

ESCOLA DE GUERRA NAVAL

CMG (EN) ROGÉRIO CORRÊA MANSO

SISTEMAS CIBERNÉTICOS NA MB: DESAFIOS E PERSPECTIVAS

Sistemas Cibernéticos de Comando e Controle da MB: Estruturação para as Demandas do
Século XXI

Rio de Janeiro

2013

CMG (EN) ROGÉRIO CORRÊA MANSO

SISTEMAS CIBERNÉTICOS NA MB: DESAFIOS E PERSPECTIVAS

Sistemas Cibernéticos de Comando e Controle da MB: Estruturação para as Demandas do
Século XXI

Monografia apresentada à Escola de Guerra
Naval, como requisito parcial para conclusão
do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Luiz Carlos de
Carvalho Roth

Rio de Janeiro
Escola de Guerra Naval
2013

AGRADECIMENTOS

À minha esposa Teresa Cristina e filhos, Tainá e Bernardo, pelo grande carinho, apoio e compreensão de minhas ausências familiares para dedicação a este trabalho e ao Curso de Política e Estratégia Marítimas.

Ao Capitão-de-Mar-e-Guerra (RM1) Luiz Carlos de Carvalho Roth, meu orientador, pelo apoio acadêmico, incentivo, vibração e profissionalismo com que me orientou.

Aos Capitão-de-Mar-e-Guerra (RM1) Roberto Barbosa David, Capitão-de-Fragata (T) Maurício Pires Malburg da Silveira, Capitão-de-Corveta (T) Marcus Rogers Cavalcante Andrade, Capitão-de-Corveta Rodrigo Abrunhosa Collazo, e Analista de Sistemas Ana Lúcia Mesiano Porthun, pela cordialidade, interesse e profissionalismo que me concederam as entrevistas fundamentais para o fechamento deste trabalho.

À Escola de Guerra Naval pela excelente infraestrutura, tratamento oferecido aos alunos e oportunidade de realizar trabalhos desta natureza em seu Curso de Política e Estratégia Marítimas de 2013.

RESUMO

O trabalho é uma análise de situação que provê sugestões para reestruturação dos sistemas de Comando e Controle (C2) da Marinha de forma a adaptar a Força ao cenário cibernético de combate do século XXI vislumbrado por documentos estratégicos brasileiros. Neste ponto, o Plano Estratégico da Marinha e a Política Cibernética de Defesa são analisados para obter as características funcionais demandadas dos sistemas de C2. Considerando a importância da interoperabilidade entre sistemas apresentada no resultado do trabalho, os principais conceitos teóricos do assunto são enunciados. Modelos de maturidade de interoperabilidade são abordados onde se destaca um modelo namibiano que, pela abrangência e praticidade de aplicação, é considerado como de grande utilidade. Características funcionais são transformadas em características técnicas com emprego de conceitos de arquitetura baseada em componente (CBA), arquitetura orientada a serviço (SOA) e modelos de referência técnica para estruturação de sistemas de C2. Sobre as características técnicas são elaboradas 27 sugestões abrangendo regulações, infraestruturas de comunicação, de computação, de serviços corporativos centrais (CES), sistemas legados e novos sistemas. Dentre as sugestões são apresentadas recomendações específicas para o Sistema de Gerenciamento da Amazônia Azul (SisGAAz), Sistema Naval de Comando e Controle (SISNC2) e Sistema de Informações sobre o Tráfego Marítimo (SISTRAM).

Palavras-chave: Sistema de comando e controle (C2); Cibernético; Interoperabilidade; Arquitetura baseada em componente (CBA); Arquitetura orientada a serviço (SOA); Serviços corporativos centrais (CES); Sistema legado; SisGAAz; SISNC2; SISTRAM.

ABSTRACT

The paper is a situation analysis that provides suggestions for restructuring Brazilian Navy' Command and Control (C2) systems in order to adapt the Force to the combat cyber scenario of 21st century, envisioned by Brazilian defense strategic documents. At this point, the Navy Strategic Plan and Defense Cyber Policy are analyzed to obtain the functional requirements demanded from C2 systems. Considering the importance of system interoperability presented among results, the main theoretical concepts of the subject are depicted. Interoperability maturity models are discussed, where a Namibian model is highlighted as very useful due to its wide scope and practical application. Functional requirements are transformed into technical requirements applying concepts of Component-Based Architecture (CBA), Service-Oriented Architecture (SOA) and technical reference models for structuring C2 systems. Based on technical requirements, 27 suggestions are issued covering regulations, communication, computing, and Core Enterprise Services (CES) infrastructures, legacy systems and new systems. Among the suggestions there are specific recommendations for the following Brazilian systems: "Sistema de Gerenciamento da Amazônia Azul" (SisGAAz), "Sistema Naval de Comando e Controle" (SISNC2) and "Sistema de Informações sobre o Tráfego Marítimo" (SISTRAM).

Keywords: Command and control (C2) system; Cyber; Interoperability; Component-based architecture (CBA); Service-oriented architecture (SOA); Core enterprise services (CES); Legacy system; SisGAAz; SISNC2; SISTRAM.

LISTA DE ILUSTRAÇÕES

Figura 1 - Sistema de C2 operando em nível <i>ISOLADO</i>	25
Figura 2 - Sistema de C2 operando em nível <i>CONECTADO</i>	27
Figura 3 - Sistema de C2 operando em nível <i>FUNCIONAL</i>	28
Figura 4 - Sistema de C2 operando em nível <i>DOMÍNIO</i>	30
Figura 5 - Sistema de C2 operando em nível <i>CORPORATIVO</i>	32
Figura 6 - Cronograma de incremento de interoperabilidade entre sistemas	37
Figura 7 - Processo de publicar e achar serviços em arquitetura SOA.....	41
Figura 8 - Transição da GIG do DoD de 2007 para uma arquitetura de GIG vislumbrada.....	45
Figura 9 - Compartilhamento de informações dentro da GIG idealizada.....	46
Figura 10 - Visão sistêmica da GIG idealizada	47
Figura 11 - Três visões de um sistema de C2 e seus relacionamentos	49
Figura 12 - Modelo de Referência Técnica para arquitetura corporativa do DoD.....	53
Figura 13 - Hierarquia de Área, Categoria, Padrão, e Especificação de Serviços.....	54
Figura 14 - TRM aplicado à conexão em rede do sistema de uma corporação a um ambiente externo.....	56

LISTA DE TABELAS

1 - Objetivos do PEM que Impactam em Características Funcionais Cibernéticas dos Sistemas de C2.....	17
2 - Diretrizes da PCD que Impactam em Características Funcionais Cibernéticas dos Sistemas de C2.....	19
3 - Novas Funcionalidades dos Sistemas de C2 Demandadas do PEM e PCD.....	20
4 - Atributos da GIG Idealizada pelo DoD.....	45
5 - Relação entre Características Funcionais dos Sistemas de C2 Demandadas do PEM e PCD e Principais Camadas Atuantes da Infraestrutura de Grade.....	59
6 - Relação entre Características Funcionais dos Sistemas de C2 Demandadas do PEM e PCD e Respectivas Características Técnicas.....	60
7 - Relação entre Características Técnicas dos Sistemas de C2 Demandadas do PEM e PCD e Respectivas Áreas, Categorias, e Padrões de Serviços do TRM	61

LISTA DE ABREVIATURAS E SIGLAS

AIS	Automatic Identification System
BA	Battlespace Awareness
C2	Comando e Controle
CAF	C4ISR Architecture Framework
CASNAV	Centro de Análise de Sistemas Navais
CBA	Component-Based Architecture
CCTOM	Centro de Comando do Teatro de Operações Marítimas
CES	Core Enterprise Services
CIO	Chief Information Officer
DISR	DoD Information Technology Standards Registry
DoD	Department of Defense of USA
DoDAF	DoD Architecture Framework
DoS	Denial of Service
DPC	Diretoria de Portos e Costas
DMZ	Demilitarized Zone (Zona Desmilitarizada)
EA	Enterprise Architecture
EB	Exército Brasileiro
EMiD	Estratégia Militar de Defesa
END	Estratégia Nacional de Defesa
FAB	Força Aérea Brasileira
FEA-RM	Federal Enterprise Architecture Reference Models
FTP	File Transfer Protocol
GIG	Grade de Informação Global
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IA	Information Assurance
IETF	Internet Engineering Task Force
IHM	Interface Homem-Máquina
INTERC2	Interoperabilidade de Sistemas de C2

IP	Internet Protocol
JTA	Joint Technical Architecture
LAN	Local Area Network
LRIT	Long Range Identification and Tracking
MB	Marinha do Brasil
MD	Ministério da Defesa
MSSIS	Maritime Safety and Security Information System
NCO	Net Centric Operation
NetOps	Network Operations
OBNAV	Objetivos Navais
OMB	Office of Management and Budget
OTHR	Over The Horizon Radar
P2P	Peer-to-Peer
PCD	Política Cibernética de Defesa
PDN	Política de Defesa Nacional
PEM	Plano Estratégico da Marinha
PMiD	Política Militar de Defesa
PND	Política Nacional de Defesa
PREPS	Programa Nacional de Rastreamento de Embarcações Pesqueiras
RECIM	Rede de Comunicações Integradas da Marinha
SAETE	Sistema de Análise de Exercícios Táticos da Esquadra
SAGBD	Sistema de Apresentação Gráfico e Banco de Dados
SGBD	Sistema Gerenciador de Banco de Dados
SID	Segurança das Informações Digitais
SIMMAP	Sistema de Monitoramento Marítimo de Apoio a Atividades de Petróleo
SIPLOM	Sistema de Planejamento Operacional Militar
SISDABRA	Sistema de Defesa Aeroespacial Brasileiro
SISFRON	Sistema Integrado de Monitoramento de Fronteiras
SisGAAz	Sistema de Gerenciamento da Amazônia Azul

SISMC2	Sistema Militar de Comando e Controle
SISNC2	Sistema Naval de Comando e Controle
SISTRAM	Sistema de Informações sobre o Tráfego Marítimo
SMTP	Simple Mail Transfer Protocol
WAN	Wide Area Network
WEB	Abreviação curta de "World Wide Web" (WWW) que significa a grande rede mundial

SUMÁRIO

1. INTRODUÇÃO	12
2. NOVAS FUNCIONALIDADES DEMANDADAS DOS SISTEMAS DE C2	15
2.1 FUNCIONALIDADES DEMANDADAS DO PEM	16
2.2 FUNCIONALIDADES DEMANDADAS DA PCD	18
2.3 NOVAS FUNCIONALIDADES DOS SISTEMAS DE C2	20
3. CONCEITOS DE INTEROPERABILIDADE EM SISTEMAS DE C2	23
3.1 INTEROPERABILIDADE	24
3.1.1 Níveis de Interoperabilidade.....	24
3.1.2 Medida do Nível de Interoperabilidade	34
3.1.3 Cronograma de Evolução de Interoperabilidade	37
3.2 PRINCIPAIS ARQUITETURAS DE INTEGRAÇÃO E INTEROPERABILIDADE	38
3.2.1 Arquitetura Baseada em Componente	38
3.2.2 Arquitetura Orientada a Serviço	40
3.3 GRADE DE INFORMAÇÃO GLOBAL.....	43
3.4 ESTRUTURA DE SISTEMAS DE C2.....	49
3.5 VISÃO TÉCNICA DOS SISTEMAS DE C2	51
4. CARACTERÍSTICAS TÉCNICAS E PADRÕES DE SERVIÇOS DEMANDADOS PELO PEM E PCD	58
4.1 DEMANDAS SISTÊMICAS	58
4.2 DEMANDAS TÉCNICAS	60
5. SUGESTÕES PARA ESTRUTURAÇÃO DOS SISTEMAS DE C2 NA MB	64
5.1 SUGESTÕES SOBRE REGULAÇÕES	64
5.2 SUGESTÕES SOBRE INFRAESTRUTURAS	65
5.3 SUGESTÕES SOBRE NOVOS SISTEMAS	67
5.3.1 SisGAAz.....	68
5.4 SISTEMAS LEGADOS	69
5.4.1 SISTRAM.....	70

5.4.2 SISNC2.....	72
6. CONCLUSÃO.....	75
REFERÊNCIAS BIBLIOGRÁFICAS.....	77
APÊNDICE A: QUADRO RESUMO DE SUGESTÕES PARA ESTRUTURAÇÃO DE SISTEMAS DE C2 NA MB	79

1. INTRODUÇÃO

O desenvolvimento dos principais sistemas de Comando e Controle (C2) na Marinha têm suas origens em 1987 e efetiva implementação nos finais dos anos 90 e início dos anos 2000, quando ao Centro de Análise de Sistemas Navais (CASNAV) foi atribuído o desenvolvimento do Sistema Militar de Comando e Controle (SISMC2) (VIVEIROS, 2007). Nesses 15 anos os sistemas de C2 ganharam mais funcionalidades, tornando-se essenciais para o acompanhamento da “consciência situacional”¹ marítima. Passaram, assim, a ser considerados ferramentas fundamentais para apoio aos processos de tomada de decisão.

A partir de 2005 muitos documentos foram criados ou revistos no nível político-estratégico. Como exemplos estão a Política Nacional de Defesa, a Estratégia Nacional de Defesa, a Política Militar de Defesa e a Estratégia Militar de Defesa. Tais documentos moldaram o atual Plano Estratégico da Marinha (PEM) (BRASIL, 2008), com a definição de 21 objetivos navais, onde alguns deverão impor mudanças na estruturação dos sistemas de C2 da Força. Como exemplo deste indício, haverá a necessidade de uma maior interação das atividades da Marinha com outros atores, militares e civis, exigindo funcionalidades de comunicação que podem inexistir nos sistemas da atualidade.

Outra alteração recente foi a criação, em 2012, da Política Cibernética de Defesa (PCD) (BRASIL, 2012), que também trouxe novos objetivos e 52 diretrizes a serem seguidas pelas três Forças Armadas. Tais diretrizes também devem ser levadas em consideração na estruturação dos atuais e futuros sistemas de C2 a serem empregados pela MB, pois essas diretrizes também deverão alterar significativamente a estruturação desses sistemas.

¹ O termo "consciência situacional" é definido de forma simples como: “aquilo que se necessita saber para não ser surpreendido”. JEANNOT, E., Kelly, C. e Thompson, D. The Development of Situation Awareness Measures in ATM Systems. Bruxelas, Bélgica: Eurocontrol, 2003.

Em termos de tecnologia da informação (TI), a partir de 1996, com a criação do "Information Technology Management Reform Act" pelo congresso estadunidense, muitos estudos, teorias, documentos e tecnologias foram desenvolvidos para permitir maior integração e interoperabilidade dos sistemas pelo mundo, aproveitando o expressivo crescimento das velocidades de redes locais e da própria internet. Este processo se acelerou após o atentado de 11 de setembro de 2001, quando a necessidade de operação em conjunto das agências de inteligência norte-americanas e de suas forças de segurança se fez mais premente. A necessidade da integração de sistemas de C2 e Inteligência, não somente de forças nacionais, mas também de forças aliadas, se tornou vital. Surge, então, o conceito de operações centradas em rede, que também contribui para mudar o escopo de abrangência dos sistemas de C2.

Este trabalho se propõe a comprovar a necessidade de reestruturação dos sistemas de C2 da MB e sugerir formas de empreendê-la para atender aos objetivos navais do PEM e às diretrizes da PCD. As sugestões estarão também aliadas às recentes evoluções nos conceitos de integração de informações de comando e controle, sendo fundamental para inserção eficaz da MB no cenário cibernético de combate do século XXI.

O trabalho trará à luz algumas necessidades de adaptação de "sistemas legados"² e especificações de novos sistemas de C2, permitindo melhorar manutenções e projetos evolutivos destes sistemas. O desenvolvimento não será abordado como estudo de caso, contudo, ao final, serão analisadas as situações e sugeridas recomendações para o Sistema de Gerenciamento da Amazônia Azul (SisGAAz), Sistema Naval de Comando e Controle (SISNC2) e Sistema de Informações sobre o Tráfego Marítimo (SISTRAM) pela importância de tais sistemas para a MB.

² Sistemas legados são sistemas que empregam hardware e/ou software de uma geração tecnológica anterior à empregada nos dias atuais (EUA, 2005). Geralmente fornecem serviços essenciais, só podendo ser desativados quando da implantação de outros sistemas modernos que prestarão os serviços que ora prestam.

O capítulo 1 é composto desta introdução para situar o leitor no contexto do assunto abordado.

No capítulo 2 é apresentada uma análise do PEM e da PCD, concluindo com uma síntese das novas características funcionais demandadas dos sistemas de C2 por estes dois documentos.

O capítulo 3 apresenta um referencial teórico com os principais conceitos de interoperabilidade e estruturação entre sistemas de C2. São discutidos diversos modelos a serem empregados no estudo de sistemas, que serão importantes para as sugestões de estruturação, ao final do trabalho.

No capítulo 4 as características funcionais obtidas no capítulo 2 serão transformadas em características técnicas, por meio da aplicação de alguns conceitos apresentados no capítulo 3. O capítulo 4 também apresentará os serviços de TI que merecem maior atenção para se adequar às novas demandas do PEM e PCD.

O capítulo 5 sugerirá várias ações para estruturação dos sistemas de C2 em atendimento ao PEM e PCD, sendo essas aplicadas sobre 4 aspectos: regulações, infraestruturas, novos sistemas, e sistemas legados.

Finalmente, no capítulo 6 será apresentada a conclusão do trabalho, com uma síntese dos pontos mais importantes abordados e os principais resultados obtidos.

2. NOVAS FUNCIONALIDADES DEMANDADAS DOS SISTEMAS DE C2

Neste trabalho, o termo "sistema de C2" refere-se a toda família de sistemas de Comando e Controle, isto é, os sistemas de C2I (C2 mais Inteligência), C2ISR (C2I mais Vigilância e Reconhecimento), C3 (C2 mais Comunicações), C3I (C3 mais Inteligência), C4 (C3 mais Computação), C4I (C4 mais Inteligência), C4ISR (C4I mais Vigilância e Reconhecimento), e C5I (C4I mais Sistemas de Combate). Todos serão chamados genericamente de sistemas de C2.

Como exposto na introdução, os sistemas de C2 da Marinha suas origens em 1987 e efetiva implementação nos finais dos anos 90 e início dos anos 2000. Ganham mais funcionalidades com o passar do tempo, passando a ser considerados fundamentais para apoio aos processos de tomada de decisão e integração de forças.

A partir de 2005 muitos documentos foram criados ou revistos no nível político-estratégico, visando adequar a sociedade brasileira às novas demandas de defesa do século XXI, pós-Guerra Fria e pós-ataques de 11 de setembro de 2001. Como exemplos destes documentos estão a Política Nacional de Defesa (PND), a Estratégia Nacional de Defesa (END), a Política Militar de Defesa (PMiD) e a Estratégia Militar de Defesa (EMiD).

Além das demandas militares terem se alterado, a tecnologia da informação disponível atualmente é muito superior à da época em que os sistemas de C2 da MB foram idealizados. Desta forma, é de se esperar que tais sistemas devam ser, e estão sendo, constantemente adaptados para incorporar as novas tecnologias no atendimento às novas funcionalidades demandadas. Neste aspecto é necessário se ter uma ideia clara de demandas.

Para sintetizar as novas funcionalidades advindas dos documentos recentemente expedidos, dois deles devem ser estudados com detalhes: o Plano Estratégico da Marinha (PEM) e a Política Cibernética de Defesa (PCD). O primeiro, por ser consequência direta de

documentos de maior escalão estratégico (como a Política de Defesa Nacional (PDN), a PMiD e a EMiD); o segundo, por fixar uma política cibernética que todos os órgãos da Defesa devem adotar.

Este capítulo está dividido em três seções. As duas primeiras abordarão separadamente as funcionalidades demandadas pelo PEM e pela PCD, respectivamente. A última seção fará uma síntese das demandas conjuntas, eliminando eventuais redundâncias.

2.1 FUNCIONALIDADES DEMANDADAS DO PEM

O PEM (BRASIL, 2008) é um documento estratégico da Marinha, que provem diretamente de documentos condicionantes de mais alto nível, como PDN, PMiD e EMiD. Assim, concentra as diretrizes emanadas dos documentos superiores, além de oferecer melhor detalhamento para espelhar as particularidades da Força e orientar as ações que aumentarão a eficácia no cumprimento da missão da Marinha do Brasil (MB). Ele define 21 objetivos navais (OBNAV), onde alguns impõem novas funcionalidades aos sistemas de C2 da Força. Em que pese a revisão deste plano ser aplicada a cada dois anos, tendo em vista a grande dimensão e o nível de comprometimento com as PND, END, PMiD e EMiD, os OBNAV tendem a ter certa estabilidade no tempo.

Uma forma de identificar as novas funcionalidades demandadas pelo PEM aos sistemas de C2 é observar cada OBNAV, verificando se este possui, ou não, impacto direto em recursos de C2. Uma vez identificado os OBNAV impactantes, faz-se as correspondentes descrições das funcionalidades demandadas, sintetizando o resultado final em uma tabela.

Este trabalho adotou a abordagem acima transcrita, em que a tabela 1 transcreve o resultado final.

TABELA 1
Objetivos do PEM que Impactam em Características Funcionais Cibernéticas dos Sistemas de C2

Objetivo do PEM	Referência no PEM, item 6.2, OBNAV	Característica Funcional Cibernética nos Sistemas de C2
Ampliação da presença da Marinha na Região Amazônica e nas áreas estratégicas do Atlântico Sul.	5	Possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira.
Incremento e aperfeiçoamento da integração operacional, da logística, do apoio mútuo e da mobilização militar, entre as FA, visando à interoperabilidade de seus principais sistemas.	7	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados pelas outras Forças Armadas, visando ao incremento e aperfeiçoamento da integração operacional.
Aperfeiçoamento da estrutura de comando e controle, da organização administrativa e da capacidade de inteligência, sobretudo nos campos estratégico e operacional.	9	Ser facilmente aperfeiçoável, de forma a permitir rápido acompanhamento das novas concepções de comando e controle.
Incremento da cooperação e da realização de operações conjuntas com as Marinhas da América do Sul, da África Atlântica e com as dos países desenvolvidos.	10	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Marinhas estrangeiras.
Contribuição para o aperfeiçoamento do gerenciamento de crises internacionais de natureza político-estratégica.	11	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências estrangeiras de forma a permitir operações combinadas no exterior para apoio no gerenciamento de crises internacionais de natureza político-estratégica.
Contribuição para a prevenção de atos terroristas e para condução de atividades de contraterrorismo, nas áreas de interesse do Poder Marítimo e na região SAR de responsabilidade do Brasil.	12	Possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira que atuem na prevenção de atos terroristas e na condução de atividades de contraterrorismo.
Participação de Força Naval, quando sob a égide de organismos internacionais e quando do interesse nacional, de forças internacionais em arranjos militares de defesa coletiva, de forças expedicionárias, de manutenção da paz e humanitárias.	13	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências estrangeiras, de forma a facilitar a participação da Marinha em forças internacionais.
Ampliação e diversificação do	15	Ser facilmente aperfeiçoável, de forma a

intercâmbio científico e tecnológico de interesse naval, no País e no exterior, com institutos de pesquisas, universidades e indústrias.		permitir acompanhamento eficaz da evolução da tecnologia da informação de interesse naval oriunda na MB ou em institutos de pesquisas, universidades e indústrias.
Manutenção da segurança contra ataques cibernéticos dos sistemas digitais de tecnologia da informação e de comunicações.	17	Possuir reconhecida segurança cibernética, obedecendo as normas da MB neste sentido.
Incremento no adestramento de operações combinadas e aprimoramento de doutrinas e dos planejamentos navais pertinentes.	21	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas visando facilitar o desenvolvimento de operações conjuntas.

Fonte: autor

É de se observar que diferentes OBNAV levaram a características funcionais muito semelhantes, o que enfatiza a importância dessas características serem atendidas pelo sistema de C2.

2.2 FUNCIONALIDADES DEMANDADAS DA PCD

Outra alteração recente no acervo de documentos técnicos de alto nível que envolvem recursos de TI foi a expedição da Política Cibernética de Defesa (PCD) (BRASIL, 2012) em 21 de dezembro de 2012. Documento recente, elaborado pelo Ministério da Defesa (MD) a partir de um Grupo de Trabalho Interforças, o expediente tem por finalidade orientar, no âmbito do MD, as atividades de Defesa Cibernética, no nível estratégico, e de Guerra Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos (BRASIL, 2012). A PCD traz explicitamente 9 objetivos e 52 diretrizes cibernéticas decorrentes a serem seguidas pelas três Forças Armadas. Tais diretrizes, quando impactantes em Comando e Controle, também têm que ser levadas em consideração na estruturação dos atuais e futuros sistemas de C2 a serem empregados pela MB. Faz-se importante identificá-

las, assim como as respectivas funcionalidades demandadas. A mesma forma de identificação empregada no PEM pode ser aplicada na PCD. A tabela 2 expressa o resultado final.

TABELA 2
Diretrizes da PCD que Impactam em Características Funcionais Cibernéticas dos Sistemas de C2

Diretriz da PCD	Referência na PCD	Característica Funcional nos Sistemas de C2
Criar e normatizar processos de Segurança Cibernética para padronizar procedimentos de acreditação no âmbito das infraestruturas críticas de informação de interesse da Defesa Nacional.	3.2.1.e	Possuir reconhecida segurança cibernética tanto pela MB como pelo MD, principalmente nas infraestruturas críticas de informação.
Estabelecer programas/projetos a fim de assegurar a capacidade de atuar em rede com segurança, fortalecendo, dessa forma, a operacionalidade da atividade de Comando e Controle (C2) no MD.	3.2.1.f	Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados pelas Forças Armadas de forma a fortalecer a operacionalidade da atividade de C2 no MD.
Determinar padrões interoperáveis de criptografia de Defesa em complemento aos das FA.	3.2.5.c	Permitir eficaz troca de dados com outros órgãos do MD por meio de criptografia a ser estabelecida por aquele ministério.

Fonte: autor

Observando a tabela 2, é de se constatar que das 52 diretrizes, somente 3 impactam diretamente nos sistemas de C2. São as que dizem respeito aos objetivos de uso efetivo do espaço cibernético e da gestão de Segurança das Informações Digitais (SID). As demais diretrizes estão ligadas a objetivos que são importantes para a obtenção e operação de sistemas de C2, mas não inserem novas funcionalidades diretas a eles, como aquelas ligadas a mobilização, capacitação de pessoal, inteligência, pesquisa e desenvolvimento, doutrina, e legislação.

2.3 NOVAS FUNCIONALIDADES DOS SISTEMAS DE C2

Uma vez identificadas as novas funcionalidades demandadas do PEM e da PCD, expressas nas tabelas 1 e 2, pode-se sintetizá-las em uma tabela que elimine as redundâncias e realce a união das características funcionais identificadas. A tabela 3 reporta esta situação, relacionando também as correspondentes orientações estratégicas, seja do PEM ou da PCD, que geraram as funcionalidades.

TABELA 3
Novas Funcionalidades dos Sistemas de C2 Demandadas do PEM e PCD

Característica Funcional nos Sistemas de C2	Diretriz da PCD ou Objetivo do PEM	Referência no PEM ou PCD
Possuir reconhecida segurança cibernética tanto pela MB como pelo MD.	Criar e normatizar processos de Segurança Cibernética para padronizar procedimentos de acreditação no âmbito das infraestruturas críticas de informação de interesse da Defesa Nacional.	PCD -3.2.1.e
	Manutenção da segurança contra ataques cibernéticos dos sistemas digitais de tecnologia da informação e de comunicações.	OBNAV-17
Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências, nacionais e estrangeiras.	Estabelecer programas/projetos a fim de assegurar a capacidade de atuar em rede com segurança, fortalecendo, dessa forma, a operacionalidade da atividade de Comando e Controle (C2) no MD.	PCD -3.2.1.f
	Incremento e aperfeiçoamento da integração operacional, da logística, do apoio mútuo e da mobilização militar, entre as FA, visando a interoperabilidade de seus principais sistemas.	OBNAV-7
	Incremento da cooperação e da realização de operações conjuntas com as Marinhas da América do Sul, da África Atlântica e com as dos países desenvolvidos.	OBNAV-10
	Contribuição para o aperfeiçoamento do gerenciamento de crises internacionais de natureza político-estratégica.	OBNAV-11
	Participação de Força Naval, quando sob a égide de organismos internacionais e quando do interesse nacional, de forças internacionais em arranjos militares de defesa coletiva, de forças expedicionárias, de manutenção da paz e humanitárias.	OBNAV-13
	Incremento no adestramento de operações combinadas e aprimoramento de doutrinas e dos planejamentos navais pertinentes.	OBNAV-21

Permitir eficaz troca de dados com outros órgãos do MD por meio de criptografia a ser estabelecida por aquele ministério.	Determinar padrões interoperáveis de criptografia de Defesa em complemento aos das FA.	PCD -3.2.5.c
Possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira.	Ampliação da presença da Marinha na Região Amazônica e nas áreas estratégicas do Atlântico Sul.	OBNAV-5
	Contribuição para a prevenção de atos terroristas e para condução de atividades de contraterrorismo, nas áreas de interesse do Poder Marítimo e na região SAR de responsabilidade do Brasil.	OBNAV-12
Ser facilmente aperfeiçoável, de forma a permitir acompanhamento eficaz da evolução da tecnologia da informação e das novas concepções de comando e controle.	Aperfeiçoamento da estrutura de comando e controle, da organização administrativa e da capacidade de inteligência, sobretudo nos campos estratégico e operacional.	OBNAV-9
	Ampliação e diversificação do intercâmbio científico e tecnológico de interesse naval, no País e no exterior, com institutos de pesquisas, universidades e indústrias.	OBNAV-15

Fonte: autor

Observando a tabela, chega-se a uma relação sucinta de cinco características funcionais para sistemas de C2, a saber:

- a) possuir reconhecida segurança cibernética, tanto pela MB como pelo MD;
- b) permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências, nacionais e estrangeiras;
- c) permitir eficaz troca de dados com outros órgãos do MD por meio de criptografia a ser estabelecida por aquele ministério;
- d) possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira; e

- e) ser facilmente aperfeiçoável, de forma a permitir acompanhamento eficaz da evolução da tecnologia da informação e das novas concepções de comando e controle.

3. CONCEITOS DE INTEROPERABILIDADE EM SISTEMAS DE C2

A interoperabilidade de um sistema de C2 com outros sistemas, sejam eles de sensoriamento, de armas, meteorológico, ou outro sistema de C2, é característica fundamental em projetos do século XXI. Assim, este assunto será estudado com maior detalhe neste capítulo de forma a possibilitar sua aplicação na estruturação dos novos sistemas da MB e na determinação dos padrões técnicos a serem observados para atendimento das características funcionais demandadas do PEM e PCD.

O capítulo é dividido em cinco seções. Na primeira seção são apresentados os níveis de interoperabilidade entre sistemas e como eles podem evoluir para tornar sistemas mais interoperáveis. A segunda seção se atém às arquiteturas³ de maior interoperabilidade. A terceira se prende na exposição das principais iniciativas do Departamento de Defesa dos EUA para garantir bons níveis de interoperabilidade em seus sistemas de C2. Na quarta seção será apresentada a forma básica em que um sistema de C2 se estrutura e como ele pode ser abordado por diferentes visões. Mostra-se, ali, a importância da abordagem apresentada para unir com eficiência as necessidades operativas de combatentes e tomadores de decisão com o projeto técnico do sistema. Por fim, a quinta seção apresenta um modelo de abordar tecnicamente um sistema de C2, mapeando suas tecnologias em áreas, categorias, serviços e padrões empregados.

³ Arquitetura é definida como "uma estrutura de componentes, seus relacionamentos, e os princípios e diretrizes que orientam seus projetos e evolução no tempo" - Fonte: padrão (standard) 610.12 do Instituto de Engenharia Elétrica e Eletrônica (IEEE)

3.1 INTEROPERABILIDADE

A interoperabilidade de um sistema é caracterizada pela sua habilidade de acessar, manipular e trocar informação de forma adaptativa e flexível com outro(s) sistema(s) (EUA, 1998). Para estudar esta interoperabilidade, o Departamento de Defesa dos EUA (DoD) expediu uma publicação chamada "*Levels of Information Systems Interoperability*" (LISI) (EUA, 1998). Mesmo considerando as evoluções futuras que a LISI recebeu, o documento de 1998 ficou marcante por dividir a interoperabilidade entre sistemas em níveis distintos. Tais níveis são bem aceitos atualmente e serão descritos sucintamente na seção 3.1.1. Para se determinar o nível de interoperabilidade entre sistemas é necessário estabelecer uma metodologia bem objetiva. Este será o tema da seção 3.1.2. Finalmente, a seção 3.1.3 reportará a evolução no tempo do nível de maturidade interoperacional entre sistemas. Para tanto serão apresentados um exemplo de cronograma, as tarefas que ele subsidia e a fundamental importância do seu emprego para sucesso da evolução.

3.1.1 Níveis de Interoperabilidade

Conforme exposto anteriormente, o DoD expediu em 1998 o LISI (EUA, 1998) para servir como um modelo objetivo de se estudar interoperabilidade entre sistemas. Nesse esforço são definidos nesta publicação cinco níveis básicos para classificação de sistemas que se interoperam: isolado, conectado, funcional, domínio, e corporativo. Tais níveis, conforme estabelecidos no LISI, serão descritos sucintamente nas próximas cinco seções.

3.1.1.1 Nível 0: ISOLADO

A figura 1 representa um sistema C2 acessando dois outros sistemas, que podem ser sensores, armas ou outro sistema C2, operando em nível ISOLADO. O ambiente computacional é considerado *manual*, onde a troca de informações é totalmente dependente da interferência do usuário, como pode ser visto na figura 1 (EUA, 1998).

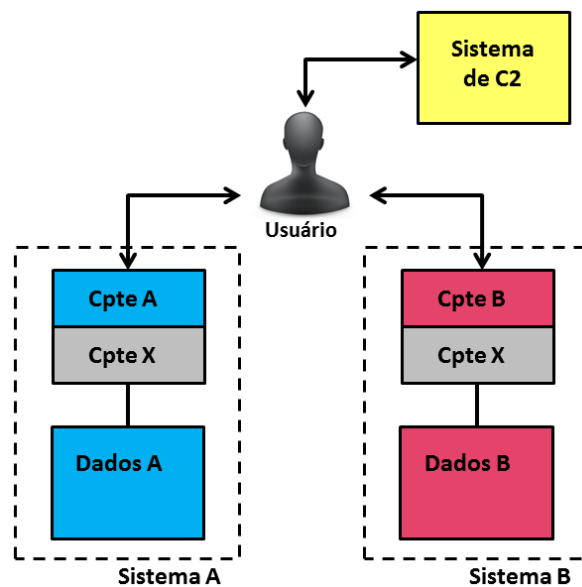


FIGURA 1 - Sistema de C2 operando em nível *ISOLADO*

Fonte: autor

O sistema A possui dois componentes de processamento principal, representados na figura 1 por "Cpte A" e "Cpte X". Este sistema A acessa seu banco de dados próprio, especialmente desenhado para ele, representado na figura por "Dados A". O sistema B possui estrutura semelhante, sendo que um dos componentes de processamento, "Cpte X", é igual ao componente X do sistema A, pois desempenha a mesma função computacional.

Observa-se que os sistemas A e B não trocam informações diretamente com o sistema de C2, necessitando da intermediação do usuário do sistema de C2 para tal. Por exemplo, o usuário pode ler, ou receber por fonia, os dados do sistema A ou B e injetá-los no sistema de C2. Ou então pode usar um "pen drive" para copiar um arquivo de dados do sistema A ou B para o sistema de C2. São exemplos de sistemas isolados:

- a) sistema de C2 que recebe dados externos por injeções manuais, "pen drives", mensageiro, holofote, e outros canais sem conexão eletrônica direta. Caso típico de navios operando com meios de outras Marinhas ou de outras FA, em que os contatos dos sistemas táticos de um meio naval são passados por fonia ao operador do sistema de C2 de outro meio, que os injeta manualmente no mesmo; e
- b) sistemas de inteligência.

Em alguns casos a ausência de interoperabilidade se dá por incompatibilidade dos recursos de segurança existentes entre os sistemas comunicantes. Este caso é muito comum na troca de informação entre agências de inteligência.

As guerras da humanidade travadas até os anos 70 (antes do advento de sistemas computadorizados de C2) utilizavam este nível de interoperabilidade para os sistemas que alimentavam de informação os comandantes responsáveis pelo comando e controle das operações. Eram empregados os canais de comunicação mais eficazes disponíveis em cada época.

3.1.1.2 Nível 1: CONECTADO

A figura 2 representa um sistema de C2 acessando informações de dois outros sistemas operando em nível CONECTADO. O ambiente computacional é considerado *peer-to-peer* (P2P)⁴.

⁴ Ambiente computacional peer-to-peer (P2P) é um ambiente de rede descentralizado e distribuído no qual um terminal individual, chamado "peer", interage com outros "peers", daí o nome "peer-to-peer", agindo como provedor e consumidor de dados e processamentos. O P2P contrasta com modelos cliente-servidor onde terminais clientes dependem de processamento provido por um servidor central.

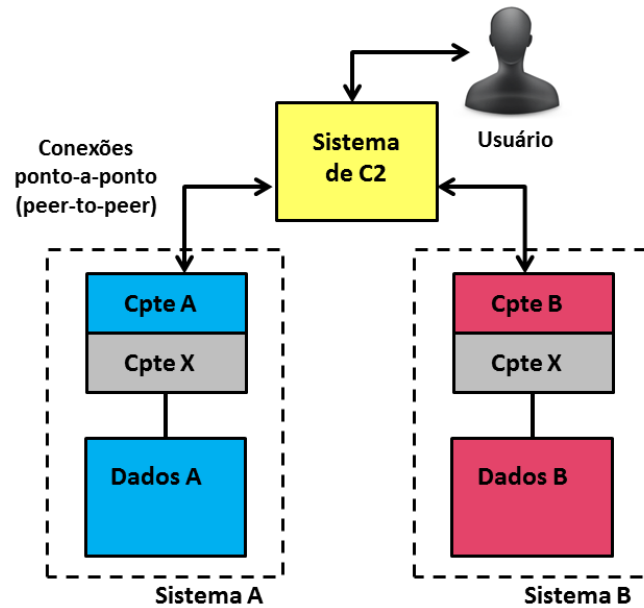


FIGURA 2 - Sistema de C2 operando em nível *CONECTADO*
Fonte: autor

Como pode ser visto na figura 2, os sistemas estão eletronicamente conectados trocando informações por meio de dados e arquivos em formato simples e predefinido, como mensagens de chat, e-mail, mensagens curtas preformatadas e até arquivos de texto ou de figuras trocados por *protocolo de transferência de arquivos - "File Transfer Protocol"* (FTP). Possui pouca capacidade de integrar informações para apoio à decisão (EUA, 1998).

São exemplos de sistemas que apresentam interoperabilidade em nível "conectado":

- a) SISTRAM quando recebe dados de outros sistemas por meio de FTP de um arquivo texto (DAVID, 2013);
- b) Sistema de Análise de Exercícios Táticos da Esquadra (SAETE) que troca informações entre navios por mensagens via rádio; e
- c) link YB e link 11, que trocam contatos táticos em mensagens simples e preformatadas por meio de enlace de rádio.

3.1.1.3 Nível 2: FUNCIONAL

A figura 3 apresenta um sistema de C2 acessando informações de dois outros sistemas operando em nível FUNCIONAL. O ambiente computacional é considerado *distribuído*⁵.

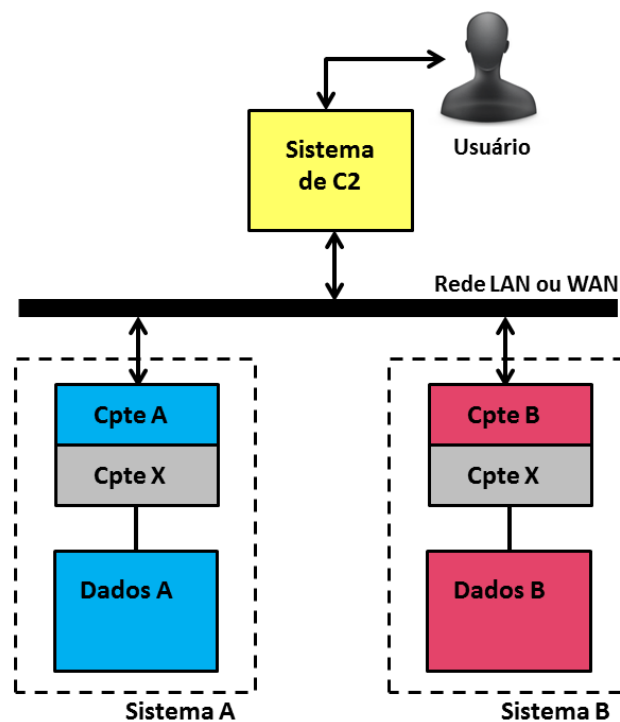


FIGURA 3 - Sistema de C2 operando em nível *FUNCIONAL*
Fonte: autor

Os sistemas se interconectam normalmente por uma rede local, "Local Area Network" (LAN), mas podem se comunicar também para fora da organização, usando redes de longa distância, "Wide Area Network" (WAN)⁶, intranet ou até a internet. Cada sistema possui seu próprio banco de dados, que é formatado de acordo com um modelo físico específico do sistema. O formato do banco de dados de um sistema é, geralmente, diferente do formato do banco do outro. Contudo, a troca de dados entre sistemas se dá na rede por meio

⁵ Ambiente distribuído é um ambiente de rede onde diferentes sistemas estão distribuídos por diferentes servidores ao longo da rede. Este ambiente permite que um aplicativo de um servidor troque ou utilize dados de outros sistemas de forma direta ou distribuída.

⁶ "Wide Area Network" (WAN) é uma rede de computadores que abrange um grande espaço geográfico, superior ao espaço de uma área metropolitana, podendo ser uma rede governamental, privada ou mista. A internet, por exemplo, pode ser considerada uma WAN.

de um modelo lógico comum de dados, isto é, um modelo que é obedecido por todos os sistemas. Antes de enviar os dados para a rede, os sistemas os convertem para este modelo comum de forma a ser compreendido pelo sistema que demandou o dado. Esta configuração permite a troca de informações complexas entre sistemas, em que dados fundidos de diversas fontes podem ser trocados e acessados. Exemplo: imagens com anotações, mapas em várias camadas e documentos com hiperlinks⁷. Aplicativos de um sistema podem, assim, acessar livremente e de forma independente os dados de outros sistemas, sendo que este acesso geralmente se dá em uma *base web*⁸ (EUA, 1998).

Uma forma relativamente simples de implantar a interoperabilidade no nível "funcional" é um sistema disponibilizar seus dados na rede em um formato de arquivo "Extensible Markup Language" (XML), previamente definido, por meio de um serviço web de "Hypertext Transfer Protocol" (HTTP). Os demais sistemas que se integram a este sistema, acessam o serviço HTTP, obtêm o arquivo XML, interpreta-o, processa-o e pode arquivar os dados obtidos deste acesso em seu próprio banco de dados.

São exemplos de sistemas que apresentam interoperabilidade em nível funcional:

- a) um Sistema de Controle Tático e de Armas embarcado que troca dados entre sensores, armamentos e demais periféricos por uma LAN ou por um barramento de serviços; e
- b) o SISTRAM quando recebe dados de outros sistemas acessando serviço web e arquivo XML (DAVID, 2013).

⁷ Hiperlink é o recurso que permite a um documento apontar para outra parte dele mesmo ou para um documento novo. Normalmente é identificado com um sublinhado ou uma cor diferente em seu texto, onde o leitor consegue seguir facilmente para o novo conteúdo clicando no hiperlink.

⁸ Acesso em base web é o acesso de um sistema a dados ou a outros sistemas por meio da intranet ou internet.

3.1.1.4 Nível 3: DOMÍNIO

A figura 4 apresenta um sistema de C2 acessando informações de dois outros sistemas operando em nível DOMÍNIO. O ambiente computacional é considerado *integrado*⁹.

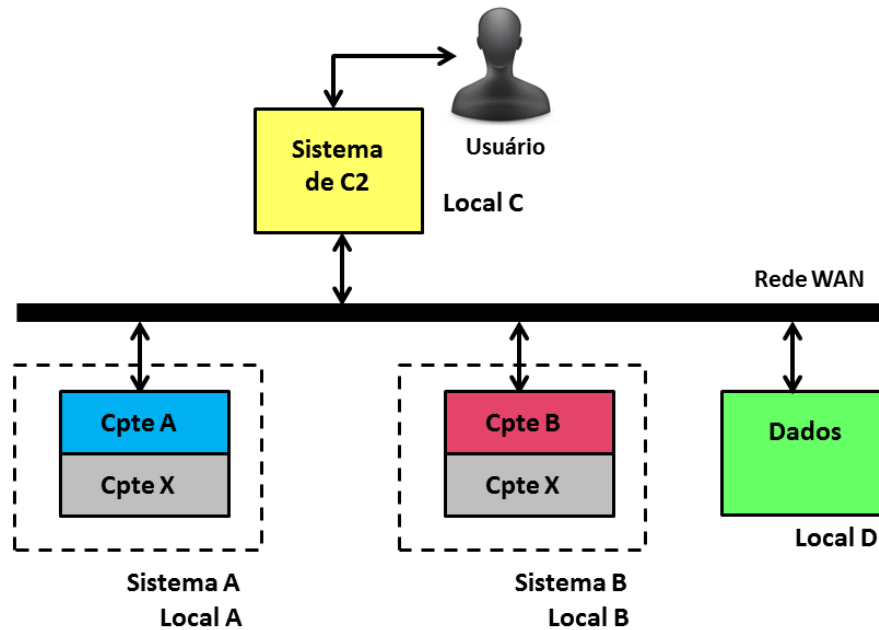


FIGURA 4 - Sistema de C2 operando em nível *DOMÍNIO*
Fonte: autor

É uma configuração de interoperabilidade na qual os sistemas compartilham bancos de dados comuns. Os programas de computador, aplicativos, continuam a residir integralmente, com todos os seus componentes de processamento, em máquinas individualizadas. Contudo acessam bancos de dados compartilhados que estão disponíveis na rede que os conectam. Esses bancos de dados podem residir de forma centralizada em um local diferente dos sistemas que os utilizarão, conforme mostra a figura 4. Podem também residir na mesma máquina de um dos sistemas ou estarem distribuídos em vários locais pela rede. É uma estrutura de interoperabilidade capaz de se conectar por redes *WAN*.

⁹ Ambiente de computação integrado é um ambiente de rede no qual diferentes sistemas se integram e trabalham juntos, compartilhando um banco de dados comum na rede em que estão conectados (EUA, 1998).

Para o compartilhamento dos bancos de dados, os sistemas adotam um modelo comum para representação das informações, chamado *modelo de dados de domínio*. Normalmente é uma configuração empregada por grupos de usuários ou organizações que lidam com um único tipo funcional, ou domínio, de dados, sendo esta a origem de sua nomenclatura. Exemplos: dados de C2 ou dados de inteligência. Por compartilhar os mesmos dados, os múltiplos sistemas possuem uma grande interação entre seus dados, caracterizando alta interoperabilidade. Permite, assim, o uso de aplicações que se utilizem de colaboração de vários usuários e fontes no trabalho com informações fusionadas que serão apresentadas aos tomadores de decisão, tornando tais informações mais detalhadas (EUA, 1998).

Como exemplo de aplicação deste nível de interoperabilidade seria um sistema de C2 para operações conjuntas das três forças singulares. O comando de operação central possuiria um sistema de C2 principal com um banco de dados a ser alimentado e compartilhado com três sistemas de C2 de apoio, empregados pelos comandos subordinados das forças singulares componentes. Outro exemplo seria a integração de sistemas de inteligência, melhorando sensivelmente as funcionalidades de acesso a uma base comum de dados.

Como contraposição a uma maior interoperabilidade vêm os aspectos de segurança cibernética, pois o comprometimento da base de dados comum compromete todos os sistemas. Quanto maior a interoperabilidade entre sistemas, maior deverá ser o cuidado com a SID.

3.1.1.5 Nível 4: CORPORATIVO

A figura 5 apresenta um sistema de C2 acessando informações de um ambiente computacional que possui arquitetura em nível CORPORATIVO, chamada *arquitetura corporativa*. O ambiente computacional é considerado *universal*¹⁰.

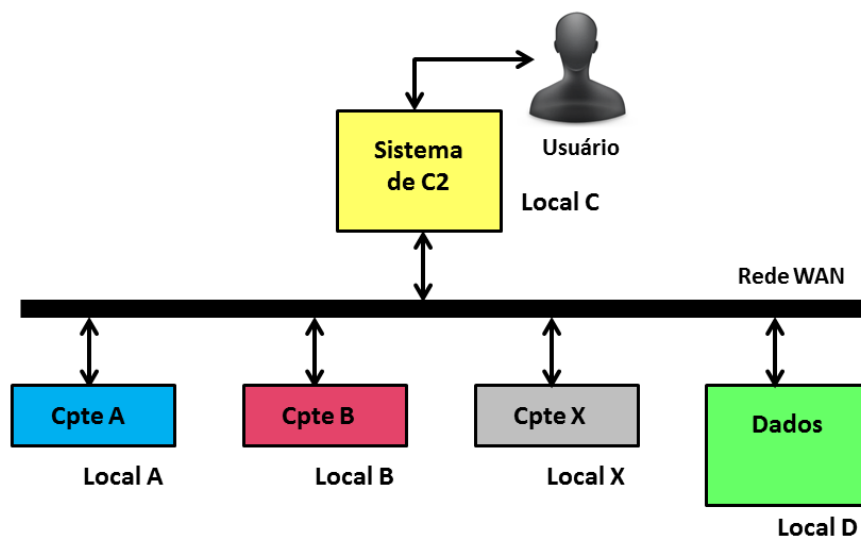


FIGURA 5 - Sistema de C2 operando em nível CORPORATIVO
Fonte: autor

Nesta configuração os sistemas compartilham bancos de dados e aplicativos em um espaço global de informações ou espaço cibernético¹¹. Os aplicativos utilizam diversos componentes de processamento, representados na figura 5 por “Cpte A”, “Cpte B”, e “Cpte X”, que residem de forma espalhada em diferentes máquinas pelo espaço cibernético. O acionamento de um conjunto destes componentes de forma coordenada dá origem à prestação de um serviço no espaço cibernético. Passa a haver uma otimização na codificação dos sistemas, pois um componente comum, na figura 5 representado pelo “Cpte X”, pode ser elaborado e disponibilizado uma única vez, sendo utilizado por vários sistemas e serviços que

¹⁰ Ambiente computacional universal é um ambiente de rede em que aplicativos do universo de diferentes domínios trabalham juntos e compartilham a mesma base de dados. Para tanto, esta base de dados é definida em um modelo corporativo comum a todos os aplicativos. (EUA, 1998).

¹¹ Espaço cibernético é um ambiente intangível formado por ativos de TI, onde dados e informações digitais são criados, armazenados, modificados, trafegados e processados (BRASIL, 2013).

recorrentemente acionam o “Cpte X”, em vez de inserir o código do “Cpte X” em suas linhas de programa.

Os serviços fazem uso de bancos de dados comuns, representado na figura 5 pelo bloco “Dados”, que também estão disponíveis no mesmo espaço cibernético. Estes dados possuem uma interpretação comum, independente do modelo físico adotado pelo banco de dados, que pode ser variado. A interpretação é provida por serviços demandados pelo sistema do usuário. Este sistema, por sua vez, faz acesso aos diferentes bancos de dados e interpretam as informações resultantes da forma estabelecida por procedimentos. É uma estrutura de interoperabilidade que permeia redes WAN de amplitude regional, como as intranets, ou globais, como a internet.

A configuração corporativa permite que múltiplos usuários interajam com dados complexos e em múltiplos domínios, de forma simultânea. Em função do grande volume de usuários, dos múltiplos domínios em que os sistemas podem trabalhar (C2, inteligência, logística), e da grande distribuição espacial dos equipamentos de TI, diz-se que esta estrutura de interoperabilidade se desenvolve em um ambiente computacional *universal*. Este ambiente é considerado o mais avançado para interoperabilidade, permitindo formas elevadas de colaboração. Surge aqui também o conceito de espaço de trabalho virtual¹² e computação em nuvem¹³ aludidos ao desconhecimento por parte dos usuários da localização dos aplicativos que ele lança mão para rodar o sistema. O elemento fundamental para o sucesso da interoperabilidade na arquitetura corporativa é o conjunto de procedimentos normativos a serem seguidos pelos sistemas e usuários conectados à rede corporativa. Ali será exposto o

¹² Espaço de trabalho virtual não está localizado no espaço geográfico, daí o termo virtual. Ele é acessível por intermédio de WANs (internet, por exemplo), que conectam os trabalhadores aos sistemas e dados necessários ao trabalho.

¹³ Computação em nuvem é um conceito onde um usuário, em vez de utilizar recursos de computação de sua estação de trabalho, como armazenamento de arquivos, o faz empregando recursos oferecidos por sistemas de um espaço cibernético.

resultado dos acordos de serviços disponíveis e a forma correta de um aplicativo acessá-los, assim como a interpretação correta dos dados entregues pelos serviços (EUA, 1998).

Como exemplo de aplicação do nível de interoperabilidade corporativa, situam-se os sistemas de C2 desenvolvidos para uso do Departamento de Defesa dos EUA (DoD) a partir de 2007, por ser esta arquitetura corporativa a adotada pelo DoD (EUA, 2007), em sintonia com as orientações do governo federal dos EUA (EUA, 2012).

Na arquitetura corporativa, os aspectos de SID e de disponibilidade da infraestrutura de redes para uma conexão global em alta velocidade são de vital importância. Os sistemas passam a ficar completamente dependentes do funcionamento e bom desempenho das redes para interoperação de seus módulos, como será abordado mais adiante neste trabalho.

3.1.2 Medida do Nível de Interoperabilidade

Na seção anterior foram apresentados os cinco níveis básicos de interoperabilidade entre sistemas. Tais níveis já permitem uma visualização básica de onde um determinado sistema se encontra, em termos de interação com outros sistemas, e dos níveis que ele pode evoluir. Contudo, o desenvolvimento de projetos de interoperabilidade exige uma visão mais aprofundada desses níveis assim como uma metodologia para determinação dos mesmos.

Uma das primeiras metodologias surgidas se deu em 1998, como resultado de estudos pioneiros sobre o assunto pelo DoD e encontra-se publicada no LISI (EUA, 1998). Seu projeto se iniciou em 1993 pela "C4ISR Integration Task Force" dos EUA para focar necessidades específicas de sistemas de C2 (STADEN, 2012). Apesar deste foco, a LISI é uma metodologia complexa e não endereça explicitamente a medição de potenciais de

interoperabilidade entre sistemas (STADEN, 2012). De qualquer forma, a LISI é a metodologia adotada pelos EUA, considerada uma referência mundial, e ponto de partida para o desenvolvimento de várias metodologias alternativas que se sucederam.

Em outubro de 2012 o "International Journal of Information Engineering and Electronic Business" (IJIEEB), conceituado veículo que publica trabalhos de pesquisa originais e de alta qualidade na área de tecnologia da informação, publicou uma metodologia alternativa para se atestar a maturidade de interoperabilidade dos sistemas de informação, chamada "Information Systems Interoperability Maturity Model" (ISIMM) (STADEN, 2012). O trabalho foi desenvolvido por Stefanus van Staden, do governo da Namíbia, em parceria com Jameson Mbale, professor do Departamento de Ciência da Computação da Universidade da Namíbia. Tem a vantagem de ser um modelo mais simples, objetivo e completo, desenvolvido especialmente para instituições que possuem muitos sistemas legados e pouca capacidade de investimento para melhorar a interoperabilidade. Tal modelo aproveita o que tem de melhor em outros modelos alternativos, como o LISI, e apresenta instrumentos de aplicação que independem de acesso "on line" a sistemas de apoio, como acontece com o LISI. É uma opção de metodologia muito interessante de ser adotada entre muitas existentes.

Independente do modelo de interoperabilidade adotado, os princípios de aplicação são os mesmos para se determinar a interação entre sistemas. Em uma primeira fase deve-se estudar o modelo a ser empregado, seus níveis e subníveis. Estes últimos são classificações intermediárias, dentro dos níveis, que servem para melhor detalhar a interoperabilidade. Normalmente o enquadramento em níveis e subníveis obedecem objetivamente ao enquadramento em quatro de cinco aspectos a seguir, dependendo do modelo empregado (EUA, 1998; e STADEN, 2012):

- a) existência e tipo de canal de conexão entre os sistemas (ex: inexistente, existente em baixa taxa de transmissão como satélites, existentes em alta taxa de transmissão como fibra ótica etc.);
- b) tipos e capacidades dos protocolos de comunicação de rede empregados (ex: permissão para comunicação unidirecional, bidirecional, em LAN, em WAN, em topologias multidimensionais);
- c) habilidade dos aplicativos empregados pelos sistemas em trocarem e compartilharem dados, corrigindo diferenças entre eles;
- d) grau de facilidade dos modelos de dados empregados serem perfeitamente compreendidos pelos diferentes sistemas que o utilizarão; e
- e) políticas e procedimentos técnicos estabelecidos para a troca de informação, capacidades e serviços entre sistemas.

Continuando com a aplicação do modelo de maturidade, depois do estudo do modelo e das características de níveis e subníveis, em uma segunda fase se fixam, em termos de nível e subnível, objetivos de maturidade de interoperabilidade técnica a serem atingidos pelos sistemas que devem se interagir.

A terceira fase diz respeito a determinar o estado de interoperabilidade técnica atual do grupo de sistemas considerado, isto é, seu nível/subnível. Para tanto, utiliza-se a metodologia fixada pelo modelo escolhido.

A quarta e última fase é a definição de um cronograma de trabalho e investimento para se atingir os objetivos estabelecidos na segunda fase.

Maiores detalhes relativos às metodologias e modelos devem ser acessados nos documentos que os descrevem constantes das referências bibliográficas.

3.1.3 Cronograma de Evolução de Interoperabilidade

Evoluir o nível de interoperabilidade entre sistemas é uma tarefa muito difícil, pois exige a modernização coordenada de sistemas e infraestrutura de TI, mas perfeitamente realizável em uma moldura de tempo de poucos anos.

A atividade demanda apurado conhecimento técnico, objetividade no que se deseja, estreita cooperação entre os órgãos da instituição, ou instituições, que possuem os sistemas que devem interagir, e investimento financeiro adequado. Daí a importância da adoção de um modelo de maturidade, da medição de níveis de interoperabilidade, do comprometimento das diversas equipes envolvidas. O processo é relativamente lento, alguns anos, exigindo um cronograma de metas parciais para seu sucesso, conforme o exemplo apresentado na figura 6:

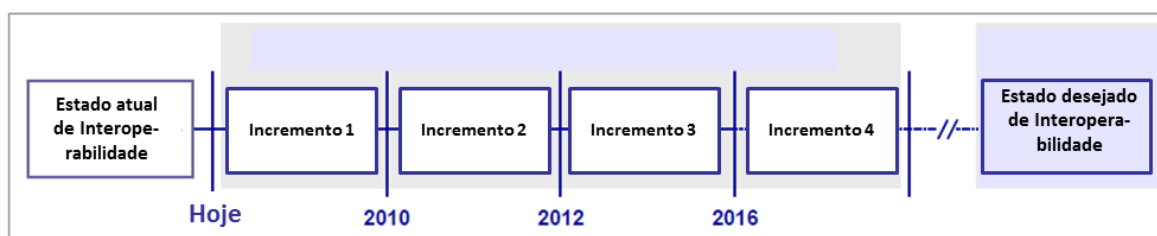


FIGURA 6 - Cronograma de incremento de interoperabilidade entre sistemas
Fonte: (EUA, 2007), adaptado pelo autor

Um cronograma como o apresentado na figura 6 é a base para a evolução. Ele servirá para:

- a) balizar as reuniões periódicas de controle do andamento do trabalho;
- b) dar clareza aos relatórios de acompanhamento;
- c) indicar próximos objetivos para as equipes técnicas; e
- d) subsidiar investimentos necessários.

3.2 PRINCIPAIS ARQUITETURAS DE INTEGRAÇÃO E INTEROPERABILIDADE

Nas décadas de 1990 e 2000 foram idealizadas e desenvolvidas duas arquiteturas de software que revolucionariam a forma como os sistemas podem se integrar, promovendo a fácil interoperação entre componentes de diferentes sistemas. Tais arquiteturas foram responsáveis pelo rápido desenvolvimento de sistemas que operam de forma globalizada e precisa, responsáveis hoje pelo acesso a um volume de informações jamais visto antes. Foram responsáveis também pelo fortalecimento e largo emprego nos dias atuais do conceito da guerra centrada em redes¹⁴.

O conhecimento dos princípios envolvidos nessas arquiteturas, "*Arquitetura Baseada em Componente*" e "*Arquitetura Orientada a Serviço*", permite visualizar com clareza a evolução de interoperabilidade que sistemas de C2 podem alcançar, assim como o esforço necessário para a implantação. As duas próximas seções se dedicarão à exposição dessas duas arquiteturas, ambientada por exemplos de emprego em sistemas de C2.

3.2.1 Arquitetura Baseada em Componente

Para se entender a *Arquitetura Baseada em Componente*, tradução do inglês de "Component-Based Architecture" (CBA), é necessário compreender o significado de um componente. Um componente é um objeto de software projetado para interagir com outros componentes e fornecer ao sistema que o utiliza um conjunto de funcionalidades. Ele tem uma forma de interfaceamento bem definida, isto é, recebe e fornece dados obedecendo a um

¹⁴ Guerra centrada em redes é o conceito no qual se objetiva a superioridade da informação pelo emprego de redes de computadores e compartilhamento de informações, de forma a aumentar a eficiência do comando e controle no planejamento e condução de operações de combate.

protocolo padronizado de acesso, comum a todos os componentes que fazem parte de certa arquitetura tecnológica (PETRITSCH, 2006). O objetivo do emprego de componentes é aumentar a qualidade e a produtividade do desenvolvimento de aplicativos. A ideia básica é criar vários componentes-padrão, de alta qualidade, que provê funcionalidades comuns a diversos sistemas e que são desenhados para serem reutilizados por vários aplicativos. Assim, facilita-se muito a construção de softwares com o emprego de componentes funcionais já criados e confiáveis, em vez de se reinventar a roda toda vez que há necessidade de uma funcionalidade ordinária dentro de um sistema. Um exemplo de um componente seria um trecho de software que fornece a latitude e a longitude de um contato quando lhe são passados os dados de latitude e longitude do navio, e de marcação e distância do contato em relação ao navio. Se este trecho de software, em vez de compor as linhas de código de um determinado sistema de C2, for escrito seguindo regras para ser reutilizável, ele se transformará em um componente passível de ser empregado por diversos sistemas de C2.

Uma CBA é a base da engenharia de software por componentes que tem como objetivo o desenvolvimento rápido e confiável de sistemas robustos baseados no reuso de componentes padrões já disponíveis. Isto requer uma mudança de paradigma de desenvolvimento, focando-se em criação de funções para uma família de sistemas ao invés de um único sistema (PETRITSCH, 2006).

A grande vantagem da facilidade de reuso de componentes desenvolvidos por terceiros gera certa desvantagem no desenvolvimento mais trabalhoso de componentes originais, que também devem ser estruturados para serem utilizados por outros. Desta forma, seguem-se padrões de construção onde são definidas as estruturas que devem ser desenvolvidas nos componentes para permitir conexão e composição com outros sistemas, assim como um comportamento colaborativo com outros componentes.

3.2.2 Arquitetura Orientada a Serviço

Quando se disponibiliza um conjunto de componentes para serem descobertos e acessados em uma rede por diversos sistemas nela conectados, esses conjuntos passam a oferecer serviços no ambiente de rede. Tem-se, assim, a *Arquitetura Orientada a Serviço*, tradução do inglês "Service-Oriented Architecture" (SOA). Desta forma, pode-se dizer a SOA é uma evolução da CBA para um ambiente de rede (PETRITSCH, 2006).

Como exemplo, suponha que um determinado sistema disponibilize na rede três componentes: um, que interroga navios obtendo suas latitudes, longitudes, marcação e distância de seus contatos; um outro, é aquele citado anteriormente que fornece latitude e longitude de um contato quando lhe são passados os dados de latitude e longitude do navio, e de marcação e distância do contato em relação ao navio; e, um terceiro componente, que converte latitudes e longitudes para uma determinada escala de vídeo, passada como parâmetro de entrada. Com esses três componentes pode-se gerar em um computador (geralmente um servidor) um serviço de plotagem na tela dos contatos obtidos por uma Força Tarefa. Mais ainda, este serviço pode ser utilizado por diversos sistemas de C2 que estejam conectados nessa rede e atenda aos requisitos de uso do serviço.

A SOA só foi possível com o advento das redes WEB¹⁵ de alta velocidade e de protocolos desenvolvidos especialmente para permitir que os sistemas descubram serviços e interajam com eles da forma adequada, como o protocolo "Simple Object Access Protocol" (SOAP). Para que haja um alto índice de reuso de serviços de forma transparente é necessário que os sistemas saibam que há certos serviços disponíveis, onde eles se encontram e como interfacear com eles. Assim, antes do efetivo uso do serviço há uma fase de busca do serviço

¹⁵ WEB é a abreviação curta de "World Wide Web" (WWW) que significa a grande rede mundial. Pode contextualizar tanto a internet como uma intranet.

usando *agências de descoberta* e protocolos específicos que permitem aos sistemas descobrir e ter uma descrição dos serviços ofertados na rede, como o "Universal Description Discovery and Integration" (UDDI) e o "Web Services Description Language" (WSDL) (PETRITSCH, 2006). A figura 7 abaixo ilustra este processo de descoberta de serviço para, posterior uso efetivo.

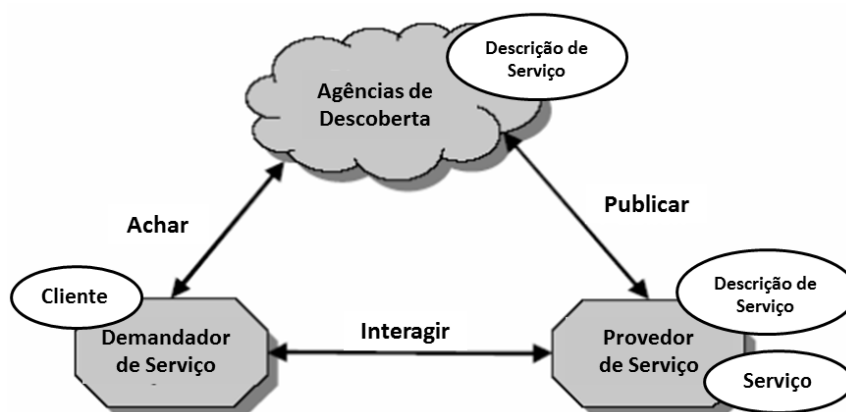


FIGURA 7 - Processo de publicar e achar serviços em arquitetura SOA
Fonte: (PETRITSCH, 2006) com tradução pelo autor

Com essa estrutura obtém-se uma situação conhecida como acoplamento frouxo ("loose coupling") entre agentes de software que se interagem, podendo oferecer seus serviços de forma trivial ao longo da WEB. Isto representa a grande força da fácil disponibilização global de serviços nos dias atuais que alavanca a troca intensa e precisa de informações pelo mundo.

No estabelecimento de serviços a serem usados e disponibilizados na rede, deve-se observar que o acesso é muito mais rápido a serviços disponíveis localmente, isto é, serviços que residem na própria máquina onde se localiza o corpo principal do sistema, ou na rede local que essa máquina pertence. Além de mais rápido, a disponibilidade e a segurança do sistema são aumentadas quando se utiliza serviços locais. Em contrapartida, o acesso a serviços remotos, isto é, localizados em redes fora da LAN na qual o corpo principal do sistema se localiza, como na WEB, tem como mérito a possibilidade de acesso a dados de

outros sistemas e a funções complexas já disponíveis na WEB. Contudo, este acesso é mais lento e, em caso de indisponibilidade, afeta a eficácia do sistema considerado. Assim, deve-se medir muito bem em termos de desempenho, disponibilidade, segurança e interoperabilidade quais serviços devem estar disponíveis localmente e quais devem ser acessados remotamente. Geralmente serviços de granularidade mais fina, isto é, aqueles acessados com muita frequência são projetados para acesso local.

O surgimento da CBA e sua posterior evolução para a SOA são inovações dos anos recentes com a intenção de desenvolver um tipo de arquitetura que permita o acoplamento frouxo e a alta reusabilidade dos seus componentes (PETRITSCH, 2006). Desta forma promoveram uma alta interoperabilidade e integração entre sistemas, transformando-se nas bases da filosofia e-government (governo eletrônico)¹⁶ de muitos países. Como exemplo, o congresso dos EUA expediu em 2002 uma lei federal, conhecida como "e-government act", para desenvolvimento de uma Arquitetura Corporativa (último nível de interoperabilidade apresentado em 3.1.1) nos órgãos da administração pública federal e em apoio à promoção de serviços de governo eletrônico. Como um dos efeitos decorrentes o DoD lançou o "DoD Architecture Framework" (DoDAF), que em 2010 ganhou sua versão 2.0. Este documento visa estabelecer uma forma padrão (framework) para desenvolver, apresentar e integrar arquiteturas em sistemas do DoD, inclusive os de C2 (EUA, 1997b). Tanto o e-government act quanto o DoDAF empregam as arquiteturas CBA e SOA como bases de desenvolvimento e integração de sistemas.

¹⁶ E-government, ou governo eletrônico, é o conceito no qual órgãos governamentais provêm informações e serviços aos cidadãos por intermédio da internet.

3.3 GRADE DE INFORMAÇÃO GLOBAL

De forma pioneira, em 1996 o congresso estadunidense emitiu o "Clinger–Cohen Act", evolução do "Information Technology Management Reform Act", também de 1996. Era uma lei que orientava os órgãos federais na melhor forma de selecionar e gerenciar recursos de TI, orientando como atualizar, manter e adquirir tais recursos de maneira a atingir os objetivos estratégicos das instituições com o correto gerenciamento das informações. De uma forma mais objetiva, a lei visava evitar o desperdício de recursos públicos na compra de ativos de TI e, para tanto, pregava uma arquitetura integrada dos órgãos de forma a evitar redundância de recursos. Mais tarde, em 2002, esta lei foi substituída por uma outra, mais ampla, conhecida como "e-government act", que visa não somente a economicidade de recursos mas também o acesso informatizado a serviços do governo pela população. A lei reforça a importância e orienta para a interoperabilidade de todas as agências federais. Para tanto recomenda o emprego de uma arquitetura corporativa, "Enterprise Architecture" (EA), para o governo federal. O e-government act criou a figura de um "Chief Information Officer" (CIO) Federal dentro do "Office of Management and Budget" (OMB) para conduzir o alinhamento dos órgãos federais à arquitetura corporativa recomendada. Este CIO Federal passa a conduzir uma política de governança por arquitetura, adotando modelos de referência de EA criados pelo OMB, os "Federal Enterprise Architecture Reference Models" (FEA-RM), a ser seguido por todos os órgãos federais (EUA, 1997b).

Muitas iniciativas começaram a ser conduzidas nos diversos órgãos do governo federal visando melhorar a integração de seus sistemas e o estabelecimento de uma arquitetura corporativa, aderente ao FEA-RM. O DoD, que havia liderado os estudos de interoperabilidade com a criação do LISI, gerou documentos específicos sobre o assunto para orientar as forças e agências subordinadas. Um importante documento, publicado em 2007,

foi o "*DoD Global Information Grid Architectural Vision*" (DoD-GIG). Ele decorre diretamente dos modelos estabelecidos pelo FEA-RM com particularidades específicas para sistemas de C2. Ali é descrito como desenvolver no DoD as capacidades de uma Grade de Informação Global (GIG) de maneira a aproveitar integralmente o poder da informação e colaboração que cruza seus estabelecimentos para alimentar o campo de batalha distante, transformando-o em uma força centrada em rede, capaz de realizar operação centrada em rede - "Net Centric Operation" (NCO) (EUA, 2007).

O conceito de GIG do DoD compreende todas as capacidades de informação, que habilitam seu acesso, sua troca e seu uso, junto com os serviços associados, por todos os usuários do DoD e seus parceiros externos. Estas capacidades incluem os dados em si, os sistemas de TI, o pessoal e os processos associados que apóiam, com provimento de informações, as diversas organizações a cumprirem suas tarefas e missões. Como o foco é o apoio ao cumprimento de tarefas e missões, a forma como combatentes, pessoal executivo e de inteligência opera tem que conduzir a forma como a GIG é estruturada e operada (EUA, 2007).

O DoD fez um levantamento de sua GIG em 2007 e concluiu que a grade estava estruturada organizacional e funcionalmente por sistemas tipo "stovepipe"¹⁷, que apresentavam diversos níveis de interoperabilidade e restrições para acesso a informações necessárias. A grade não explorava suficientemente o potencial das tecnologias da era da informação e não atendia integralmente à máxima operativa da informação certa na hora certa. Era uma grade estática, ao invés de dinâmica, incapaz de se adaptar rapidamente para o atendimento de necessidades imprevistas de comunicação e novos usuários. Desta forma, a GIG não estava adequada para trabalhar com NCO (EUA, 2007).

¹⁷ Sistema "stovepipe" é um sistema isolado, que não usa e nem fornece dados e funcionalidades compartilhados com outros sistemas. A analogia se faz com o duto de exaustão de um fogão que o conecta a uma chaminé própria em um prédio, obrigando um estabelecimento que tenha 10 fogões a ter 10 chaminés. Esta imagem se opõe a um sistema de exaustão compartilhado, mais eficiente, que conduza a uma única chaminé.

O DoD estabeleceu um plano de transformação de sua GIG orientado principalmente para a evolução da interoperabilidade e integração de seus sistemas. Assim, seguindo o modelo LISI, estabeleceu o plano mostrado na figura 8.

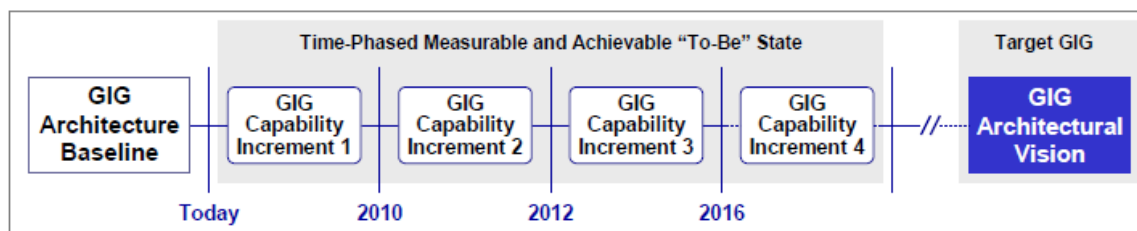


FIGURA 8 - Transição da GIG do DoD de 2007 para uma arquitetura de GIG vislumbrada
Fonte: (EUA, 2007)

A GIG de 2007 é representada na figura 8 por “GIG Architecture Baseline”, enquanto a GIG idealizada, alvo da evolução, é chamada “Target GIG”.

A GIG idealizada pelo DoD deverá atender os atributos apresentados na tabela 4.

TABELA 4
Atributos da GIG Idealizada pelo DoD

Atributo	Descrição
Semelhança com Internet e WWW	Adaptação de construções e padrões adotados pela Internet e navegação WEB, inserindo melhorias para mobilidade e funcionalidades exclusivamente militares, como precedência e preempção.
Segurança e disponibilidade no transporte de informação	a) Criptografia inicial para transporte central no backbone; b) Foco na troca de dados ponta-a-ponta; c) Robustecimento contra Denial of Service (DoS).
Proteção e garantias da informação e dados	a) Provedor/editor marca as informações e dados para classificação e manuseio; b) Prevê mecanismos para assegurar autenticidade, integridade e não repúdio aos pacotes de dados.
Publicação em paralelo	Provedor/editor torna informações e dados visíveis e acessíveis sem atrasos, de maneira que os usuários obtém informação quando e como desejada (ex: info bruta, analisada, arquivada).
Acesso inteligente	Os usuários podem encontrar e acessar diretamente, subscrever ou usar serviços de valor agregado (ex: descoberta). Quadro Operativo Definido pelo Usuário X Quadro Operativo Comum.
Foco na informação/dados	Informação/dados separados de aplicativos e serviços. Minimiza a necessidade de softwares especiais ou proprietários.
Aplicativos e serviços compartilhados	Quando usuários precisam de colaboração, eles podem acionar múltiplos aplicativos para acessar os mesmos dados ou escolher os mesmos aplicativos.
Acesso confiável e	Acesso ao transporte da informação, à informação em si / dados,

diferenciado	aplicativos e serviços, acesso esse diferenciado quanto a credencial e capacidade técnica do usuário.
Qualidade de serviço	Orientado para o tipo de informação a trafegar: voz, imagens paradas, imagens em movimentos, vídeos, dados e colaboração.

Fonte: (EUA, 2007)

Do ponto de vista dos usuários na frente de combate, a GIG idealizada apresenta a configuração apresentada na figura 9.

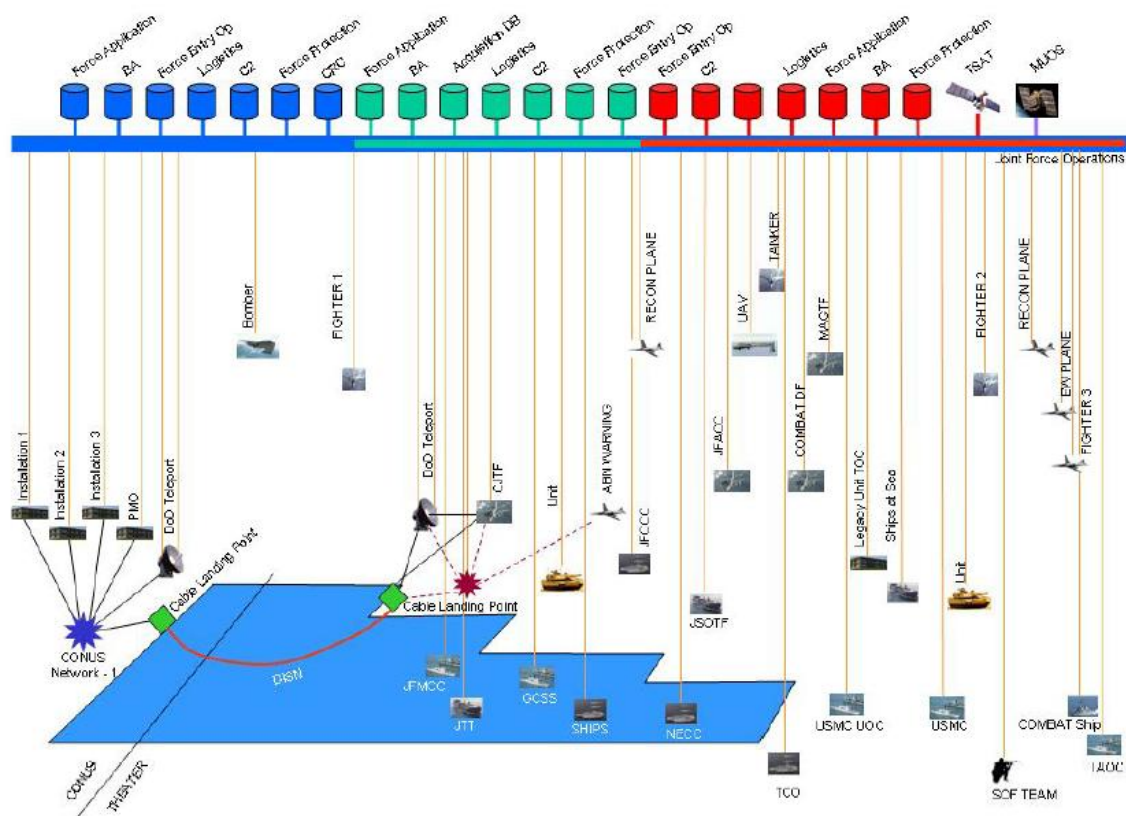


FIGURA 9 - Compartilhamento de informações dentro da GIG idealizada

Fonte: (EUA, 2007).

A figura 9 mostra o compartilhamento de informações na GIG pela perspectiva tática dos combatentes, mostrados na parte inferior, em uma operação conjunta de três forças singulares. Devidamente autenticados no sistema dentro de seus níveis de credenciamento, os usuários podem produzir e usufruir de serviços e informações compartilhados, mostrados na parte superior da figura. Observa-se que as forças tipo, representadas cada uma por uma cor diferente (azul, verde e vermelha), possuem seus bancos de dados, sistemas de C2, de consciência situacional do campo de batalha, "Battlespace Awareness" (BA), e outros

compartilhados com os combatentes em uma infraestrutura comum (rede) de serviços, computação e comunicação. Os combatentes acessam tais serviços por intermédio de sistemas táticos embarcados e terminais inteligentes. O objetivo final é habilitar a formação de grupos dinâmicos e colaborativos, geograficamente distribuídos no teatro de operações. (EUA, 2007).

Uma outra visão da GIG idealizada pelo DoD é a visão sistêmica apresentada na figura 10.



FIGURA 10 - Visão sistêmica da GIG idealizada
Fonte: (EUA, 2007).

A visão sistêmica da figura 10 divide a GIG em 5 camadas envoltas por uma "infraestrutura de garantia de informação" - "Information Assurance" (IA) - e permeadas por

um "serviço de suporte e segurança de operações de rede" - Network Operations (NetOps). Os usuários encontram-se na camada de topo interagindo com a parte de apresentação dos sistemas, onde situam-se as interfaces homem-máquina (IHM) dos mesmos. Esta camada é, portanto, chamada de "interação homem computador". Logo abaixo desta camada situa-se a camada de "aplicativos, serviços e informações". Ali se estabelecem as funcionalidades centrais de processamento e armazenamento de informações dos sistemas, considerada a camada de inteligência computacional e de banco de dados da GIG. As 3 camadas inferiores formam a infraestrutura para o tráfego das informações. São elas as infraestruturas de "comunicação", de "computação" e de "serviços corporativos centrais", "Core Enterprise Services" (CES). Na infraestrutura de CES é onde estão localizados os servidores que permitem a operação da GIG em arquiteturas CBA e SOA. Ali estão localizados os serviços de diretório, de descoberta, de colaboração, de mensagens entre máquinas, de autenticação de usuários, de políticas de acesso, de mediação, e outros, operando protocolos como SOAP, UDDI e WSDL.

Nas duas camadas inferiores, relativas às infraestruturas de "computação" e "comunicação", independente do canal empregado, as informações têm que seguir em pacotes que obedecem ao "Internet Protocol" (IP) como padrão a ser empregado. Assim, possuindo um protocolo IP comum a todas as redes, uma informação trafega por um terminal satélite para um terminal de rádio UHF, ou para uma conexão por fio a outro terminal de forma transparente para os usuários.

Concluindo esta seção, o que foi percebido pelo governo estadunidense é que o melhor caminho para a melhoria de integração de sistemas é a *governança por arquitetura*. Esta governança ocorre quando governos e ministérios orientam seus órgãos subordinados para aquisições que obedecem ao alinhamento com uma certa arquitetura de ativos de TI a ser adotada por todos, arquitetura essa que pode ser abordada com o conceito de GIG, conforme

fez o DoD. Com o passar do tempo os órgãos vão alinhando suas aquisições, sistemas legados e treinamento de pessoal com a arquitetura padronizada.

3.4 ESTRUTURA DE SISTEMAS DE C2

Uma boa abordagem para estruturar um sistema de C2 é aquela que divide tais sistemas em três visões: operativa, sistêmica e técnica. Esta abordagem foi empregada pelo DoD no início de seus estudos de padronização e integração de sistemas de C2 em 1997, quando lançou a publicação "C4ISR Architecture Framework" (CAF). No que pese em 2010 esta publicação ter sido substituída pelo DoDAF, mais genérica que abrange todos os tipos de sistemas do DoD e não somente os de C2, a CAF é melhor para o estudo de sistemas de C2 por ser mais focada nesses sistemas.

Cada uma das três visões de um sistema de C2 se relaciona com as demais, conforme apresentado na figura 11.

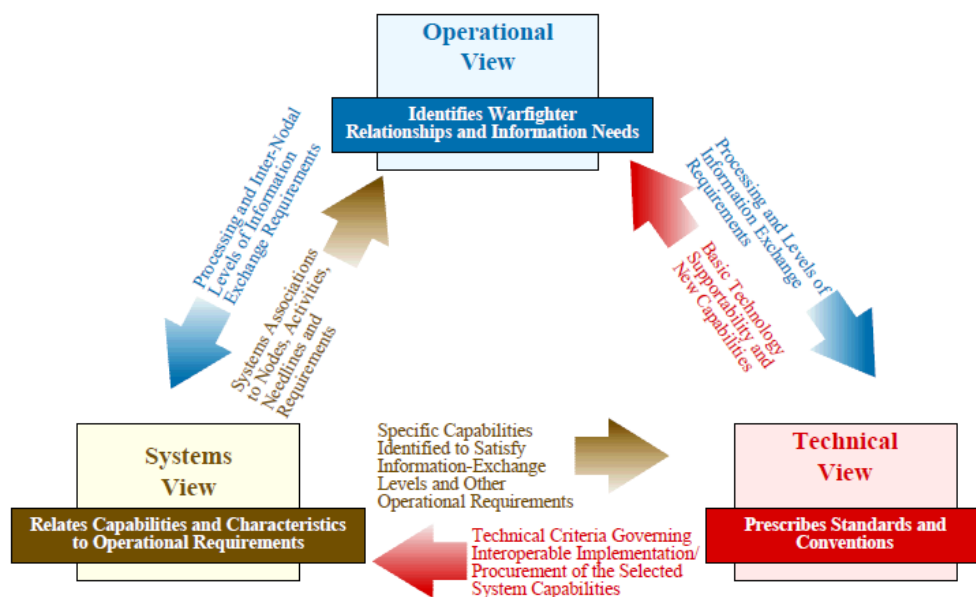


FIGURA 11 - Três visões de um sistema de C2 e seus relacionamentos
Fonte: (EUA, 1997a).

A visão operativa é a que comanda as demais. Nesta visão são definidos os requisitos operativos que se traduzem em características funcionais que o sistema deve apresentar para cumprir as missões operativas em que será empregado, assim como as respectivas medidas de eficácia operacional para controle de desempenho. A partir deste ponto pode-se estabelecer que tipo de informação o sistema necessitará, em que nível de detalhamento e de onde serão obtidas estas informações. Desta forma, a partir de uma análise dos requisitos operativos obtidos na visão operativa, estabelecem-se os requisitos de troca de informação, integração com outros sistemas e processamento de tal informação, que servirão de base para construção das duas outras visões: sistêmica e técnica.

A visão sistêmica é uma descrição do sistema, subsistemas e suas interconexões para prover funções operativas de combate. Esta descrição, que inclui diagramas e figuras, detalha construções internas, suas formas de operação, pontos de conexão física, localização, quais sistemas estão interconectados, como e onde estão localizadas as conexões com outros sistemas, quais os nós-chave de interconexão externa, características tecnológicas dos circuitos, redes e plataformas de combate nos quais o sistema de C2 interfaceia. Outra descrição importante obtida na visão sistêmica é a dos parâmetros de desempenho (MTBF¹⁸, disponibilidade etc.), associando padrões de desempenho de recursos físicos com os requisitos operativos da visão operativa (EUA, 1997a).

Como pode ser visto na figura 11, na visão sistêmica se identifica que sistemas ou subsistemas que podem atender os requisitos operacionais e se traduz o grau de interoperabilidade exigido em um conjunto de capacidades específicas, ou características técnicas, a serem atendidas pela visão técnica. Por fim, se compara as implementações vislumbradas com as capacidades específicas necessárias (EUA, 1997a).

¹⁸ MTBF: “Mean Time Between Failure”, isto é, Tempo Médio Entre Falhas.

A visão técnica, por ser de grande importância neste trabalho, merece destaque e será descrita na próxima seção.

3.5 VISÃO TÉCNICA DOS SISTEMAS DE C2

A visão técnica provê o conjunto mínimo de regras técnicas que governam o arranjo de sistemas ou subsistemas, suas partes e suas interações, tomando por base os padrões técnicos disponíveis para implementação, de forma a assegurar a conformidade com a visão sistêmica e operativa do sistema.

Nesta visão se define inicialmente as linhas mestras de implementação técnica do sistema. Sobre elas serão estabelecidas as especificações de engenharia, os blocos comuns de construção a serem empregados e as linhas de produto que devem ser desenvolvidas. Aqui são considerados uma coleção de padrões técnicos e regras de implementação, mapeados em perfis, que permitem o atendimento aos serviços solicitados do sistema. Esta coleção de padrões técnicos e regras constitui os critérios técnicos que governarão a interoperabilidade do sistema, a ser considerada na visão sistêmica, conforme mostrado na figura 11 (EUA, 1997a).

Uma maneira eficaz de se escolher os padrões técnicos a serem empregados em sistemas de C2 é escolhê-los com base em uma lista, mapeada por serviços associados aos padrões. Deve-se ter em conta que os padrões técnicos também se distribuem pelas diversas camadas da GIG, vide figura 10. Assim, temos padrões associados às infraestruturas de comunicação (ex: padrão de comunicação satélite), de computação (ex: padrão de dispositivos de armazenamento para banco de dados), de CES (ex: padrão de protocolo para descobrimento de serviços em arquiteturas SOA), de aplicativos, serviços e informação (ex:

padrões de imagens a serem trocadas, reportes de consciência situacional, serviço meteorológico disponível).

Para facilitar a visualização da coletânea de padrões técnicos a ser adotada no desenvolvimento de sistemas de defesa, o DoD expediu em 2005 um modelo de mapeamento chamado "DoD Enterprise Architecture Technical Reference Model" (TRM) (EUA, 2005). O modelo serve para visualizar esquematicamente os elementos de tecnologia que coletivamente compõem os sistemas, abordando-os na arquitetura CBA. O TRM é um instrumento de apoio na transformação da arquitetura corporativa do DoD em uma arquitetura centrada em rede, alinhando-a com o FEA-RM. Devido a este alinhamento, o TRM é todo focado em arquiteturas SOA e CBA (EUA, 2005). Seu uso permite uma visualização fácil da escolha de tecnologias a serem padronizadas para permitirem reuso máximo e o mínimo de estruturas redundantes desnecessárias na GIG.

A figura 12 apresenta como os diversos padrões técnicos podem ser mapeados no TRM.



FIGURA 12 - Modelo de Referência Técnica para arquitetura corporativa do DoD
Fonte: (EUA, 2005).

A ideia básica é um padrão técnico estar associado a um serviço, sendo este padrão considerado a especificação técnica do serviço a ser prestado na rede de usuários. No quadro da figura 12 um serviço é classificado em 3 níveis de profundidade a saber: área de serviço; categoria de serviço dentro da área; e padrão de serviço dentro da categoria. Dentro de um padrão de serviço pode-se escolher sua especificação técnica, ou seja, qual o padrão técnico a ser seguido pelo serviço. A figura 13 esquematiza esta hierarquia de níveis de classificação de um serviço, incluindo a escolha final do padrão técnico (especificação do serviço).

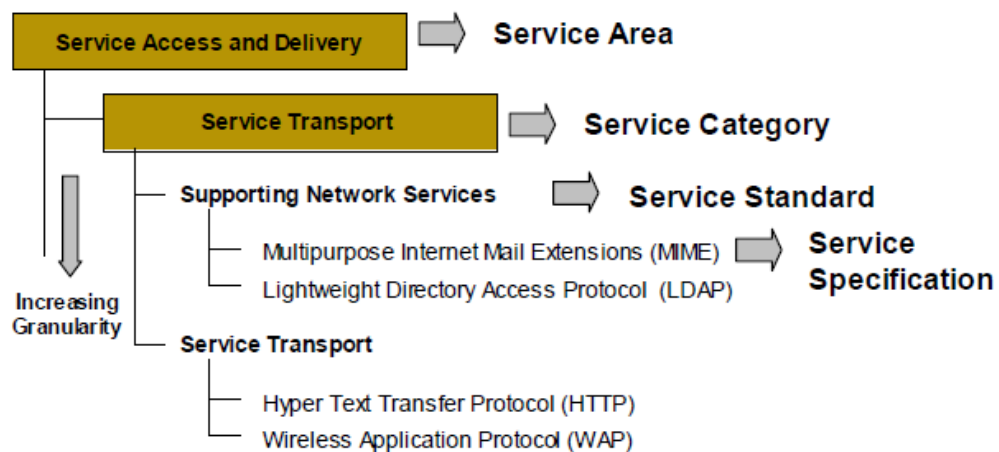


FIGURA 13 - Hierarquia de Área, Categoria, Padrão, e Especificação de Serviços
Fonte: (EUA, 2005)

O primeiro nível de classificação de serviços é a área à qual ele está associado. Como pôde ser visto na figura 12, os serviços estão divididos em quatro áreas: acesso e entrega; plataforma e infraestrutura; estruturação de componente; e interface e integração. O enquadramento em cada área é descrito a seguir segundo (EUA, 2005):

- a) área de Acesso e Entrega: serviços que possibilitam o acesso, troca e entrega de componentes ou capacidades de serviço. Inclui também aspectos legislativos e regulatórios que governam o acesso e uso de um determinado componente de serviço;
- b) área de Plataforma e Infraestrutura: serviços relacionados com as plataformas de entrega (exemplos: plataforma WEB, portal) e suporte (ex: plataforma sem fio), com as capacidades infraestruturais (ex: capacidade de videoconferência) e com requisitos de hardware para construção, manutenção e disponibilização de componentes (ex: servidores, computadores);
- c) área de Estrutura de Componente: serviços relacionados com as fundações básicas, tecnologias, e especificações pelas quais os componentes são construídos, trocados e distribuídos ao longo da rede SOA (ex: serviços de

segurança, como criptografias, e serviços de gerenciamento de banco de dados); e

- d) área de Interface e Integração: serviços relacionados com tecnologias, metodologias, padrões e especificações que governam como os diversos órgãos vão interfacear (internamente e externamente) com os componentes (exemplos: protocolo de descoberta e descrição de serviços), e os métodos pelos quais os componentes irão interfacear e integrar com sistemas legados (ex: padrões de formatação e transformação de dados).

O segundo nível de classificação de serviços é a categoria que ele pertence dentro da área. São 18 categorias que se distribuem dentro das 4 áreas. Em cada categoria o serviço ainda é classificado em padrões, terceiro nível de classificação. Ao todo são 57 padrões de serviços.

Um sistema geralmente tem serviços ocupando as 18 categorias e pelo menos um padrão dentro de cada categoria. Assim, o modelo de mapeamento da figura 12 fornece um instrumento prático de se documentar e visualizar os serviços, e respectivas especificações técnicas, disponibilizados nas 18 categorias. Seu uso evita a não consideração de um determinado serviço de apoio que poderá ser, em última análise, o ponto-chave de uma impossibilidade de integração do sistema com outros ou uma redundância, por já existir este serviço disponível em outro sistema local.

O mapeamento da arquitetura existente em uma corporação pelo TRM facilita a visualização de estratégias de migração para nova arquitetura centrada em rede e SOA. Tal procedimento oferece a possibilidade de se descobrir capacidades a serem trabalhadas e configurações de tecnologias em vários componentes dos sistemas (EUA, 2005).

A figura 14 mostra como diferentes categorias de serviço são empregadas para conectar um sistema que opera dentro de um ambiente interno a um órgão ou corporação, com o ambiente externo por meio de uma "Zona Desmilitarizada" (DMZ).

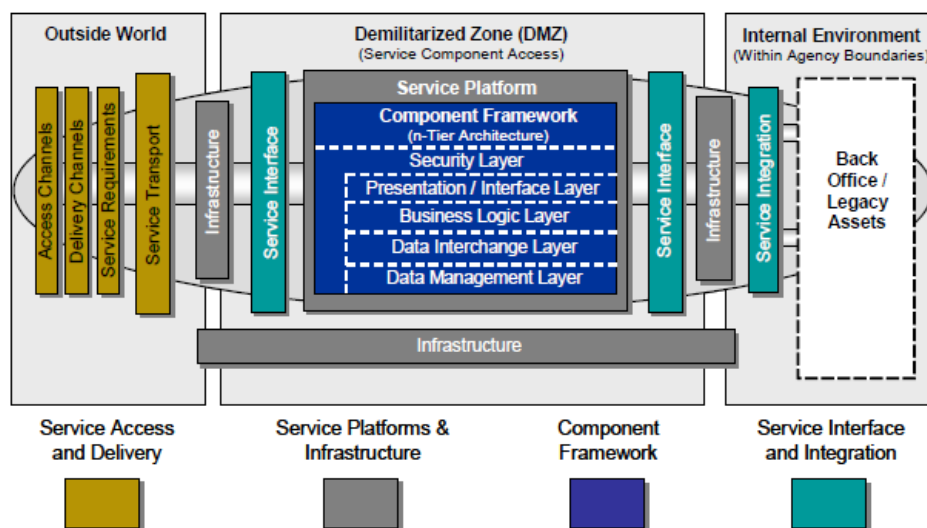


FIGURA 14 - TRM aplicado à conexão em rede do sistema de uma corporação a um ambiente externo por intermédio de uma DMZ
Fonte: (EUA, 2005)

Os blocos são as categorias de serviços a serem documentadas ou pensadas. Eles estão pintados de cores indicativas da área que cada categoria corresponde.

Este esquema da figura 14 de interfaceamento entre ambientes interno e externo por intermédio de uma DMZ é muito útil no projeto de interfaces e sistemas de firewall. Ele fornece uma orientação precisa das categorias de serviços, e padrões tecnológicos correspondentes, que o projetista precisa se preocupar para permitir um interfaceamento o mais interoperável possível com a rede de sistemas que serão interconectados. Aplicativos que fornecem dados para o ambiente externo devem residir na DMZ, evitando que usuários externos acessem o ambiente interno da corporação. É uma estrutura típica a ser empregada na evolução da interoperabilidade de sistemas legados.

Em 2003 o DoD expediu um outro documento de apoio à visão técnica de sistemas de C2. Com o título de "Joint Technical Architecture" (JTA), este documento

relaciona os padrões de tecnologia, isto é, especificações técnicas que podem ser empregadas na visão técnica de um sistema integrado à arquitetura corporativa do DoD. (EUA, 2003). O projetista, então, após mapear as categorias e padrões de serviço de seu sistema com o TRM, pode escolher na lista do JTA qual especificação técnica para o serviço deverá ser empregada.

Como exemplo, suponha que uma equipe de desenvolvimento de um sistema de C2 queira definir como os dados de um teatro de operações devam ser apresentados às forças combatentes. Considerando que este sistema deva atender àquela força armada que está desenvolvendo o sistema, mas também ser interoperável, isto é, possa ser usado total ou parcialmente por combatentes de outras forças armadas, nacionais ou estrangeiras amigas, esta apresentação deverá seguir um padrão técnico de simbologia, de forma a ser um sistema amigável que não suscite dúvidas no que está sendo apresentado. Se este problema estiver no DoD, a equipe técnica já teria mapeado esta necessidade do TRM como um serviço ocupando a área de "Estrutura de Componente" ("Component Framework"), categoria "Apresentação/Interface" ("Presentation/Interface"), padrão "Display Estático" ("Static Display"). Recorreria então ao JTA e constataria que deveria necessariamente seguir o padrão "MIL-STD-2525B, Common Warfighting Symbology".

Em 2007, o DoD substituiu o JTA por um sistema "on line" no qual somente usuários cadastrados podem fazer acesso, o "DoD Information Technology Standards Registry" (DISR). Este é o sistema empregado atualmente. Possui a grande vantagem de ser dinâmico, isto é, na medida em que surgem novas tecnologias consolidadas e aprovadas pelo DoD, elas são inseridas no DISR sem necessidade de se expedir novo documento, como seria o caso do JTA. Desta forma é importante a todos que trabalham no desenvolvimento ou integração de sistemas de C2 que tenham acesso ao DISR. Caso contrário ficarão limitados ao retrato tecnológico de 2003, na consulta do JTA.

4. CARACTERÍSTICAS TÉCNICAS E PADRÕES DE SERVIÇOS DEMANDADOS PELO PEM E PCD

O capítulo 2 identificou as características funcionais que os sistemas de C2 devem apresentar para estarem aderentes com o PEM e a PCD. Tais características, como apresentado no capítulo 3 (seção 3.4), representam demandas na visão operativa dos sistemas de C2.

Visando estudar e sugerir formas de estruturar os sistemas de C2 da MB para atender aos objetivos navais do PEM e às diretrizes da PCD, deve-se transformar as demandas da visão operativa em demandas para a visão sistêmica e, posteriormente, para características a serem seguidas pela visão técnica. As duas seções a seguir apresentarão as decorrentes demandas sistêmicas, sob o enfoque da visão sistêmica de grade, e as consequentes demandas na visão técnica, respectivamente. Como consequência da análise da última seção, obtêm-se as características técnicas e os respectivos padrões de serviços da grade de operações dos sistemas de C2 que devem ser bem estruturados para se atender às demandas do PEM e PCD.

4.1 DEMANDAS SISTÊMICAS

Uma primeira abordagem da visão sistêmica de um sistema de C2 é visualizá-lo nas camadas sistêmicas da grade na qual ele vai operar, onde o conceito de grade e suas camadas é aquele apresentado na seção 3.3. Para tanto será empregada como visão sistêmica da grade aquela apresentada na figura 10. Nesta figura pode-se determinar a(s) principal(is) camada(s) na qual(is) o sistema deve atuar para apresentar as características funcionais

solicitadas. A tabela 5 apresenta a relação entre características funcionais dos sistemas de C2 demandadas do PEM e PCD e as principais camadas de infraestrutura de grade:

TABELA 5
Relação entre Características Funcionais dos Sistemas de C2 Demandadas do PEM e PCD e Principais Camadas Atuantes da Infraestrutura de Grade

Característica Funcional dos Sistemas de C2	Camada da Infraestrutura de Grade
Possuir reconhecida segurança cibernética tanto pela MB como pelo MD.	Todas as camadas, incluindo a infraestrutura de "Garantia da Informação" e o serviço de "Suporte e Segurança de Operações de Rede"
Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências, nacionais e estrangeiras.	"Aplicativos, Serviços e Informações"; e "Serviços Corporativos Centrais";
Permitir eficaz troca de dados com outros órgãos do MD por meio de criptografia a ser estabelecida por aquele ministério.	"Aplicativos, Serviços e Informações"
Possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira.	"Comunicação"
Ser facilmente aperfeiçoável, de forma a permitir acompanhamento eficaz da evolução da tecnologia da informação e das novas concepções de comando e controle.	"Aplicativos, Serviços e Informações"; e "Serviços Corporativos Centrais";

Fonte: autor

Observando a tabela 5 pode-se fazer uma primeira aproximação de ações necessárias. As maiores demandas do PEM e PCD recaem sobre as camadas de "Aplicativos, Serviços e Informações" e "Serviços Corporativos Centrais". Isto significa que os esforços de criação e adaptação de sistemas de C2 devem se concentrar em melhorias nos aplicativos, seus bancos de dados e nos serviços corporativos (serviços de diretório, de descoberta, de colaboração, de mensagens entre máquinas, de autenticação de usuários, de políticas de acesso, de mediação, e outros) disponibilizados na rede de atuação destes sistemas.

Na Marinha, a melhoria de serviços corporativos é importante para implantação de serviços na CES da Rede de Comunicações Integradas da Marinha (RECIM), o que permitirá o emprego de arquitetura SOA no espaço cibernético da MB, como é o caso dos serviços de descoberta e de publicação de serviços, ainda inexistentes (ANDRADE, 2013).

Continuando a observar a tabela 5, nota-se que os canais de comunicação devem ser revistos quanto ao alcance a plataformas isoladas. As demais camadas devem ter atuação concentrada em aspectos de segurança.

4.2 DEMANDAS TÉCNICAS

A partir da identificação das infraestruturas sistêmicas a serem trabalhadas, vistas na seção 4.1, e à luz dos conceitos de interoperabilidade expostos no capítulo 3, pode-se definir de forma mais clara as características técnicas que estão sendo demandadas pelo PEM e PCD. Tais características estão consolidadas na tabela 6.

TABELA 6
Relação entre Características Funcionais dos Sistemas de C2 Demandadas do PEM e PCD e Respectivas Características Técnicas

Característica Funcional dos Sistemas de C2	Camada da Infraestrutura de Grade	Característica Técnica
Possuir reconhecida segurança cibernética tanto pela MB como pelo MD.	Todas as camadas, incluindo a infraestrutura de "Garantia da Informação" e o serviço de "Suporte e Segurança de Operações de Rede"	Ser compatível com as normas de segurança cibernética fixadas pela MB e aquelas a serem estabelecidas pelo MD. Estas normas devem ter abrangência total na grade de operação dos sistemas, abordando aspectos das infraestruturas de garantia de informação, de comunicação, de computação, de serviços corporativos, assim como os serviços disponibilizados por aplicativos, bancos de dados, IHM e o serviço de suporte e segurança de operações de rede.
Permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências, nacionais e estrangeiras.	"Aplicativos, Serviços e Informações"; e "Serviços Corporativos Centrais";	Ajustar e projetar aplicativos, bancos de dados e serviços corporativos de rede para operarem com máxima disponibilização de canais de acesso e entrega de informação, empregando formatos de dados padronizados por especificações internacionalmente adotadas.
Permitir eficaz troca de dados com outros órgãos do MD por meio de criptografia a ser estabelecida por aquele ministério.	"Aplicativos, Serviços e Informações"	Prever a inclusão de um futuro serviço de criptografia proprietária do MD, obedecendo uma arquitetura SOA, a ser disponibilizado na camada de "aplicativos, serviços e informações" na arquitetura corporativa da Marinha.

Possibilitar eficaz troca de dados com plataformas isoladas e muito distantes da costa brasileira.	"Comunicação"	Reforçar o emprego do canal satelital na infraestrutura de comunicação, trafegando serviços que apresentem bom desempenho em banda típicas satelitais, como 512 kbps.
Ser facilmente aperfeiçoável, de forma a permitir acompanhamento eficaz da evolução da tecnologia da informação e das novas concepções de comando e controle.	"Aplicativos, Serviços e Informações"; e "Serviços Corporativos Centrais";	Aumentar gradativamente a interoperabilidade entre sistemas no rumo de arquiteturas SOA e CBA na rede corporativa da Marinha, concentrando a implantação de novos códigos somente na camada de “aplicativos, serviços e informações”, e reforçando a infraestrutura de “serviços corporativos centrais”, de forma a facilitar ao máximo o aperfeiçoamento e o acesso a novas funcionalidade nos sistemas de C2.

Fonte: autor

A partir da identificação das características técnicas demandadas do PEM e PCD, apresentadas na tabela 6, pode-se aplicar o TRM para identificar as principais áreas, categorias e padrões de serviços associados a essas características. A tabela 7 apresenta estas informações.

TABELA 7

Relação entre Características Técnicas dos Sistemas de C2 Demandadas do PEM e PCD e Respectivas Áreas, Categorias, e Padrões de Serviços do TRM

Característica Técnica	Áreas de Serviços	Categorias de Serviços	Padrões de Serviços
Ser compatível com as normas de segurança cibernética fixadas pela MB e aquelas a serem estabelecidas pelo MD. Estas normas devem ter abrangência total na grade de operação dos sistemas, abordando aspectos das infraestruturas de garantia de informação, de comunicação, de computação, de serviços corporativos, assim como os serviços disponibilizados por aplicativos, bancos de dados, IHM e o serviço de suporte e segurança de operação de rede.	Todas as quatro áreas, com ênfase em: acesso e entrega, e estrutura de componente	Todas as categorias, com ênfase em: segurança, canais de acesso, e canais de entrega	Em cada categoria deve ser estudado que padrões de serviço merecem atenção de segurança. Destacam-se os serviços de: certificação digital, assinatura digital, apoio a segurança, navegadores WEB, rede sem fio, acesso a dispositivos portáteis, internet, intranet, e redes privadas virtuais
Ajustar e projetar aplicativos, bancos de dados e serviços corporativos de rede para operarem com máxima disponibilização de canais de acesso e entrega de informação, empregando	acesso e entrega, estrutura de componente, e interface e	canais de acesso, canais de entrega, requisitos de serviço, transporte de serviço,	navegação na WEB, comunicações de colaboração, internet, intranet, P2P, VPN, autenticação,

formatos de dados padronizados por especificações internacionalmente adotadas.	integração	intercâmbio de dados, gerenciamento de dados, integração, interoperabilidade e interface	transporte, troca de dados, conectividade de banco de dados, acesso a banco de dados, "middleware", formato de dados, transformação de dados, descoberta de serviço, descrição de serviço / interfaceamento
Prever a inclusão de um futuro serviço de criptografia proprietária do MD, obedecendo uma arquitetura SOA, a ser disponibilizado na camada de "aplicativos, serviços e informações" na arquitetura corporativa da Marinha.	estrutura do componente	segurança	apoio de segurança
Reforçar o emprego do canal satelital na infraestrutura de comunicação, trafegando serviços que apresentem bom desempenho em banda típicas satelitais, como 512 kbps.	plataforma e infraestrutura	infraestrutura de hardware	comunicações satélite
Aumentar gradativamente a interoperabilidade entre sistemas no rumo de arquiteturas SOA e CBA na rede corporativa da Marinha, concentrando a implantação de novos códigos somente na camada de "aplicativos, serviços e informações", e reforçando a infraestrutura de "serviços corporativos centrais", de forma a facilitar ao máximo o aperfeiçoamento e o acesso a novas funcionalidade nos sistemas de C2.	interface e integração	integração, interoperabilidade, e interface	"middleware", acesso a banco de dados, processamento de transação, "object request broker", integração de aplicações corporativas, formato de dados / classificação, tipos de dados / validação, transformação de dados, descoberta de serviço, descrição de serviço / interfaceamento

Fonte: autor

A partir da última coluna da tabela 7, tem-se o conjunto de padrões de serviço que devem ter suas especificações técnicas bem definidas e padronizadas para todos os sistemas que necessitarão fazer uso delas. Para se escolher que especificação(ões) técnica(s) a empregar, deve-se escolhê-la(s) dentro de uma lista internacionalmente aceita de tecnologias amadurecidas e empregadas em sistemas de C2, como a constante do DISR, ou do JTA. No caso de empregar o JTA, deve-se ter o cuidado de verificar se aquela tecnologia já não foi

substituída por outra mais recente, lembrando que o JTA é de 2003. Por exemplo, suponha que se queira especificar um serviço no padrão de serviços "comunicações de colaboração". O serviço escolhido é o de correio eletrônico. Consultando o JTA, poder-se-ia utilizar o padrão técnico da "Internet Engineering Task Force" (IETF) "IETF RFC 2821, Simple Mail Transfer Protocol - SMTP", para transporte de mensagens, e o "IETF RFC 2822 Internet Message Format" para o formato das mensagens de médio grau de garantia de segurança. Neste exemplo foram utilizadas duas especificações técnicas para um dos serviços (correio eletrônico) de um padrão de serviços (comunicações de colaboração).

Como pode ser verificado, o volume de padrões a se especificar é muito grande, mas muito importante de ser feito. Desta forma se garante especificações técnicas comuns para um desenvolvimento uniforme de sistemas, independente do desenvolvedor, com a garantia que os sistemas serão interoperáveis entre si e com o resto do mundo.

Os sistemas legados também se beneficiam do emprego de especificações padronizadas. Para suas eventuais adaptações deve-se empregar estruturas como a da figura 14. Lembrando que as cores das áreas de serviços e os nomes das categorias na figura 14 chamam a atenção dos padrões de serviços que deverão ser introduzidos para fazer o interfaceamento.

5. SUGESTÕES PARA ESTRUTURAÇÃO DOS SISTEMAS DE C2 NA MB

As características técnicas e padrões de serviço a serem incentivados na grade onde atuam os sistemas de C2 da MB, obtidos no capítulo 4, orientarão as sugestões para estruturação desses sistemas. Os conceitos de interoperabilidade, apresentados no capítulo 3, serão largamente empregados.

As sugestões serão divididas em 4 seções. A primeira seção tratará de sugestões para se obter regulações necessárias para suportar maior interoperabilidade. A segunda seção será dedicada a melhorar as infraestruturas de comunicação, computação e serviços corporativos centrais. A terceira seção abordará sugestões para desenvolvimento de novos sistemas, enquanto a quarta sugerirá ações nos sistemas legados. O quadro do APÊNDICE A apresenta uma compilação resumida das sugestões.

5.1 SUGESTÕES SOBRE REGULAÇÕES

Conforme foi visto na seção 2.2, a PCD é um documento estratégico, criado no final de 2012, que emanou 9 objetivos com 52 diretrizes cibernéticas decorrentes. Tais diretrizes carecem de esforços adicionais a serem estabelecidos pelo MD, como normatizações mais detalhadas, definição de programas, doutrinas e desenvolvimento de padrões criptográficos. Tais esforços serão chamados genericamente de regulações, que condicionarão os sistemas de TI das três Forças Singulares, principalmente os de C2. Neste contexto, surgem as primeiras sugestões de estruturação dos sistemas de C2:

- 1) MB participar ativamente, com pessoal tecnicamente qualificado em TI, junto ao MD na elaboração das regulações;

- 2) buscar o máximo de alinhamento na elaboração das regulações do MD com as regulações já existentes na MB e que estejam de acordo com este trabalho, visando facilitar o aumento da interoperabilidade entre sistemas de C2 das Forças Singulares e do próprio MD;
- 3) rever as publicações estratégicas de TI da MB inserindo orientações quanto ao cumprimento de regulações específicas do MD, assim como orientar o emprego de uma governança por arquitetura, onde um modelo de arquitetura corporativa da MB deve ser idealizado;
- 4) revisar a coletânea de publicações técnicas de TI da MB que atendam os níveis operacional e tático, em sintonia com as regulações específicas do MD e com o modelo de arquitetura corporativa idealizado para a MB; e
- 5) na ausência das regulações específicas do MD, adotar as publicações do DoD (GIG, DoDAF, TRM, JTA) como base para a criação ou revisão dos documentos da MB. São documentos de referência mundial, usados pelos EUA e países da OTAN. Neste contexto deve-se envidar esforços junto ao governo dos EUA para permitir o acesso ao DISR, de forma a especificar as melhores tecnologias para emprego em um certo padrão de serviço.

5.2 SUGESTÕES SOBRE INFRAESTRUTURAS

Imaginando o espaço cibernético da MB como uma estrutura de grade, onde a visão sistêmica da figura 10 pode ser aplicada, as sugestões aqui referem-se às infraestruturas de comunicação, de computação e de serviços corporativos centrais (CES). Para facilitar a identificação das sugestões, suas numerações continuarão a ordem sequencial da seção anterior. Seguem as mesmas:

- 6) idealizar uma arquitetura corporativa para MB, com abordagens SOA e CBA, para ser empregada na governança por arquitetura proposta na sugestão 3. Tal arquitetura deve se espelhar na GIG do DoD, pois, além de favorecer o trabalho colaborativo e a interoperabilidade no espaço cibernético dentro de um modelo mundialmente referenciado, seu uso facilitaria muito o trabalho de integração de sistemas de C2 da MB com outros sistemas mundiais;
- 7) estabelecer o uso obrigatório do protocolo IP como base no transporte de informações para todos os sistemas de C2 a serem empregados no espaço cibernético da MB. Os novos sistemas deverão ter este aspecto nas especificações de obtenção, assim como os sistemas legados que eventualmente não atendam a este protocolo deverão se adaptar para atendê-lo;
- 8) ter preocupação constante com o aumento da velocidade de comunicação de dados ("baud rate" ou banda) das estruturas de rede que conectam os sistemas de C2 com seus usuários, principalmente o "backbone"¹⁹ da RECIM. A arquitetura SOA privilegia a troca intensa de informações entre componentes do espaço cibernético que podem estar em localidades bem afastadas, necessitando de uma rede de alta velocidade para garantir desempenho eficiente;
- 9) implementar serviços que permitam o emprego da arquitetura SOA na infraestrutura de CES da RECIM, como os serviços de descoberta e de publicação de serviços;

¹⁹ Backbone é o segmento principal de uma WAN que interliga várias redes metropolitanas ou locais dispersas geograficamente. Normalmente é um trecho de alta velocidade da WAN em virtude do elevado fluxo de pacotes de dados que conduz. Seu nome é uma alusão à espinha dorsal dos vertebrados, que conduz a enervação principal da distribuição nervosa nesses animais.

- 10) instalar componentes de um mesmo sistema de C2, com alta troca de informações entre si, o mais próximos possíveis no espaço cibernético. Se possível na mesma máquina física;
- 11) implantar o serviço de comunicação satélite, verificando constantemente a possibilidade de aumento de banda do mesmo nos navios, principalmente os de maior deslocamento e aqueles menores que operam constantemente afastados da costa ou escoteiros; e
- 12) implantar redundância nos serviços pertencentes às áreas de "acesso e entrega" e "interface e integração" (vide figura 12). Pela importância para todos os sistemas de C2 dos 23 padrões de serviço que compõem estas áreas, eles têm que dispor de redundâncias, de preferência em máquinas e localidades diferentes no espaço cibernético da MB.

5.3 SUGESTÕES SOBRE NOVOS SISTEMAS

As sugestões aqui visam ações a serem tomadas antes da obtenção de novos sistemas de C2 para a MB. A numeração seguirá a ordem sequencial interrompida na seção anterior. Abrir-se-á uma seção específica para o SisGAAz em função da importância que este sistema possui para a MB. Seguem as sugestões:

- 13) identificar os sistemas de informação que operarão conjuntamente com o novo sistema de C2, mapeando seus serviços no modelo TRM. O mapeamento facilitará a visualização das especificações técnicas que o sistema de C2 terá de atender ou interagir;

- 14) garantir que as características técnicas preceituadas pelo PEM e PCD, com seus respectivos padrões de serviço associados, constantes da tabela 7, estejam presentes na especificação do novo sistema de C2 a ser obtido; e
- 15) listar as especificações técnicas que o novo sistema de C2 deve atender em forma de tabela, com divisões por área, categoria e padrões de serviço, conforme preceituado no TRM. É uma forma completa de não esquecer a especificação de nenhum serviço, assim como documentá-los de forma tabular.

5.3.1 SisGAAz

O Sistema de Gerenciamento da Amazônia da Azul (SisGAAz) está sendo concebido para ser um sistema de C2 para monitoração, controle e proteção das águas adjacentes ao litoral brasileiro que compõem a Amazônia Azul. O SisGAAz funcionará integrado a outros sistemas dentro e fora da MB. Internamente à Marinha, destacam-se o SISNC2 e o SISTRAM, que convergem informações de outros sistemas como o "Long Range Identification and Tracking" (LRIT), o "Automatic Identification System" (AIS), e o Programa Nacional de Rastreamento de Embarcações Pesqueiras (PREPS). Fora da MB, o SisGAAz se integrará com sistemas de C2 relacionados à defesa nacional, como o SISMC2 do MD, o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), do Exército Brasileiro (EB), o Sistema de Defesa Aeroespacial Brasileiro (SISDABRA), da Força Aérea Brasileira (FAB). Também se integrará a sistemas de instituições não pertencentes à defesa nacional como aquelas ligadas aos Ministérios da Fazenda, Transporte, Minas e Energia, Ciência e Tecnologia, Justiça e outros, além de agências reguladoras e empresas (exemplo: Petrobras). Como se não bastasse esse nível de integração, o SisGAAz também deverá receber

dados diretamente de diversas fontes como: radares além do horizonte (OTHR), aeronaves de patrulha marítima da FAB, veículos aéreos não-tripulados (VANT) e outros (PESCE, 2012).

Considerando a diversidade de informação, a necessidade de integração e a variedade de sistemas interagentes, o SisGAAz é um sistema típico para operar em um espaço cibernético com arquitetura SOA, empregando conceito de GIG prevendo o máximo nível de interoperabilidade. Sendo assim, seguem as sugestões:

16) SisGAAz: ser desenvolvido considerando a necessidade de operar em ambiente de rede que obedeça a arquitetura SOA com nível máximo de interoperabilidade, isto é, nível "corporativo"; e

17) SisGAAz: implantar serviços na RECIM na infraestrutura de serviços corporativos centrais para permitir a operação de sistemas em arquitetura SOA, como serviços de descoberta e descrição. Neste aspecto, devem-se disponibilizar serviços e padronizar especificações de todos os padrões de serviço relacionados à área de “interface e integração” do TRM, em sintonia com o cronograma de desenvolvimento do SisGAAz.

5.4 SISTEMAS LEGADOS

Os sistemas legados caracterizam-se por serem sistemas importantes para a Marinha e que foram desenvolvidos empregando tecnologias de gerações anteriores. Desta forma, as sugestões serão voltadas para aumentar a integração desses sistemas com os demais. Serão feitas sugestões gerais que se aplicam a qualquer sistema legado e sugestões específicas para o SISTRAM e o SISNC2 em função do nível de importância que têm para a Marinha. Seguem as sugestões:

- 18) mapear pelo modelo do TRM os serviços disponíveis no sistema legado em questão para se ter uma visão técnica dos mesmos, facilitando o estudo de incremento de interoperabilidade;
- 19) empregar o modelo ISIMM (ou LISI como segunda opção) para medir o nível inicial de interoperabilidade (baseline) do sistema legado com seus sistemas contraparte. Em seguida, com o mesmo modelo, definir o nível de interoperabilidade alvo desejado. Por fim, estabelecer um cronograma de aumento gradual do nível de interoperabilidade, de forma a atingir o nível alvo. Considerar prazos exequíveis, tendo em vista os investimentos em tecnologia e desenvolvimentos necessários;
- 20) para interfaceamento com componentes de ambiente externo, desenvolver interfaces de acesso empregando a representação em topologia de rede do TRM, conforme figura 14; e
- 21) ao usar serviços web para troca dados com outros sistemas, como na troca de dados por arquivos XML, empregar protocolos seguros, como o "Hypertext Transfer Protocol Secure" (HTTPS) ao invés do HTTP.

5.4.1 SISTRAM

O Sistema de Informações sobre o Tráfego Marítimo, SISTRAM, tem como propósito o acompanhamento e monitoramento de embarcações, nacionais e estrangeiras, que navegam na área de busca e salvamento (SAR) brasileira. Para tanto o SISTRAM dispõe de recursos de apresentação geográfica de contatos (mercantes, navios de guerra, pesqueiros) recebidos de diferentes fontes como: próprias embarcações, meios navais e aéreos em patrulha naval, e outros sistemas de acompanhamento de tráfego marítimo. Em sua última versão, o

SISTRAM IV é capaz de interfacear com os seguintes sistemas e redes: LRIT, AIS, PREPS, Sistema de Monitoramento Marítimo de Apoio a Atividades de Petróleo (SIMMAP), "Maritime Safety and Security Information System" (MSSIS) e "Trans-Regional Maritime Network" (T-RMN). O SISTRAM IV ainda recebe, processa e apresenta informações advindas de mensagens do *Plano de Coordenação da Defesa do Tráfego Marítimo Interamericano* (mensagens RAINFORM), do *Posto de Controle de Entrada de Porto* do Rio de Janeiro (mensagens PCEP), e de informações de atracação e desatracação dos navios mercantes (mensagens MOVMEC). O SISTRAM também fornece dados para o SISNC2, permitindo com isso uma conexão indireta ao SISNC2 das diversas fontes de dados que alimentam o SISTRAM. (CUNHA, 2006; DAVID, 2013; FONSECA, 2013).

Observa-se que o SISTRAM IV necessita interagir com muitos sistemas, cujos servidores encontram-se dentro e fora da Marinha, e que podem estar enquadrados como legados. Dentre os níveis de interoperabilidade apresentados na seção 3.1.1, o SISTRAM IV opera em 3 níveis distintos, dependendo do sistema com o qual interage. Quando é alimentado de contatos detectados por meios navais, a injeção normalmente é manual. Neste caso está operando no nível 0, "isolado". Quando recebe dados do PREPS, SIMMAP, AIS e MSIS, o faz por intermédio de FTP de arquivos texto, operando assim no nível 1, "conectado". Também opera no nível "conectado" quando fornece dados para o SISNC2. Já com sistemas desenhados para operarem na internet, como o LRIT e o T-RMN, este último se destacando o "Virtual-Regional Maritime Traffic Centre" (VRMTC) italiano, há uma troca por serviço web de arquivos XML, operando desta forma no nível 2, "funcional" (DAVID, 2013).

O volume de informações de embarcações processadas pelo sistema vem aumentando expressivamente nos últimos anos. Em 2010 foram 2.400.000, em 2011 3.600.000 (aumento de 50% em relação ao ano anterior) e em 2012 foram 5.600.000 (aumento de 56%) (FONSECA, 2013). Isto se deve a 2 fatores. O primeiro refere-se ao

recebimento de dados por conectividade a outros sistemas estabelecida nos últimos anos, como ao AIS e T-RMN. O segundo está ligado ao aumento da atividade marítima na costa brasileira. Segundo o Anuário Estatístico da Marinha de 2012, o fornecimento de cartas náuticas aumentou de 20.654, em 2010, para 39.156, em 2011, representando um aumento de 90% em 1 ano (BRASIL, 2011).

Considerando o expressivo aumento na demanda de informações no SISTRAM e o fato de que ele será um importante elo com o SisGAAz em futuro próximo, seguem as sugestões:

- 22) SISTRAM: aumentar o nível de interoperabilidade do sistema para "funcional" na troca de dados com todos os sistemas, e dispor de serviços que permitam operá-lo no nível "corporativo", quando interagindo com sistemas da MB, como o SISNC2 e o SisGAAz; e
- 23) SISTRAM: no serviço de gerenciamento de dados procurar utilizar um Sistema Gerenciador de Banco de Dados (SGBD) considerado referência em uso por sistemas de controle de tráfego marítimo internacionais. Tal SGBD deverá ser o mesmo empregado pelo SisGAAz para agilizar a rápida troca de dados entre estes sistemas no futuro.

5.4.2 SISNC2

O Sistema Naval de Comando e Controle (SISNC2) é o principal sistema de C2 da MB. Operado a partir do Centro de Comando do Teatro de Operações Marítimas (CCTOM), o sistema é empregado para acompanhamento das forças, dos meios navais e de embarcações selecionadas, apresentando um quadro estratégico-operacional, marítimo ou

fluvial, para auxílio no planejamento, no processo de tomada de decisão e no controle da ação planejada das operações navais (VIVEIROS, 2007).

O SISNC2 possui o serviço de processamento de dados provido pelo Sistema de Apresentação Gráfico e Banco de Dados (SAGBD), que se encontra desde 2006 operando em sua versão 3. Para desempenhar suas atividades, o SAGBD troca dados com os meios navais e aeronavais da MB, com o SAETE, com o SISTRAM e com o Sistema de Planejamento Operacional Militar (SIPLOM), sendo este último o sistema de processamento de dados do SISMC2, empregado e operado pelo MD. O recebimento de dados pelo SAGBD referentes aos meios navais e aeronavais se dá no início de uma operação, por meio de injeção manual das informações constantes na diretiva desta operação. Neste ponto o SAGBD opera no nível 0 ("isolado") de interoperabilidade. Com o desenrolar das operações o SAGBD estabelece uma conexão P2P com o sistema SAETE do navio capitânia e obtém um arquivo texto com os dados dos meios navais registrados no SAETE. Opera, assim, com o SAETE em uma conexão nível 1 ("conectado"). O SAGBD, também opera com o SISTRAM em conexão nível 1 ("conectado"), obtendo dados daquele sistema por meio de um arquivo texto disponibilizado no servidor do SISTRAM. Da mesma forma, o SAGBD opera em outra conexão nível 1 ("conectado"), quando fornece dados para o SIPLOM. A diferença é que o SAGBD passa para o SIPLOM um arquivo XML, contudo por uma conexão P2P em protocolo FTP (SILVEIRA, 2013).

Em relação às opções de interoperabilidade, o SAGBD ainda não se interconecta automaticamente com os sistemas da Diretoria de Portos e Costas (DPC), o que dificulta a inserção de dados do Sistema de Segurança do Tráfego Aquaviário (SSTA) no sistema. (SILVEIRA, 2013). Outra restrição de interoperabilidade diz respeito à conexão com o SIPLOM, que já poderia operar em nível 2 ("funcional"), ou até superior. Contudo, a interoperabilidade dos sistemas de C2 das três Forças Singulares com o SIPLOM depende da

aprovação por parte do MD do projeto de "Interoperabilidade de Sistemas de C2" (INTERC2), desenvolvido pelo CASNAV, em fase de estudos no ministério (COLLAZO, 2013).

Considerando que o SISNC2, o qual contém o SAGBD, poderá ser o principal sistema do futuro SisGAAz (PESCE, 2012) e a importância cada vez maior dos compartilhamentos de informações de C2 para os meios navais, seguem as sugestões:

- 24) SAGBD: aumentar o nível de interoperabilidade do sistema para "funcional", em conexão segura, quando trocando dados com o SAETE, da MB, e SIPLOM, do MD. Dispor de serviços que permitam operá-lo no nível "corporativo", quando interagindo com o SISTRAM e o futuro SisGAAz;
- 25) SAGBD: Expandir a interoperabilidade do sistema para oferecer conexão segura (HTTPS ou similar) em nível "funcional" com sistemas da DPC;
- 26) SAGBD: no serviço de gerenciamento de dados procurar utilizar um SGBD moderno, com formatação de dados de ampla utilização em forças internacionais de referência. Tal SGBD deverá ser o mesmo empregado pelo SisGAAz para agilizar a rápida troca de dados entre os sistemas no futuro; e
- 27) SAGBD: envidar esforços junto ao MD para avanços no projeto INTERC2, de forma a permitir que não somente o SAGBD possa aumentar o nível de interoperabilidade com o SIPLOM, mas também que os sistemas de C2 do EB e da FAB também possam fazê-lo, permitindo até que esses sistemas troquem dados diretamente com o SAGBD. Este seria um grande avanço no futuro da interoperabilidade de operações conjuntas.

6. CONCLUSÃO

O trabalho comprovou que tanto o PEM como a PCD impõem a necessidade de reestruturação nos sistemas de C2 da MB, de forma a atender às novas características funcionais apontadas na seção 2.3. Dentre essas características destaca-se a necessidade de permitir fácil e eficaz interoperabilidade com vários tipos de sistemas de C2 empregados por outras Forças Armadas e grandes agências, nacionais e estrangeiras.

O surgimento de modelos de maturidade de interoperabilidade, a exemplo do ISIMM, desenvolvido de forma criativa e simples por cientistas da Namíbia, apresentado na seção 3.1.2, traz uma forma de avaliar metodicamente o nível de interoperabilidade de sistemas legados. Mais ainda, oferece uma forma objetiva de estabelecer um cronograma de metas para evoluir a interoperabilidade de sistemas como o SISTRAM e SISNC2. As ações da sugestão 19 da seção 5.4 exploram o emprego do modelo de interoperabilidade dando uma perspectiva interessante para modernização dos sistemas.

A importância da governança por arquitetura SOA e CBA, a partir de um projeto de compartilhamento de componentes, se mostra fundamental para o empreendimento de colaborações e integração de sistemas de C2 nos dias atuais, conforme abordado na seção 3.2. Neste aspecto, o conceito de GIG, da seção 3.3, surge e se mostra como uma orientação de estruturação do espaço cibernético da MB, convergindo com as recentes evoluções internacionais nos conceitos de integração de informações de comando e controle.

Outro aspecto importante é transformar características funcionais operativas em características técnicas para balizar o planejamento de um sistema. Neste ponto, a mudança de visão dos sistemas de C2, de operativa para sistêmica, conforme apresentado na seção 3.4, se mostra fundamental. Em sequência, o emprego de um modelo de referência técnica, como o TRM, abordado na seção 3.5, no mapeamento de sistemas de C2, viabiliza uma visão técnica

dos mesmos e permite uma abordagem pragmática de padrões de serviços a serem trabalhados para desenvolver as características técnicas levantadas. Assim, o modelo TRM se mostra como importante ferramenta tanto na especificação de novos sistemas como na modernização de sistemas legados, sendo empregado em algumas sugestões do capítulo 5.

De forma a melhor visualizar as 27 sugestões de reestruturação dos sistemas de C2, expostas no capítulo 5, o APÊNDICE A retrata um mapa sintético das mesmas, onde merece importante destaque aquelas relacionadas à infraestrutura do espaço cibernético da MB, base para a interoperabilidade de sistemas.

Realça-se, igualmente, a necessidade de se modernizar a infraestrutura de CES da RECIM, conforme sugestão nove, em paralelo com a modernização de sistemas legados, como o SISTRAM e o SISNC2 (SAGBD), sugestões de 22 a 27. O cronograma dessas melhorias também deverá estar em sintonia com o desenvolvimento de novos sistemas de grande importância, como o SisGAAz (sugestões 16 e 17), para que haja sinergia na modernização.

Por fim, as sugestões deste trabalho servem como diretrizes para ações técnicas mais aprofundadas. Tais ações exigem estudos detalhados, caso a caso, das tecnologias específicas aplicadas em determinados sistemas que interagem entre si e com o segmento de rede que os conectam, fugindo do escopo de um trabalho de nível estratégico. Contudo, o autor acredita que a visualização das sugestões aqui colocadas como diretrizes, em muito facilitará a reestruturação dos sistemas de C2 da MB, de forma a aumentar sobremaneira a velocidade e a qualidade das informações tanto no nível do planejamento estratégico quanto nos níveis dos decisores operacionais e combatentes táticos.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDRADE, Marcus Rogers Cavalcante. Encarregado da Divisão de Infraestrutura do Centro de Dados da Marinha no Centro de Tecnologia da Informação da Marinha. Rio de Janeiro, 12 jul. 2013. Entrevista concedida a Rogério Corrêa Manso.

BRASIL. Marinha do Brasil. Diretoria de Administração da Marinha. **Anuário Estatístico da Marinha - 2011**. Rio de Janeiro, 39ª ed., p. 186, 2011.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Plano Estratégico da Marinha - EMA 300 - Volume I - 2ª revisão: capítulo 6**. Brasília, 2008.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. **Doutrina de Tecnologia da Informação da Marinha (Manual de Guerra Cibernética Volume II)**. Brasília, 2013.

BRASIL. Ministério da Defesa. **Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012. Aprova a Política Cibernética de Defesa (PCD) - MD31-P-02**. Brasília, 2012.

COLLAZO, Rodrigo Abrunhosa. Gerente do Projeto SIPLM do Centro de Análise de Sistemas Navais. Rio de Janeiro, 10 jul. 2013. Entrevista concedida a Rogério Corrêa Manso.

CUNHA, Edmundo Augusto dos Reis Monteiro da. SISTRAM: A Evolução de um Sistema de Apoio ao SAR para uma Ferramenta de C²I. **Revista Passadiço**, Rio de Janeiro, p. 16-19, 2006.

DAVID, Roberto Barbosa; PORTHUN, Ana Lúcia Mesiano. Gerência do Projeto SISTRAM IV do Centro de Análise de Sistemas Navais. Rio de Janeiro, 10 jul. 2013. Entrevista concedida a Rogério Corrêa Manso.

EUA. Department of Defense. **C4ISR Architecture Framework Version 2.0**. Washington, DC, 1997a. Disponível em: < <http://www.afcea.org/education/courses/archfwk2.pdf>>. Acesso em: 06 jun. 2013.

EUA. Department of Defense. **Department of Defense Global Information Grid Architectural Vision**. Washington, DC, 2007. Disponível em: <http://www.msco.mil/documents/_7_GIG%20Architectural%20Vision%20-%20200706%20v1.0.pdf>. Acesso em: 09 jun. 2013.

EUA. Department of Defense. **DoD Architecture Framework Version 2.0**. Washington, DC, 1997b. Disponível em: < <http://www.afcea.org/education/courses/archfwk2.pdf>>. Acesso em: 06 jun. 2013.

EUA. Department of Defense. **DoD Enterprise Architecture Technical Reference Model**. Washington, DC, 2005. Disponível em: < http://ce.sharif.edu/courses/87-88/1/ce448/resources/root/EIAP-methodologies-references-models/DOD_TRM_V0.4_10Aug.pdf>. Acesso em: 06 jun. 2013.

EUA. Department of Defense. **Joint Levels of Information Systems Interoperability (LISI)**. Washington, DC, 1998. Disponível em: <http://www.eng.auburn.edu/~hamilton/security/DO_DAF/LISI.pdf>. Acesso em: 03 jun. 2013.

EUA. Department of Defense. **Joint Technical Architecture -Volume I - Version 6.0**. Washington, DC, 2003. Disponível em: <<http://www.acq.osd.mil/osjtf/pdf/jta-vol-I.pdf>>. Acesso em: 04 jun. 2013.

EUA. Executive Office of the President of United States. **The Common Approach to Federal Enterprise Architecture**. Washington, DC, 2012. Disponível em: <http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/common_approach_to_federal_ea.pdf>. Acesso em: 10 jun. 2013.

FONSECA, Luiz Fernando Palmer. **O Comando de Operações Navais e a Diretoria Geral de Navegação**. Rio de Janeiro, 2013. Palestra proferida para o Curso de Política e Estratégia Marítimas, na Escola de Guerra Naval, em 21 jun. 2013.

PESCE, Eduardo Italo; CARNEIRO, Mario Roberto Vaz. SisGAAz: monitorando e protegendo a Amazônia Azul. **Segurança e Defesa**, Rio de Janeiro, v.107, p. 04-10, 2012.

PETRITSCH, Helmut. **Service-Oriented Architecture (SOA) vs. Component Based Architecture**. Viena, Austria: Vienna University of Technology, 2006. Disponível em: <http://petritsch.co.at/download/SOA_vs_component_based.pdf>. Acesso em: 16 jun. 2013.

SILVEIRA, Maurício Pires Malburg da. Encarregado da Divisão de Tecnologia da Informação do Comando de Operações Navais. Rio de Janeiro, 10 jul. 2013. Entrevista concedida a Rogério Corrêa Manso.

STADEN, Stefanus Van; MBALE, Jameson. The Information System Interoperability Maturity Model (ISIMM): Towards Standardizing Technical Interoperability and Assessment within Government. **International Journal of Information Engineering and Electronic Business**. Modern Education & Computer Science Publisher, Online, v. 2012-5, p. 36-41, 2012. Disponível em: <<http://www.mecs-press.org/ijieeb/ijieeb-v4-n5/IJIEEB-V4-N5-5.pdf>>. Acesso em: 11 jun. 2013.

VIVEIROS, Cláudio Portugal de. **Fatores de Comando e Controle Aplicáveis nas Operações Combinadas: O Sistema Militar de Comando e Controle**. 2007. 67 f. Monografia (Curso de Política e Estratégia Marítimas) - Escola de Guerra Naval, Rio de Janeiro, 2007.

APÊNDICE A: QUADRO RESUMO DE SUGESTÕES PARA ESTRUTURAÇÃO DE SISTEMAS DE C2 NA MB

Seção	Num	Sugestão
Regulações	01	MB participar ativamente, com pessoal tecnicamente qualificado em TI, junto ao MD na elaboração das regulações.
	02	Buscar o máximo de alinhamento na elaboração das regulações do MD com as regulações já existentes na MB e que estejam de acordo com este trabalho, visando facilitar o aumento da interoperabilidade entre sistemas de C2 das Forças Singulares e do próprio MD.
	03	Rever as publicações estratégicas de TI da MB inserindo orientações quanto ao cumprimento de regulações específicas do MD, assim como orientar no seguimento de uma governança por arquitetura, onde um modelo de arquitetura corporativa da MB deve ser idealizado.
	04	Revisar a coletânea de publicações técnicas de TI da MB que atendam os níveis operacional e tático, em sintonia com as regulações específicas do MD e com o modelo de arquitetura corporativa idealizado para a MB.
	05	Na ausência das regulações específicas do MD, adotar as publicações do DoD (GIG, DoDAF, TRM, JTA) como base para a criação ou revisão dos documentos da MB. São documentos de referência mundial, usados pelos EUA e países da OTAN. Neste contexto deve-se envidar esforços junto ao governo dos EUA para permitir o acesso ao DISR, de forma a especificar as melhores tecnologias para emprego em um certo padrão de serviço.
Infraestruturas de comunicação, de computação e de serviços corporativos centrais (CES)	06	Idealizar uma arquitetura corporativa para MB, com abordagens SOA e CBA, para ser empregada na governança por arquitetura proposta na sugestão 3. Tal arquitetura deve se espelhar na GIG do DoD, pois, além de favorecer o trabalho colaborativo e a interoperabilidade no espaço cibernético dentro de um modelo mundialmente referenciado, seu uso facilitaria muito o trabalho de integração de sistemas de C2 da MB com outros sistemas mundiais.
	07	Estabelecer o uso obrigatório do protocolo IP como base no transporte de informações para todos os sistemas de C2 a serem empregados no espaço cibernético da MB. Os novos sistemas deverão ter este aspecto nas especificações de obtenção, assim como os sistemas legados que eventualmente não atendam a este protocolo deverão se adaptar para atendê-lo.
	08	Ter preocupação constante com o aumento da velocidade de comunicação de dados ("baud rate" ou banda) das estruturas de rede que conectam os sistemas de C2 com seus usuários, principalmente o "backbone" da RECIM. A arquitetura SOA privilegia a troca intensa de informações entre componentes do espaço cibernético que podem estar em localidades bem

		afastadas, necessitando de uma rede de alta velocidade para garantir desempenho eficiente.
	09	Implementar serviços que permitam o emprego da arquitetura SOA na infraestrutura de CES da RECIM, como os serviços de descoberta e de publicação de serviços.
	10	Instalar componentes de um mesmo sistema de C2, com alta troca de informações entre si, o mais próximo possível no espaço cibernético. Se possível na mesma máquina física.
	11	Implantar o serviço de comunicação satélite, verificando constantemente a possibilidade de aumento de banda do serviço nos navios, principalmente os de maior deslocamento e aqueles menores que operam constantemente afastados da costa ou escoteiro.
	12	Implantar redundância nos serviços pertencentes às áreas de "acesso e entrega" e "interface e integração" (vide figura 12). Pela importância para todos os sistemas de C2 dos 23 padrões de serviço quem compõem estas áreas, eles têm que dispor de redundâncias, de preferência em máquinas e localidades diferentes no espaço cibernético da MB.
Novos Sistemas em Geral	13	Identificar os sistemas de informação que operarão conjuntamente com o novo sistema de C2, mapeando seus serviços no modelo TRM. O mapeamento facilitará a visualização das especificações técnicas que o sistema de C2 terá de atender ou interagir.
	14	Garantir que as características técnicas preceituadas pelo PEM e PCD, com seus respectivos padrões de serviço associados, constantes da tabela 7, estejam presentes na especificação do novo sistema de C2 a ser obtido.
	15	Listar as especificações técnicas que o novo sistema de C2 deve atender em forma de tabela, com divisões por área, categoria e padrões de serviço, conforme preceituado no TRM. É uma forma completa de não esquecer a especificação de nenhum serviço, assim como documentá-los de forma tabular.
SisGAAz	16	SisGAAz: ser desenvolvido considerando a necessidade de operar em ambiente de rede que obedeça a arquitetura SOA com nível máximo de interoperabilidade, isto é, nível "corporativo".
	17	SisGAAz: implantar serviços na RECIM na infraestrutura de serviços corporativos centrais para permitir a operação de sistemas em arquitetura SOA, como serviços de descoberta e descrição. Neste aspecto, devem-se disponibilizar serviços e padronizar especificações de todos os padrões de serviço relacionados à área de "interface e integração" do TRM, em sintonia com o cronograma de desenvolvimento do SisGAAz.
Sistemas Legados em Geral	18	Mapear pelo modelo do TRM os serviços disponíveis no sistema legado em questão para se ter uma visão técnica dos mesmos, facilitando o estudo de incremento de interoperabilidade.
	19	Empregar o modelo ISIMM (ou LISI como segunda opção) para medir o nível inicial de interoperabilidade (baseline) do

		sistema legado com seus sistemas contraparte. Em seguida, com o mesmo modelo, definir o nível de interoperabilidade alvo desejado. Por fim, estabelecer um cronograma de aumento gradual do nível de interoperabilidade, de forma a atingir o nível alvo. Considerar prazos exequíveis, tendo em vista os investimentos em tecnologia e desenvolvimentos necessários.
	20	Para interfaceamento com componentes de ambiente externo, desenvolver interfaces de acesso empregando a representação em topologia de rede do TRM, conforme figura 14.
	21	Ao usar serviços web para troca dados com outros sistemas, como na troca de dados por arquivos XML, empregar protocolos seguros, como o "Hypertext Transfer Protocol Secure" (HTTPS) ao invés do HTTP.
SISTRAM	22	SISTRAM: aumentar o nível de interoperabilidade do sistema para "funcional" na troca de dados com todos os sistemas, e dispor de serviços que permitam operá-lo no nível "corporativo", quando interagindo com sistemas da MB, como o SISNC2 e o SisGAAz.
	23	SISTRAM: no serviço de gerenciamento de dados procurar utilizar um Sistema Gerenciador de Banco de Dados (SGBD) considerado referência em uso por sistemas de controle de tráfego marítimo internacionais. Tal SGBD deverá ser o mesmo empregado pelo SisGAAz para agilizar a rápida troca de dados entre estes sistemas no futuro.
SISNC2 (SAGBD)	24	SAGBD: aumentar o nível de interoperabilidade do sistema para "funcional", em conexão segura, quando trocando dados com o SAETE, da MB, e SIPLOM, do MD. Dispor de serviços que permitam operá-lo no nível "corporativo", quando interagindo com o SISTRAM e o futuro SisGAAz.
	25	SAGBD: Expandir a interoperabilidade do sistema para oferecer conexão segura (HTTPS ou similar) em nível "funcional" com sistemas da DPC.
	26	SAGBD: no serviço de gerenciamento de dados procurar utilizar um SGBD moderno, com formatação de dados de ampla utilização em forças internacionais de referência. Tal SGBD deverá ser o mesmo empregado pelo SisGAAz para agilizar a rápida troca de dados entre os sistemas no futuro.
	27	SAGBD: envidar esforços junto ao MD para avanços no projeto INTERC2, de forma a permitir que não somente o SAGBD possa aumentar o nível de interoperabilidade com o SIPLOM, mas também que os sistemas de C2 do EB e da FAB também possam fazê-lo, permitindo até que esses sistemas troquem dados diretamente com o SAGBD. Este seria um grande avanço no futuro da interoperabilidade de operações conjuntas.