes de Compensação Comercial, Industrial e Tecnológica do Ministério da Defesa” (BRASIL, 2002). As Forças Singulares possuem diretivas próprias sobre o tema. Na Força Aérea, os atos normativos que versam sobre compensações são a DCA 360-1, que institui a “Política e Estratégia de Compensação Comercial, Industrial e Tecnológica da Aeronáutica” (BRASIL, 2005) e a ICA 360-1, que veicula os “Preceitos para a Negociação de Acordos de Compensação Comercial, Industrial e Tecnológica na Aeronáutica” (BRASIL, 2005a). Na Marinha, as normas sobre acordos de compensação estão contidas no capítulo 14 das “Normas Sobre Licitações, Acordos e Atos Administrativos (NOLAM)” (BRASIL, 2008) e no anexo 7 da Portaria nº 59 do Gabinete do Comandante da Marinha, que veicula as “Diretrizes para a Compensação Comercial, Industrial e Tecnológica da Marinha” (BRASIL, 2010). O documento equivalente no Exército é o “Normas para Gestão de Acordos de Compensação Comercial, Industrial e Tecnológica no Exército Brasileiro” (BRASIL, 2011a).

Na exposição acima se evidencia a primeira, e possivelmente a maior, discrepância entre o arcabouço normativo brasileiro e as “melhores práticas internacionais”. Ao passo que, no Brasil, cada uma das forças

---

<sup>9</sup>Para uma descrição dos problemas enfrentados já nos primeiros estágios de um programa de offset, ver MARTINS (2013, p. 59-60).

possui seu manual próprio, os demais Estados parecem convergir para a gestão de offsets em um órgão comum, mormente o Ministério da Defesa. A “singularização” das políticas tem consequências. Ainda que harmonizadas entre si – posto estarem fundamentadas nas mesmas leis – há discrepâncias entre as normas das três forças, o que leva os industriários brasileiros a queixarem-se de que “cada uma faz offset de um jeito”<sup>10</sup>.

As diferenças na execução observadas pelo empresariado nacional aparecem também na redação das normas de cada força. Em observância ao Decreto 7.456, as três estabelecem o patamar mínimo a partir do qual exigem offsets; 5 milhões de dólares para Força Aérea e Exército (BRASIL, 2005a, p. 15; BRASIL, 2011a, p. 55) e R\$ 1 milhão para a Marinha (BRASIL, 2008, p. 92). A Portaria nº 59 do Comandante da Marinha retifica esse valor para R\$ 5 milhões. As três admitem a possibilidade de requerer compensações em aquisições de menor monta. A Marinha, porém, é a única a fazer uma exigência que se assemelhe a uma cobrança de offsets de uma empresa nacional ao afirmar que “[q]uando, para cumprimento de um contrato com a MB, uma empresa nacional tiver que importar bens e/ou serviços, será exigido também um AC<sup>11</sup> entre a empresa contratada e o fornecedor estrangeiro”. (BRASIL, 2008, p. 90). A redação desse item é dúbia, todavia, pois não deixa claro sobre quem recai a obrigação junto à Marinha (se sobre a companhia brasileira ou sobre a estrangeira). E postula algo para o qual não foi localizado precedente em documentos estrangeiros: um acordo de compensação entre duas empresas e não entre a empresa estrangeira e o governo local. Reconhece-se, entretanto, que essa pode ser apenas uma imprecisão na maneira como se redige o artigo, sem maiores consequências para a execução de compensações.

As três forças admitem o acúmulo (“banking”) de offsets, mas apenas a Marinha restringe de maneira mais clara a transferência de créditos acumulados de uma empresa para outra (BRASIL, 2008, p. 94). As outras duas forças são reticentes sobre a matéria, não permitindo nem proibindo expressamente tal transferência (BRASIL, 2005a, p. 10; BRASIL, 2011a, p. 62). Nenhuma das três estabelece um prazo da validade para créditos acumulado ou estipula um limite para o quanto de uma obrigação futura pode ser cumprida utilizando crédito excedente de offsets passados.

---

<sup>10</sup> Comunicação realizada por representante de empresa, durante o “Workshop de Offset - Atualizações e Perspectivas”, organizado pelo Centro para a Competitividade e Inovação CECOMPI entre os dias 11 e 12 de dezembro de 2014. Em 12-12-2014, São José dos Campos.

<sup>11</sup> “AC” é a sigla para “Acordo de Compensação” no documento citado.

O Exército é o único a prever no texto de suas Normas a aplicação de penalidades à empresa estrangeira por atrasos ou descumprimentos. Todavia, ele não estabelece modalidades e é pouco claro na definição dos marcos temporais sobre os quais aplicará sanções. Há a menção a punições nos documentos da Marinha e da Força Aérea. Elas não são feitas, todavia, no texto das normas em si e só aparecem em seus anexos. No anexo Z da NOLAM, chamado “Modelo de Acordo de Compensação”, a Marinha estabelece um sistema de multas que incidem sobre o percentual não cumprido de obrigações (BRASIL, 2008, p. 210-211). No Anexo I da ICA 360-1, chamado “Acordo de Compensação Comercial, Industrial e Tecnológica”, a Força Aérea apresenta uma sistemática para incidência de penalidades consideravelmente mais sofisticada do que outros Estados pesquisados, incluindo fórmulas para o cálculo de multas e prevendo períodos para solicitação de recursos (BRASIL, 2005a, p. 46). O que permanece como fator gerador de dúvida e imprecisão é o fato de que essas penalidades não são explicadas no texto das normas. Duas questões ficam, portanto, em suspenso: se a previsão de sanções é mandatória ou se dependerá da discricionariedade do gestor; e, em havendo penalidades, se elas seguirão as fórmulas mostradas nos anexos ou serão negociadas *ad hoc* entre as partes.

Somente nos documentos da Força Aérea foram localizadas menções à exigência de uma garantia financeira. Ainda assim, os mesmos problemas anteriores se repetem. A primeira menção é feita em um anexo (“C - Exemplo de Instrumento Convocatório”) e a linguagem com que a cláusula é formulada é pouco específica quando comparada àquela encontrada em documentos estrangeiros. Diz apenas que “[p]oderão ser exigidas garantias financeiras para assegurar a plena execução do Acordo de Compensação, principalmente quando a vigência do Acordo de Compensação não coincidir com a do contrato associado” (BRASIL 2005a, p. 27). A outra menção à existência de um seguro ocorre no supramencionado artigo que trata de penalidades por atraso (BRASIL, 2005a, p. 46). Como as provisões sobre garantias financeiras aparecem apenas nos anexos, não há clareza sobre sua obrigatoriedade e nem sobre as formas que podem tomar.

Os documentos brasileiros – Decreto nº 7546 da Casa Civil, Portaria Normativa nº 764 do Ministério da Defesa, DCA 360-1, ICA 360-1, NOLAM, Portaria nº 59 do Gabinete do Comandante da Marinha e as “Normas para Gestão de Acordos de Compensação Comercial, Industrial e Tecnológica no

Exército Brasileiro” – não fazem listas de tecnologias que pretendem obter por intermédio de offsets, mas tratam com mais detalhes do que suas contrapartes internacionais do processo de prospecção de necessidades junto à indústria nacional. Eles também discorrem mais extensamente sobre os objetivos e prioridades de suas respectivas políticas de compensação.

Outro ponto que se sobressai nas normas das forças armadas nacionais é o grau de detalhamento com o que todo o processo decisório relativo aos contratos de compensação é descrito. Ainda assim, chama atenção o fato de que questões as quais outros Ministérios da Defesa buscaram detalhar tenham sido tratadas com imprecisão nos documentos nacionais. Convém rediscutir o tema para, idealmente, redigir um documento único para as três forças e formular respostas claras às questões para as quais outros Estados dedicaram especial atenção.

Cumprе ressaltar que o Ministério da Defesa, por meio de sua Secretaria de Produtos de Defesa (SEPROD), envida esforços para a elaboração de uma Política Nacional de Compensação Comercial, Industrial e Tecnológica (PNAC). Debates têm sido realizados envolvendo diversos atores, tanto do setor público quanto do privado.<sup>12</sup> A formulação concertada de uma política nacional de offset pode vir a ser um importante passo no sentido de orientar entes públicos em negociações e posturas relativas a contratos de compensação em aquisições de defesa. Pode, ainda, vir a considerar e esclarecer várias das questões apresentadas ao longo deste trabalho.

## CONSIDERAÇÕES FINAIS

Na busca por elementos úteis à política e à gestão de compensações comerciais, industriais e tecnológicas em aquisições de defesa, este trabalho perscrutou subsídios na experiência internacional, comumente referidas como “boas práticas”. Sem pretender oferecer lições, foram apresentadas informações sobre as tendências globais das políticas de offset de países grandes compradores de sistemas de defesa. Importa, evidentemente, evitar a adoção acrítica das políticas de gestão de offset praticadas alhures, afinal, o que rendeu bons resultados em outros Estados ou em outras épocas pode não ter o mesmo efeito no Brasil atual.

---

<sup>12</sup> Disponível em: <<http://www.defesa.gov.br/index.php/noticias/17382-defesa-debate-politica-nacional-de-compensacao-comercial-com-a-fiesp>>. Acesso em: 12 jun. 2016.

Todavia, a análise dos documentos internacionais revela a emergência de alguns padrões. Eles parecem convergir, por exemplo, em torno da gestão em nível ministerial (e não de forças singulares); da delimitação mais restrita das modalidades de compensação que aceitam; da não aceitação de taxas de licenciamento e afins (ao menos para efeito de cálculo de créditos de offset); da estipulação de um sistema claro de penalidades; e da exigência de títulos de performance. Isso não quer dizer que os países formulem requerimentos idênticos em torno dessas questões, mas sim que elas estão presentes em seus manuais ou guias de procedimento, de uma maneira ou de outra, em diferentes graus de exigência.

Cabe, ainda, destacar que documentos de diretrizes e/ou de gestão de offsets não são estanques. Ao contrário, seu dinamismo reflete as mudanças tecnológicas dos produtos de defesa a que estão vinculados e das empresas que atuam no setor, caracterizadas pela necessidade de inovar regularmente. Canadá e Emirados Árabes Unidos, por exemplo, chegam, em determinados períodos, a atualizar suas políticas bianualmente. Convém, portanto, rediscutir a gestão de offsets no Brasil, formulando um documento único de diretrizes para as três forças que, partindo de uma reflexão aprofundada sobre as “boas práticas internacionais”, responda aos problemas e às demandas nacionais.



# OFFSETS POLICIES AND MANAGEMENT IN DEFENCE ACQUISITIONS: CONTRIBUTIONS OF INTERNATIONAL BEST PRACTICES TO BRAZIL

## ABSTRACT

---

This paper explores the characteristics of the commercial, industrial and technological compensation agreements, commonly known as “offsets”, practiced internationally. Through the elaboration of a theoretical and conceptual framework, this paper seeks to infer - from the international best practices - contributions for the improvement of defense offset management in Brazil. Based on a master’s research by the first author, under the supervision of the second, this article summarizes contributions that can inform the reflections of agents involved in the formulation of the legal and normative frameworks regarding offset administration.

**Keywords:** Defense Acquisition. Offsets. Transfer of Technology.

## REFERÊNCIAS

BALAKRISHNAN, Kogila. *Evaluating the Effectiveness of Offsets as a Mechanism for Promoting Malaysian Defence Industrial and Technological Development*. 2007. 526 f. Tese (Doutorado) - Cranfield University, 2007.

BASKARAN, Angathevar. The role of offsets in Indian defense procurement policy. In: BRAUER, Jurgen; DUNNE, J Paul. *Arms trade and economic development: theory, policy, and cases in Arms trade offsets*. Londres: Routledge, 2004.

BEHERA, Laxman. *Defence Offsets: International Best Practices and Lessons for India*. IDSA Monograph Series No. 45. Nova Delhi: Institute for Defence Studies and Analyses, 2015.

BRASIL. Aeronáutica. *Política e Estratégia de Compensação Comercial, Industrial e Tecnológica da Aeronáutica*. Brasília, 2005.

BRASIL. Aeronáutica. *Preceitos para a Negociação de Acordos de Compensação Comercial, Industrial e Tecnológica na Aeronáutica*. Brasília, 2005a.

BRASIL. Marinha. *Diretrizes para a Compensação Comercial, Industrial e Tecnológica da Marinha*. Brasília, 2010.

BRASIL. Exército. Estado-Maior. *Normas para Gestão de Acordos de Compensação Comercial, Industrial e Tecnológica no Exército Brasileiro*. 2011a.

BRASIL. Secretaria-Geral da Marinha. *Normas sobre Licitações, Acordos e Atos Administrativos*. 2008.

BRAUER, Jurgen; DUNNE, J Paul (Org.). *Arming the South: The Economics of Military Expenditure, Arms Production and Arms Trade in Development Countries*. Londres: Palgrave, 2002.

BRAUER, Jurgen; DUNNE, J Paul (Org.). *Arms Trade and Economic Development: Theory, Policy, and Cases in Arms Trade Offsets*. Londres: Routledge, 2004.

BRAUER, Jurgen; DUNNE, J Paul. COYNE, Christopher (Org.). *Arms Trade Offsets: What do We Know?* In: *The Handbook On The Political Economy of War*. Northampton: Edward Elgar Publishing, 2011.

CANADA. Innovation, Science and Economic Development Canada. *IRB Bidder Instructions*. 2013.

CANADA. Innovation, Science and Economic Development Canada. *IRB Evaluation Plan*. 2013a.

CANADA. Innovation, Science and Economic Development Canada. IRB *Terms and Conditions*. 2013b. Disponível em: <<https://www.ic.gc.ca/eic/site/042.nsf/eng/00067.html>> Acesso em: 22 jan. 2016.

CHINWORTH, Michael. Offset policies and trends in Japan, South Korea, and Taiwan. In: BRAUER, Jurgen; DUNNE, J Paul. *Arms Trade and Economic Development: Theory, Policy, and Cases in Arms Trade Offsets*. Londres: Routledge, 2004.

COREIA DO SUL. Defense Acquisition Program Administration. *Offset Program Guidelines*. 2014.

DUMAS, Lloyd. Do offsets mitigate or magnify the military burden? In: BRAUER, Jurgen; DUNNE, J Paul. *Arms Trade and Economic Development: Theory, Policy, and Cases in Arms Trade Offsets*. Londres: Routledge, 2004.

EMIRADOS ÁRABES UNIDOS. *Tawazun Economic Program Guidelines*. 2015.

FERGUSSON, James. Search of a Strategy: The Evolution of Canadian Industrial and Regional Benefits Policy. In: MARTIN, Stephen. (Org.) *The Economics of Offsets: Defence Procurement and Countertrade*. Nova York: Routhledge, 1996.

GAMELL, Denis. *Nota sobre Compensação (Offset)*. Disponível em: <<http://denisgamell.jusbrasil.com.br/artigos/163749563/nota-sobre-compensacao-offset>> Acesso em: 29 jan. 2016.

GILPIN, Robert. *Global Political Economy: Understanding the International Economic Order*. Princeton: Princeton University Press, 2001.

HALL, Peter; MARKOWSKI, Stefan. On the Normality and Abnormality of Offsets Obligations. *Defence and Peace Economics*, v. 5, 1994.

HAMMOND, Grant. *Countertrade, Offsets and Barter in International Political Economy*. Nova York: St. Martin's Press, 1990.

HAN, Nam Sung; PARK, Joon Soo. The Defense Offset Policy in South Korea. *The KIDA Papers*, n. 4. Seul: Korea Institute for Defense Analyses, 2004.

INDIA. *Defence Procurement Procedure 2013: Capital Procurement*. Nova Delhi, 2013.

JUSTEN FILHO, Marçal. *Comentários a Lei de Licitações e Contratos Administrativos*. 16 ed. Rio de Janeiro: Editora Revista dos Tribunais, 2014.

KELLER, William. *Arm in Arm: The Political Economy of the Global Arms Trade*. Nova York: Basic Books, 1995.

KIRCHWEHM, Heinz. Success Factors in Offset Deals: A Case Study Based Examination. *International Journal of Business Research and Management (IJBRM)*, v. 5, n. 2, 2014.

LONGO, Waldimir Pirró e. Tecnologia Militar: conceituação, importância e cerceamento. *Revista Tensões Mundiais*, Fortaleza, CE, v. 3, n. 5, p. 111-143, 2007.

MARKUSEN, Ann. Should We Welcome a Transatlantic Defense Industry? In: REPPY, J. (Org.) *The Place of the Defense Industry in National Systems of Innovation*. Ithaca: Cornell University Press, Peace Studies Program, 2000. p. 25-47.

MARTIN, Stephen. (Org.) *The Economics of Offsets: Defence Procurement and Countertrade*. Nova York: Routledge, 1996.

MATTHEWS, Ron. Saudi Arabia: Defense Offsets and Development. In: BRAUER, Jurgen; DUNNE, J Paul (Org.) *Arming the South: The Economics of Military Expenditure, Arms Production and Arms Trade in Development Countries*. Londres: Palgrave, 2002. p. 195-219.

MIRUS, Rolf; YEUNG, Bernard. *The Economics of Barter and Countertrade*. Cheltenham: Edward Elgar Publishing, 2001.

MITRA, Anuradha. A Survey of Successful Offset Experiences Worldwide. *Journal of Defence Studies*, v. 3, n. 1. 2009.

RAMADY, Mohamed. Components of technology transfer: a comparative analysis of offset and non-offset companies in Saudi Arabia. *World Review of Science, Technology and Sustainable Development*, v. 2, n. 1, 2005.

Recebido em: 07/03/2016

Aceito em: 09/12/2016



# O EXÉRCITO BRASILEIRO E A EMULAÇÃO DOS MODELOS FRANCÊS E ESTADUNIDENSE NO SÉCULO XX

Eduardo Munhoz Svartman<sup>1</sup>

## RESUMO

---

Na primeira metade do século XX o Exército Brasileiro empreendeu reformas para modernizar-se e reequipar-se com armas e doutrinas atualizadas. Este processo, apesar de conduzido pelas autoridades brasileiras, dependeu do estabelecimento de convênios com duas grandes potências, a França e os Estados Unidos. Em função disso, texto investiga, numa perspectiva comparada, os processos de emulação decorridos da vigência da Missão Militar Francesa (1919-39) e dos acordos militares firmados pelo Brasil com os Estados Unidos em 1942 e 1952. A análise privilegia os aspectos relativos às negociações e interesses envolvidos nos dois convênios; alcance da cooperação; adoção de armas, equipamentos e doutrinas; resistências e adaptações; bem como as implicações políticas, internas e externas, da adoção dos dois modelos. **Palavras-chave:** Emulação militar; modernização; relações Brasil-França; relações Brasil-Estados Unidos.

---

<sup>1</sup>Doutor em Ciência Política, professor dos programas de pós-graduação em Ciência Política (PPG-Pol) e em Estudos Estratégicos Internacionais (PPG-EEI) da UFRGS, Porto Alegre, RS, Brasil. E-mail: eduardosvartman@gmail.com.

## INTRODUÇÃO

Na primeira metade do século XX o Exército Brasileiro empreendeu reformas no sentido de modernizar-se e de melhor aparelhar-se para o desempenho das funções militares clássicas. Este processo, apesar de conduzido pelas autoridades brasileiras, dependeu do estabelecimento de convênios com duas grandes potências, a França e os Estados Unidos. Considerando o impacto e a sua contiguidade temporal, este texto investiga, numa perspectiva comparada, os processos de emulação de modelos organizacionais decorridos da vigência da Missão Militar Francesa (1919-39) e dos acordos militares firmados pelo Brasil com os Estados Unidos em 1942 e 1952. A análise privilegia os aspectos relativos às negociações e interesses envolvidos nos dois convênios; adoção de armas, equipamentos e doutrinas; resistências e adaptações bem como as implicações políticas, no Brasil, da adoção dos dois modelos.

A emulação militar consiste na deliberada imitação de aspectos do sistema militar de um país por parte de outro. Trata-se de um processo distinto de simples reformas, já que estas podem ocorrer sem a adoção de um modelo externo a ser emulado, e não gera uma cópia idêntica, mas um híbrido que guarda características tanto do modelo emulado quanto da organização prévia (RESENDE-SANTOS, 2007). A teoria neorrealista propõe que esta seja uma prática inerente ao comportamento dos Estados em face às mudanças na estrutura sistêmica. Num ambiente de competição, os estados copiam as práticas bem sucedidas de outros, de modo que a emulação militar consiste numa forma eficaz e rápida de incrementar o poder e a segurança estatal (WALTZ, 2002). Sendo, portanto, uma forma de balanceamento interno. Este comportamento, contudo, possui padrões diferenciados. Após a derrota de 1870, a França passou a emular aspectos importantes do modelo alemão, como a organização do estado-maior e a retomada do recrutamento universal sem, contudo, haver a contratação de missões militares do rival vencedor. Países periféricos, por sua vez, tendem a não emular seus vizinhos ou rivais regionais, mas as potências militares centrais e historicamente o fizeram através acordos especiais de assessoria, treinamento e transferência de armamentos que envolviam outras questões políticas e diplomáticas para além das estritamente militares.

O fenômeno da modernização militar pela via da contratação

de missões reformadoras foi bastante disseminado entre as décadas finais do século XIX e o início do XX. Japão, China e Turquia constituem casos bastante conhecidos de modernização de suas forças de terra e mar amparados em reformas assessoradas por militares estrangeiros. Num cenário de crescente competição entre as grandes potências e de acelerado desenvolvimento tecnológico dos armamentos, vários países com pouca ou nenhuma indústria trataram de reorganizar suas forças armadas. Seu objetivo era replicar, em alguns casos até superar, a estrutura organizacional da “nação em armas” praticada pelas potências continentais europeias e capacitar suas tropas para o novo tipo de guerra moderna que então se vislumbrava. Já as potências, especialmente Alemanha e França e mais tarde Estados Unidos, viam nessas demandas a oportunidade de ampliar suas esferas de influência, firmar alianças e de garantir escala para suas indústrias bélicas nacionais. As implicações da emulação militar em larga escala são bastante relevantes, tanto no plano internacional, revelando novas potências, como o Japão, quanto no plano doméstico, reforçando capacidades dos governos centrais em face aos locais e fazendo das modernas e profissionalizadas corporações armadas importantes atores políticos em seus respectivos países.

A América do Sul não esteve à margem deste processo. Após a Guerra do Pacífico, o Peru recorreu à França para remodelar seu recém-derrotado exército, enquanto o Chile, mesmo vitorioso, contratou uma influente missão militar alemã, mobilizando a Argentina a fazer o mesmo em 1899. Na primeira década do século XX um clima de corrida armamentista se instalava na região, bem como a percepção de que o Brasil deveria melhor organizar, treinar e aparelhar suas forças armadas, o que impulsionou a renovação da Marinha Brasileira, calcada na aquisição de modernos navios ingleses, a compra de novos armamentos para o Exército e estudos para a contratação de uma missão militar estrangeira para esta força.

Apesar de enviar oficiais para estagiar na Alemanha entre 1906 e 1912, e de um limitado esforço de emulação do modelo prussiano, protagonizado pelos chamados jovens turcos, o Brasil foi menos célere que seus vizinhos e só contratou uma missão de instrução para o Exército em 1919, da França. Por duas décadas oficiais franceses se fizeram presentes no ensino e nas reformas organizacionais que remodelaram o exército brasileiro. Esta longa presença francesa, contudo, foi abruptamente substituída por uma igualmente longa interação com os Estados Unidos que se estendeu, formalmente, de 1942 a 1977.



O tema da importação de modelos militares na América do Sul e suas implicações nos planos doméstico e externo não é, por certo, novo. Ainda nos anos 1980, Frederick Nunn (1983) publicou um instigante estudo comparando as experiências argentina, chilena, brasileira e peruana que ajuda a colocar em perspectiva os diferentes padrões de ação política dos militares destes países, fundamentalmente no nível doméstico. Mais recentemente, João Resende-Santos (2007) empreendeu outro estudo comparado envolvendo Argentina, Brasil e Chile acentuando a dimensão internacional dos processos de emulação e procurando fornecer uma teoria que explique o fenômeno. Fora do campo dos estudos comparados, há os elucidativos trabalhos de Manuel Domingos Neto (1980; 2007) sobre a missão militar francesa e os de Frank McCann (1983, 2007), cujas extensas pesquisas sobre a influência estrangeira no exército brasileiro permitem ao leitor estabelecer conexões entre as experiências acumuladas sob a missão francesa e o início da influência estadunidense. Não avançando, contudo, para além de 1945. Embora existam vários estudos sobre as relações militares entre Brasil e EUA (MCCANN, 1994; DAVIS, 1996; SVARTMAN, 2014), ainda falta um estudo comparando as duas experiências brasileiras de emulação militar no século XX, lacuna que este artigo pretende preencher.

No presente momento, no qual o Exército Brasileiro empreende um novo movimento de modernização, marcado pela busca por maior autonomia tecnológica e retomada da indústria de defesa, pretende-se aqui por em perspectiva duas experiências passadas de modernização por outra via, a da emulação militar. Como se trata de um tema já bastante investigado, não se pretende recuperar toda a dinâmica de cada uma das experiências, mas de comprara-las com base em quatro aspectos específicos e, com isso, apreender melhor as particularidades e as características comuns de cada uma dessas experiências, bem como o seu legado.

## NEGOCIAÇÕES E INTERESSES

A contratação da missão militar francesa pelo Exército foi objeto de acirrada disputa internacional e decorrência de uma série de manobras políticas. Desde a gestão de Hermes da Fonseca no ministério da Guerra reformas vinham sendo implantadas no sentido de melhorar a organização, o preparo e o armamento do Exército. Esperava-se, também, que um exército mais profissionalizado e disciplinado mantivesse seus

quadros ocupados com seu ofício e não com rebeliões, como a de 1904. Fazendo frente a uma organização na qual predominavam oficiais cindidos entre os “tarimbeiros” (com pouca ou nenhuma formação técnica) e os “doutores” (mais versados em matemática e filosofia que em assuntos militares), iniciou-se um processo de aproximação com a Alemanha que envolveu tanto a compra de armamentos quanto o envio de oficiais para estágios. Tomava impulso um importante movimento reformador que, apesar de encontrar eco na sociedade, com a aprovação da lei que instituiu o serviço militar obrigatório, não fora capaz de garantir a contratação de uma missão alemã. Na verdade não havia consenso, mesmo entre os militares reformadores, quanto à adoção de um modelo estrangeiro e a subordinar oficiais brasileiros aos instrutores de outro país. A ascendência da cultura francesa sobre as elites civis brasileiras e manobras diplomáticas contribuíram para obstar uma influência alemã mais significativa sobre o Exército naquele momento. Posteriormente, o resultado da I Guerra Mundial colocou o exército francês como a grande referência a ser adotada e, em 1919, oficiais que haviam estagiado na Alemanha publicavam artigos na influente revista *A Defesa Nacional* apoiando a recém-contratada missão militar francesa (NUNN, 1983; MCCANN, 2007).

A missão deveria reformular o Estado-Maior, reescrever regulamentos e conferir ao ensino um caráter mais técnico e especializado, bem como introduzir novos serviços, como a aviação. Isso tudo e os armamentos a serem adquiridos deveriam conferir ao Brasil maior prestígio internacional e uma posição mais confortável que permitisse balancear o tradicional rival, a Argentina – que já havia modernizado e ampliado seu poder militar. Para os franceses, a missão faria parte de um jogo de balanceamento contra a Alemanha, representada na região justamente pela Argentina, que havia contratado de Berlim uma missão militar. Contudo, os termos do contrato e o zelo do primeiro chefe da missão pelo seu cumprimento à risca indicam que o maior objetivo da França era comercial. O contrato assegurava o monopólio francês no fornecimento de assessoria, armamentos e equipamentos militares ao Brasil. O general Maurice Gamelin mostrou-se sempre atuante no sentido de defender a influência e de ampliar a presença francesa no mercado brasileiro. Embora seja mais lembrado no Brasil por sua atuação como instrutor e reformador, o general francês tratou de assegurar às indústrias francesas encomendas de aviões, viaturas, telégrafos, cozinhas de campanha e até tecidos para fardamento (DOMINGOS NETO, 2007).

Ainda que estivesse no horizonte o fato das rivalidades entre Brasil e Argentina espelharem as da França e da Alemanha, o contrato militar firmado entre Brasil e França não constituía uma aliança no sentido estrito do termo. Ao emular a organização militar francesa os militares brasileiros estavam adquirindo, a preços de mercado, produtos e serviços franceses.

A intensificação dos laços entre os exércitos do Brasil e dos Estados Unidos foi sensivelmente mais complexa, uma vez que as motivações políticas e estratégicas sobrepunham-se às comerciais e que o Exército Brasileiro, apesar de pequeno e pouco equipado, já contava com um corpo de oficiais em dia com a modernidade militar de sua época. McCann (1983) chama atenção para as iniciativas dos adidos militares estadunidenses para estreitar laços com o Brasil durante os anos 1920 sem, contudo, melindrar os franceses enquanto vigorava o contrato da missão. Na década seguinte, contudo, Washington e o Rio de Janeiro mostraram-se muito mais ativos. O processo de aproximação das Forças Armadas brasileiras às estadunidenses inseriu-se no quadro do alinhamento diplomático do Brasil com os Estados Unidos e da projeção deste país na América Latina (MOURA, 1980). Neste marco mais amplo, que se delineava no início dos anos 1930, as Forças Armadas brasileiras, e o Exército em particular, tiveram um protagonismo crescente no Brasil, influenciando em diferentes esferas da política nacional. Isso lhes permitiu fazer das suas necessidades de reequipamento um item importante da agenda de política externa brasileira, de modo a compor os termos da barganha brasileira pelo seu alinhamento na II Guerra Mundial. Até a ruptura de relações diplomáticas do Brasil com o Eixo, em janeiro de 1942, os militares brasileiros buscaram o atendimento de suas demandas por material bélico tanto na Alemanha ou na Itália quanto, eventualmente, nos EUA de forma que o mercado brasileiro foi objeto de uma intensa competição entre diferentes potências (HILTON, 1977).

Não se tratava apenas de compra de armas, o que também estava em pauta eram os alinhamentos para o grande conflito que se avizinhava. Em função disso, os Estados Unidos, que desde a implantação da *política de boa vizinhança* vinham num processo de aproximação diplomática, empreenderam um movimento semelhante na esfera militar de modo a difundir uma imagem positiva de Washington e a criar canais e vínculos que lhe fossem convenientes. No caso brasileiro, a iniciativa era importante para deslocar a influência militar europeia em favor dos EUA; o que facilitaria as negociações em torno da cedência de bases e de uso do espaço aéreo, importantes para a segurança de determinados pontos críticos, como o canal do Panamá, bem como as negociações relativas ao fornecimento de matérias primas estratégicas. Num contexto em que ainda

havia restrições legais à exportação de armas nos EUA, o Brasil fazia parte da estratégia estadunidense de consolidar a América Latina como região fora do alcance da influência europeia e com isso garantir a projeção da sua influência política e econômica sobre o continente, fortalecendo sua posição face às potências rivais (SCHULTZ, 2000)<sup>2</sup>.

A diplomacia brasileira procurava explorar essa rivalidade para melhor atender às demandas em favor da fundação das bases para a industrialização, da projeção política regional do Brasil e do rearmamento das Forças Armadas, as quais também consideravam a industrialização essencial para garantir a defesa nacional no longo prazo. Até a eclosão da guerra na Europa, o Brasil usou seus trunfos (matérias-primas e posição estratégicas e o desejo de comprar armas) para jogar uma política pendular. Com a irrupção do conflito, acentuou-se a importância do Brasil na estratégia regional norte-americana, o que permitiu, nas negociações bilaterais paralelas às conferências interamericanas, que a adesão brasileira aos Aliados e a cedência de bases no nordeste fossem barganhadas por créditos para a construção de uma siderúrgica e pelo reequipamento de suas Forças Armadas (MOURA, 1980, 1991).

Diferente da experiência francesa, as relações militares do Brasil com os EUA envolveram uma aliança militar efetiva, embora profundamente assimétrica. Selada em 1942, ela se desdobrou não apenas na cedência de bases em território brasileiro, mas em operações de guerra no Atlântico e na Itália. Após a II Guerra Mundial, essa aliança bilateral se diluiu no pacto de segurança coletiva do Tratado Interamericano de Assistência Recíproca, o TIAR, e foi reconfigurada nos termos da Guerra Fria no polêmico acordo militar de 1952.

## INCORPORAÇÃO DE MODELOS ORGANIZACIONAIS

A atuação da missão militar francesa foi sentida inicialmente na instrução de oficiais. O grupo inicial de 20 oficiais franceses chefiados por Gamelin foi agregado ao Estado-Maior, que supervisionava a formação de oficiais do Exército. Seus instrutores iniciaram os trabalhos na Escola de Estado-Maior (EEM), dedicada à formação de oficiais superiores responsáveis pelas funções de planejamento e estratégia daquela força. A EEM atendia

---

<sup>2</sup>O esforço de aproximação estadunidense do Brasil não esteve circunscrito apenas aos militares, um número significativo de intelectuais, artistas, escritores e estudantes também visitou os EUA a convite do Departamento de Estado ou de agências especializadas montadas para a “boa vizinhança” e o pan-americanismo, como o Office of the Coordinator of Inter-Americans Affairs. Para esta questão, ver TOTA, 2000.

majores e tenentes-coronéis e a aprovação em seu curso tornou-se condição para a ascensão ao generalato; formava, portanto, os futuros comandantes do Exército e provavelmente por isso foi a primeira instituição a receber os franceses. A EEM forneceu também cursos de “atualização” para coronéis, todavia os “discípulos” da missão militar francesa foram majoritariamente oficiais jovens. A missão também coordenou a organização da Escola de Aperfeiçoamento de Oficiais, voltada a capitães e tenentes. Além de procurar repassar os “ensinamentos da Grande Guerra”, a ênfase do ensino recaía em exercícios “práticos”, seja em problemas sobre carta, seja em manobras de campo. Paralelamente, a missão tratou de reformular a infinidade de manuais que regulavam o dia-a-dia das unidades militares, conferindo particular atenção à adoção de manobras periódicas e treinamentos continuados para que oficiais e praças estivessem permanentemente familiarizados com os procedimentos e técnicas da guerra moderna (DOMINGOS NETO, 2007; MCCANN, 2006). Outro aspecto importante no processo de emulação foi a incorporação da doutrina de emprego francesa. Depois dos massacres da Grande Guerra, o estado-maior francês abandonou a doutrina da ofensiva à *outrance* em favor de uma doutrina eminentemente defensiva (POSEN, 1984). A adoção de uma doutrina militar defensiva estava em sintonia com a orientação diplomática do Brasil que há pouco concluíra a definição de suas fronteiras pela via diplomática.

Os franceses desempenharam também um papel importante na implantação da aviação do exército. A criação da escola no Campo dos Afonsos foi obra de um primeiro grupo de instrução incorporado à missão, permitindo que, já em 1919 fossem apresentados os primeiros pilotos. Os termos do contrato e a criação da Escola asseguraram importantes encomendas de aeronaves à indústria francesa (MCCANN, 1983). No plano organizacional, a missão orientou a criação do corpo de intendência, responsável pela logística da força, e assessorou a reformulação do Estado-Maior, responsável pela escolha dos armamentos a serem adquiridos, cujas especificidades técnicas tinham também implicações doutrinárias (DOMINGOS NETO, 2007). Com vistas a modelar o exército brasileiro em termos similares ao francês, grandes unidades foram reorganizadas no sentido de receber as reservas oriundas do serviço militar obrigatório e novos armamentos modernos foram introduzidos, como a companhia de carros de assalto (MAGALHÃES, 2001). A sugestão de criação do Conselho de Defesa Nacional, em 1927, e a ênfase na mobilização refletem a orientação francesa, partilhada pelo comando brasileiro, de preparar o exército conforme o modelo da “nação em armas”. Apesar das resistências, críticas e tensões hierárquicas, a missão rompeu a inércia e viabilizou uma

significativa modernização do exército. Apesar de seu refluxo, decorrente da preponderância da influência militar estadunidense, posteriormente a missão militar francesa foi revalorizada e passou a ser cultuada como uma espécie de mito fundador do Estado-maior do Exército (ARAÚJO, 2008).

A adoção de referenciais organizacionais e equipamentos norte-americanos se deu de forma discreta nos anos 1930, em áreas não cobertas pela missão francesa. Oficiais médicos e engenheiros foram convidados a visitar instalações nos EUA e, em 1934, uma missão fora contratada para treinar e reorganizar a artilharia de costa brasileira. A avaliação positiva permitiu que, em pouco tempo, o pequeno grupo de oficiais norte-americanos também atuasse na Escola Técnica do Exército, o futuro Instituto Militar de Engenharia (MCCANN, 1983). Somente com a entrada dos dois países na II Guerra Mundial iniciou efetivamente a emulação brasileira do modelo estadunidense. Nesse sentido a Força Expedicionária Brasileira (FEB) foi decisiva. Durante a sua preparação, centenas de oficiais das armas combatentes foram realizar cursos e estágios nas unidades de suas respectivas armas naquele país. O contato com as instalações militares, industriais e com a sociedade mobilizada para a guerra, entre os anos de 1943 e 1945, teve forte impacto na atitude dos oficiais brasileiros a respeito dos Estados Unidos. Manuais foram traduzidos e uma grande quantidade de armas e equipamentos foram transferidos para o Brasil. O planejamento, recrutamento, treinamento, envio e atuação de uma divisão expedicionária, com suporte dos EUA, constituiu um singular aprendizado para o Exército Brasileiro. Treinamento, alimentação e disciplina passaram a ter um enfoque distinto desde então (MAXIMIANO, 2010).

Depois de 1945 as transferências de armamentos para o Brasil sofreram severa redução em relação ao registrado durante a II Guerra Mundial; ainda assim, os Estados Unidos mantiveram-se como o principal fornecedor de material bélico para o Brasil até meados dos anos 1970 (MOTT, 2002). Essa dependência material era refletida nas mudanças organizacionais implantadas com assessoria norte-americana. Os estudos para criação do Estado-Maior Geral, mais tarde Estado-Maior das Forças Armadas, e a reforma do Ministério da Guerra foram acompanhados por oficiais dos EUA que atuavam junto a Comissão Militar Mista Brasil-Estados Unidos, no Rio de Janeiro. A reestruturação da artilharia de campanha, o processo de motomecanização e a criação da Escola de Paraquedismo do Exército também se deram em estreita cooperação com militares e na dependência dos equipamentos fornecidos por Washington. A Escola de Estado Maior

tratou de incorporar as experiências acumuladas pelos oficiais superiores em cursos nos EUA e nos combates da FEB e a Escola Superior de Guerra foi igualmente criada com assessoria direta de militares estadunidenses.

## RESISTÊNCIAS E ADAPTAÇÕES

Antes mesmo da contratação, a missão francesa criou tensões na organização. Oficiais mais antigos, “tarimbeiros” e “doutores”, temiam por suas posições quando novos saberes profissionais fossem incorporados, especialmente pelos jovens oficiais. Todavia, depois da I Guerra Mundial, os “antimissionistas”, não foram capazes de barrar a atuação de uma cúpula disposta a modernizar o exército e de um grupo de jovens oficiais que militavam em prol da contratação de uma missão estrangeira, os jovens turcos. Ainda assim a direção brasileira foi cautelosa ao definir as atribuições da missão militar. Sua atuação tendeu a ficar restrita às instituições de ensino, o que gerou vários desajustes entre o primeiro chefe da missão militar francesa e o Estado-Maior brasileiro, que pretendia manter certo nível de autonomia, como na elaboração dos planos de defesa do país (BANHA, 1984). Havia uma clara diferença entre a visão de determinadas lideranças brasileiras, que viam a missão como um “remédio temporário” e a perspectiva tutelar e comercial francesa, que procurava alongar o convênio ao máximo. A ênfase escolar conferida à missão militar francesa acentuou uma clivagem geracional que já vinha se desenhando desde a atuação dos *jovens turcos*, parte deles veteranos dos estágios na Alemanha entre 1906 e 1912. Os oficiais saídos das escolas modernizadas pelos franceses eram melhor instruídos que seus chefes imediatos; de modo que em várias unidades produzia-se não apenas uma tensão, mas uma inversão numa das características fundamentais da hierarquia militar (MAGALHÃES, 2001).

Com relação ao material bélico adquirido na França, havia certo ceticismo quanto a sua efetiva qualidade, particularmente em relação ao alemão adquirido na década anterior. No decorrer ainda dos anos 1920, ficara evidente a dificuldade dos fornecedores franceses atenderem as, limitadas, demandas brasileiras e a fazer frente à concorrência de outros fabricantes (DOMINGOS NETO, 2007). Apesar do importante impacto organizacional, da vigência e da longevidade da missão, renovada sucessivamente até o final dos anos 1930, as relações militares Brasil-França acompanharam o declínio geral da influência francesa na América



Latina no entre-guerras (ROLLAND, 2005) e o Brasil em breve reveria suas parcerias militares.

O que poderia ser chamado de uma americanização do exército brasileiro durante a II Guerra não deixou de criar tensões e resistências internas. Leitão de Carvalho narra em detalhes a reticência da cúpula militar quanto à criação da FEB<sup>3</sup>. Durante a guerra, o processo de emulação militar ocorreu em dois níveis e velocidades distintos. O da FEB, intensivo e rápido, e o do restante da força, superficial e lento. A rápida desmobilização da divisão expedicionária e a distinção que se criou entre o “Exército da FEB” e o “Exército de Caxias” expressam a ambiguidade não apenas do regime, mas da própria organização quanto às mudanças ocorridas entre 1943 e 1945.

No pós-guerra havia outros entraves à assimilação e reprodução do modelo estadunidense no Brasil. Alguns oficiais percebiam a doutrina daquele país como uma simplificação da que lhes foi transmitida pelos franceses antes da guerra. Todavia, o limite maior decorria do fato de que, sustadas as massivas transferências de armamentos em 1945, o Brasil não dispunha de orçamento, meios materiais ou mesmo estradas para replicar e manter um exército motorizado e moderno. A isso somava-se que a doutrina de emprego das forças de terra norte-americanas, particularmente depois da guerra da Coréia, assentava-se na projeção de poder e no emprego massivo de um esmagador poder de fogo só possível de ser alcançado com ampla mobilização de recursos humanos e industriais (WEIGLEY, 1973). Havia, ainda, outro desencontro nas relações militares entre os dois países. A orientação de longo curso das Forças Armadas brasileiras de conquistar autonomia, militar e industrial, não coincidia com a estratégia dos Estados Unidos para a América Latina, que tendia a repassar aos países da região material já obsoleto empregado na II Guerra para que desempenhasse funções predominantemente constabulares, o que gerou tensões e um progressivo distanciamento nas décadas posteriores (SVARTMAN, 2011).

A escalada da guerra fria a partir de 1947 pôs no topo da agenda o principal ponto de convergência, e de tensões internas, entre as duas Forças: o anticomunismo. No final dos anos 1940, marcados pela intensificação da mobilização política da sociedade brasileira, e pelas polêmicas em torno do modelo de exploração do petróleo e do nacionalismo, as Forças Armadas brasileiras, mais do que moderadoras do jogo político brasileiro, tornavam-se palco e objeto de disputas políticas (PEIXOTO, 1980; SMALLMANN, 2004).

---

<sup>3</sup> CARVALHO, Estevão Leitão de. A serviço do Brasil na II Guerra Mundial. Rio de Janeiro: A Noite, 1952.



Neste contexto, as relações militares com os EUA constituíam um divisor de águas ideológico, sendo contestadas pelos segmentos mais à esquerda, particularmente do Exército, e objeto de negociações reservadas que deram origem ao novo acordo militar de 1952 e ao acirramento das clivagens ideológicas.

## IMPLICAÇÕES POLÍTICAS

Frederick Nunn chama a atenção para o fato de o treinamento militar fornecido pelas potências europeias na América Latina ter proporcionado não apenas o profissionalismo militar (*expertise*, espírito de corpo, carreiras estruturadas), mas o *militarismo profissional*: “um conjunto de atitudes que podem fazer uso da ação política para encontrar soluções para problemas sociais e econômicos usando métodos baseados no *ethos* militar”. E vai mais além ao assinalar que os exércitos francês e alemão desempenhavam papéis políticos importantes em seus países e que isso não teria passado despercebido na América Latina (NUNN, 1983). Temas como o papel do serviço militar obrigatório como elemento de construção da nacionalidade, a necessidade de planejamento e controle, para uso militar, do sistema de transportes e o da necessidade de uma base industrial nacional, que sustentasse as modernas operações de guerra, passaram a ser recorrentes na literatura militar da região (RESENDE-SANTOS, 2007).

A recepção e os usos dados aos saberes e modelos transplantados ou adaptados depende, por certo, das características de cada país e de suas forças armadas. No Brasil, a interação com os oficiais franceses e a emulação do modelo militar daquele país deu-se num período de erosão da hegemonia da oligarquia cafeeira e de mudanças sociais e políticas. A contestação à ordem estava posta dos sindicatos às vanguardas artísticas e a insatisfação nas fileiras do exército tampouco era pequena. Mais de dois terços da oficialidade comprimia-se nas patentes de primeiro e segundo tenentes, as promoções eram lentas e incertas e mesmo a cúpula militar estava relativamente distante das elites mineira e paulista (CARVALHO, 2005). A isso se somava a clivagem entre oficiais mais jovens, em dia com a modernidade militar fornecida pelos franceses, e seus superiores pouco ou nada familiarizados com as novas técnicas. O ambiente era particularmente propício a insurreições.

Assim, as implicações políticas da missão militar francesa, ou do seu legado, são um tanto contraditórias. De um lado, o reforço da

organização e do profissionalismo militar acentuava o espírito de corpo, sempre reivindicado nos episódios de 1922, 24 e 30. A emulação de um exército moderno e vitorioso da I Guerra Mundial acabou reforçando disposições para a intervenção política de frações da oficialidade brasileira. Para estes segmentos, o “Exército estava modernizado, o País continuava arcaico. A realização dos objetivos corporativistas passaria, portanto, pela interferência no processo de desenvolvimento socioeconômico nacional” (DOMINGOS NETO, 1980). Por outro lado, o profissionalismo tende a reforçar a hierarquia e a disciplina e, de fato, nos três episódios referidos as adesões foram, no máximo, parciais (CARVALHO, 2005). De toda forma, este fortalecimento organizacional foi decisivo em 1937, em 1945 e conferiu outro patamar de poder para a organização durante a Guerra Fria. A missão militar francesa não conferiu ao Brasil capacidade material de balancear a Argentina, mas permitiu a formação de um corpo de oficiais profissionalizado capaz de negociar doméstica e externamente este objetivo.

A interação militar do Brasil com os Estados Unidos tornou-se bastante intensa durante o Estado Novo, uma ditadura civil fortemente amparada no Exército. Reformas asseguraram o empoderamento organizacional e político do Exército e as transferências de armamentos dos Estados Unidos durante a II Guerra Mundial lhe conferiram os meios de força. O pós-guerra foi marcado por uma série de mudanças políticas internas e externas que afetaram sensivelmente as relações militares entre Brasil e Estados Unidos. O golpe que pôs fim ao Estado Novo em 1945 marcou o limite da aliança de Getúlio Vargas com os militares, que viam na eventual inflexão à esquerda e continuísta do ditador uma ameaça comunista. Cada vez mais o anticomunismo seria ponto central na agenda política da cúpula militar brasileira. A colaboração entre militares brasileiros e estadunidenses nesta área foi intensa e precedeu a formulação das doutrinas e sistemas de alianças que marcaram os primeiros anos da Guerra Fria, de modo que se sedimentou uma longa convergência em torno do combate ao comunismo (SVARTMAN, 2014). Neste sentido, a ESG desempenhou um papel importante ao disseminar uma doutrina que combinava anticomunismo com o reforço de disposições intervencionistas em nome do planejamento da segurança e do desenvolvimento nacional. É importante frisar que, apesar dos laços estreitos, a elaboração doutrinária de combate ao comunismo no Exército teve coloração própria, combinando também a literatura francesa produzida na esteira da guerra da Indochina, divulgada no meio militar brasileiro ainda na década de 1950 (MARTINS FILHO, 2008).

Contudo, nem tudo era anticomunismo no Exército brasileiro. Os segmentos mais à esquerda da oficialidade e de suboficiais contestavam essa agenda e o alinhamento com os Estados Unidos. Repercutindo movimentos sociais e políticos mais amplos, defendiam, sob a bandeira do nacionalismo, o projeto nacional-desenvolvimentista. Essa clivagem ideológica alimentou uma luta feroz nas corporações militares até os expurgos posteriores a 1964. Em outro nível, a cúpula militar mantinha uma agenda com os Estados Unidos que não era restrita ao combate ao comunismo. Havia a expectativa de que Washington cooperasse com o fortalecimento militar e industrial do Brasil através da transferência de armamentos modernos e de tecnologia. Contudo, o declínio da importância estratégica da região para os EUA até a revolução cubana produziu um relegamento bastante frustrante para as expectativas brasileiras. Na estratégia estadunidense de então, o Brasil não se diferenciava de seus vizinhos e, como os demais, deveria cooperar no esforço anticomunista fornecendo matérias primas e mantendo forças armadas capazes de garantir a ordem interna. Essa condição e a dependência do material bélico, quase sempre obsoleto, que nos anos 1950 tornou a ser transferido para o Brasil sob a égide dos programas de assistência militar estadunidense da Guerra Fria acentuaram as disposições militares brasileiras para desenvolver capacidade autônoma em setores como a indústria bélica e nuclear, bem como buscar novos fornecedores na Europa.

## CONSIDERAÇÕES FINAIS

A comparação das duas dinâmicas de modernização militar pela via da importação de modelos permite que se identifique com mais clareza as especificidades de cada processo de emulação e o que há em comum nas duas experiências. Como foi visto, a contratação da missão militar francesa, apesar das implicações políticas internacionais, teve um forte conteúdo comercial, cujo declínio relativo da potência e a crescente concorrência dos anos 1930 não permitiu que, em diversas circunstâncias, as demandas brasileiras fossem de todo atendidas. Já a aliança estabelecida com os Estados Unidos decorreu de negociações estratégicas seladas durante a II Guerra Mundial e se desdobrou na Guerra Fria num padrão calcado mais na “assistência militar” para a “defesa do mundo livre” do que na venda de armas ou equipamentos. A cooperação militar com a superpotência em ascensão não foi linear. Apesar da convergência em

torno do anticomunismo, sobretudo nas primeiras décadas do conflito bipolar, e da disposição do polo dominante do Exército a engajar-se no combate à “subversão”, a Força nunca se dispôs a abrir mão por completo do preparo para uma guerra convencional em favor de um papel de polícia. Certamente isso se deu em função da expertise já adquirida com os franceses no desempenho das funções clássicas de um exército moderno calcado no recrutamento universal. Apesar de enxertado numa sociedade que dava seus primeiros passos rumo à industrialização e das debilidades materiais e de treinamento da tropa, o corpo de oficiais brasileiros se percebia como moderno e estava a par do debate profissional de sua época quando a interação com os Estados Unidos tornou-se mais forte.

As duas experiências trouxeram consigo tensões internas, resistências e forçaram adaptações, que evidenciaram a impossibilidade de um transplante linear da organização militar francesa ou norte-americana. Em ambos os casos o Brasil selou acordos que visavam atualizar a estrutura de seu exército e a formação de seus oficiais, bem como ter acesso às armas e equipamentos modernos empregados por grandes potências. O atraso, sobretudo em relação aos países vizinhos, fora corrigido, contudo ao preço de uma incômoda dependência. Embora fosse notória a dependência em relação à França e, posteriormente, aos Estados Unidos, as lideranças militares brasileiras buscaram, em várias circunstâncias, diversificar seus fornecedores e, de forma progressiva, desenvolver autonomia em relação a seus mentores. No decorrer deste longo processo, houve aprendizado brasileiro ao lidar com a contratação de missões e a importação de modelos organizacionais. Na verdade o Brasil queria mais da relação com os Estados Unidos do que quis ou teve com a França: armas, supremacia regional, saberes e tecnologia para o desenvolvimento de sua indústria de defesa e para a industrialização geral do país, o que ajuda a compreender a trajetória daquele segmento nas décadas seguintes e a sua recente retomada.

As experiências de interação do Exército brasileiro com seus pares franceses e norte-americanos transformaram uma série de aspectos na sua estrutura organizacional. Bastante visíveis na capacitação do corpo de oficiais, no poderio dos meios de força e nas doutrinas de emprego, essas mudanças não passaram ao largo do intenso protagonismo político que militares brasileiros tiveram entre 1922 e 1985. Ambas as experiências reforçaram a capacidade militar e o poder político do exército, fazendo do corpo de oficiais um singular grupo de pressão que em vários momentos mostrou-se fortemente inclinado à ação política. Profissionalismo e

espírito de corpo reforçados não apartaram os militares brasileiros da cena política nos anos 1920 e menos ainda durante a Guerra Fria.

Em relação aos seus vizinhos, a primeira experiência brasileira de emulação militar foi mais tardia e seletiva, ainda assim esteve imbuída da mesma lógica partilhada pelos demais de balanceamento interno das capacidades militares do país rival, no caso a Argentina. A segunda experiência contou com o aprendizado da primeira e, apesar das clivagens internas, tensões e frustrações com os Estados Unidos, possibilitou o fortalecimento organizacional que ensejou tanto o protagonismo político militar acima referido quanto o desenvolvimento de capacidades estatais que sustentassem uma longa busca por autonomia. Ambas deixaram um legado modernizante, industrializante e de uma percepção instrumental junto à oficialidade a respeito da necessidade de convênios com atores centrais do sistema como meio para obtenção de maior capacidade nacional.

# THE BRAZILIAN ARMY AND THE EMULATION OF FRENCH AND AMERICAN MODELS IN THE 20TH CENTURY

## ABSTRACT

---

In the first half of the twentieth century the Brazilian Army undertook reforms to modernize and retool with up-to-date weapons and doctrines. This process, although controlled by the Brazilian authorities, depended on the establishment of agreements with two major powers, France and the United States. This paper discusses, in a comparative perspective, the two processes of military emulation that came about as a result of the French Military Mission (1919-39) and the military agreements signed by Brazil with the United States in 1942 and 1952. The analysis focuses on the negotiation aspects and interests involved in the two agreements; the scope of the cooperation; weaponry and doctrines adopted; Institutional resistances and adaptations; as well as the domestic and foreign political implications of adopting both models. **Key-words:** military emulation; modernization; Brazil-France relations, Brazil-US relations

## REFERÊNCIAS

ARAÚJO, Rodrigo. A influência francesa dentro do Exército brasileiro (1930 – 1964): declínio ou permanência? *Revista Esboços*, v. 15, n. 20, 2008.

BANHA, Paulo. *História do Estado-maior do Exército*. Rio de Janeiro: Bibliex, 1984.

CARVALHO, Estevão Leitão de. A serviço da Brasil na segunda Guerra Mundial. Rio de Janeiro: A Noite, 1952.

DAVIS, Sonny. *A brotherhood of arms: Brazil and United States military relations, 1945-1977*. Niwot: University Press of Colorado, 1996.

DOMINGOS NETO, Manuel. Influência estrangeira e luta interna no Exército. (1889-1930) In: ROUQUIÉ, Alain (Org.) *Os partidos militares no Brasil*. Rio de Janeiro: Record, 1980.

DOMINGOS NETO, Manuel. Gamelin, o modernizador do Exército. *Tensões Mundiais*, v. 3, n. 4, jan./jun., 2007.

HILTON, Stanley. *O Brasil e as grandes potências: 1930-1939, aspectos políticos da rivalidade comercial*. Rio de Janeiro: Civilização Brasileira, 1977.

HILTON, Stanley. The United States, Brazil and the Cold War, 1945-1960: end of a special relationship. *The journal of American history*, v. 68, n. 3, dez, 1981.

MAGALHÃES, JB. *A evolução militar do Brasil*. Rio de Janeiro: Bibliex, 2001.

MARTINS FILHO, João Roberto. A influência doutrinária francesa sobre os militares brasileiros nos anos de 1960. *Revista Brasileira de Ciências Sociais*, v. 23, p. 39-50, 2008.

MAXIMIANO, Cesar. *Barbudos, sujos e fatigados: soldados brasileiros na II Guerra Mundial*. São Paulo: Grua, 2010.

McCANN, Frank. A influência estrangeira e o Exército brasileiro 1905-1945. In: *A Revolução de 30*. Seminário Internacional CPDOC/FAV. Brasília: Editora da UnB, 1983.

\_\_\_\_\_. *Soldados da Pátria: história do Exército Brasileiro (1888-1937)*. São Paulo: Companhia das Letras, 2007.

MOURA, Gerson. *Autonomia na Dependência: a política externa brasileira de 1935 a 1942*. Rio de Janeiro: Nova Fronteira, 1980.

\_\_\_\_\_. *Sucessos e ilusões: relações internacionais do Brasil durante e após a II Guerra Mundial*. Rio de Janeiro: FGV, 1991.

- NUNN, Frederick. *Yesterday soldiers: European military professionalism in South America, 1890-1940*. Lincoln, University of Nebraska Press, 1983.
- PEIXOTO, Antônio. O clube militar e os confrontos no seio das Forças Armadas (1945-1964). In: ROUQUIÉ, Alain (Org.) *Os partidos militares no Brasil*. Rio de Janeiro: Record, 1980.
- POSEN, Barry. *The sources of military doctrine: France, Britain, and Germany between the world wars*. Ithaca: Cornell University Press, 1984.
- RESENDE-SANTOS, João. *Neorealism, states, and the modern mass army*. Cambridge University Press, 2007.
- SCHOULTZ, Lars. *Estados Unidos: poder e submissão: uma história da política norte-americana em relação à América Latina*. Bauru: EDUSC, 2000.
- SMALLMANN, Shawn. A profissionalização da violência extralegal das Forças Armadas no Brasil (1945-64) In: CASTRO C., IZECKSOHN, V., KRAAY, H. (Orgs.) *Nova história militar brasileira*. Rio de Janeiro: Editora da FGV, 2004.
- SVARTMAN, Eduardo. Brazil-United States Military Relations during the Cold War: Political Dynamic and Arms Transfers. *Brazilian political science review*, v. 5, p. 96-122, 2011.
- SVARTMAN, Eduardo. Da II Guerra Mundial à Guerra Fria: Conexões entre os exércitos do Brasil e dos Estados Unidos. *Latin American Research Review*, v. 49, p. 83-103., 2014.
- TOTA, Antônio. *O imperialismo sedutor: a americanização do Brasil na época da Segunda Guerra*. São Paulo: Companhia das Letras, 2000.
- WALTZ, Kenneth. *Teoria das relações internacionais*. Lisboa, Gradiva, 2002.
- WEIGLEY, Russell. *The American way of war: A history of United States military strategy and policy*. Bloomington: Indiana University Press, 1973.

Recebido em: 03/04/2016

Aceito em: 09/12/2016





# A QUESTÃO DA SEGURANÇA E DEFESA DO ESPAÇO CIBERNÉTICO BRASILEIRO, E O ESFORÇO POLÍTICO- ADMINISTRATIVO DO ESTADO

Eduardo André Araujo de Souza<sup>1</sup>

Nival Nunes de Almeida<sup>2</sup>

## RESUMO

---

O presente trabalho tem por objetivo estudar a Questão de Segurança e Defesa do Espaço Cibernético, seu meio regulatório, político e administrativo no que tange ao Estado Brasileiro. Abordam-se os esforços: a elaboração de políticas públicas, a reestruturação de órgãos governamentais e suas atualizações, e, são apontados desafios para o país como destacado pela Estratégia Nacional de Defesa.

Adota-se como base teórica a linha de pensamento construtivista das Relações Internacionais sob a ótica dos ensaios da Escola de Copenhague e sua Teoria da Securitização. Considera-se ainda ao final, a corroboração da ideia de grande agilidade na politização e crescente securitização do Espaço Cibernético por parte do Estado Brasileiro suplantando o desafio histórico da baixa percepção do conceito de defesa.

**Palavras-chave:** Ciberespaço. defesa, segurança, políticas públicas.

---

<sup>1</sup> Mestre pelo Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da Escola de Guerra Naval (EGN), Rio de Janeiro, RJ, Brasil. E-mail: eduardoandre@yahoo.com.br

<sup>2</sup> Doutor em Engenharia Elétrica. Professor do PPGEM-EGN, Rio de Janeiro, RJ, Brasil. E-mail: nivalnunes@yahoo.com.br

## INTRODUÇÃO

Notadamente a primeira década dos anos 2000 no Brasil revelou a busca de uma maior representatividade do Estado Brasileiro junto à comunidade internacional, a estabilidade político-financeira do período permitiu que esforços nesse sentido fomentassem a pretensão incansável de um assento permanente no Conselho de Segurança da Organização das Nações Unidas por meio de ações militares de paz, como a MINUSTHA<sup>3</sup> e UNIFIL<sup>4</sup>.

Os objetivos estratégicos e geopolíticos possibilitaram a retomada do investimento na segurança e na defesa sob a forma de projetos como o PROSUB<sup>5</sup> e PROGRAMA FX2<sup>6</sup>, impulsionados pelas relações bilaterais das Indústrias de Defesa entre Brasil-França e Brasil-Suécia. Além disso, a questão da segurança cibernética,

---

<sup>3</sup>MINUSTAH - A Missão das Nações Unidas para Estabilização do Haiti foi criada pela Resolução N° 1576/2004 do Conselho de Segurança da ONU em seu 5090º encontro (em 29 de Novembro de 2004) para restabelecer a segurança e normalidade institucional do país após sucessivos episódios de turbulência política e violência, que culminaram com a partida do então presidente, Jean Bertrand Aristide, para o exílio. A participação do Brasil foi autorizada pelo Decreto Legislativo N° 207/2004 publicado no Diário Oficial da União - Seção 1 de 20/05/2004.

<sup>4</sup>UNIFIL - A Força Interina das Nações Unidas no Líbano criada em 1978 pelas Resoluções: N° 475/1978 do Conselho de Segurança da ONU em seu 2074º encontro e 476/1978 do Conselho de Segurança da ONU em seu 2075º encontro para estabilizar a região meridional libanesa durante a retirada de tropas israelenses da área; reativada em 2006 pela Resolução N° 1701/2006 do Conselho de Segurança da ONU em seu 5511º encontro (11 de Agosto de 2006). A participação brasileira dá-se desde 2011 com o comando da missão de paz da Força-Tarefa Marítima (FTM) autorizada pelo Decreto Legislativo N° 741, de 2010.

<sup>5</sup>(PROSUB) - Programa de Desenvolvimento de Submarinos: firmado um acordo de transferência de tecnologia entre Brasil e França. O programa viabilizará a produção de quatro submarinos convencionais, que se somarão à frota de cinco submarinos já existentes. E culminará na fabricação do primeiro submarino brasileiro com propulsão nuclear. O PROSUB vai dotar a indústria brasileira da defesa com tecnologia nuclear de ponta – ponto destacado na Estratégia Nacional de Defesa. A concretização do programa fortalece, ainda, setores da indústria nacional de importância estratégica para o desenvolvimento econômico do país. Priorizando a aquisição de componentes fabricados no Brasil para os submarinos, o PROSUB é um forte incentivo ao nosso parque industrial. Além dos cinco submarinos, o PROSUB contempla a construção de um complexo de infraestrutura industrial e de apoio à operação dos submarinos, que engloba os Estaleiros, a Base Naval e a Unidade de Fabricação de Estruturas Metálicas (UFEM), no Município de Itaguaí. Disponível em: <<https://www1.mar.mil.br/prosub/institucional>>, acessado em 20 de novembro de 2016.

<sup>6</sup>PROGRAMA FX2 - Projeto FX-2 ou Programa FX-2 é um programa de reequipamento e modernização da frota de aeronaves militares supersônicas da FAB - Força Aérea Brasileira, criado em 2006 no governo do então presidente Luiz Inácio Lula da Silva, em substituição ao programa anterior, denominado Projeto FX, após acréscimos de vários requisitos e uma mudança nos requisitos estabelecidos no então Projeto FX. Disponível em: <<http://www1.folha.uol.com.br/fsp/brasil/fc0310200913.htm>>. Acesso em: 20 nov. 2016.

percebida em razão de incidentes desta natureza, promovidos ora por entes estatais, ora por organizações autônomas, revelou a vulnerabilidade dos sistemas no âmbito governamental e motivou uma gama de medidas, traduzidas em políticas públicas e leis que regulamentaram ainda mais o Espaço Cibernético<sup>7</sup> Brasileiro.

Houve ainda os eventos de repercussão mundial, nesta segunda década dos anos 2000, como a Jornada Mundial da Juventude (2013), a Copa do Mundo (2014), as Olimpíadas e Paraolimpíadas (2016), que fomentaram a criação de órgãos e políticas públicas, concernentes ao tema, em resposta à crescente sensação de medo presente na sociedade, quanto à potencialidade de uma gama diversa de ameaças, aumentando a preocupação com a proteção de dados confidenciais e *infraestruturas críticas*<sup>8</sup> em nosso país.

Assim, com base no conceito de segurança numa vertente de pensamento das Relações Internacionais que lida com a ótica do Construtivismo e sua Teoria da Securitização, fundamentadas na Escola de Copenhagen, investiga-se a evolução do tema Segurança e Defesa cibernética na Administração Pública Federal e suas implicações no esforço do Estado Brasileiro em adaptar-se ao novo cenário de ameaças desta nova fronteira tecnológica.

## FUNDAMENTOS DE SECURITIZAÇÃO

Não se intenciona aqui revisar os fundamentos teóricos das Relações Internacionais, mas demarcar algumas premissas, para que, em momento oportuno, se possa relacioná-las com o tema central do trabalho. Na visão dos teóricos das Relações Internacionais, o *realismo* define o sistema internacional como anárquico, condicionado pela incessante

---

<sup>7</sup> Espaço Cibernético ou ciberespaço - Um domínio global dentro do ambiente de informação que consiste de redes interdependente em infraestruturas de tecnologia da informação e dados incluindo a Internet, redes de telecomunicações, sistemas de computador, e processadores e controladores embarcados. (JP 12/03). ESTADOS UNIDOS DA AMÉRICA. Joint Chiefs of Staff. JP 3-13: Information Operations. 2006. Disponível em: <[http://www.dtic.mil/doctrine/new\\_pubs/jp1\\_02.pdf](http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf)>. Acesso em: 18 ago. 2016. (tradução dos autores).

<sup>8</sup> Infraestruturas Críticas (IC) - instalações, serviços, bens e sistemas exercem significativa influência na vida de qualquer pessoa e na operação de setores importantes para o desenvolvimento e manutenção do país, como é o caso do setor industrial. Elas são importantes pelas facilidades e utilidades que fornecem à sociedade e, principalmente, por subsidiarem, na forma de recurso ou serviço, outras Infraestruturas Críticas, mais complexas ou não. Ao passar dos anos, a interdependências verticais das Infraestruturas Críticas, caracterizadas por um baixo acoplamento entre elas, deu lugar às interdependências horizontais altamente acopladas, com muitos pontos de interação em suas dimensões (BAGHERY, 2007).

busca de poder pelos Estados, priorizando a segurança militar na política internacional. Nesse sentido, os realistas enxergam a segurança como um segmento do poder, em que um ator alcança sua segurança quando ocupa uma posição dominante. Dessa forma, a anarquia caracteriza-se pela inexistência de um formulador de política internacional que seja independente e soberano acima do nível estatal. Portanto, a visão predominante do conceito de segurança realista está ligada ao poder de cada Estado para assegurar a sua sobrevivência, sendo este poder obtido em linhas gerais pelo emprego da força militar.

Clausewitz lembra ainda que os litígios entre Estados no modelo realista culminam através da violência extremada dos conflitos bélicos, sendo estes a expressão da política por outros meios:

“A guerra, então, é apenas um verdadeiro camaleão, que modifica um pouco a sua natureza em cada caso concreto, mas é também, como fenômeno de conjunto e relativamente às tendências que nela predominam, uma surpreendente trindade em que se encontra, antes de mais nada, a violência original de seu elemento, o ódio e a animosidade, que é preciso considerar como um cego impulso natural, depois, o jogo das probabilidades e do acaso, que fazem dela uma livre atividade da alma, e, finalmente, a sua natureza subordinada de instrumento da política por via da qual ela pertence à razão pura.” (CLAUSEWITZ, 2010, p.30).

A partir deste entendimento, optou-se pela busca de um segmento teórico das Relações Internacionais que ampliasse seus fundamentos não só na inter-relação de estruturas Estatais visto que o conceito de novas guerras<sup>9</sup>, e a assimetria destas, acaba por envolver uma significativa ordem de atores não estatais, desde Organizações Não Governamentais (ONGs) a grupos paramilitares e terroristas, que não são privilegiados nos estudos do Realismo tão pouco do *Neorealismo*<sup>10</sup>.

---

<sup>9</sup> Ver Kaldor, Mary (2013) In defence of new wars. Stability: International Journal of Security and Development.

<sup>10</sup> O Neorealismo ou realismo estrutural é uma teoria das Relações Internacionais, apresentado inicialmente por Kenneth Waltz em seu livro de 1979, *Theory of International Politics*. O neorealismo surgiu a partir da doutrina estadunidense de ciência política, e reformula a tradição realista de Edward Hallett Carr, Hans Morgenthau e Reinhold Niebuhr. Os realistas em geral argumentam que o poder é o fator mais importante nas relações internacionais. O neorealismo ainda se subdivide em ofensivo e defensivo (tradução nossa). Jakobsen, Jo. Neorealism in International Relations – Kenneth Waltz. Disponível em: <<http://www.popularsocialscience.com/2013/11/06/neorealism-in-international-relations-kenneth-waltz>>. Acesso em: 26 Jul. 2016.

Na visão construtivista, linha dominante de pensamento da Escola de Copenhague<sup>11</sup>, considera-se a anarquia como um constructo social, sendo esta o que os Estados fazem dela, portanto diferenciando-se da visão realista nesse ponto.

No que tange à segurança internacional, construtivismo e realismo aproximam-se, na medida em que têm o Estado como unidade privilegiada na estrutura política internacional. Assim, cria-se a ideia de que a realidade é socialmente construída, em que suas estruturas são formadas por ideias compartilhadas (WENDT, 1992).

Logo, não há limitação do conceito de segurança, já que o mesmo sofre continuamente processos de construção e reconstrução, abrindo espaço para a permanente possibilidade de transformação. No que diz respeito ao campo da segurança, as possíveis mudanças sistêmicas acontecem sempre relacionadas ao Estado. Assim sendo, o construtivismo possui uma maior abertura empírica que possibilita maior moldagem para tratar também de questões relacionadas às percepções de ameaça à segurança. Essas percepções, então, são construídas a partir de estímulos externos.

Diante dos questionamentos sobre segurança, ameaças e paz na agenda de segurança internacional, e por estes relacionarem-se estritamente às temáticas militares, fez-se necessário a criação de conceitos e categorizações específicas para acompanhar a demanda de diferentes tópicos que foram incluídos nas agendas estratégicas dos Estados. Assim, Buzan et al (1998, p.23) desenvolveram a teoria da securitização, a qual se refere ao processo metodológico de apresentação de uma questão em termos de segurança.

Dessa forma, a dinâmica de cada uma das categorias/setores de segurança pode ser classificada como Militar, Ambiental, Social, Econômica e Política, e determinada por Objetos de referência, como Atores funcionais, Atores de securitização e Dinâmica de funcionamentos particulares (BUZAN et al, 1998, p. 27).

---

<sup>11</sup> A Escola de Copenhague de Estudos de Segurança é uma escola de pensamento acadêmico com suas origens nas teorias de Relações Internacionais publicadas na obra de Barry Buzan: Povos, Estados e o Medo: O Problema de Segurança Nacional em Relações Internacionais. A Escola de Copenhague coloca particular ênfase nos aspectos sociais da segurança. Seus principais teóricos associados com a escola são: Barry Buzan, Ole Wæver e Jaap de Wilde. Muitos dos membros da escola trabalharam no Instituto de Pesquisa da Paz de Copenhague. A principal contribuição da Escola de Copenhague e a obra: Segurança: Um Novo Enquadramento para Análise, escrito por Buzan, Wæver e de Wilde. A teoria centra-se em três conceitos-chave: Setores; Complexos de Segurança Regionais; Securitização. (Eriksson, Johan 'Revisiting Copenhagen Observers or Advocates?: On the Political Role of Security Analysts', *Cooperation and Conflict* 34, n. 3, 1999, p. 311-3.

Os setores para securitização seriam espécies de lentes pelas quais as questões são observadas. O analista, por exemplo, deve ter consciência de que, em cada setor, encontram-se valores e características próprios, e de que a natureza das ameaças modifica-se de setor para setor, tornando a securitização institucional ou *ad hoc* (BUZAN et al, 1998, p.27, tradução nossa). Nas palavras dos autores da Escola de Copenhague, “a definição exata e os critérios de securitização são constituídos pelo estabelecimento intersubjetivo de uma ameaça existencial com um indicativo suficiente para ter efeitos políticos substanciais” (BUZAN et al, 1998, p.25, tradução nossa).

No que se refere aos objetos, Buzan et al (1998, p.25) afirmam também que qualquer grupo ou indivíduo pode tornar-se um objeto de referência, caso tenha sua segurança/existência ameaçada. Porém, para que uma ameaça se torne um problema de segurança na agenda política, é preciso que “um representante estatal declare uma condição de emergência, reivindicando o direito de utilizar quaisquer meios necessários para barrar um desenvolvimento ameaçador” (BUZAN et al, 1998, p.21, tradução nossa).

No construtivismo, trabalha-se ainda a ideia de segurança como “um discurso por meio do qual as identidades e as ameaças são constituídas em vez de ser uma condição objetiva” (BUZAN; HANSEN, 2012, p.366).

Sendo assim, o ator de securitização é aquele que securitiza uma questão, declarando que o objeto de referência encontra-se ameaçado. Logo, o ator funcional é aquele que afeta a dinâmica do setor do qual faz parte.

Dessa forma, enquadra-se a segurança como um tipo especial de política, definindo a abrangência de questões públicas em três categorias, a saber: não politizado, politizado e securitizado. Buzan et al (1998, p.23) afirmam que a primeira acontece quando o Estado não lida e não faz da questão um assunto de debate público e de decisão e, portanto, não requer atenção ao nível político; a segunda ocorre quando o assunto torna-se parte de políticas públicas, exigindo decisão governamental e alocação de recursos; até chegar à condição de securitizado, significando que a questão é vista como uma ameaça existente, que requer medidas de emergência aceleradas, podendo violar regras legais e sociais, sendo, assim, uma versão mais extremada da politização.

Nesse sentido, é importante ressaltar que se deve entender o conceito de ameaça como “qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que pode ser causador de danos, materiais ou morais [para algum objeto], podendo ser de

variada natureza” (COUTO, 1988, p.329). Desse modo, os teóricos da Escola de Copenhagen veem a segurança como uma questão de sobrevivência e, portanto, quando existir qualquer preocupação, esta será definida como sendo uma ameaça existencial, não necessariamente pela existência em si, mas pela justaposição a algum objeto referente, podendo ser, tradicionalmente, mas não obrigatoriamente, o Estado, incorporando o governo, o território e a sociedade.

Nesse contexto, apresenta-se uma narrativa de um processo de securitização ocorrido durante os protestos populares no Brasil em 2013, quando fica claro que, em decorrência de todas as suas etapas, culminou-se com as ações “*não discursivas*” de monitoração das redes sociais pelo Centro de Defesa Cibernética (CDCiber) e pela Agência Brasileira de Inteligência (ABIN). Nesse caso, os Órgãos de Inteligência, como Agente Securitizador, identificam uma Ameaça (à paz social) e convencem as autoridades (Poder Executivo) a adotar medidas securitizadoras, atuando assim na monitoração das redes sociais.

### A QUESTÃO DA CIBERNÉTICA NO BRASIL: POLITIZAÇÃO VERSUS SECURITIZAÇÃO?

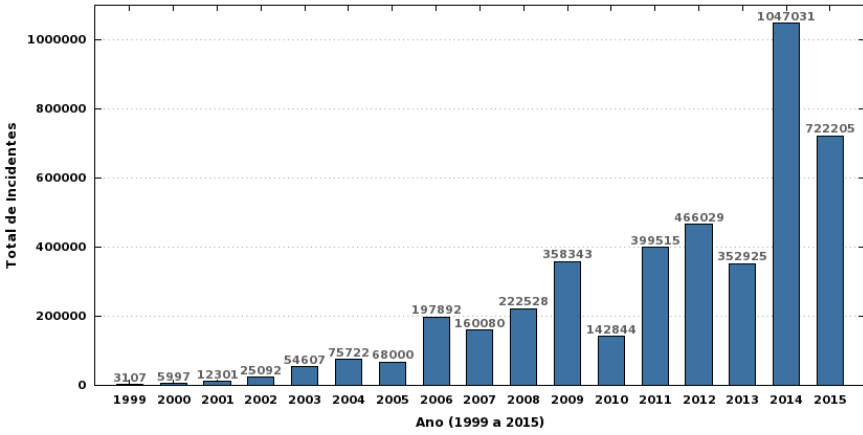
“a preocupação tanto com os conteúdos quanto com o tipo de uso, e a respectiva segurança da Internet, crescem em igual medida aos desenvolvimentos tecnológicos e ao número de usuários, observados, especialmente, ao longo dos últimos anos.” (Livro Verde – Segurança Cibernética no Brasil, Brasil, 2010, p.31).

De acordo com o Centro de Estudos de Resposta e Tratamento de Incidentes de Segurança para a Internet Brasileira (CERT.br), o Brasil possui o maior número de internautas da América Latina, cerca de 50 milhões<sup>12</sup>. Em 2013, o CERT.br recebeu notificações de 352.925 tipos de ataques no país, número que chegou a alcançar 466.029 em 2012. Comparando-se com o relatório de 2002, quando se reportou pouco mais de 25.000 ataques, os incidentes cibernéticos apresentaram um aumento superior a 1.800% em uma década. Isso demonstra o crescimento vertiginoso não só de usuários de internet no país como também na quantidade e diversificação dos ataques virtuais, conforme constatado no *Gráfico I* abaixo. Ainda de acordo com as estatísticas de 2015, advindas do *Gráfico II*, os incidentes reportados partiram majoritariamente de dentro do território nacional (54,02%), seguido por EUA (11,16%) e, depois, China (10,59%).

<sup>12</sup> Ver <<http://cetic.br/noticia/nic-br-divulga-segunda-parte-da-pesquisa-tic-domicilios-sobre-o-uso-da-internet-no-brasil/>>. Acesso em 10 out 2016.

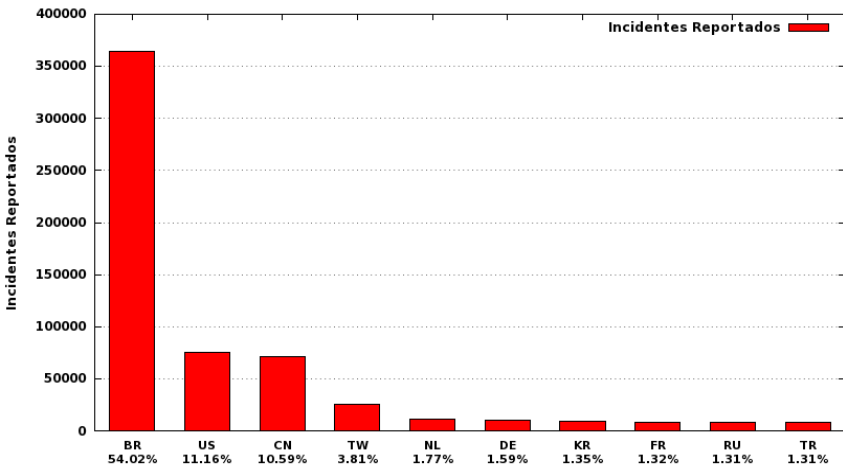


Gráfico I: Total de incidentes reportados ao CERT.br por ano



fonte: <http://www.cert.br/stats/incidentes/>

Gráfico II: CERT.br Incidentes reportados (Top 10 CCs origem de ataques)



fonte: <http://www.cert.br/stats/incidentes/2015-jan-dec/top-atacantescc.png>

Em 2011, os incidentes reportados pelo Centro tinham como alvo, preferencialmente, empresas privadas e bancos. Já nos anos seguintes, os ataques estenderam-se para *sites* e sistemas governamentais, entre eles, os *sites* da Presidência da República e da Receita Federal. Essa situação revela uma potencial preocupação com a fragilidade do sistema de segurança cibernética do governo brasileiro <sup>13</sup>.

<sup>13</sup> Ver <http://www.cert.br/stats/incidentes/>. Acesso em: 10 Out. 2016.

Por exemplo, um ataque que paralisasse o *site* da Receita Federal, às vésperas do prazo de entrega das declarações de imposto de renda do cidadão brasileiro, poderia trazer grandes prejuízos não só de ordem financeira para a União, mas à imagem da Secretaria da Receita Federal.

Portanto, faz-se necessário uma categorização e tipificação das várias formas de conflito no ciberespaço, das possíveis vulnerabilidades, das ameaças e das suas fontes, “para que sejam alocadas responsabilidades aos cidadãos, ao Estado; sejam estabelecidas contramedidas e investigações criminais” (DUNN, 2010, p.1, tradução nossa). De acordo com Buzan et al (1998, p.25), dependendo de como se enquadra uma questão, as respostas a ela irão variar. Assim, quanto mais securitizado for um evento social, mais excepcional e extremo podem ser as respostas governamentais a ele. Tratar da mesma forma o ativismo, os crimes, o terrorismo e os atos de guerra cibernéticos seria um erro. Por isso mesmo, o Guia de Referência para a Segurança das Infraestruturas críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JÚNIOR, 2010, p.129-139) conceitua e determina tais elementos.

Ainda que se possa afirmar que o Espaço Cibernético não tenha sido plenamente securitizado no Brasil, pode-se dizer que a cibernética é objeto de preocupação no âmbito da segurança e da defesa. Assim, a cibernética tem sido uma área priorizada recentemente pelo governo brasileiro, notando-se isso especialmente pelo que afirma Celso Amorim, ex-ministro da Defesa:

“Ao contrário de cem anos atrás, tempo do Barão do Rio Branco, quando o Brasil comprava do exterior praticamente todos seus principais equipamentos de defesa sem a capacidade de nacionalizar sua produção, hoje o desenvolvimento de capacidades autônomas na indústria de defesa é um objetivo fundamental de nossa política. A Estratégia Nacional de Defesa, cuja segunda edição foi lançada no ano passado e agora acaba de ser apreciada pelo Congresso Nacional, define três áreas prioritárias desse esforço: a nuclear, a cibernética e a espacial”. (AMORIM, 2013, p.308-309).

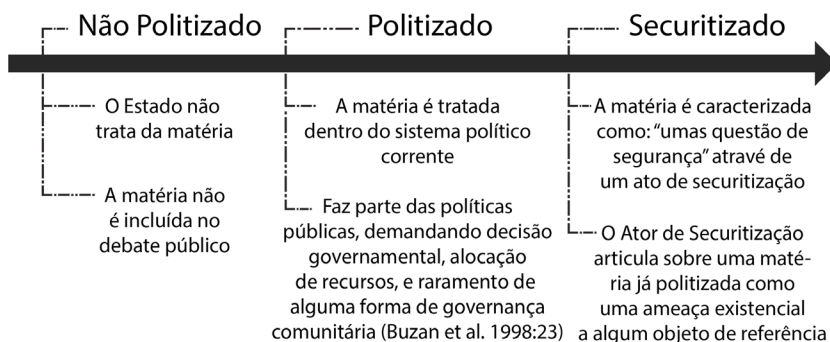
Da mesma forma, o general do Exército Brasileiro e então comandante do Centro de Defesa Cibernética (2011) no Brasil, José Carlos dos Santos, em entrevista para a revista *Época*, ao ser perguntado se a cibernética será um novo campo das Forças Armadas, afirmou:

“É uma nova governança. Eu diria que diversos países estão na mesma situação. Os Estados criaram seu comando cibernético em 2009. A Alemanha ativou seu centro de defesa cibernética neste ano, a Inglaterra no ano passado. O Brasil criou o Centro de Defesa Cibernética em agosto do ano passado. Essa era digital é um contexto novo. [...] Podemos, sim, contratar civis. Está dentro de nossas previsões a contratação de especialistas em regime de prestação de serviços. Basicamente estamos cuidando da formação do nosso pessoal. A partir de 2012, a matéria tecnologia para informação e comunicação se tornará obrigatória para todos os nossos futuros oficiais. Nas escolas de formação dos nossos sargentos, o assunto também será introduzido. É uma possibilidade contratar [hackers]. A imprensa diz que os Estados Unidos já fazem isso. Eles teriam até um grupo de hackers que trabalharia em prol do governo americano. Eles não se identificam como tal, mas trabalham. [No Brasil] São registrados milhares de incidentes de rede por dia. Logicamente um porcentual desses incidentes é de tentativas de intrusão em serviços internos do Exército. Recentemente, tivemos no Recife uma intrusão num serviço social, de distribuição de água. Um grupo, o FatalErrorCrew, conseguiu acessar um banco de dados dessa operação. Foi dado crítico? Bom, crítico, não. Mas mostrou uma vulnerabilidade. Eram dados de militares vinculados àquela operação”. (SANTOS, 2011).

Sendo assim, encontra-se no âmbito militar brasileiro uma preocupação com a defesa e a segurança cibernética dos sistemas virtuais e da infraestrutura do país. A política adotada pelas Forças Armadas brasileiras é a de defesa-ativa<sup>14</sup>, não buscando atacar outras nações, seguindo a linha pacifista histórica de posicionamento e obediência direta ao texto constitucional em seu Artigo 4º incisos I a VII, visando primordialmente proteger os próprios sistemas e neutralizar possíveis ataques e intrusões.

Levando-se em consideração a elaboração de Buzan et al (1998), referente à categorização do tratamento de questões públicas, podemos dividir o tratamento da segurança cibernética pelo Brasil em três etapas: até o ano 2000, não politizado; a partir de então, politizado; e em 2008, se inicia um processo de securitização, conforme se ilustra na Figura 1.

<sup>14</sup> Defesa-ativa: Capacidade de identificar o ataque cibernético e sua origem e na mesma medida, se oportuno for, retaliar o atacante e seus sistemas. Disponível em <<https://gestao.consegi.serpro.gov.br/cobertura/noticias/a-favor-de-uma-defesa-ativa-contrataques-ciberneticos>>, acesso em: 16 ago. 2016.

Figura 1: *Spectro de Securitização*

fonte: *Contemporary Security Studies*, pag. 170 <sup>15</sup>

Cronologicamente, até o final dos anos 1990, não foram criados documentos relevantes concernentes ao tema, nem debates ou preocupações quanto aos riscos e às vulnerabilidades foram observados. Certamente, pelo fato da cibernética e seus elementos se encontrarem em processo de formação e evolução, juntamente com as Tecnologias de Informação e Comunicação (TICs). A partir de então, conforme o Estado Brasileiro percebe a necessidade e a importância de tal tecnologia, há uma institucionalização da questão, designação de capacidades e demarcação de conceitos.

A partir do ano 2000, tem-se o marco inicial do processo de politização da questão de Segurança e Defesa Cibernética com o Livro Verde Sociedade da Informação no Brasil (TAKAHASHI, 2000), do Ministério da Ciência e Tecnologia. O livro representa uma visão mais ampla para estabelecer contornos e diretrizes de um programa de ações rumo à Sociedade da Informação no Brasil.

O referido programa versa sobre as oportunidades e os riscos de uma sociedade em rede e informatizada; sobre economia, trabalho e comércio eletrônico; sobre universalização dos serviços de internet como forma de

<sup>15</sup> Collins Alan. *Contemporary Security Studies*. Oxford University Press, 12 de jan de 2016.

cidadania; sobre como a informatização auxilia a educação; sobre transparência governamental para colocar o “governo ao alcance de todos”, além de abordar questões mais específicas de Pesquisa e Desenvolvimento (P&D) e infraestrutura avançada. Basicamente, são definidos conceitos ligados à informática e são propostos projetos de disseminação da internet pelo território nacional.

Em termos de segurança cibernética (até então denominado segurança da informação), no mesmo ano, o governo publicou o Decreto No. 3.505 de 13 de junho de 2000, instituindo a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, aplicando a definição de pressupostos básicos, conceituações, objetivos, diretrizes, alocação de recursos e de responsabilidades. A legislação federal ainda instituiu o Comitê Gestor da Segurança da Informação (CGSI), o qual tinha a função de assessoria e era subordinado à Secretaria-Executiva do Conselho de Defesa Nacional; portanto, nota-se uma preocupação inicial com a segurança da informação do Estado.

Em seguida, por meio da Lei Federal No 10.683, de 28 de maio de 2003, foi criado o Gabinete de Segurança Institucional da Presidência da República (GSI/PR), o qual tinha como uma de suas competências a de coordenar as atividades de inteligência federal e de segurança da informação. O GSI/PR passou por diversas revisões de funções e atividades, tendo sido atualizado com o Decreto No. 8.100 de 04 de setembro de 2013.

Ainda, na estrutura do GSI/PR, destacam-se dois órgãos “cujas atividades por eles desenvolvidas inserem-se no esforço de construção de estratégia da segurança cibernética” (BARROS, 2011). Não obstante, o Decreto Presidencial No. 5.772 de 08 de maio de 2006 criou o Departamento de Segurança da Informação e Comunicações (DSIC), com o objetivo de exercer exatamente as atividades de segurança da informação. O segundo órgão é a Agência Brasileira de Inteligência (ABIN), o qual atua nas vertentes de inteligência e contra inteligência em prol do Estado, tendo como função, entre outras, “avaliar as ameaças internas e externas à ordem constitucional”.

Outros órgãos criados serviram para potencializar o surgimento da segurança cibernética, quais sejam o Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações (CEPESC), o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.gov), o Comitê Gestor da Internet (CGI), o Núcleo de Informação e Coordenação do Ponto BR (Nic.br) – este último mantendo também o já citado CERT.br –, o Centro de Estudos sobre as Tecnologias

da Informação e da Comunicação (CETIC.br) e o Centro de Estudos e Pesquisas em Tecnologias de Rede e Operações (CEPTRO.br), entre outros.

Assim sendo, até 2005, houve um processo de politização do tema da segurança cibernética – inicialmente entendido como segurança da informação –, com a criação de órgãos, documentos oficiais, discussões, centros de estudos, determinação de recursos, etc. O tema ainda não havia alcançado um grau de preocupação concernente a uma ameaça existencial propriamente dita, mas apenas um objeto de preocupação inicial e de debate político. Observa-se, assim, que há um processo de entendimento da área cibernética como uma questão de segurança, senão plenamente, ao menos potencialmente existente, iniciando, portanto, a construção de uma ideia de securitização.

Nesse sentido, a Política Nacional de Defesa (Decreto No. 5484, de 30 de Junho de 2005) menciona brevemente o tema em duas seções. Dessa forma, temos as primeiras citações diretas referentes ao tema “ataque cibernético”:

**“6.19 Para minimizar os danos de possível ataque cibernético, é essencial a busca permanente do aperfeiçoamento dos dispositivos de segurança e a adoção de procedimentos que reduzam a vulnerabilidade dos sistemas e permitam seu pronto restabelecimento. [...] XII - aperfeiçoar os dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos e, se for o caso permita seu pronto restabelecimento”.** (BRASIL, 2005, grifo nosso).

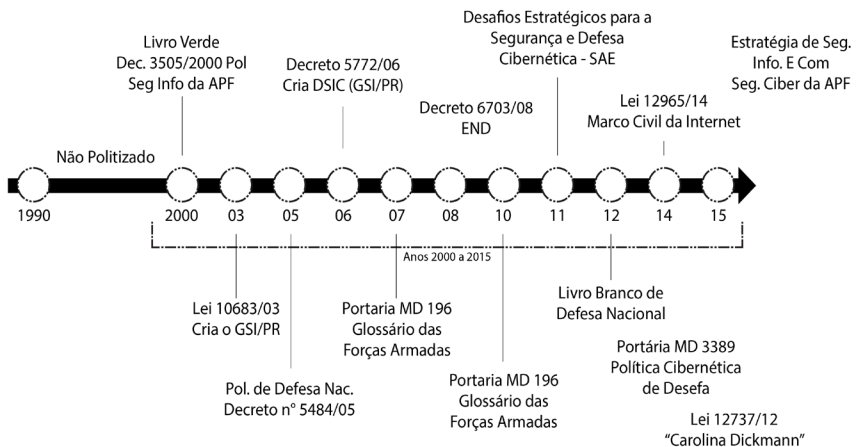
A partir dessa Política Nacional de Defesa, ampliam-se as produções de documentos legais brasileiros os quais fomentam o debate público de Defesa Nacional, incluindo então a segurança cibernética; sendo eles o Glossário Militar das Forças Armadas (2015), a Estratégia Nacional de Defesa<sup>16</sup> (2008; 2012), o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JUNIOR, 2010), o Livro Verde: Segurança Cibernética no Brasil (CANONGIA; MANDARINO, 2010), o relatório

<sup>16</sup> A Estratégia Nacional de Defesa (END) foi aprovada pelo Decreto Nº 6.703, de 18 de Dezembro de 2008; revisada em 2012 de acordo com o Decreto Legislativo Nº 373, de 25 de Setembro de 2013 implicando em alterações na Política Nacional de Defesa e no Livro Branco da Defesa

Desafios Estratégicos para a Segurança e Defesa Cibernética (BARROS; GOMES, 2011), o Livro Branco de Defesa Nacional (BRASIL, 2012a), a Política Cibernética de Defesa (BRASIL, 2012b) e a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (BRASIL, 2015). A consequência é a percepção pelo Estado brasileiro da potencialidade e dos riscos de ataques cibernéticos às infraestruturas críticas e da segurança da informação no país, alocando publicamente espaços em documentos legais que promovem a discussão e o crescimento da importância do tema, tendo o Gabinete de Segurança Institucional da Presidência da República e o Exército Brasileiro como órgãos principais de atuação no setor cibernético.

Em síntese, pode-se apresentar a evolução da tratativa da segurança cibernética pelo Estado Brasileiro com um direcionamento da questão para uma possível securitização. Temática esta que, nos anos 1990, ainda se encontrava não politizada e que, em consequência da maior integração da sociedade brasileira com o Espaço Cibernético, somada a eventos de ordem internacional (*Malware Stuxnet – Irã/2011*, e ciberataque DDoS – Estônia/2007), adquiriu maior relevância, principalmente nas forças armadas brasileiras, que responderam, por meio de documentos oficiais, conforme ilustrado na Figura 2, os quais serão tratados na próxima seção.

Figura 2: Arcabouço Político-Administrativo do Espaço Cibernético Brasileiro



fonte: Elaborado pelos autores

## RESPONSABILIDADES, POLÍTICAS E ESTRATÉGIAS NO ESPAÇO CIBERNÉTICO DO BRASIL

Em um primeiro momento, cabe relembrar uma diferenciação semântica, descrita no Glossário das Forças Armadas (BRASIL, 2015), entre defesa e segurança e, então, estudar sua aplicação e estruturação no ambiente cibernético brasileiro. O termo defesa é entendido como “o ato ou conjunto de atos realizados para obter, resguardar ou recompor a condição reconhecida como de segurança” (BRASIL, 2015, p.76), ou ainda, como uma “reação contra qualquer ataque ou agressão real ou iminente”. (BRASIL, 2015, p.76).

Por sua vez, segurança é colocada como uma “Condição que permite ao País a preservação da soberania e da integridade territorial, a realização dos seus interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais. Sentimento de garantia necessária e indispensável a uma sociedade e a cada um dos seus integrantes, contra ameaças de qualquer natureza. Condição que resulta do estabelecimento e conservação de medidas de proteção que assegurem um estado de inviolabilidade contra atos ou influências hostis” (BRASIL, 2015, p.252).

A segurança no âmbito cibernético contempla ações que compreendem aspectos e atitudes tanto preventivas quanto repressivas, enquanto defesa cibernética refere-se a ações operacionais, de caráter ofensivo, caracterizadas por ataques cibernéticos (neste sentido composto pela participação de elementos estatais). Sendo assim, apesar de algumas diferenças conceituais, não se pode isolar completamente um conceito do outro.

Existe uma interligação de atribuições em relação ao setor cibernético que demanda atuação tanto em defesa quanto de segurança, haja vista que, no meio cibernético, a origem é de difícil determinação, os meios utilizados e os danos prováveis de um ataque podem atingir tanto sistemas militares como também serviços públicos da sociedade (CANONGIA, 2009, p.98). Nessa linha, o então Ministro da Defesa à época, Celso Amorim, em discurso de abertura no terceiro Seminário de Defesa Cibernética em outubro de 2012 pronunciou-se da seguinte maneira:

“Não tenho dúvidas, por exemplo, de que a proteção de estruturas críticas do país – usinas hidroelétricas, linhas de transmissão, bases de dados do sistema financeiro, para não falar dos próprios meios das Forças Armadas



– pertencem à Defesa. A identificação e perseguição de *hackers* ou *crackers* é tarefa da Segurança [pública]. Mas há áreas cinzentas entre uma e outra”. (AMORIM, 2012).

Dessa forma, no Brasil, o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e o Ministério da Defesa (MD) – acompanhado ainda pela Secretaria de Assuntos Estratégicos (SAE), pela Marinha do Brasil, pela Força Aérea Brasileira e pelo Exército Brasileiro (catalizador do assunto conforme indicado no Tópico CT&I, Item2, pag. 37 da Estratégia Nacional de Defesa) –, atuam na condução das políticas, debates públicos e projetos do setor cibernético para o país. No tocante à segurança pública, a identificação de *hackers* em território nacional, por exemplo, fica sob a responsabilidade da Polícia Federal (PF) – subordinada ao Ministério da Justiça, como atributos de crime comum, ou seja, a PF estaria encarregada por ações de prevenção de incidentes e de repressão também no âmbito cibernético. No entanto, ao se levar em consideração a participação das Forças Armadas (Exército) nas ações de segurança cibernética em grandes eventos que ocorreram no país, tais quais: a Conferência Rio+20 em 2012, a Copa das Confederações em 2013 e a Copa do Mundo em 2014, notamos uma situação nebulosa, isto é, uma sobreposição de atribuição de funções em operações.

Dessa forma, o GSI/PR e o MD destacam-se na construção de um ambiente politizado que caminha para a securitização da cibernética, tornando-se os líderes na elaboração das diretrizes desse setor. Nesse sentido, o GSI/PR tem como uma de suas funções de coordenar: a inteligência e a segurança da informação, transformando-a na engrenagem principal para a organização da estratégia da segurança cibernética no país (MANDARINO JR., 2009). Da estrutura do GSI/PR, destacam-se ainda o DSIC e a ABIN.

O DSIC tem como atribuições, entre outras, regulamentar a segurança da informação e comunicações para toda a Administração Pública Federal (APF), realizar acordos internacionais de troca de informações sigilosas, ser o ponto de contato com a Organização dos Estados Americanos (OEA) para assuntos de terrorismo cibernético e manter o centro de tratamento e resposta (CERT.br) a incidentes nas redes de computadores da APF.

A ABIN atua nas tarefas de inteligência, por meio da produção de conhecimentos sobre fatos e situações de imediata ou potencial influência no processo decisório; na ação governamental, sobre a salvaguarda e sobre a segurança da sociedade e do Estado; e nas atividades de contra inteligência pela adoção de medidas que protejam os assuntos sigilosos relevantes para o Estado e a sociedade e que neutralizem ações de inteligência executadas em benefício de interesses estrangeiros.

A construção da securitização cibernética não ocorre tão somente por documentos legais e criação de órgãos da APF, mas também por meio de discursos públicos. Primeiramente, durante a 68ª Assembleia Geral das Nações Unidas, em discurso de abertura, a então presidente do Brasil Dilma Rousseff proferiu as seguintes palavras:

“As tecnologias de telecomunicação e informação não podem ser o novo campo de batalha entre os Estados. Este é o momento de criarmos as condições para evitar que o espaço cibernético seja instrumentalizado como arma de guerra, por meio da espionagem, da sabotagem, dos ataques contra sistemas e infraestrutura de outros países” (ROUSSEFF, 2013).

Percebe-se, nesse caso, a conclamação internacional para a construção de uma governança<sup>17</sup> global da internet e uma real preocupação com os riscos de um ataque cibernético, especialmente quando coloca os sistemas e infraestruturas como objetos de referência e, portanto, como algo existencialmente ameaçado. O discurso da presidente ainda demonstrou preocupação com a privacidade e com os dados pessoais dos cidadãos brasileiros, alvo de espionagem pela agência americana *National Security Agency* (NSA) em 2013, colocando, assim, a sociedade brasileira como um objeto referencial. Ademais, o fato gerador provocado pelo incidente de violação de segurança cibernética foi estopim e motivador para que, em 2014, fosse aprovado o Marco Civil da Internet, projeto que estava com pauta de votação trancada desde sua proposição em 2009. Ainda que não tenha propriamente fins de defesa ou segurança nacional, a Lei Ordinária de Nº 12.965, de 23 de Abril de 2014 regula a utilização da internet no país, prevendo princípios, garantias, direitos, responsabilidades e deveres para usuários e empresas, tratando de neutralidade, privacidade, retenção de informações e dados, entre outros. Portanto, esse Marco Civil representa uma importante regulamentação interna e, igualmente, uma abertura ainda maior da discussão do tema para a sociedade.

---

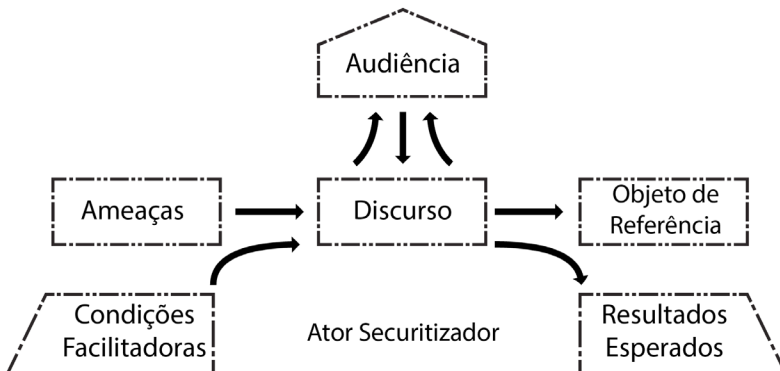
<sup>17</sup> “Governança é um conjunto de práticas, padrões e relacionamentos estruturados, assumidos por executivos, gestores, técnicos e usuários de TI de uma organização, com a finalidade de garantir controles efetivos, ampliar os processos de segurança, minimizar os riscos, ampliar o desempenho, otimizar a aplicação de recursos, reduzir os custos, suportar as melhores decisões e consequentemente alinhar TI aos negócios.” PERES, João Roberto. A vez da governança corporativa. Revista Abinee. Numero 43, pagina 25, Outubro 2007. Disponível em: <http://www.abinee.org.br/informac/revista/43j.pdf>. Acesso em: 16 ago. 2016.

Anteriormente, na apresentação do Livro Verde: Segurança Cibernética no Brasil (BRASIL, 2010b), o então Ministro Chefe do Gabinete de Segurança Institucional da Presidência da República, Jorge Armando Felix, não só apregou a necessidade de garantir a segurança nacional, como também proclama a formulação de uma Política Nacional de Segurança Cibernética, expressando o tema como uma ameaça à segurança estatal:

“Assim, motivado por esta missão e considerando a necessidade de assegurar dentro do espaço cibernético ações de segurança da informação e comunicações como fundamentais para a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação; a possibilidade real e crescente de uso dos meios computacionais para ações ofensivas por meio da penetração nas redes de computadores de setores estratégicos para a nação; e o ataque cibernético como sendo uma das maiores ameaças mundiais na atualidade; foi instituído Grupo Técnico para estudo e análise de matérias relacionadas à Segurança Cibernética. [...] Recomendo, portanto, a leitura desta obra, cuja publicação considero significativo incremento no arcabouço de documentos que objetivam garantir a Segurança Nacional, e convido-os a contribuir com propostas e sugestões para a evolução da mesma, visando formular, colaborativamente, à Política Nacional de Segurança Cibernética” (CANONGIA; MANDARINO, 2010, p.5-6).

Ao final de suas palavras, percebe-se um chamamento à audiência pública, para que haja participação e contribuições com propostas e sugestões, levando o tema mais uma vez para a esfera da sociedade, expondo assim de maneira clara o modelo teórico da Teoria da Securitização proposto por Buzan et al (1998, p. 25) e todos os seus componentes, conforme a Figura 3.

Figura 6: Modelo teórico da Teoria da Securitização



Fonte: Security: A New Framework for Analysis

Em relação ao papel do MD, num primeiro momento, o Exército Brasileiro foi designado para conduzir o setor cibernético no país; havendo previsibilidade para a criação de um Comando de Defesa Cibernética das Forças Armadas – como acontece nos EUA com a USCYBERCOM<sup>18</sup> – no qual a Marinha, o Exército e a Força Aérea trabalhariam integradamente.

Importante analisar a END de 2008, na qual os primeiros esforços com viés político-estratégico foram feitos com relação ao setor cibernético. Segundo a respectiva estratégia, “o Ministério da Defesa e as Forças Armadas intensificarão as parcerias estratégicas nas áreas cibernética, espacial e nuclear” (BRASIL, 2008), colocando particular ênfase no “aperfeiçoamento dos dispositivos e procedimentos de segurança que reduzam a vulnerabilidade dos sistemas relacionados à Defesa Nacional contra ataques cibernéticos” (BRASIL, 2008). Nota-se pelo documento, portanto, que a cibernética é colocada pela primeira vez como um setor decisivo para a conservação do país ao alegar que os “três setores estratégicos – o espacial, o cibernético e o nuclear – são essenciais para a defesa nacional” (BRASIL, 2008).

Mesmo assim, como consequência da END de 2008, em 09 de novembro de 2009, o MD, por meio da Diretriz Ministerial 14 (Doutrina Militar de Defesa Cibernética), determinou as responsabilidades de coordenação e integração do setor cibernético ao Exército Brasileiro, no âmbito das Forças Armadas.

Em seguida, em 2010, foi lançado o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação (CANONGIA; GONÇALVES JÚNIOR; MANDARINO JUNIOR, 2010), elaborado e organizado por especialistas de 13 órgãos da APF, propondo como objetivos gerais: (i) levantar e avaliar as potenciais vulnerabilidades e riscos que possam vir a afetar a segurança das infraestruturas críticas, identificando e monitorando suas interdependências; (ii) propor, articular e acompanhar medidas necessárias das infraestruturas; (iii) - estudar, propor e acompanhar a implementação de um sistema de informações com dados atualizados das infraestruturas; (iv) pesquisar e propor um método de identificação de alertas e ameaças da segurança de infraestruturas críticas da informação.

---

<sup>18</sup>United States Cyber Command (USCYBERCOM) é um comando conjunto das forças armadas norte-americanas subordinado ao Comando Estratégico dos Estados Unidos da América. O comando está localizado em Fort Meade, Maryland, e centraliza as operações no ciberespaço, organiza os recursos cibernéticos existentes e sincroniza defesa de redes militares dos EUA.

Nesse caso, percebe-se novamente uma preocupação de alta relevância com as infraestruturas críticas do país, colocando-as como potenciais vítimas à ameaça cibernética. Ainda em 2010, foi lançado o Livro Verde: Segurança Cibernética no Brasil (CANONGIA; MANDARINO, 2010), o qual apresenta uma breve visão do país no que se refere às oportunidades e aos desafios em termos político-estratégicos, econômicos, sociais e ambientais, ciência, tecnologia e inovação, educação, legalidade, cooperação internacional, e segurança das infraestruturas críticas, tendo como foco central a segurança cibernética. Além do mais, contém diretrizes estratégicas para formulação de uma possível futura Política Nacional de Segurança Cibernética para o país (BRASIL, 2010b, p. 17, 33).

Mais tarde, em 2012, é elaborado o documento que, pela primeira vez, aloca publicamente recursos para o setor cibernético. O Livro Branco de Defesa Nacional (BRASIL, 2012a) – que, apesar de aprovado na Câmara dos Deputados e no Senado, e ainda não sancionado, é documento disponível no site do governo brasileiro – trata a cibernética como um desafio, denominando-a com um tipo de “conflito do futuro” (BRASIL, 2012a, p.28), e coloca a defesa cibernética propriamente como um novo tema no plano internacional. O livro também observa as infraestruturas do país como ameaça existencial ao afirmar que a “ameaça cibernética tornou-se uma preocupação por colocar em risco a integridade de infraestruturas [...] essenciais à operação e ao controle de diversos sistemas e órgãos diretamente relacionados à segurança nacional” (BRASIL, 2012a, p.69). O documento supracitado ainda defende que a proteção do espaço cibernético abrange variadas áreas, desde capacitação, inteligência, pesquisa científica, preparo e emprego operacional e gestão de pessoal até a proteção dos próprios ativos e capacidade de atuação em rede.

Outra publicação importante concernente ao tema em âmbito brasileiro foi a Política Cibernética de Defesa de 2012. A finalidade da Política é nortear “as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos” (BRASIL, 2012b). Esse documento solidifica o entendimento acerca das possibilidades e dos limites da atuação cibernética brasileira, tendo em vista a sensibilidade que esse espaço e ferramenta de poder possui. Mais uma vez, para além da atuação do MD, uma audiência pública é convocada para colaborar com processo de construção do setor cibernético:

“a) a eficácia das ações de Defesa Cibernética depende, fundamentalmente, da atuação colaborativa da sociedade brasileira, incluindo, não apenas o MD, mas também a comunidade acadêmica, os setores público e privado e a base industrial de defesa;” (BRASIL, 2012b).

O documento cita o Sistema Militar de Defesa Cibernética (SMDC), órgão militar com o intuito de prevenir ataques aos sistemas de informática de todo o Brasil, o qual é coordenado pelo Estado-Maior Conjunto das Forças Armadas. Dessa forma, o país insere-se no modelo de gestão cibernética das grandes potências, ainda que apenas inicialmente.

Por fim, tem-se na Estratégia Nacional de Defesa de 2012, que é uma atualização da END de 2008, um documento legal, possuindo alguns pontos atualizados importantes que merecem ser citados. Primeiramente, nessa nova estratégia o setor cibernético adquire uma seção exclusiva para apontamento de prioridades. Uma delas é expansão do CDCiber para uma atuação integrada das Forças Armadas, ao afirmar que se deve “fortalecer o Centro de Defesa Cibernética com capacidade de evoluir para o Comando de Defesa Cibernética das Forças Armadas” (BRASIL, 2012c).

Outra prioridade é conduzir o tema para o debate acadêmico ao propor a necessidade de “fomentar a pesquisa científica voltada para o Setor Cibernético, envolvendo a comunidade acadêmica nacional e internacional” (BRASIL, 2012c). Inclusive, neste ponto, propõe-se um estudo conjunto entre Ministros, Secretários e GSI/PR com vistas à “criação da Escola Nacional de Defesa Cibernética” (BRASIL, 2012c).

Portanto, no campo da segurança cibernética, as ações ganharam maior investida a partir da criação do DSIC no GSI/PR<sup>19</sup>, em 2006, e no campo da Defesa Cibernética, destaque maior passou a ser dado através da elaboração da END. O conjunto regulatório até aqui apresentados, acompanhados pela criação e atuação de órgãos estatais possuem papel imprescindível pela atribuição de competências no que tange a segurança e defesa cibernéticas, podendo ser encarados como uma sistematização do processo de enfrentamento às ameaças existentes no setor cibernético.

Ponderando-se a mesma medida, os breves discursos apresentados podem ser vistos como uma forma de alcançar a legitimação junto à opinião pública em busca da securitização, haja vista que seu discurso torna-se mais aceitável em virtude da associação entre possíveis ataques cibernéticos em âmbito nacional com incidentes ocorridos diariamente. Sendo assim, conforme apontou Buzan e Hansen (2012, p.366), a segurança Defesa Cibernética a uma securitização ainda em desenvolvimento no país.

---

<sup>19</sup> O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) deu lugar a Casa Militar sob o Ministério da Casa Civil conforme a Medida Provisória Nº 696 de 2 de Outubro de 2015.

## CONSIDERAÇÕES FINAIS

Na abordagem inicial deste trabalho, foram apontadas as aspirações do Estado brasileiro a uma participação mais ativa junto à comunidade internacional, cujos esforços, nesse sentido, foram materializados com a presença crescente de nossas forças armadas junto às ações de caráter humanitário da Organização das Nações Unidas, em razão do favorável cenário econômico mundial nos anos 2000, que colocaram o Brasil em destaque. Todavia, neste contexto, o Governo brasileiro foi vitimado como objeto de espionagem cibernética de origem estatal norte-americana. Ainda nesse sentido, foi possível perceber que existe no Estado brasileiro uma estrutura basilar pronta para atuar nas áreas de segurança e defesa cibernética, ainda que em desenvolvimento, perante os desafios internacionais que se apresentam.

Num segundo momento, o estudo buscou uma referência teórica para analisar o processo evolutivo do arcabouço político-administrativo na questão de Segurança e Defesa do Espaço Cibernético Brasileiro. Dentre as linhas de pensamento sobre o conceito de Segurança das Relações Internacionais declinou-se da linha de pensamento realista, por esta última, em sua essência, trabalhar precipuamente com entes estatais na arena internacional e sua busca pelo poder, afastando de sua essência a atuação dos demais atores não estatais e sua ordem de influência na cena geopolítica.

Encontrou-se amparo na Teoria da Securitização, advinda da “Escola de Copenhagen”, segundo a qual o conceito de Segurança dá-se por um constructo social numa postura construtivista, em razão do posicionamento pós Guerra-fria, em que, diante da possibilidade de um holocausto nuclear, afastou-se a visão exclusivamente militarista para resolução dos conflitos e deu-se sustentação ao posicionamento das relações do Estado com demais atores de ordem diversa (Estatais ou não), abrindo a possibilidade de uma assimetria nessas interações tão comuns no enfrentamento de ameaças cibernéticas.

Avaliou-se o tema Segurança Cibernética, provocado derradeiramente por casos de forte clamor social, como a “espionagem da National Security Agency”, que tornou oportuno acelerar medidas e projetos, que impulsionaram investimentos e capacitação, visando à formação e à organização de um Sistema Nacional de Segurança e Defesa Cibernética, principalmente no âmbito da Defesa por força da END, em

detrimento de históricos e significativos obstáculos afeitos à cultura de Defesa. de históricos e significativos óbices afeitos a cultura de Defesa.

Grandes eventos internacionais transcorridos no País nos últimos anos representaram a oportunidade de trazer a baila o apoio e o envolvimento da opinião pública para a matéria de Segurança e Defesa, materializando-se através da ação direta do Ministério da Defesa no âmbito da segurança orgânica dos locais onde se realizaram os eventos e junto ao Ministério da Justiça, Polícia Federal, na manutenção da ordem e da paz no Espaço Cibernético.

A instabilidade da Ordem Mundial do pós Guerra ao Terror - campanha militar desencadeada pelos Estados Unidos em resposta aos ataques de 11 de setembro de 2001 -, devido à assimetria das ações terroristas, está presente também em uma arena tecnologicamente superior e de ordem quase que “etérea” como o Espaço Cibernético. Essa instabilidade trouxe uma oportunidade para os atores governamentais de materializar discursos, políticas e ações nos setores de Segurança e Defesa cibernética, mesmo que estes não repercutam em investimentos proporcionais às reais necessidades do Estado Brasileiro. No entanto, conseguiu-se estruturar uma ordem de políticas públicas e instituições com intuito de trabalhar nesta nova fronteira de atuação, desde questões públicas não politizadas até politizadas.

Por fim, destacou-se, neste artigo, apoiado na Escola de Copenhague, que a segurança não é uma condição objetiva, mas sim um discurso que constitui identidades e ameaças. Assim sendo, pode-se depreender que o Estado Brasileiro busca por identidades e ameaças cibernéticas, conduzindo a questão da Segurança e Defesa Cibernética a uma securitização, que está em desenvolvimento no país.



# BRAZILIAN CYBERSPACE'S ISSUE ON SECURITY AND DEFENSE, AND THE POLITICAL- ADMINISTRATIVE EFFORT OF THE STATE

## ABSTRACT

---

The present work aims to study Cyberspace's Security and Defense issues, its regulatory aspects, political and administrative sets to the Brazilian State. Focusing the efforts made as: public policies development; government agencies restructuring and updating, and the challenges for the country are pointed out on the National Defense Strategy. International Relations' foundation on constructivism is adopted as an academic basis from Copenhagen School perspective essays and its Theory of Securitization as a support for analysis and research. It is also considered at the end, corroborating the idea of great agility in the politicization and growing securitization of the Cybernetic Space by the Brazilian State supplanting the historical challenge of the low perception of Defense's concept.

**Key-words:** Cyberspace, defense, Security, public policies.

## REFERÊNCIAS

AMORIM, Celso. Discurso de abertura. In: SEMINÁRIO DE DEFESA CIBERNÉTICA, 3., 2012, Brasília: MD. Disponível em: <<https://www.youtube.com/watch?v=dkUcymtvcUk>>. Acesso em: 20 set. 2015.

\_\_\_\_\_. Segurança Internacional: novos desafios para o Brasil. *Contexto Internacional*, Rio de Janeiro, v. 35, n.1, p.287-311, 2013. Disponível em: <<http://www.scielo.br/pdf/cint/v35n1/a10v35n1.pdf>>. Acesso em: 26 set. 2015.

JORGE, Bernardo Wahl Gonçalves Araújo. Estados Unidos, poder cibernético e a “guerra cibernética: do Worn Stuxnet ao Malware Flame/Skywiper-e além. *Boletim Meridiano* 47, v.13, n. 131, 2012. Disponível em: <<http://seer.bce.unb.br/index.php/MED/article/view/7051/5623>>. Acesso em: 25 set. 2015.

AZAMBUJA, Darcy. *Teoria geral do estado*. São Paulo: Globo, 1957. p. 17-53. Disponível em: <<http://www.faroldoconhecimento.com.br/livros/Pol%C3%ADtica/AZAMBUJA,%20Darcy.%20Teoria%20geral%20do%20Estado.pdf>>. Acesso em: 20 set. 2015.

BARROS, Otávio Santana de Rêgo; GOMES, Ulisses de Mesquita (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Secretaria de Assuntos Estratégicos, 2011. Disponível em: <[http://www.sae.gov.br/site/wpcontent/uploads/Seguranca\\_Cibernetica\\_web.pdf](http://www.sae.gov.br/site/wpcontent/uploads/Seguranca_Cibernetica_web.pdf)>. Acesso em: 16 dez. 2014.

BRASIL. Decreto nº 5.484, de 30 de junho de 2005. Aprova a Política de Defesa Nacional, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 30 jun. 2005. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2004-2006/2005/Decreto/D5484.htm](http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm)>. Acesso em: 10 jun. 2015.

BRASIL. Decreto nº 6.703, de 18 de dezembro de 2008. Aprova a Estratégia Nacional de Defesa, e dá outras providências. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 18 dez. 2008. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/Decreto/D6703.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm)>. Acesso em: 12 dez. 2015.

BRASIL. Ministério da Defesa. Portaria nº 3.389/MD, de 21 de dezembro de 2012. Política Cibernética de Defesa. *Diário Oficial [da] República Federativa do Brasil*, Brasília, DF, 21 dez.2012b. Disponível em: <<http://www.jusbrasil.com.br/diarios/44578940/dou-secao-1-27-12-2012-pg-11>>. Acesso em: 10 mai. 2015.

BRASIL. Ministério da Defesa. Portaria normativa nº 9/GAP/MD, de 13 de Janeiro de 2016, MD35-G-01. Aprova o Glossário das Forças Armadas. 5 ed. 2015. Disponível em: <[http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35\\_g\\_01\\_glossario\\_ffaa\\_5\\_ed\\_2015.pdf](http://www.defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35_g_01_glossario_ffaa_5_ed_2015.pdf)>. Acesso em: 16 ago. 2016.

BRASIL. Ministério da Defesa. Portaria normativa nº 196/GAP/MD, de 22 de fevereiro de 2007, MD-MD35-G-01. Aprova o Glossário das Forças Armadas.

BRASIL. Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília: MD, 2012a. Disponível em: <<http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf>>. Acesso em: 20 jan. 2015.

BRASIL. Ministério da Defesa. *Estratégia Nacional de Defesa*. Brasília: MD, 2012c. Disponível em: <<http://www.defesa.gov.br/arquivos/2012/mes07/end.pdf>>. Acesso em: 11 jan. 2015.

BAGHERY, E. et al. *The State of the Art in Critical Infrastructure Protection: a framework for convergence*. Faculty of Computer Science, University of New Brunswick, Fredericton, N.B. Canada, 2007. Disponível em: <<http://glass.cs.unb.ca/~ebrahim/papers/CIPFramework.pdf>>. Acesso em: 11 jan. 2016.

BUZAN, Barry. *People, States and Fear: an Agenda for the International Security Studies in the Post-Cold War Era*. Boulder, Colorado: Lynne Rienner, 1991.

BUZAN, Barry; HANSEN, Lene. *A evolução dos estudos de segurança internacional*. São Paulo: Editora Unesp, 2012. 576p.

BUZAN, Barry; WAEVER, Ole; WILDE, Jaap de. *Security: a new framework for analysis*. Londres: Lynne Rienner Publishers, 1998.

CANONGIA, Claudia; MANDARINO, Raphael (Org.). *Livro Verde: segurança cibernética no Brasil*. Brasília: GSIPR/SE/DSIC. 2010. Disponível em: <[http://dsic.planalto.gov.br/documentos/publicacoes/1\\_Livro\\_Verde\\_SEG\\_CIBER.pdf](http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf)>. Acesso em: 02 dez. 2014.

CANONGIA, Claudia; GONÇALVES JÚNIOR, Admilson; MANDARINO JUNIOR, Raphael. (Org.). *Guia de Referência para a Segurança das Infraestruturas Críticas da Informação*. Brasília: Gabinete de Segurança Institucional da Presidência da República, nov. 2010. Disponível em: <[http://dsic.planalto.gov.br/documentos/publicacoes/2\\_Guia\\_SICI.pdf](http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf)>. Acesso em: 13 jan. 2015.

CANONGIA, Claudia; MANDARINO, Raphael. Segurança Cibernética: o desafio da nova sociedade da informação. *Revista Parcerias Estratégicas do Centro de Gestão e Estudos Estratégicos*; v.14; n.29; p. 21-46, 2009. Disponível em: <<http://dsic.planalto.gov.br/artigos/101-artigo-sobre-seguranca-ciber-netica-revista-parceriasestrategicas-cgee>>. Acesso em: 16 abr. 2015.

CARREIRO, Marcelo. A guerra cibernética: ciberwarfare e a securitização da internet. *Revista Cantareira*, ed. 17, 2012. Dossiê guerras, conflitos e tensões, p. 123-137. Disponível em: <<http://www.historia.uff.br/cantareira/v3/wp-content/uploads/2013/05/e17a9.pdf>>. Acesso em: 15 nov. 2014.

CARVALHO, Paulo Sérgio Melo de. Conferência de Abertura: o Setor Cibernético nas Forças Armadas Brasileiras. In: BRASIL. *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Brasília, Secretaria de Assuntos Estratégicos da Presidência da República, 2011.

CAVALCANTI, Elmano Pontes. Revolução da informação: algumas reflexões. *Caderno de Pesquisa em Administração*, São Paulo, v.1, n.1, 1995. Disponível em: <<http://www.ancibe.com.br/artigos%20de%20si/artigo%20-%20Revolu%C3%A7%C3%A3o%20da%20informa%C3%A7%C3%A3o%20-%20algumas%20reflex%C3%B5es.pdf>>. Acesso em: 28 mar. 2015.

CLARKE, Richard; KNAKE, Robert. *Cyber War: the next threat to National Security and what to do about it*. New York: Harper Collins, 2010.

CLAUSEWITZ, Carl Von. *Da Guerra*. São Paulo: Editora WMF Martins Fontes, 2010, p.30.

CRUVINEL, Tereza; CAVALCANTI, Leonardo. Celso Amorim diz que Brasil é vulnerável contra ataques cibernético: as ações de espionagem da agência americana de segurança revelaram a fragilidade do Brasil na proteção a dados e informações. *Correio Braziliense*, Brasília, 22 set. 2013. Disponível em: <[http://www.correiobraziliense.com.br/app/noticia/politica/2013/09/22/internas\\_polbraeco,389429/celso-amorim-diz-que-brasil-e-vulneravel-contra-ataques-cibernetico.shtml](http://www.correiobraziliense.com.br/app/noticia/politica/2013/09/22/internas_polbraeco,389429/celso-amorim-diz-que-brasil-e-vulneravel-contra-ataques-cibernetico.shtml)>. Acesso em: 11 jun. 2015.

DUNN, Myriam. Cyberwar: concepts, status quo, and limitations. *CSS Analysis in Security Police*, ETH Zurich, n. 71, p. 1-3, April 2010. Disponível em: <<http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf>>. Acesso em: 11 jan. 2015.

FERREIRA NETO, Walfredo Bento. *Por uma geopolítica cibernética: apontamentos da grande estratégia brasileira para uma nova dimensão da guerra*. 2013. 178 f. Dissertação (Mestrado em Estudos Estratégicos da Defesa e da Segurança) - Programa de Pós-Graduação em Estudos Estratégicos. Universidade Federal Fluminense, Rio de Janeiro, 2013.

HANSEN, Lene; NISSENBAUM, Helen. Digital Disaster, Cyber Security and the Copenhagen School. *International Studies Quarterly*, n.53, p. 1155-1175, 2009. Disponível em: <<http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf>>. Acesso em: 15 jan. 2015.

KALDOR, Mary. *New and Old Wars: organized violence in a Global Era*. Polity Press, 1998. p.1-216.

\_\_\_\_\_. *Old Wars, Cold Wars, New Wars, and the War on Terror*. Cold War Studies Center, School of Economics, London. p.1-10. Feb. 2005. Disponível em: <<http://dspace.cigilibrary.org/jspui/bitstream/123456789/8613/1/Old%20Wars%20Cold%20Wars%20New%20Wars%20and%20the%20War%20on%20Terror.pdf?1>>. Acesso em: 11 fev. 2015.

MANDARINO JR, Raphael. *Um Estudo sobre a Segurança e a Defesa do Espaço Cibernético*. 2009. Monografia (Especialização em Ciência da Computação: gestão da segurança da informação e comunicações) - Universidade de Brasília, Brasília, 2009. Disponível em: <[http://dsic.planalto.gov.br/documentos/cegsic/monografias\\_1\\_turma/raphael\\_mandarino.pdf](http://dsic.planalto.gov.br/documentos/cegsic/monografias_1_turma/raphael_mandarino.pdf)>. Acesso em: 03 mai. 2015.

\_\_\_\_\_. Reflexões sobre Segurança e Defesa Cibernética. In: BARROS, Otávio Santana de Rêgo; GOMES, Ulisses de Mesquita (Org.). *Desafios Estratégicos para a Segurança e Defesa Cibernética*. Secretaria de Assuntos Estratégicos. 2011. Disponível em: <[http://www.sae.gov.br/site/wp-content/uploads/Seguranca\\_Cibernetica\\_web.pdf](http://www.sae.gov.br/site/wp-content/uploads/Seguranca_Cibernetica_web.pdf)>. Acesso em: 16 jun. 2015.

MUGGAH, Robert; GLENN, Misha; DINIZ, Gustavo. *Securitização da Cibersegurança no Brasil*. Instituto Igarapé. Disponível em: <<http://igarape.org.br/desconstruindo-a-seguranca-cibernetica-no-brasilameacas-e-respostas>>. Acesso em: 12 jul. 2016.

PERES, João Roberto. A vez da governança corporativa. *Revista Abinee*. Numero 43, pagina 25, Outubro 2007. Disponível em: <http://www.abinee.org.br/informac/revista/43j.pdf>. Acessado em: 16 ago. 2016.

ROUSSEFF, Dilma. Discurso da Presidente. In: *Debate Geral da 68ª AGNU*. Nova Iorque/EUA. 2013. Disponível em: <http://www2.planalto.gov.br/acompanhe-oplanalto/discursos/discursos-da-presidenta/discorso-da-presidenta-da-republica-dilma-rousseff-naabertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua>. Acesso em: 15 jan. 2015.

SANTOS, José Carlos dos. Podemos recrutar “hackers”. *Revista Época*. 2011. Disponível em: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTO+S+PODEMOS+RECRUTAR+HACKERS.<html>>. Acesso em: 03 mai. 2015.

SENIWATI. The Securitization Theory and Counter Terrorism in Indonesia. *Academic Research International*, Hasanuddin University, v. 5, n.3, p.231 - 238, 2014. Disponível em: [www.savap.org.pk/journals/ARInt/Vol.5\(3\)/2014\(5.3-26\).pdf](http://www.savap.org.pk/journals/ARInt/Vol.5(3)/2014(5.3-26).pdf). Acesso em: 14 jul. 2016.

TAKAHASHI, Tadao (Org.). *Sociedade da Informação no Brasil: Livro Verde*. Brasília: Ministério da Ciência e Tecnologia, 2000. Disponível em: <http://livroaberto.ibict.br/bitstream/1/434/1/Livro%20Verde.pdf>. Acesso em: 03 mai. 2015.

WENDT, Alexander. Anarchy is what States Make of it: the social construction of power politics. *International Organization*, v.46, n.2, p.391-425. 1992. Disponível em: <http://ic.ucsc.edu/~rlipsch/Pol272/Wendt.Anarch.pdf>. Acesso em: 20 out. 2016.

Recebido em: 22/04/2016

Aceito em: 09/12/2016



# PEACEKEEPING AT SEA? A CASE STUDY OF THE MARITIME TASK FORCE IN LEBANON<sup>1</sup>

Luiz Gustavo Aversa Franco<sup>2</sup>

## ABSTRACT

---

Since the end of the Cold War, naval forces have become more and more important to peacekeeping and conflict management efforts, a novelty whose best example is the Maritime Task Force (MTF) established within the United Nations Interim Force in Lebanon (UNIFIL). The objective of this work is to present the potentialities of the employment of naval forces in peace operations to fulfil their mandates through the case study of UNIFIL-MTF, emphasizing the role played by Brazil and how it boosts the country's projection in international peace and security. Using the operational concepts of "maritime interdiction" and "peacekeeping", this paper presents an overview of the utility of naval forces in peace operations in general, a brief background of the 2006 conflict in Lebanon, the performance of UNIFIL-MTF and the importance of the Task Force to the Brazilian participation in peace operations. The main contribution of this research is to fill a gap in the existing literature on the issue, which has very few updated titles dedicated to this subject.

**Key-words:** UNIFIL-MTF; peacekeeping; maritime interdiction; Brazil.

---

<sup>1</sup>The author thanks Prof. Ana Flávia Granja e Barros and Prof. Alcides Costa Vaz for their valuable contributions, exempting them of any responsibility.

<sup>2</sup>PhD Candidate at the University of Brasília's Graduate Studies Program in International Relations (PPGRI-UnB), Brasília, DF, Brazil and member of the International Security Studies and Research Group (GEPIS). The present work was carried with support of the CNPq, National Council for Scientific and Technological Development – Brazil. E-mail: luizgafranco@gmail.com



## INTRODUCTION

Since the late 1940s, the United Nations (UN) has employed military forces voluntarily granted by its member-states to assist in conflict management and resolution efforts in what has been known as peacekeeping or peace operations. Such operations have been carried out mostly by ground troops, with maritime forces playing a small and partial role. However, with the end of the Cold War and the changing nature of armed conflicts around the world (i.e., the decrease of classic international/interstate conflicts and the simultaneous increase of internal/intrastate conflicts), this scenario has changed and naval forces have become more and more important to peacekeeping and conflict management. This novelty is best illustrated by the establishment of the Maritime Task Force (MTF) as an integrating part of the United Nations Interim Force in Lebanon (UNIFIL). Initially, this was a largely European force, commanded and composed by European armed forces. However, since 2010, the Europeans have reduced their forces, with emergent countries filling the gap, among them Brazil, who has the command of the Task Force in 2011.

The first (and so far only) example of naval forces being placed under the UN flag as an integral part of a peacekeeping operation, the MTF has been established in the aftermath of the 2006 Israel-Hizbollah war as part of a redesign of UNIFIL, deployed since 1978. The Task Force's main purpose is to enforce the arms embargo imposed by the United Nations Security Council (UNSC) against unofficial armed groups in Lebanon, and it does so by conducting maritime interdiction operations on the Lebanese coast. Unlike other cases when naval power was employed to conduct such operations in support of a peacekeeping mission, the units that comprise the MTF are an integral part of the UN force (and not an independent force acting in parallel), representing a "groundbreaking innovation for the UN system" (MATTELAER, 2013).

Peace operations are historically a highly important issue for students of International Relations, International Security and Peace Studies. However, even with the considerable attention given to the employment of multinational naval forces in peace operations during the last decades, the knowledge about these forces' potential in such operations is not yet widespread. Real life cases are few and recent, which makes

the general understanding of this issue considerably underdeveloped. This leads to the following **research problem**: how does the employment of naval forces contribute to the maintenance of international peace and security within the peace operations framework? In an attempt to satisfactorily answer it, the following **research hypothesis** will be tested: the employment of naval forces as components of peace operations can be useful to a large extent in the fulfilment of their mandate as exemplified by the case of UNIFIL-MTF.

In this sense, the general objective of this work is to present the potentialities of the employment of multinational naval forces in peace operations to fulfil their mandates through the case study of UNIFIL-MTF, emphasizing the role played by Brazil and how it boosts the country's projection in international peace and security. In order to do so, the present work is divided in seven sections, including this Introduction. The second section presents the operational concepts that lay the analytical foundations for this study: maritime interdiction and peacekeeping. The third section provides an overview of the role played by naval forces in peacekeeping operations in general. The fourth section briefly presents the background of the 2006 conflict in Lebanon and how UNIFIL has been redesigned to tackle the situation and its main developments. The fifth section will analyze the role of the MTF as part of UNIFIL, its contribution to the fulfilment of the mission's mandate and its development from inception to the present day. The sixth section addresses the importance of the MTF to Brazil's participation in peace operations, underlining the Brazilian perspective on the issue. Finally, the Conclusion will present the study's main findings and final argument.

The main contribution of this paper is to fill a gap in the existing literature on the issue, which has very few updated titles dedicated to this subject. In fact, it will be perceptible along the next sections that very little attention has been given to the role played by UNIFIL-MTF in conflict management in Lebanon, especially in the last years. In addition, there is almost no examples of published works that address the Brazilian contribution to the mission and its perspectives on the subject. Therefore, it is hoped that the analysis presented here contributes to the advance of other researches on naval peacekeeping and the role played by Brazil in this scenario.

## OPERATIONAL CONCEPTS: MARITIME INTERDICTION AND PEACEKEEPING

In order to properly analyze the role of naval forces in peacekeeping operations in general and the role of the UNIFIL-MTF in particular, it is necessary to present and clarify the main aspects of two operational concepts that are fundamental to this study: maritime interdiction and peacekeeping.

According to Fernando dos Santos (2013, p. 499), the concept of maritime interdiction “in its most generic conceptualization, encompasses the capacity to interfere in the use of the sea by third parties”, and involves “any measure, imposed by a Naval Power, that limits maritime transport or navigation, even partially or temporarily”. Also referred to as Maritime Interdiction Operation (MIO), this concept is operationally defined by the North Atlantic Treaty Organization (NORTH ATLANTIC TREATY ORGANIZATION) as encompassing:

seaborne enforcement measures to intercept the movement of certain types of designated items into or out of a nation or specific area (...) normally restricted to the interception and, if necessary, boarding of vessels to verify, redirect or impound their cargoes in support of the enforcement of economic or military sanctions (NATO, 2005, p. 1).

Before advancing further, it is important to differentiate maritime interdiction from blockade operations. On the one hand, MIOs share similarities with these last ones “by employing the same classic strategic conception” while, on the other, being distinct of them “as regards to the possibilities of employment and to tactical-operational procedures”. In this sense, the main difference between MIOs and blockade operations is that the former are not usually unilaterally undertaken by an individual state, being normally related to an authorization from an international organization (IO) that is seen as legitimate, even by the interdiction’s target state.<sup>3</sup> It follows from this understanding that a fundamental trait of MIOs is the “non-state character of the application of military force”,

<sup>3</sup>In legal terms, the basis for such action is found in the United Nation Charter’s Article 24,

which grants powers to the UNSC to maintain international peace and security.

which must be “determined by a competent body recognized by the international community as the holder of such power and appreciate the respect for state sovereignty by limiting the application of force to the minimum necessary” (SANTOS, 2013, p. 508-509).

It must also be noted that MIOs are not only limited to the application of sanctions and that they do not necessarily imply the denial of the use of the sea by a state. In other words, MIOs are not a necessarily coercive measure, with its use being either imposed or requested (the case of UNIFIL-MTF, as it will be seen, is the latter type). Regardless of the category in which it fits, however, MIOs have a few fundamental traits: the contribution to international peace and security as its goal; the selective restriction of the use of the sea; the “contained and moderate stance” of the use of force; a “non-state, collective and agreed character”; its limitation to the maritime environment; the naval means, material goods or people and extraction of sea resources activities as targets of interdiction; and the ability to impose military force without undermining state sovereignty (SANTOS., p. 511). This kind of operation has two objectives, being the determination “if a vessel is in compliance with or in violation of the stated reason for interdiction” its primary one and the gathering of intelligence regarding the “vessel’s itinerary and future intentions” and “[m]ilitary and shipping activity in and around an embargoed nation’s ports” (NATO, 2005, p. 1-2).

In general, units engaged in MIOs have the authority to perform tasks such as: interrogation of vessels “for reasons other than safe navigation”; dispatching “armed boarding parties to visit vessels bound to, through, or out of a defined area”; examination of a ship’s paper and cargo; searching for “evidence of prohibited items”; diversion of vessels that fail to comply with the guidelines established by the sanctioning body; and the seizing of vessels and their cargo in case of refusal to divert. When it comes to the enforcement of embargoes and/or sanctions, the effectiveness of a MIO “is related to compliance with the sanctions or embargo, reduction in the flow of prohibited items, and/or prevention of escalating hostilities”. In this sense, the responsible authority must address the following points during the establishment of a MIO: the level of force authorized in the conduction of the operation; the specification of prohibited items; the geographic limitations; and the disposition or not to divert and/or seize vessels (NATO., p. 1-1 – 1-2).

There has been a considerable number of MIOs conducted since the establishment of the UN System, with documented occurrences including the Beira Patrol (1966-1975), the maritime interdictions in

the Middle-East (1990-2003) and in the Adriatic Sea (1992-1996), the embargo imposed on Haiti (1993-1994), NATO's Operation Unified Protector on Libya (2011) and, finally, the one conducted by UNIFIL-MTF (2006 - ). All these operations were approved by the UNSC on the grounds of a Chapter VII resolution,<sup>4</sup> which presented a specified list of prohibited items and limited the military activities to the maritime area (SANTOS, 2013). The UN is unique among the authorities capable of launching such operations because it is "recognized as a legitimate representative of the community of states in global scale (...) and a tool for the application of a specific naval power capable of respecting states' sovereignty". Its range of operations include conflict prevention, establishment of exclusion zones, maritime interdiction and peace operations (SANTOS., p. 512).

In parallel with the idea of maritime interdiction, the other operational concept for the development of this study is peacekeeping. The UN defines peacekeeping as "one among a range of activities undertaken by the United Nations and other international actors to maintain international peace and security throughout the world", and as "a technique designed to preserve the peace, however fragile, where fighting has been halted, and to assist in implementing agreements achieved by the peacemakers" (UNITED NATIONS, 2008b, p. 17-18).<sup>5</sup>

Developed in the 1940s-1950s as a conflict management tool to fill the gaps left by the post-war collective security regime, peacekeeping operations have become one of the main activities conducted by the UN in the area of peace and security. The main purpose of these operations is, in principle, "to support the implementation of a cease-fire or peace agreement" and, although not being fully-fledged military warfighting operations, peacekeeping missions "may also use force at the tactical level, with the authorization of the Security Council, to defend themselves

---

<sup>4</sup>Chapter VII of the UN Charter is dedicated to "action with respect to threats to the peace, breaches of the peace, and acts of aggression" and provides the UNSC authority to establish coercive measure in crisis management.

<sup>5</sup>Peacekeeping is, actually, one specific type of the broader concept of peace operations, which encompasses other activities such as peace enforcement and post-conflict peace-building and may be conducted by the UN, regional organizations and *ad hoc* multinational coalitions. For the purposes of this research, however, only peacekeeping operations conducted under the UN flag will be addressed.

and their mandate, particularly in situations where the State is unable to provide security and maintain public order” (UNITED NATIONS., p. 19). Its three basic principles are: (I) the consent of the parties; (II) impartiality; and (III) the non-use of force except in self-defense and defense of the mandate (UNITED NATIONS., p. 31). Since 1948, the UN has deployed almost 70 peacekeeping operations around the globe and, nowadays, it has 16 missions on the field with more than 120 thousand personal (including troops, military observers, police and civilian personnel) involved.<sup>6</sup>

Until the late 1980s, peacekeeping missions were almost exclusively deployed to contain interstate conflicts, patrolling borders among warring states and overseeing the fulfillment of cease-fires and peace agreements. Since the end of the Cold War, however, due to the large increase of internal conflicts and civil wars, peacekeeping operations were adapted to properly handle contemporary conflict situations. This new configuration is called “multi-dimensional” peacekeeping, and its core functions are: the creation of “a secure and stable environment while strengthening the State’s ability to provide security, with full respect for the rule of law and human rights”; the facilitation of the “political process by promoting dialogue and reconciliation and supporting the establishment of legitimate and effective institutions of governance”; and the provision of “a framework for ensuring that all United Nations and other international actors pursue their activities at the country-level in a coherent and coordinated manner”. In fact, these operations often help to “fill the security and public order vacuum that often exists in post-conflict settings”, having “a critical role in securing the peace process, and ensuring that humanitarian and development partners are able to work in a safe environment” (UNITED NATIONS., p. 23-24).

With the proper understanding of how peacekeeping missions are useful as conflict management efforts by the international community and how MIOs may be used to support such efforts in the maritime environment, it is necessary to analyze the general aspects of the role played by naval forces in peacekeeping operations. This is the purpose of the following section.

---

<sup>6</sup> United Nations Peacekeeping. Available at: <<http://www.un.org/en/peacekeeping/>>. Access on 19 May 2016.

## OVERVIEW OF THE ROLE OF NAVAL FORCES IN PEACEKEEPING

There is an increasing importance of the role played by naval forces in peace operations, with some analysts arguing that “naval peacekeeping support operations are proliferating” (SIEGEL, 2009, p. 101). Conceptually speaking, there are two ways of understanding the role of naval forces in peace operations (often referred to as “naval peacekeeping”): “naval peacekeeping as a derivation of peacekeeping concepts on land and naval peacekeeping as an autonomous concept adjusted to the peculiarities of the maritime context”. Empirical evidence suggest that the first category is the one more observable, with very few cases of the second category being registered – and only very recently, such as the counter-piracy operations off the coast of Somalia since 2008 (OLIVEIRA, 2012, p. 49). Due to its larger empirical support and greater applicability to the case studied, the first understanding is the one adopted here.

In more general terms, naval forces in peace operations have a “broad range of (...) tasks”, encompassing possibilities that vary from the most “benign” (such as “use of Navy vessels to transport relief supplies or a UN contingent”) to the most belligerent (like bombardment) across the conflict spectrum, with some tasks (such as sealift) being applicable throughout its entirety.<sup>7</sup> Unlike ground troops, “involvement in peace operations does not present navies with missions that are at odds with training for traditional blue-water operations” because, for naval forces, “peacekeeping is not significantly different from regular operations”. In fact, for such forces, the main difference between its traditional warfighting roles and peace operations lies in the location of the operations and its interaction with other forces, i.e., “where those operations take place and the joint nature of the exercises”. There are three main types of UN naval operations: “authorizations” (“when the United Nations authorizes nations to conduct an operation”), “designation” (“when the United Nations designates a lead nation to conduct and command a mandated operation”) and “integration” (“when naval assets are directly integrated into an UN-controlled, ground-based operation”). Such operations have been conducted to transport UN personnel or equipment, riverine monitoring

---

<sup>7</sup> A detailed examination of the roles of naval forces in peace operations across the conflict spectrum has been presented by Adam Siegel (2009, p. 99).



and/or sanctions enforcement, monitoring and conduct military operations in support of a UN resolution by member-states. Naval forces have also been employed to support a UN peace operation in an independent manner (SIEGEL, 2009, p. 98-100).

In this sense, naval forces have six distinct tasks in UN peace operations, three regarded as “fundamental” and the other three as “ancillary” (MCLAUGHLIN, 2009, p. 49-54). The first fundamental task is force delivery, which can happen in three different ways: the physical delivery of “land and air forces to distant territory”; the delivery of strikes in support of a UN operation;<sup>8</sup> and the delivery of “latent force, or presence, in support of a message or warning on behalf of the UN or international community”. The second fundamental task is to “patrol and monitor”, which can be carried out by “monitoring compliance with UN resolutions and peace agreements”, “monitoring and enforcing UN sanctions and embargoes” or “policing compliance with other specific arrangements that are considered integral to a particular mission”. The third and last fundamental task undertaken by naval forces in UN peace operations is logistical support, once the majority of “supplies, equipment and replacement forces provided on a continuing basis during UN peace operations are delivered from the sea”. The first ancillary task of naval forces is to serve as the initial (often primary) command and control platform for the provision of communication facilities in support of UN operations. The second ancillary task is to support the evacuation of non-combatants from a conflict zone. Finally, the third and last ancillary task is the provision of “neutral ground” for negotiations and discussions between parties to a conflict, and between these parties and the international community”.

When it comes to maritime interdiction more specifically, there are two main roles played by naval forces in peace operations: economic/diplomatic “peaceful coercion” and the use of force “for international peace and security purposes”. The first, characterized as a “passive” role, is more commonly related to the enforcement of sanctions and involves the deployment of naval forces as the “obvious observer, whose duty is to monitor and report on compliance and non-compliance rather than to act as an enforcer”. Its legal/conceptual basis is the UN Charter’s

---

<sup>8</sup> This can be carried out through means such as “naval gunfire support, detection and targeting intelligence, and aircraft and missile strike” and must be explicitly authorized in the mission’s mandate and explained in its rules of engagement.



Chapter VI, related to the “*pacific settlement of disputes*”. The second role is characterized as “*active*” and loosely resembles classic blockade operations, with the “*use of force for the preservation of international peace and security*” involving the “*use of naval forces to actively implement and enforce compliance*” based on the UN Charter’s Chapter VII and the Law of Naval Warfare – LoNW (MCLAUGHLIN, 2009, p. 125-128).

The employment of naval forces in peace operations has a number of unique advantages and associated challenges which are worthy of examination. One of the main advantages is that naval forces, when operating under national command (i.e., not part of the UN operation), can serve as “*reserves*” for the mission, standing “*ready to intervene with full combat capability to protect or otherwise support*” troops in the ground “*without the UN itself having to assert a combative posture*”. Another important advantage of naval forces in peace operations is their interoperability, i.e., “[t]he ability of naval units to switch from one task to another” (SIEGEL, 2009, p. 101, 104). In this sense, such forces are able to provide added value to a peace operation due to its ability to range “*from the perennial synergy between naval power and diplomacy (...) through constabulary functions (...) to military roles*”. Naval forces can also be of great use to peace operations due to its multi-dimensional flexibility, which can be divided in flexibility of movement, flexibility of presence and flexibility of employment. In terms of movement, naval forces enjoy virtually unrestricted freedom of movement through the ocean and are much lesser prone to the legal, political and practical boundaries that restrict the movement of ground troops. When it comes to presence, naval assets’ greater freedom of movement and easier access to a conflict zone through the sea facilitates the ability of the UN to emphasize or de-emphasize its presence in the scenario through the prompt use of such assets. In addition, naval forces enjoy considerable flexibility of employment, since they can rapidly switch between various levels of force posture due to their interoperability. This “*organic, ‘multi-purpose configuration’*” of military naval vessels “*is what lends naval force its greatest utility for UN peace operations*” (MCLAUGHLIN, 2009, p. 38, 48).

Naval forces' interoperability, however, can be perceived as a liability too. Unlike ground forces, it is more difficult to adapt a warship from full combat capability to more passive stances usually desired for peacekeeping units. Aside from the inherent nature of these different assets (ground troops and maritime forces), the number of potential contributing states of naval forces is considerably smaller than those contributing ground forces, which lowers the number of assets potentially available for a UN peace operations (SIEGEL, 2009; MCLAUGHLIN, 2009). Other disadvantages of naval forces acting in peace operations are its costs and integrated command issues. Maritime forces are inherently expansive to operate, which makes the integration of large naval contingents under the aegis of a UN peace operation with its considerably limited budget not very feasible. These forces also require a considerable degree of compatibility to achieve interoperability and to act effectively, which makes it easier for them to operate under the same national or allied command than the standard multinational integrated command structure of a peace operation (SIEGEL, 2009). The aforementioned flexibility that naval forces provide for peace operations generates a counterpart: the need for increased awareness by the drafters of the mandate of the "character and uses of naval forces" (MCLAUGHLIN, 2009, p. 54). In this sense, peace operations that contemplate a more active role for naval forces must have clearer guidelines for the use of such assets, running the risk of rendering these assets irrelevant.

Beyond the operational advantages and disadvantages associated to naval forces in peace operations scenarios, there are also a few legal and legitimacy issues derived from the presence of such assets that need to be tackled. In its most generic terms, the use of the seas is governed by two sets of rules. The 1982 Law of the Sea Convention (LOSC) – also known as Montego Bay Convention – is the principal legal document that governs the peaceful uses of the seas and oceans. However, when it comes to their belligerent uses, the main referent is the LoNW, which is frequently understood as a subcomponent of the International Law of Armed Conflict/International Humanitarian Law. In the specific context of peace operations, another highly important set of norms and rules is the regime established by the UN Charter, more specifically its Chapter VII. In this sense, there are important

tensions between the provisions established by Chapter VII and those of the LOSC, which generates complications for naval forces in UN peace operations.<sup>9</sup> However, this is an issue that remains “relatively untouched”, which makes the understanding of the relationship between these two important sources of international law “far from clear”.<sup>10</sup> Still, questions regarding “UN Chapter VII operations, use of force, the LOSC, and their relationship” will continue to be significant, due to the “escalating tempo and intrusiveness of UN peace operations at sea” (MCLAUGHLIN, 2009, p. 13, 24).

Regardless of the confusions and tensions between the LOSC, LoNW and the UN Charter, the provisions of the last one are quite telling about the legal and legitimacy aspects of the role of naval forces in UN peace operations. In fact, Chapter VII, specifically articles 40-42, have important implications for such operations, although remaining “ambiguous”, especially ‘in the case of interdiction operations’ (MCLAUGHLIN, 2009, p. 129). At first, Article 40 gives the UNSC powers to adopt “provisional measures” to prevent an ongoing crisis from escalating, which may include the deployment of naval forces for monitoring and observing. Secondly, Article 41 regards which “measures not involving the use of armed force (...) to be employed to give effect to its decisions”, including “complete or partial interruption of economic relations and of (...) sea (...) means of communication”. Finally, Article 42 establishes that, if the UNSC “consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces to maintain or restore international peace and security”, which “may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations”.<sup>11</sup>

---

<sup>9</sup>In sum, while the rights and duties established by the LOSC create “no go zones” in coastal states jurisdictional waters, the provisions of the UN Charter Chapter VII allow the trespassing of such spaces if mandated by the UNSC. It is exactly that there is no legal mechanisms that determine when the provisions of one norm cede to the other that make the relationship between the two confusing and problematic.

<sup>10</sup>According to Rob McLaughlin (2009, p. 17), “[w]hilst scholarship and practice has scratched the surface of the separate relationships between LoNW and the UN Charter, and the LoNW and the LOSC, there is scarce analysis of the third element of this triangle – the interaction between UN Charter Chapter VII and the LOSC”, a relationship that is “seminal for UN naval peace operations”.

<sup>11</sup>UN Charter (full text). Available at: <<http://www.un.org/en/sections/un-charter/un-charter-full-text/index.html>>. Access on: 31 May 2016.

While Article 41 is seen as a “mandatory sanctions regime” that “must be complied with by all states and parties whether UN members or not”, Article 42 provides a “clear and unequivocal” authorization to “use force during an interdiction operation”. This textual distinction, however, is “is far from clear” in practice (MCLAUGHLIN, 2009, p. 130, 132). Indeed, Rob McLaughlin argues that the relationship between the measures provided by these two articles should not be viewed as a “clear-cut distinction”, but rather as a “continuum”. This continuum varies from the minimum of “enforcement”, which demands “the authority to approach, board, demand documents, search, and if required, divert and arrest”, to the extreme situation when “if a vessel refuses to comply, this authority ultimately extends to firing across that vessel’s bows or, as a last resort, disabling it with direct fire” (MCLAUGHLIN, 2009, p. 133). In this context, the territorial sea acquires special meaning for being “the most significant sphere of maritime activity” in cases where peace operations are authorized to use force. It is the “oceanspace most closely linked to any land territory that is subject to a UN mandate” and most of the typical tasks undertaken by naval forces on such space are “closely linked with, and often vital to, the success of UN peace operations ashore” (MCLAUGHLIN, 2009, p. 33).

The analysis of past practice has revealed that the UN has a potential authority to mandate MIOs in the territorial sea (even without consent) to enforce sanctions regimes. Some of the most illustrative cases include interdiction operations conducted during the First Gulf War and the Yugoslav Wars, occasions in which interdiction can be seen as “as an aspect of the UNSC’s authority to use force in Territorial Seas during peace operations”. On the one hand, the interdiction operation conducted during the First Gulf War is viewed as “the modern precedent for such operations”, with its authorization provided by UNSC resolution 665 being the “fundamental conceptual precedent for modern UN naval interdiction operations” and its operational conduct representing “the modern recapitulation of practice in such operations”, a precedent that “has dominated and been repeated in UN naval interdiction operations since 1990”. On the other, the operations conducted during the Yugoslav Wars have been seen as “the most complex and provoking example of such operations” due to “the fact that this crisis clearly and overtly raised, in particular, the issue of UN interdiction operations in the Territorial Sea” (MCLAUGHLIN, 2009, p. 135, 137-138, 140, 152).

Once the general role of naval forces in UN peace operation is clarified, the analysis can proceed with the examination of the role played by UNIFIL-MTF. However, before moving to this, it is important to understand the general dynamics of the conflict in Lebanon, how it has led the UN to intervene and how it has evolved since its early days to the present. The next section will provide this background, with the following section dedicated to the analysis of UNIFIL-MTF specifically.

## BRIEF BACKGROUND OF THE CONFLICT AND UN PEACEKEEPING IN LEBANON

The conflicts in Lebanon involving Israel as well as the presence of international troops under the UN flag on the region have been present for decades, with the conflict's final resolution and the total withdrawal of peacekeepers not predicted anytime soon. In general, it is another protracted conflict that has demanded considerable attention and direct involvement of the international community and that will probably last as long as its root causes – the border disputes and the situation of the Palestinian refugees (MATTELAER, 2013) – are not addressed. Still, both the conflict itself and its management by the international community have evolved, especially in the last decade, in a way that it demands closer examination.

The main factors that resulted in the confrontations between Israel and Lebanon are the Lebanese civil war of 1975 and the Palestinian presence in that country, which included both refugees fleeing from the Israelis first conflict with its Arab neighbors in 1948 as well as the establishing of strongholds of the Palestinian Liberation Organization (PLO) in southern Lebanon in the 1970s (MATTELAER, 2013). In March 1978, PLO armed elements based in Lebanon carried out attacks in Israel, leading to the first Israeli invasion of Lebanon, in which the Israel Defense Forces (IDF) occupied the entire Southern part of the country (MAKDIS *et al.*, 2009). After protests from the Lebanese government, the UNSC approved resolutions 425 and 426 demanding an immediate cessation of all Israeli military activity and the complete withdrawal of its forces from the Lebanese territory. It was in this context that the Council established UNIFIL, with three main purposes: “confirming the withdrawal of Israeli forces; restoring international peace and security; and assisting the Government of Lebanon in ensuring the return of its effective authority in the area”.<sup>12</sup> Initially approved for a period of six months and a four thousand-strong force, latter resolutions extended the missions mandate and increased its contingent.

---

<sup>12</sup> UNIFIL Background. Available at: <<http://www.un.org/en/peacekeeping/missions/unifil/background.shtml>>. Access on 02 June 2016.

Throughout the following years, “little progress was made” (EDSTRÖM, GYLLENSPORRE, 2013, p. 71), and new confrontations in 1982 lead to a new Israeli military campaign against Lebanon. The fighting lasted for three years and, during that period, UNIFIL remained behind Israeli lines and restricted its role to “providing protection and humanitarian assistance to the local population to the extent possible”.<sup>13</sup> In 1985, Israel conducted a partial withdrawal of its forces, maintaining control of the Southern part of the country. On that same year, another important player would come into the scene: the Islamic resistance movement called Hizbollah (MAKDIS *et al.*, 2009), the “Party of God”.

On the year 2000, Israel unilaterally withdrew its forces from Lebanon. However, “there was no comprehensive peace deal between Israel and Lebanon”, and “the Lebanese government refused to deploy its armed forces to fill the vacuum the Israeli forces left behind in the south”, allowing Hizbollah to “grow into a state within the state of Lebanon” and to build-up its territorial defenses. In the meanwhile, UNIFIL’s contingent was decreased and it “was gradually transformed into an observer mission” (MATTELAER, 2013, p. 82). This “illusion of peace”, in which Hizbollah “continued to stockpile weapons and reinforce its po-sitions in southern Lebanon, amidst fears that Israel would launch further incursions” (MAKDIS *et al.*, 2009, p. 21), set up the stage for new confrontations.

On 12 July 2006, Hizbollah carried out a “dramatic raid” against an Israeli army patrol (killing three soldiers, wounding two and making two others captive), attacking Israel’s third largest city (Haifa) on the following day. These events provoked a “sharp military response” from Israel (MATTELAER, 2013, p. 82), which resulted in a new occupation of Lebanon, including the imposition of a “total land, sea and air blockade” of the country (MAKDIS *et al.*, 2009, p. 21). After 34 days of fighting with “no decisive result” (MATTELAER, 2013, p. 83), the UNSC approved resolution 1701 in order to put an end to the conflict (INTERNATIONAL CRISIS GROUP, 2006). The resolution called for a “full cessation of hostilities”, including “the immediate cessation by Hizbollah of all attacks and the immediate cessation by Israel of all offensive military operations”, as well as the support of both Israel and Lebanon to “a permanent ceasefire and a long-term solution” to the conflict. Other important provisions of the resolution included the determination that “the situation in Lebanon constitutes a threat to international peace and security” (which may be considered an indirect and implicit reference of Chapter VII),

---

<sup>13</sup> Idem

the establishment “between the Blue Line and the Litani river of an area free of any armed personnel, assets and weapons other than those of the Government of Lebanon and of UNIFIL”, as well as “the disarmament of all armed groups in Lebanon, so that (...) there will be no weapons or authority in Lebanon other than that of the Lebanese State” and the prohibition of any “sales or supply of arms and related materiel to Lebanon except as authorized by its Government”. In addition, the Security Council called upon “the Government of Lebanon to secure its borders and other entry points to prevent the entry in Lebanon without its consent of arms or related materiel”, requesting UNIFIL to “to assist the Government of Lebanon at its request” (UNITED NATIONS, 2006b, p. 2-4). In this sense, the mission was significantly enhanced to a 15 thousand-strong force with an expanded mandate, which included an authorization to:

take all necessary action in areas of deployment of its forces and as it deems within its capabilities, to ensure that its area of operations is not utilized for hostile activities of any kind, to resist attempts by forceful means to prevent it from discharging its duties under the mandate of the Security Council (*Ibid.*, p. 3-4).

This contingent increasing and mandate expansion made some analysts refer to the new phase of the mission as “UNIFIL II” (MAKDIS *et al.*, 2009; MARTA, 2009).

Although successfully accepted by all parties of the conflict, resolution 1701 received some criticism from various observers, with some “uncontroversial parts”, however, “whose implementation marked steady, even surprising progress” (ICG, 2006, p. 1-2). Some of them were the aforementioned strengthening of UNIFIL and the imposition of an arms embargo (MARTA, 2009).

Regarding the strengthened UNIFIL, its effectiveness has been “hotly debated” (ABDENUR, 2016, p. 395), with the extent to which the mission’s “robustness’ has succeed in transforming UNIFIL II into a more effective peacekeeping unit” remaining “controversial” (MAKDIS *et al.*, 2009, p. 7). In fact, the expansion of the mandate allowing the operation to use force would have made, for some, the operation to “trode [the] fine line between peacekeeping and peace enforcement, a policy that ultimately



backfired" (MAKDIS *et al.*, 2009, p. 10). Although it is recognized that "UNIFIL contributed to containing the outbreak of renewed hostilities", it is also affirmed that it "does not address the underlying conflict dynamics, which are political in nature and go far beyond UNIFIL's mandate". In fact, such analysts argue that "the enhanced UNIFIL can never be strategically decisive" because "it contains conflict on an interim basis, but does not make peace" (MATTELAER, 2013, p. 99, 114).

Following the establishment of the arms embargo (designed to prevent the rearming of Hizbollah), Israel announced, in September 2006, that it would begin to lift the blockade imposed on Lebanon earlier. In the Mediterranean, a temporary European naval force composed of seven vessels under Italian command replaced Israeli forces. In 15 October 2006, in response to a request from the Lebanese government, the UN established the MTF as part of UNIFIL. An "important innovation in the enhanced UNIFIL" and "the very first time a UN operation included naval assets" (MATTELAER, 2013, p. 89-90), the MTF was designed to "patrol international waters off Lebanon's coast as a way of assisting the government, which", at that time, had "no significant naval capability, in enforcing the arms embargo" (ICG, 2006, p. 11).

## THE ROLE PLAYED BY UNIFIL-MTF

As presented in the previous section, the MTF was established as an integral part of UNIFIL to enforce the arms embargo imposed against non-state actors in Lebanon due to the inability of that country's government to do so by its own means. In this sense, the MTF's importance for the peacekeeping efforts in Lebanon may be resumed in two points: maritime interdiction and capacity building.

As a MIO, UNIFIL-MTF is a one-of-a-kind, since it represented the first time that such operations were conducted by request of the host state and that the naval force was truly part of the UN peace operation (and not an independent force acting in support of it). Another singularity of this mission is that it is "the first maritime interdiction that occurred in accordance with the government *de facto* and *de jure* and in favor of the focal state's exercise of sovereignty". Since its action is dependent on the Lebanese government's request, UNIFIL-MTF demonstrate that an MIO does not necessarily imply the denial of a state's use of the sea, even though it restricts its use for purposes such as trafficking and smuggling of prohibited items. In fact, the MTF is "employed to support the jurisdiction of" Lebanon (SANTOS, 2013, p. 506, 509).



The main tasks of the MTF are “to establish a naval presence and surveillance over the Area of Maritime Operations, with priority to the Lebanese territorial waters” and “to conduct Maritime Interdiction Operations (...), including identification and, within the Lebanese territorial waters, stopping/diverting or referring suspect Merchant Vessels for inspection by Lebanese authorities”. Its long-term objective is “to hand over security responsibilities to the” Lebanese Armed Forces-Navy (LAF-Navy) “in a gradual manner”, which includes direct assistance and training (SANDALI, 2010, p. 7). It is important to note that “the Lebanese Navy carries out all inspections, thus permitting the MTF to maintain a high degree of neutrality, and by extension, a credibility respected by all parties” (MAKDIS *et al.*, 2009, p. 28).

The MTF units operate within the Area of Maritime Operations (AMO), an area of approximately 5 thousand square nautical miles that “runs along the entire coastline of Lebanon and stretching westward up to 43 nautical miles into the Mediterranean Sea”.<sup>14</sup> Within this area, the MTF conducts “continuous surveillance of merchant traffic, particularly along the approach corridors to the three main harbours of Lebanon: Beirut, Tripoli and Sidon.” (SANDALI, 2010, p. 7).

The first activities undertaken by the Task Force were “rescue and humanitarian action (...) and subsequently patrolling activities (...), both within a national framework first and later a multinational one” (MARTA, 2009, p. 4). One of the difficulties faced by the MTF in its initial stages was the “lack of pre-established UN maritime operation procedures”, making necessary that “that such procedures had to be created in close collaboration with the (...) LAF, as well as with the Israeli and Syrian Navies” (MAKDIS, *et al.*, 2009, p. 28).

From October 2007 to 26 February 2016,<sup>15</sup> the MTF has carried out a “dual mandate”, which included two main activities. The first was to conduct MIOs “along the Lebanese coast to prevent the entry into Lebanon of unauthorized arms and related materiel”. The second was the “[c]ooperation between the Task Force and the Lebanese navy”, including a “joint training programme” (UNITED NATIONS, 2008a, p. 7). Throughout this period, the Task Force has maintained its presence and readiness to act in the AMO while, simultaneously, providing training for the Lebanese authorities to assume their responsibilities.

---

<sup>14</sup> The first 12 nautical miles from the Lebanese coastline constitute the country’s territorial sea. Beyond this point are international waters.

<sup>15</sup> Date of the latest report of the UN Secretary-General on the implementation of the Security Council resolution 1701 by the time of writing

From November 2008 to November 2013, “[j]oint training exercises, aimed at enhancing the operational capacity of UNIFIL and the Lebanese Armed Forces” were undertaken (UNITED NATIONS, 2009b, p. 5). Since June 2009, the joint exercises included “personnel with the Coastal Radar Organization and the Lebanese naval chain of command” and added a “particular focus on response to unexpected events” (UNITED NATIONS, 2009a, p. 6). In some occasions, the joint exercises included “an amphibious and an artillery exercise” involving “land and maritime forces” (UNITED NATIONS, 2010, p. 4). Other important training activities included MIO exercises,<sup>16</sup> workshops, cadet training sessions and training exercises on land and at sea.<sup>17</sup>

In one of his reports regarding the implementation of UNSC resolution 1701, the UN Secretary-General asserted that “the improved capabilities of the Lebanese navy will gradually enable it to assume some responsibilities and tasks presently performed by the Maritime Task Force” and that “continued material and technical support will remain critical over the medium to long term” (UNITED NATIONS, 2008a, p. 7). In a similar way, a further report of the same kind affirmed that “[t]he lack of adequate naval units presents a major challenge to the Lebanese navy in assuming increased responsibilities on a sustainable basis” (UNITED NATIONS, 2009a, p. 8). Therefore, the “international support for training the Lebanese armed forces” is “crucial.” (EDSTRÖM, GYLLENSPORRE, 2013, p. 80).

Since March 2009, the LAF-Navy has “assumed responsibility inside the [Lebanese] territorial waters for hailing vessels approaching the main Lebanese ports, while the Maritime Task Force has assumed a monitoring role” (UNITED NATIONS, 2009c, p. 7). On three occasions between November 2009 and February 2010, the MTF was requested to “assist in search and rescue operations” (UNITED NATIONS, 2010, p. 6).

Between November 2011 and 28 June 2012, due to “requests by Lebanese naval authorities”, the MTF “intensified its surveillance activities in certain parts of the area of maritime operations to prevent suspected smuggling activities” (UNITED NATIONS, 2012a, p. 5; 2012b, p. 6). In two during the February-June 2012 period, “the Lebanese authorities reported

---

<sup>16</sup> Conducted five times (lasting five days each) from February to June 2012 and three times (lasting two days each) from June to November 2012. Similar exercises were also conducted in nine occasions during the 1 March – 28 June 2013 period.

<sup>17</sup> There are registers of “one workshop and 11 cadet training session, as well as 31 at-sea training activities on-board the Maritime Task Force vessels, for Lebanese junior officers” (UNITED NATIONS, 2012c, p. 7) conducted during the June-November 2012 period; “13 workshops on land and 20 at-sea training exercises” (UNITED NATIONS, 2013a, p. 6) conducted during the 30 October 2012 – 28 February 2013 period; and “42 training exercises on land and 151 at sea” (UNITED NATIONS, 2013b, p. 6) conducted during the 1 March –28 June 2013 period.

to UNIFIL that they had found unauthorized cargo consisting of weapons and military equipment, which were being smuggled into Lebanon from the sea in violation of resolution 1701" (UNITED NATIONS, 2012b, p. 6). Investigations by the Lebanese authorities concluded that, in both instances, the apprehended weapons were destined to rebel groups in neighboring Syria. These were considered the "the most significant attempts to breach the arms embargo reported by the Lebanese authorities since the adoption of resolution 1701" (UNITED NATIONS, 2012b).

Earlier analysis had already stressed that, although a "considerable MTF presence should be maintained within the UNIFIL framework to act as a deterrent or buffer force between the conflicting parties (...), MTF needs fewer large ships, and more small vessels, which would be faster and thus facilitate maritime manoeuvres." In due time, "these rapid patrol boats would and should be operated by the Lebanese Navy, endowed with the sovereign capacity to stop, inspect and detain suspect ships" (MAKDIS *et al.*, 2009, p. 29). In this sense, in late 2014, to streamline the MTF's requirements "while maintaining its operational capability", the UN's Department for Peacekeeping Operations (DPKO), in coordination with the mission's staff, "carried out a desktop ship-to-task analysis and recommended reconfiguring the Maritime Task Force in phases by gradually substituting frigates with corvettes" (UNITED NATIONS, 2014, p. 12).

As early as 2006, the first report of the UN Secretary-General on the implementation of UNSC resolution 1701 argued that the establishment of a "maritime unit for patrolling the coastline" was one of the "most urgent" needs "to reinforce UNIFIL" (UNITED NATIONS, 2006a, p. 5). A further report of the same kind (UNITED NATIONS, 2007, p. 12) emphasized that such an "innovative measure", driven by the "circumstances in which the newly expanded UNIFIL was established", introduced important assets that "have been critical to the successful implementation of UNIFIL's mandate". Years later, one of the MTF's former commanders argued that its efforts "have contributed to the implementation of UN Security Council resolution 1701, proved as a strong deterrence against illegal activity in the area and have helped generally enhance the security of maritime shipping, with significant benefits to the economy,

trade, welfare and overall stability of Lebanon” (SANDALI, 2010, p. 7).

As the Lebanese authorities’ capacities to assume security responsibilities in their jurisdiction has improved, the size and scope of UNIFIL-MTF has been scaled down to less and smaller vessels. This points to an at least partial success of the Task Force in assisting local authorities in capacity building, while, simultaneously, maintaining a vigilant presence. By the time of writing, the MTF had hailed approximately 63 thousand ships and referred about six thousand vessels for further inspection by the Lebanese Navy and Customs officials.

## **PARTICIPATION IN UNIFIL-MTF AND THE BRAZILIAN PERSPECTIVE ON NAVAL PEACEKEEPING**

From its inception until 2011, European States were responsible for the leadership of the MTF, as well as most of its composition (MAKDIS et al., 2009). When these countries reduced or withdrew their contingents, the gap was filled mostly by Asian countries, such as Bangladesh, Cambodia, Indonesia, Malaysia, Nepal and Sri Lanka (EDSTRÖM; GYLLENSPORRE, 2013). However, none of them was able to assume the Task Force’s command, which made the UN and the parties involved to look for a substitute. On 24 February 2011, the command of MTF was transferred to Brazil.<sup>18</sup> It has been argued that this country was chosen for the task due to its “solid relations with both Lebanon and Israel” as well as its “accumulated experience (...) in UN peacekeeping” after seven years commanding the military component of the UN operation in Haiti (ABDENUR, 2016, p. 405).

The case of UNIFIL-MTF presents a “dilemma of continuity” for Brazil’s contribution to UN peacekeeping operations, entailing “a series of opportunities, as well as new risks”. The country has a historic aspiration to “play a more direct role in international security”, having contributed to UN peacekeeping since its inception in the late 1940s and mid-1950s. To date, Brazil has contributed with troops, police and civilian personnel to 25 UN peacekeeping missions around the world, having around 1,300 personnel deployed by August 2016.<sup>19</sup> Consequently, expectations for the country’s involvement with matters of international security have increased in later years.

<sup>18</sup> Maritime Task Force. Available at: <<http://unifil.unmissions.org/Default.aspx?tabid=11584&language=en-US>>. Access on: 06 June 2016.

<sup>19</sup> Including five police, 24 military observers and 1,274 troops (data provided by the DPKO).

This, coupled with criticisms that “Brazil is a ‘security free-rider’, ‘benefitting more from the international security system than it actually contributes’” led to its decision to assume the command of UNIFIL-MTF (ABDENUR, 2016, p. 390, 397, 401).

Although entailing “a variety of risks, including political and security ones” and representing a “different set of challenges, at additional expense and in a distant region of the planet”, the Brazilian decision to assume this responsibility may be explained by three main reasons. The first is the country’s desire for greater projection in international security; secondly, the strengthening of its bilateral ties with Lebanon; and, lastly, “naval capacity-building” (ABDENUR, 2016, p. 402-403).

Regarding the objective of improving Brazil’s projection in international security, which includes greater involvement in the Middle East, the decision to assume the command of UNIFIL-MTF would arguably “help to demonstrate Brazil’s commitment to international security” and make sure that it would “remain relevant to Middle Eastern security for a number of years” (ABDENUR, 2016, p. 403-404). According to the country’s former Minister of Defense, Celso Amorim (2012, p. 13), this decision “underlines the diversity of our contribution to the cause of peace and security”. Aside from its well-known desire for greater involvement in international security, Brazil has interests of its own in the Middle East, which are constantly affected by the recurring conflicts in the region. In this sense, the pursuit of deeper ties with Middle Eastern governments was “an important element of consideration”, making the Middle East “an increasingly important way for Brazil to expand its global reach, in security and beyond” (ABDENUR, 2016, p. 405).

When it comes to the objective of strengthening Brazil’s bilateral relations with Lebanon, the Brazilian decision was seen as an opportunity to deepen the ties with the Middle Eastern country. In fact, by the time Brazil was invited to assume command of the MTF, both its government and the UN emphasized the “demographic, cultural and economic ties between Brazil and Lebanon” (ABDENUR, 2016).<sup>20</sup>

Finally, with respect to the objective of naval capacity-building, the Brazilian participation in UNIFIL-MTF “is particularly relevant (...) due to the opportunities for enhanced cooperation with multiple navies from around the world”.

---

<sup>20</sup> There are approximately 10,000 Brazilians living in Lebanon, especially in Beirut and in the Bekaa Valley (ABDENUR, 2016, p. 406), as well as a large population of Lebanese immigrants and descendants living Brazil, including the country’s president, Michel Temer.

Even though having previous experience with cooperation initiatives with other naval forces (including naval exercises), joining and commanding a UN peacekeeping operation represented “a vastly different level of experience acquisition” for the Brazilian Navy. The case of UNIFIL, specifically, was seen as “a very different set of experiences” than the ones lived in Haiti, offering “officers and sailors alike to acquire first-hand experience, along with Marines” (*Ibid.*, p. 407-408). It is also important to note that, in assuming the command of the Task Force, Brazil became the first non-NATO country to lead a UN peacekeeping naval force – or even a multinational – fleet ever (*Ibid.*).

By the time of writing, the Brazilian contingent in Lebanon was 279-strong.<sup>21</sup> Aside from the Brazilian Flag Ship (the frigate *Independência*), the Task Force is also composed of vessels from Bangladesh (two ships), Germany, Greece, Indonesia and Turkey (one ship each).<sup>22</sup>

A general evaluation of the Brazilian participation in UNIFIL-MTF shows that not only “naval peacekeeping is aligned with the country’s maritime strategy”, but also that “it is widely considered to be a relatively efficient way of maintaining Brazil on the global peacekeeping stage and of boosting its image and role as a contributor to humanitarian efforts” (ABDENUR, 2016, p. 409). In fact, the Brazilian Navy has the “participation of the Naval Force under the aegis of international bodies in collective defense arrangements and in peace missions and humanitarian aid” as part of its objectives for its increasing international relationship and action (WIEMER, 2012, p. 193). This indicates that naval peacekeeping represents a “promising area” for the country to expand its contributions to UN peacekeeping. These contributions are not limited to the “deployment of personnel, vessels and equipment”, but also help to “shape the normative debates about how naval components may be more effectively incorporated into multilateral peace missions”. Furthermore, these are not only related to the “role that naval forces play in preventing the inflow of arms contraband into conflict-prone areas”, but also to the “capacity of naval forces to prevent blockades that undermine local economic activity and development” as well (ABDENUR, 2016, p. 411).

<sup>21</sup> 256 military personnel aboard the frigate *Independência*, 13 as part of the MTF’s Joint Staff, three as part of UNIFIL’s Joint Staff and seven inserted at the Spanish Brigade (data provided by the Brazilian Ministry of Defense).

<sup>22</sup> Maritime Task Force. Available at: <<http://unifil.unmissions.org/Default.aspx?tabid=11584&language=en-US>>. Access in: 06 June 2016.

## CONCLUSION

Naval forces have been playing an important role in peace operations for decades. Especially after the end of the Cold War and the changing nature of conflicts, the employment of naval assets to prevent the (re)arming of warring parties and the further fueling of hostilities has been vital for the maintenance of international peace and security as well as conflict management and resolution. Since this pattern of conflict is not likely to change in any foreseeable future, it is right to expect that navies throughout the world will continue to be highly valuable assets in such efforts.

The role played by navies in such conflict scenarios may vary on a case-by-case basis and will certainly be determined by the conflict's intensity and the intervening parties' willingness to use force. With an inherent ability to shift from a more passive support stance to a more proactive full-scale fighting stance in a very short time period, maritime forces may be invaluable to international actors in cases of a rapidly rising hostilities and escalation of conflicts. The correct and timely deployment of naval forces by the international community in such scenarios may be the very difference between considerable success and a huge failure to prevent, manage and solve a conflict.

The case of UNIFIL-MTF is a clear example of this, showing that naval forces can be greatly useful in peace operations' contexts by tackling both short and long term goals of the mission's mandate – the enforcement of an arms embargo and capacity-building respectively. It is perceptible from both official sources and outside analysts that the MTF has provided a very important contribution to the peacekeeping efforts in Lebanon. The absence of any further confrontation in that country since the 2006 Israel-Hizbollah war proves that such efforts have been successful (at least partially). If the current trend remains, it can be expected a further gradual decrease of the Task Force's size and strength alongside the Lebanese authorities greater and improved capacity to act, which would ultimately render the naval force's presence no longer necessary. In time, this unique example may become a model for the use of maritime forces as an integrating part of UN peace operations in which such forces fulfill a dual role of conducting MIOs in accordance with UNSC resolutions while assisting local authorities with capacity building to reassume their responsibilities.



In this sense, it is vital that any country willing and able to play a significant role in international peace and security through peace operations maintain a strong and ready to act naval force prepared to assume such responsibilities and contribute to such efforts. As it has been the case during the last decades, those states with a naval power that can be called to action in a timely fashion are the ones with the greater ability to influence an armed conflict's development and outcome. Whether if such forces are employed independently or in an integrated manner under the auspices of an IO like the UN, it will probably be the states that can make their naval forces more easily available that will have greater influence in matters of international peace and security.



# MANUTENÇÃO DA PAZ NO MAR? UM ESTUDO DE CASO DA FORÇA TAREFA MARÍTIMA NO LÍBANO

## RESUMO

---

Desde o fim da Guerra Fria, forças navais têm se tornado cada vez mais importantes para os esforços de manutenção da paz e gerenciamento de conflitos, cujo melhor exemplo é a Força Tarefa Marítima (FTM) estabelecida dentro da Força Interina das Nações Unidas no Líbano (UNIFIL). O objetivo deste trabalho é apresentar as potencialidades do emprego de forças navais em operações de paz para cumprir seus mandatos por meio do estudo de caso da FTM-UNIFIL, enfatizando o papel desempenhado pelo Brasil e como isso impulsiona a projeção do país na paz e na segurança internacionais. Usando os conceitos operacionais de “interdição marítima” e “manutenção da paz”, este artigo apresenta uma visão geral da utilidade das forças navais em operações de paz em geral, um breve pano de fundo do conflito de 2006 no Líbano, a atuação da FTM-UNIFIL e a importância da Força Tarefa para a participação brasileira em operações de paz. A principal contribuição desta pesquisa é preencher uma lacuna na literatura existente sobre o tema, que possui poucos títulos atualizados dedicados ao assunto.

**Palavras-chave:** FTM-UNIFIL; interdição marítima; manutenção da paz; Brasil.

## REFERENCES

- ABDENUR, Adriana Erthal. Rising powers in stormy seas: Brazil and the UNIFIL maritime task force. *International Peacekeeping*, v. 23, n. 3, p. 389-415, 2016.
- AMORIM, Celso. A política de defesa de um país pacífico. *Revista da Escola de Guerra Naval*, v. 18, n. 1, p. 7-17, 2012.
- BRASIL. Ministério da Defesa. [Site]. c 2014. Disponível em: <www.defesa.gov.br>. Acesso em: 2 maio 2016.
- EDSTRÖM, Håkan; GYLLENSPORRE, Dennis. *Political Aspirations and Perils of Security: unpacking the military strategy of the United Nations*. Basingstoke: Palgrave Macmillan, 2013.
- ICG – International Crisis Group. Israel/Hizbollah/Lebanon: avoiding renewed conflict. *Middle East Report*, n. 59, 1 November 2006.
- MAKDIS, Karim; GÖKSEL, Timur; KAUCK, Hans Bastian; REIGELUTH, Stuart. UNIFIL II: emerging and evolving European engagement in Lebanon and Middle East. *Euromesco Paper*, n. 76, Jan. 2009.
- MARTA, Lucia. The UNIFIL II mission in Lebanon: Italy's contribution. *Security & Defence – ARI*, n. 125, 2009.
- MATTELAER, Alexander. *The Politico-Military Dynamics of European Crisis Response Operations*. Basingstoke: Palgrave Macmillan, 2013.
- MCLAUGHLIN, Rob. *United Nations Naval Peace Operations in the Territorial Sea*. Leiden: Martinus Nijhoff Publishers, 2009.
- NORTH ATLANTIC TREATY ORGANIZATION (NATO). Allied maritime interdiction operations. Brussels: NATO Standardization Agency. April, 2005.
- OLIVEIRA, Gilberto Carvalho de. Naval peacekeeping and piracy: time for a critical turn in the debate. *International Peacekeeping*, v. 19, n. 1, p. 48-61, 2012.

SANDALI, Paolo. Maritime task force's role in UNIFIL. *AlJanoub*, n. 06, p. 6, Jan. 2010.

SANTOS, Fernando Roberto dos. Uma força naval para a paz e a segurança internacional. *Revista da Escola de Guerra Naval*, v. 19, n. 2, p. 497-522, 2013.

SIEGEL, Adam B. An examination of maritime peace support operations. In: WIRTZ, James J; LARSEN, Jeffrey A. *Naval peacekeeping and humanitarian operations: stability from the sea*. New York: Rotugledge, 2009. p. 97-109.

UNITED NATIONS. *Eighteenth report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 28 Feb. 2012a.

UNITED NATIONS. *Eleventh report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 2 Nov. 2009a.

UNITED NATIONS. *Ninth report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 3 Mar. 2009b.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006): for the period 11 to 17 August 2006*. New York: United Nations Security Council, 18 Aug. 2006a.

UNITED NATIONS. *Report of the Secretary-General on the implementation of Security Council resolution 1701 (2006)*. New York: United Nations Security Council, 30 Oct. 2007.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 28 Feb. 2008a.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 28 June 2012b.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006): reporting period from 29 June to 30 October 2012*. New York: United Nations Security Council, 14 Nov. 2012c.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006)*: reporting period from 30 October 2012 to 28 February 2013. New York: United Nations Security Council, 27 Feb. 2013a.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006)*: reporting period from 1 March to 28 June 2013. New York: United Nations Security Council, 26 June 2013b.

UNITED NATIONS. *Report of the Secretary-General on the implementation of resolution 1701 (2006)*: reporting period from 27 June to 5 November 2012. New York: United Nations Security Council, 5 Nov. 2014.

UNITED NATIONS. *Security Council Resolution: S/RES/1701*. United Nations Security Council, New York, 11 Aug. 2006b.

UNITED NATIONS. *Tenth report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 29 June 2009c.

UNITED NATIONS. *Twelfth report of the Secretary-General on the implementation of resolution 1701 (2006)*. New York: United Nations Security Council, 26 Feb. 2010.

UNITED NATIONS. *United States Peacekeeping Operations: principles and guidelines*. New York: Department of Peacekeeping Operations/Department of Field Support, 2008b.

UNITED NATIONS. [Site]. c 2016. Disponível em: <<http://www.un.org>>. Acesso em: 2 maio 2016.

UNITED NATIONS INTERIM FORCE IN LEBANON (UNIFIL). [Site]. c 2016. Disponível em: <<http://unifil.unmissions.org>>. Acesso em: 2 maio 2016.

WIEMER, Fernando Eduardo Studart. Aula inaugural dos cursos de Altos Estudos Militares da Escola de Guerra Naval no ano de 2013: a concepção político-estratégica e a atuação internacional da Marinha do Brasil. *Revista da Escola de Guerra Naval*, v. 18, n. 2, p. 2012.

Recebido em: 07/03/2016

Aceito em: 09/12/2016



# INSTRUÇÕES EDITORIAIS PARA OS AUTORES

A Revista da Escola de Guerra Naval é uma publicação semestral, editada pelo Centro de Estudos Político-Estratégicos (CEPE), de natureza acadêmica, sem fins lucrativos.

A política editorial da Revista da Escola de Guerra Naval estabelece que os trabalhos devem apresentar uma reflexão inovadora e contribuir para o desenvolvimento de um pensamento estratégico autóctone em matéria de Defesa, particularmente, no que se refere ao poder marítimo.

**Os artigos publicados pela Revista são de exclusiva responsabilidade de seus autores, não expressando, necessariamente, o pensamento da Escola de Guerra Naval nem o da Marinha do Brasil.**

## SUBMISSÕES DE ARTIGOS

Os artigos (em português, inglês, francês ou espanhol) de cerca de 5.000 a 10.000 palavras devem ser submetidos por intermédio do *site* da Revista: [http:// revista.egn.mar.mil.br](http://revista.egn.mar.mil.br), conforme as instruções. Destaco que o arquivo contendo o artigo, no formato *word*, não deverá conter qualquer identificação ou referência sobre o autor.

Por norma de segurança, outro arquivo do artigo identificado contendo a qualificação e vinculação do autor deverá também ser obrigatoriamente enviado para o e-mail: [revista@egn.mar.mil.br](mailto:revista@egn.mar.mil.br)

## IDIOMA DE PUBLICAÇÃO

Os textos poderão ser apresentados em português, inglês, francês ou espanhol.

## DECLARAÇÃO DE DIREITO AUTORAL

Ao enviar o artigo para a Revista da Escola de Guerra Naval, os autores **declaram o ineditismo da obra** e o envio exclusivo a esta revista. Concordam que os direitos autorais dos artigos ficam reservados à revista da Escola de Guerra Naval, condicionando-se a sua reprodução parcial ou integral, e as citações eventuais às obrigatoriedades da citação da autoria e da revista da Escola de Guerra Naval. Declaram também que a obra não infringe direitos autorais e/ou outros direitos de propriedade de terceiros, que a divulgação de imagens (caso existam) foi autorizada e que assumem

integral responsabilidade moral e/ou patrimonial pelo seu conteúdo, perante terceiros.

### COMPOSIÇÃO E ENCAMINHAMENTO DOS TRABALHOS

A Revista somente aceitará trabalhos **inéditos**, não sendo permitida a sua apresentação simultânea em outro periódico, relacionados a assuntos de Defesa em Geral, nas áreas de Ciência Política, Geopolítica, Estratégia, Relações Internacionais, Direito Internacional, Gestão e outras correlacionadas.

Após o recebimento do artigo, será enviado um e-mail acusando o seu recebimento, de modo a dar partida ao processo de seleção.

Para artigos com autoria múltipla, é necessário informar a ordem de apresentação dos autores, obedecendo o constante no item declaração de responsabilidade, e declaração de cada um autorizando a publicação.

Os artigos que cumprirem as normas acima passarão por um processo de avaliação por pares, sem que os revisores tenham acesso ao nome do autor (*blind peer review*). Ao fim deste processo, o autor será notificado via e-mail de que seu artigo foi aceito ou não, e que aguardará a primeira oportunidade de impressão.

A revista se reserva o direito de efetuar nos originais alterações de ordem normativa, ortográfica e gramatical, com vistas a manter o padrão culto da língua, respeitando, porém, o estilo dos autores.

### INDICAÇÃO DE RESPONSABILIDADE

No que se refere à indicação de responsabilidade pelo artigo, caso não seja a mesma de todos os autores, deve ser indicada logo abaixo do título ordenada segundo o critério abaixo: (1) Concepção e projeto ou análise e interpretação dos dados; (2) Redação do manuscrito ou; (3) Revisão crítica relevante do conteúdo intelectual. Com base nestes critérios, os proponentes deverão indicar, em nota de rodapé na página final do artigo, como ocorreu a participação de cada autor na elaboração do manuscrito.

### FORMA DE APRESENTAÇÃO DA AFILIAÇÃO

A afiliação deve conter: 1- Nome da instituição ao qual está vinculado o pesquisador (Programa/Universidade) - por extenso com abreviatura entre parênteses. 2- Cidade e Estado da Federação (quando houver). 3- País (por extenso e na grafia do idioma original). Exemplo:

Professor do Programa de Pós-Graduação em Relações Internacionais (PPGRI-UERJ), Rio de Janeiro, RJ, Brasil.

### CONFLITO DE INTERESSES

A publicação segue as recomendações do Código de Boas Práticas Científicas da FAPESP de 2014, no que diz respeito aos conflitos de interesses:

“3.4.1. Há conflito potencial de interesses nas situações em que a coexistência entre o interesse que deve ter o pesquisador de fazer avançar a ciência e interesses de outra natureza, ainda que legítimos, possa ser razoavelmente percebida, por ele próprio ou por outrem, como conflituosa e prejudicial à objetividade e imparcialidade de suas decisões científicas, mesmo independentemente de seu conhecimento e vontade.

3.4.2. Nessas situações, o pesquisador deve ponderar, em função da natureza e gravidade do conflito, sua aptidão para tomar essas decisões e, eventualmente, deve abster-se de tomá-las.

3.4.3. Nos casos em que o pesquisador esteja convencido de que um conflito potencial de interesses não prejudicará a objetividade e imparcialidade de suas decisões científicas, a existência do conflito deve ser clara e expressamente declarada a todas as partes interessadas nessas decisões, logo quando tomadas.”

Fonte:<[http://www.fapesp.br/boaspraticas/FAPESP-Codigo\\_de\\_Boas\\_Praticas\\_Cientificas\\_2014.pdf](http://www.fapesp.br/boaspraticas/FAPESP-Codigo_de_Boas_Praticas_Cientificas_2014.pdf)>

### PROCESSOS DE AVALIAÇÃO POR PARES

Os originais submetidos à Revista que atenderem à política editorial, serão encaminhados ao Conselho Editorial, que fará uma pré-análise considerando o mérito científico e o escopo da revista. Aprovados nesta fase serão encaminhados para pelo menos dois pareceristas *ad hoc* de reconhecida competência na temática abordada.

Os pareceristas, após receberem o artigo, emitem um parecer com os respectivos comentários e avaliação final. Este parecer retorna aos editores, que encaminham o resultado ao candidato, indicando, quando necessário, as alterações sugeridas e o prazo de reenvio do artigo.

A decisão final sobre a publicação ou não do original é sempre do Conselho Editorial, ao qual é reservado o direito de efetuar os ajustes que



julgar necessários.

### **FORMATO DE APRESENTAÇÃO**

A Revista da Escola de Guerra Naval adota as regras da Associação Brasileira de Normas Técnicas (ABNT), <http://www.abnt.org.br/>:

Artigo: NBR 6022 – Artigo em publicação periódica científica e impressa.

**Título e Resumo: em Português e Inglês (máximo de 200 palavras). Incluir, no mínimo, três palavras-chave por idioma.**

**Identificação do autor: Nome completo dos autores na ordem em que deverá aparecer no texto, titulação, instituição, endereço postal e eletrônico.**

**Referências: NBR 6023/2002 – Referências – Elaboração.**

**Numeração de seções: não deverá haver numeração de seções.**

**Referências: as referências podem vir ao longo do texto no formato completas por meio de notas de rodapé ou abreviadas pelo sistema autor-data. Ao fim do texto devem constar todas as referências utilizadas pelo autor em ordem alfabética e não numeradas.**

**Tipologia: Times New Roman 12, espaço 1,5 e margens de 2,5 cm.**

**Figuras e gráficos: o uso de tabelas e figuras deverá se restringir ao mínimo necessário, podendo vir ao longo do texto. Solicita-se que as tabelas e figuras sejam enviadas em separado para efeitos de diagramação. Estas deverão estar digitalizadas em 300dpi e no formato JPG.**

Toda correspondência referente à Revista deve ser encaminhada à:  
Escola de Guerra Naval – Centro de Estudos Político-Estratégicos.  
Avenida Pasteur, 480 – Praia Vermelha – Urca.

Rio de Janeiro – RJ

CEP: 22.290-240

e-mail: [revista@egn.mar.mil.br](mailto:revista@egn.mar.mil.br)

Aos cuidados do Editor da Revista da Escola de Guerra Naval

A Revista da Escola de Guerra Naval é um periódico semestral, editado pelo Centro de Estudos Político-Estratégicos (CEPE) e vinculado ao Programa de Pós-Graduação em Estudos Marítimos (PPGEM), que tem o propósito de disseminar e promover intercâmbio, em níveis nacional e internacional, de conhecimentos relativos à Defesa, com ênfase na área de Ciência Política e Relações Internacionais. Publica, prioritariamente, trabalhos originais e inéditos, que contribuem para o estudo do aperfeiçoamento e a evolução do pensamento político-estratégico naval brasileiro, proporcionando maior integração entre a Marinha do Brasil e a comunidade acadêmica nacional e internacional.



Protegendo nossas riquezas,  
cuidando da nossa gente.



PODE SER ABERTO PELA ECT

ESCOLA DE GUERRA NAVAL (EGN)  
REVISTA DA ESCOLA DE GUERRA NAVAL

Av. Pasteur, 480 - Praia Vermelha - Urca - 22290-240 - Rio de Janeiro - RJ