CENTRO DE DEFESA CIBERNÉTICA

C D CIBER

PROTEGE E COMBATE

OBJETIVO

CONHECER AS CAPACIDADES DO CENTRO DE DEFESA CIBERNÉTICA

SUMÁRIO

1. INTRODUÇÃO
   - Quem somos?

2. DESENVOLVIMENTO
   - Situações de emprego
   - Missão síntese
   - Organização
   - Princípios de atuação
   - Áreas funcionais
   - Atuação sistemática
   - Atuação episódica
   - CRI - Operações de Informação

3. CONCLUSÃO

CENTRO DE DEFESA CIBERNÉTICA

INTRODUÇÃO

CENTRO DE DEFESA CIBERNÉTICA

ComDCiber

BRAÇO OPERACIONAL DO ComDCiber

CENTRO DE DEFESA CIBERNÉTICA

MISSÃO SÍNTESE

**EXECUTAR AÇÕES CIBERNÉTICAS
EM SITUAÇÕES DE PAZ, DE CRISE E DE CONFLITO ARMADO
NO AMPLO ESPECTRO DAS OPERAÇÕES.**

CAPACIDADES OPERATIVAS


EB70-MC-10.232

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
COMANDO DE OPERAÇÕES TERRESTRES

Manual de Campanha

GUERRA CIBERNÉTICA

1ª Edição
2017

Capacidade Operativa	Descrição
Proteção Cibernética	Ser capaz de conduzir ações para neutralizar ataques e exploração cibernética contra os nossos dispositivos computacionais, redes de computadores e de comunicações, incrementando as ações de guerra cibernética em face de uma situação de crise ou conflito. É uma atividade de caráter permanente.
Ataque Cibernético	Ser capaz de conduzir ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes de computadores e de comunicações do oponente.
Exploração Cibernética	Ser capaz de conduzir ações de busca ou coleta nos Sistemas de Tecnologia da Informação de interesse, a fim de obter dados. Deve-se, preferencialmente, evitar que essas ações sejam rastreadas e sirvam para a produção de conhecimento ou para a identificação das vulnerabilidades desses sistemas.

CENTRO DE DEFESA CIBERNÉTICA

"Os **Módulos Especializados** constituem as F Emp Estrt, **possuindo capacidades para agregar poder de combate**, de acordo com cada situação."

F Emp Estrt
Bda Inf Pqdt
12ª Bda Inf L (Amv)
23ª Bda Inf Sl
4ªBda C Mec
5ª Bda C Bld
EFETIVO 24.000 Mil
Módulos Especializados:
Cmdo Av Ex (02 BAVEx)
Cmdo Op Esp
Cmdo Art Ex (01 GMF)
Cmdo AD/3 (+01 GAC 155 AP)
Bda AAAe (01 GAAAe)
6º BIM/ 1º Btl Op Psico /1º Btl DQBRN
1º BGE /Cia C²/ **CDCiber**
01 BEng Cmb/ 01 BPE
B Ap Log Ex

CENTRO DE DEFESA CIBERNÉTICA

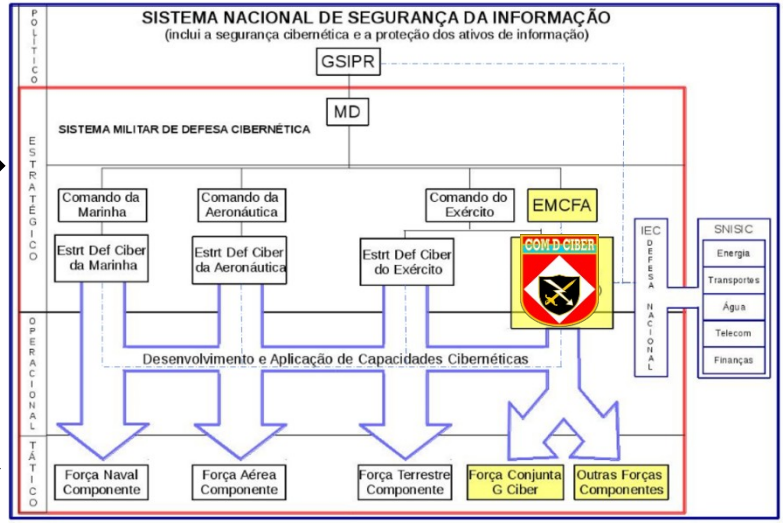
SITUAÇÕES DE EMPREGO

PRONTIDÃO OPERATIVA

CENTRO DE OPERAÇÕES CIBERNÉTICAS

MÓDULO ESPECIALIZADO Def Ciber/G Ciber

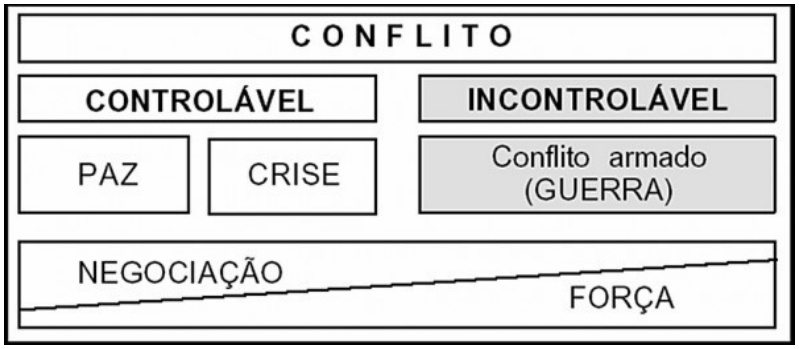
SMDC



COM D CIBER

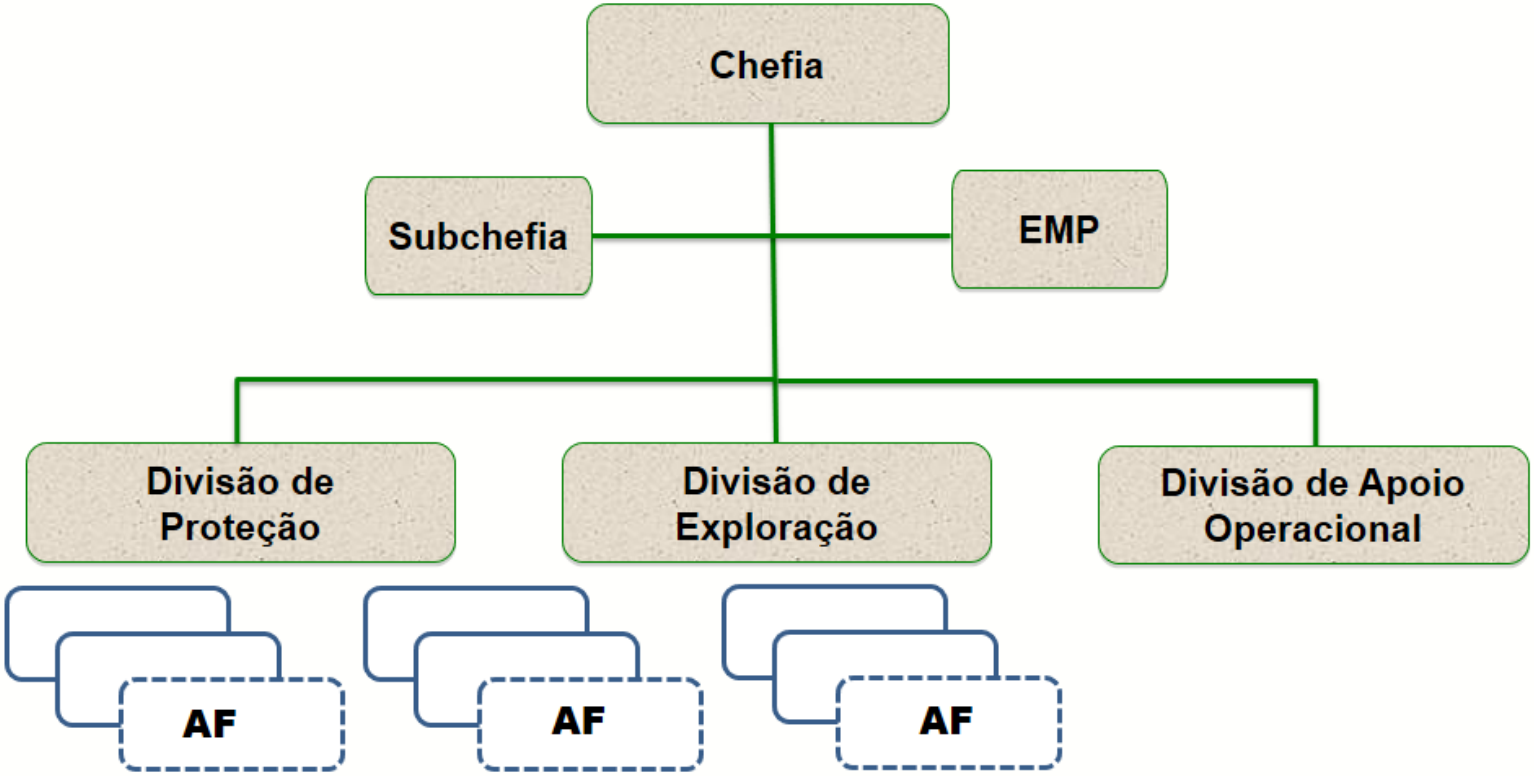
MINISTÉRIO DA DEFESA — MARINHA — EXÉRCITO — FORÇA AÉREA — ESTADO-MAIOR CONJUNTO DAS FORÇAS ARMADAS — COTER

OPERAÇÕES MILITARES



CENTRO DE DEFESA CIBERNÉTICA

ORGANIZAÇÃO



CENTRO DE DEFESA CIBERNÉTICA

PRINCÍPIOS DE ATUAÇÃO

ATUAÇÃO COLABORATIVA

SUSTENTABILIDADE

MODULARIDADE

ELASTICIDADE

FLEXIBILIDADE

ADAPTABILIDADE

CENTRO DE DEFESA CIBERNÉTICA

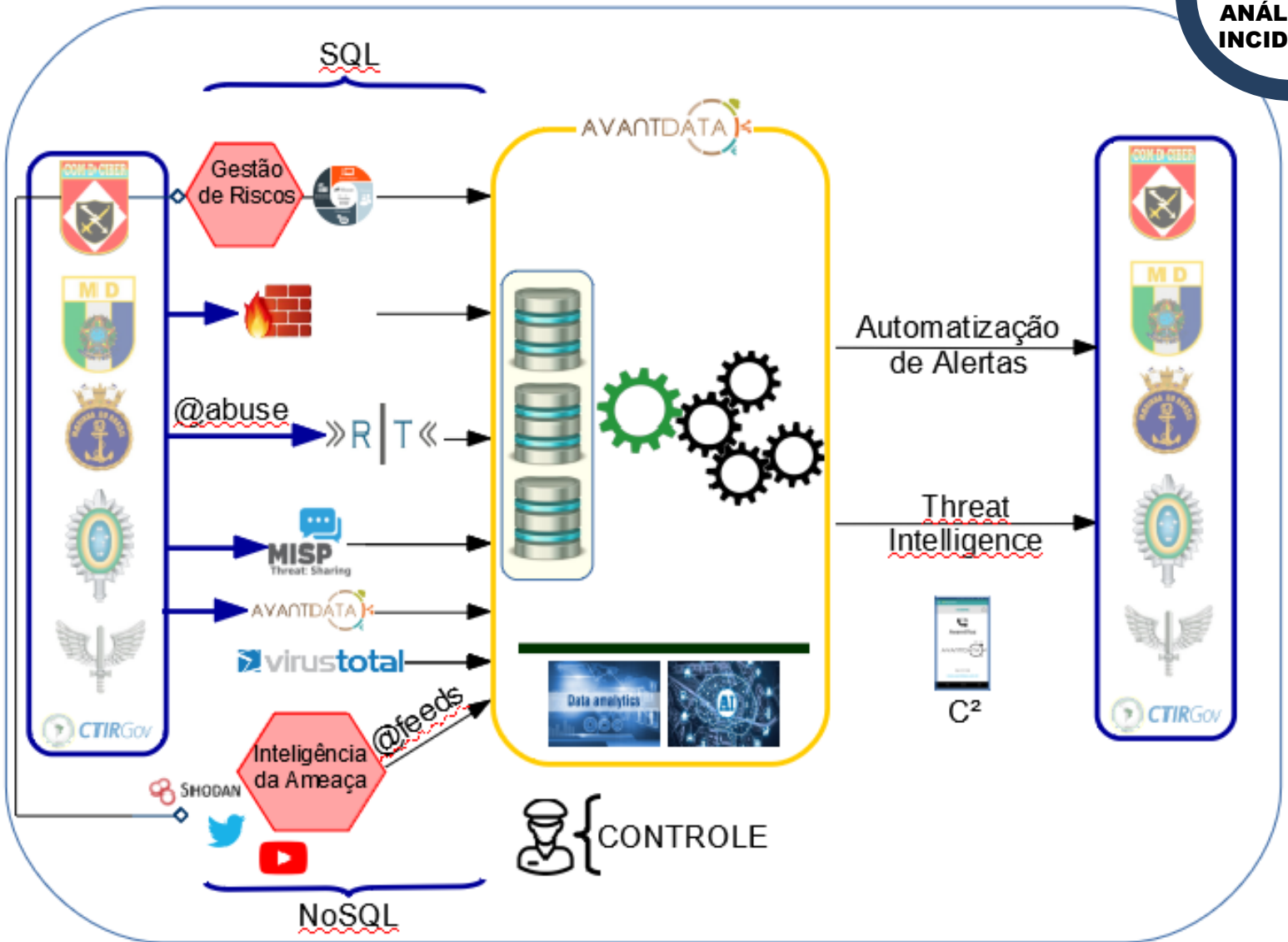
ÁREAS FUNCIONAIS

ANÁLISE DE INCIDENTES

PRONTIDÃO OPERATIVA

CENTRO DE DEFESA CIBERNÉTICA

ANÁLISE DE INCIDENTES



CENTRO DE DEFESA CIBERNÉTICA

Página inicial | Procurar | Reports | Artigos | Assets | Ferramentas | Admin | Ligado como edsonceser | RT para CDCiber

Found 27,58

- Tickets
  - Pesquisa Simples
  - Nova Pesquisa
  - Recently Viewed
- Artigos
- Utilizadores
- Assets

Novo Pedido em | SDS | Procurar...

Editar Pesquisa | Avançado | Mostrar Resultados | Actualização em bloco | Gráfico | Feeds

#	Assunto / Requerente	Estado / Criado	Queue / actualizado	Dono / Última actualização	Prioridade / Tempo disponível
68556	**mx1.campogrande.ms.gov.br -> [177.53.204.30] enviando phishing** CCTIR/EB <cctir@citex.eb.mil.br>	resolvido 19 horas ago	Abuse	felipe (CDCIBER) 19 horas ago	Media
68553	**Possível Vazamento de banco de dados do Corpo de Bombeiros de São Paulo** CTIR GOV <ctir@ctir.gov.br>	resolvido 38 horas ago	Abuse 35 horas ago	pedro (CDCIBER) 19 horas ago	Media
68551	Alerta sobre envio de phishing. [CTIR.mar #8056] CTIR FAB <abuse@ctir.aer.mil.br>, CTIR MAR <abuse@marinha.mil.br>, NUSIC DEFESA <nusic@defesa.gov.br>	resolvido 4 days ago	Abuse 4 days ago	peccatiello 19 horas ago	Media
68550	SPLUNK - Sitio OFFLINE - http://www.11icfex.eb.mil.br/ peccatiello	resolvido 4 days ago	Abuse	peccatiello 4 days ago	Media
68549	mx.go.gov.br -> [187.5.111.49] enviando phishing CCTIR/EB <cctir@citex.eb.mil.br>	resolvido 4 days ago	Abuse	Nobody in particular 4 days ago	Media
68548	sn02566.prodemge.gov.br -> [200.198.28.70] enviando phishing CCTIR/EB <cctir@citex.eb.mil.br>	resolvido 4 days ago	Abuse	Nobody in particular 4 days ago	Media
68547	smtp4.etice.ce.gov.br -> [189.90.161.224] enviando phishing CCTIR/EB <cctir@citex.eb.mil.br>	resolvido 4 days ago	Abuse	Nobody in particular 4 days ago	Media
68546	NOTIFICAÇÃO NR 009 - 07 ABR 19	resolvido 5 days ago	Abuse	portugal (CDCIBER) 4 days ago	Media
68545	NOTIFICAÇÃO NR 008 - 07 ABR 19 <cdciberint@cdciber.eb.mil.br>, CTIR GOV <ctir@ctir.gov.br>	resolvido 5 days ago	Abuse	Nobody in particular 4 days ago	Media
68544	Sql injection em página de domínio do Exército.	resolvido 7 days ago	Abuse	portugal (CDCIBER) 7 days ago	Media

ANÁLISE DE INCIDENTES

CENTRO DE DEFESA CIBERNÉTICA

ÁREAS FUNCIONAIS

ANÁLISE DE INCIDENTES

PESQUISA E ANÁLISE DE AMEAÇAS

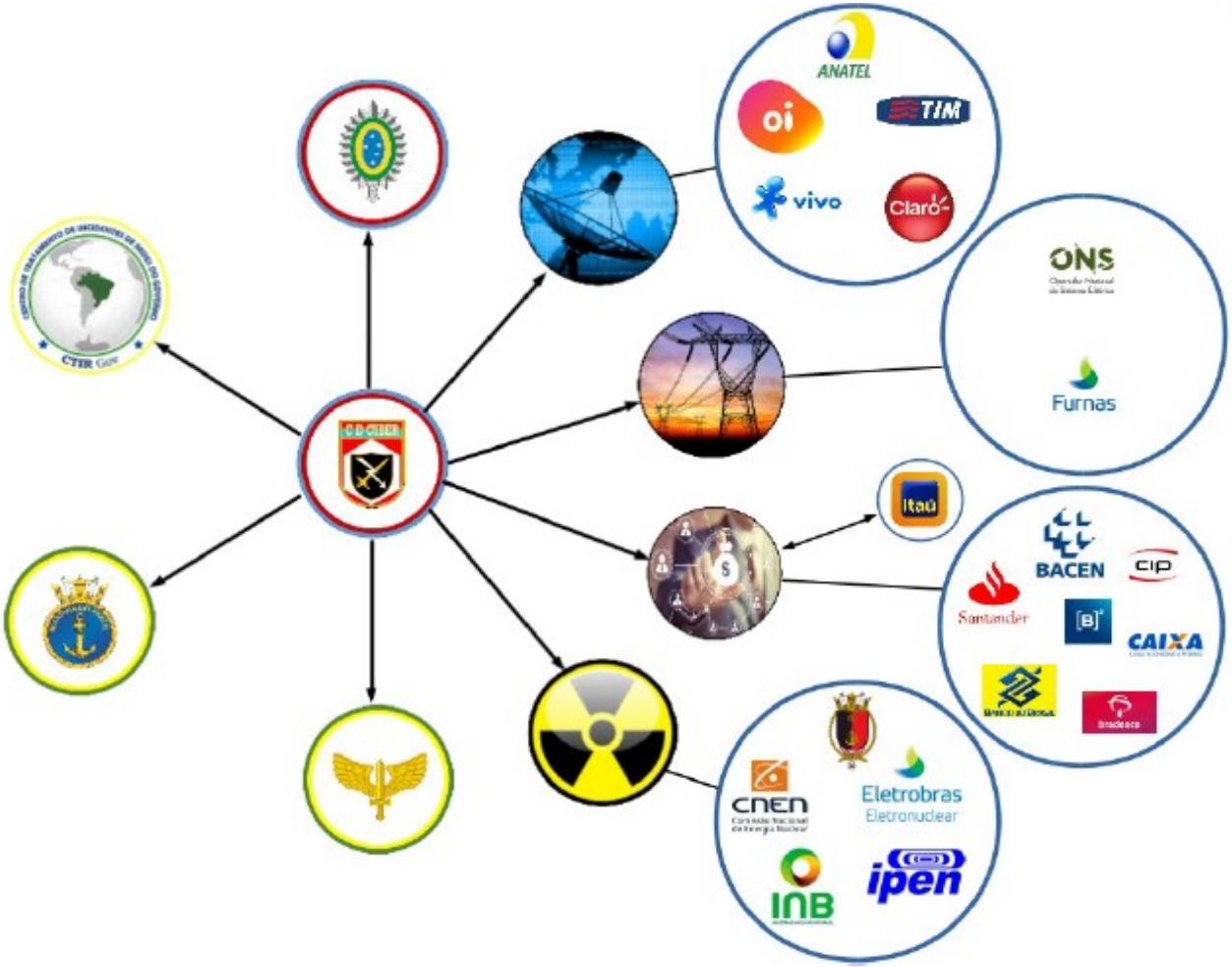
PRONTIDÃO OPERATIVA

CENTRO DE DEFESA CIBERNÉTICA

ÁREAS FUNCIONAIS

PESQUISA E ANÁLISE DE AMEAÇAS

MISP
Threat Sharing



CENTRO DE DEFESA CIBERNÉTICA

ÁREAS FUNCIONAIS

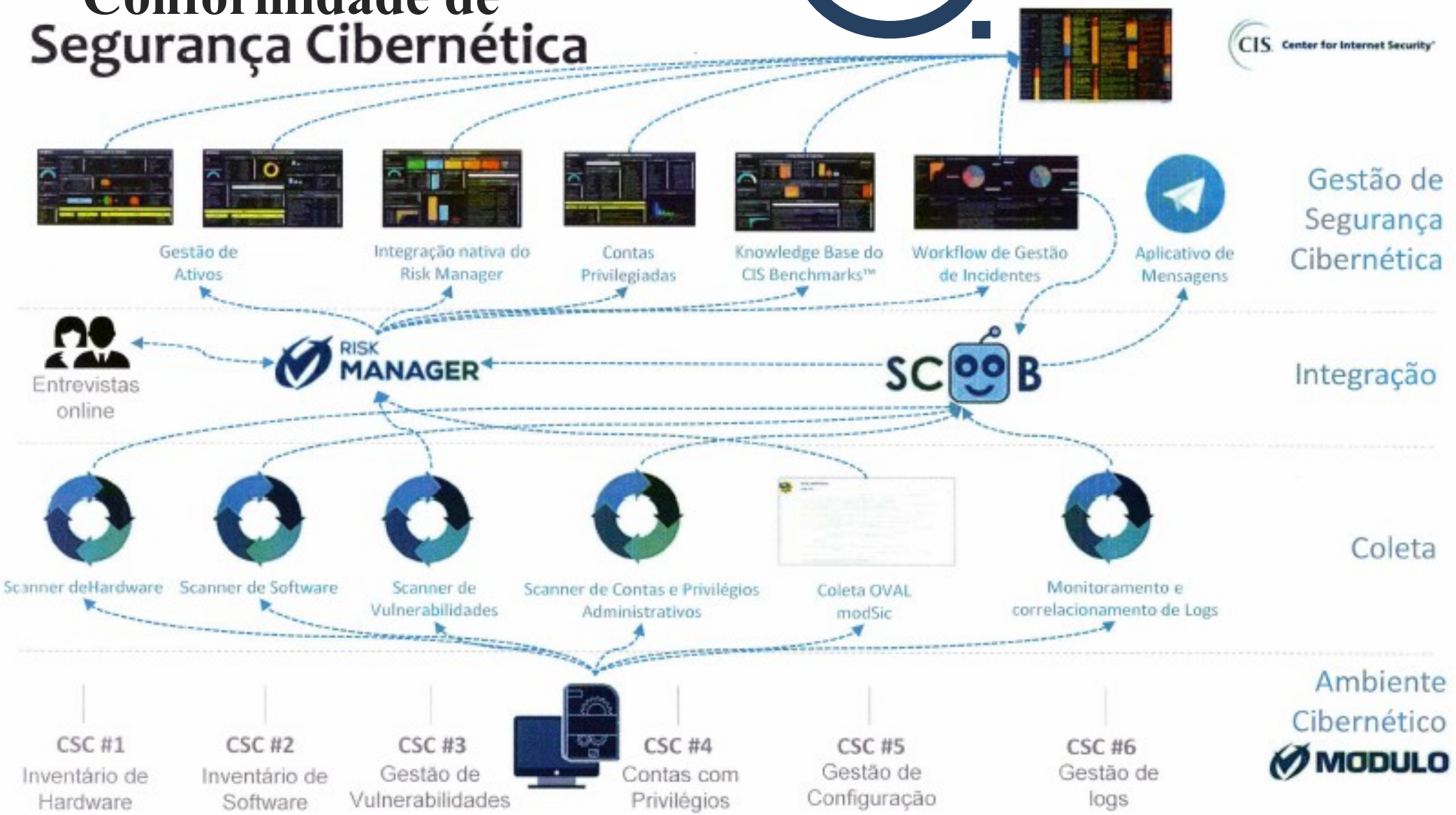
CENTRO DE DEFESA CIBERNÉTICA

ANÁLISE DE RISCOS

CENTRO DE DEFESA CIBERNÉTICA

ANÁLISE DE RISCOS

Conformidade de Segurança Cibernética



CENTRO DE DEFESA CIBERNÉTICA

ANÁLISE DE RISCOS

CIS Benchmarks → modSIC

CIS Controls

elasticsearch

OSSEC

Registro de Ocorrências

Processos

Pessoas

Ambiente

Gestão de Incidentes

Remediação

Alertas

Visão Executiva

Planejamento

Active Directory

spiceworks

Nessus vulnerability scanner

CENTRO DE DEFESA CIBERNÉTICA

ÁREAS FUNCIONAIS

CENTRO DE DEFESA CIBERNÉTICA

ATUAÇÃO SISTEMÁTICA

C D CIBER

IDT/EXPL VULNERAB

Sistemas de Informação críticos

IEC/Def Nac

Honey pot

ECI/SMDC

DEFESA ATIVA

PESQUISA E ANÁLISE

ANÁLISE DE RISCOS

FORENSE/ ANÁLISE DE MALWARE

ANÁLISE DE INCIDENTES

COORDENADOR
EQUIPE DE TRIAGEM
EQUIPES DE ANALISTAS
ESPECIALISTAS

MISP

Parceiros externos

MISP Threat Sharing

POLICIA FEDERAL

FIC 2018

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

CTIRGov

cert.br

Honey pot

SERPRO

CENTRO DE DEFESA CIBERNÉTICA

ATUAÇÃO EPISÓDICA

A — REALIZAR CONFORMIDADE DE SEGURANÇA EM SISTEMA DE INFORMAÇÃO CRÍTICO DE INTERESSE DA DEFESA NACIONAL E EM ÓRGÃOS DA APF (Em Coor com o GSI e Mdt Autz do MD)

B — REALIZAR FORENSE COMPUTACIONAL EM SISTEMA DE INFORMAÇÃO CRÍTICO DE INTERESSE DA DEFESA NACIONAL COM SUSPEITA DE COMPROMETIMENTO

C — APOIAR A RECUPERAÇÃO DE SISTEMA DE INFORMAÇÃO CRÍTICO DE INTERESSE DA DEFESA NACIONAL QUE TENHA SIDO INFECTADO E/OU COMPROMETIDO

PRONTIDÃO OPERATIVA

CENTRO DE DEFESA CIBERNÉTICA

ATUAÇÃO EPISÓDICA

D — AGREGAR PODER DE COMBATE NAS OPERAÇÕES DE GLO, OP INTERAGÊNCIAS, OP DE COMBATE A ILÍCITOS TRANSFRONTEIRIÇOS E OUTRAS OP DE NÃO GUERRA

E — INTEGRAR A F Cj G Ciber E/OU Dst Cj G Ciber NAS OPERAÇÕES MILITARES CONJUNTAS (HE)

F — SUPLEMENTAR OS MEIOS DE DEFESA E/OU GUERRA CIBERNÉTICAS DA MB E DA FAB, POR SOLICITAÇÃO DO EMA E/OU DO EMAER

PRONTIDÃO OPERATIVA

CENTRO DE DEFESA CIBERNÉTICA

ATUAÇÃO EPISÓDICA

G

COORDENAR E INTEGRAR A SEGURANÇA E DEFESA CIBERNÉTICAS, EM ÂMBITO NACIONAL, DE FORMA EPISÓDICA (CDA e CSDC)

JMJ Rio2013

Rio2016

RIO+20 United Nations Conference on Sustainable Development

BRASIL 2013 FIFA CONFEDERATIONS CUP

Brasil 2014 FIFA WORLD CUP

Rio2016 JOGOS PARALÍMPICOS

PRONTIDÃO OPERATIVA

CENTRO DE DEFESA CIBERNÉTICA

ÁREAS FUNCIONAIS

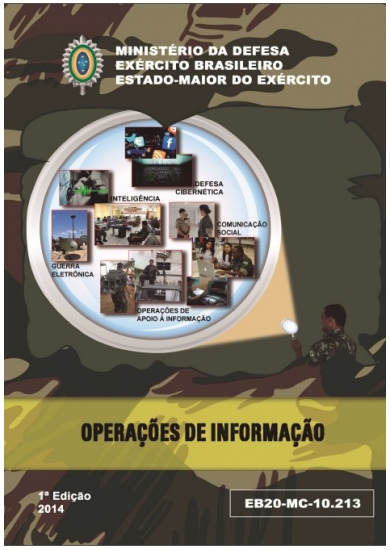
- ANÁLISE DE INCIDENTES
- ANÁLISE DE RISCOS
- DEFESA ATIVA
- IDT/EXPL VULNERAB
- FORENSE/ ANÁLISE DE MALWARE
- PESQUISA E ANÁLISE DE AMEAÇA

INFRAESTRUTURA		EDUCAÇÃO	ADESTRAMENTO
DOUTRINA	ORGANIZAÇÃO (PROCESSOS)	MATERIAL (SISTEMAS)	PESSOAL

OPERAÇÕES DE INFORMAÇÃO

6.6.3 As Operações de Informação (Op Info) consistem na atuação, metodologicamente integrada, de capacidades relacionadas à informação, em conjunto com outros vetores, para informar e influenciar grupos e indivíduos, bem como afetar o ciclo decisório de oponentes, ao mesmo tempo protegendo o nosso. Além disso, visam a evitar, impedir ou neutralizar os efeitos das ações adversárias na Dimensão Informacional.

SUPERIORIDADE DA INFORMAÇÃO



CENTRO DE DEFESA CIBERNÉTICA

SUPERIORIDADE DA INFORMAÇÃO

CRI

GE
COM SOC
INTLG
OP PSICO
G CIBER

ATUAÇÃO DAS CRI

- PROTEÇÃO DAS INFORMAÇÕES OPERACIONAIS CRÍTICAS
- PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO CRÍTICOS
- PROTEÇÃO DO AMBIENTE OPERACIONAL (HIGIENE OPERACIONAL)
- ADOÇÃO DE MEDIDAS DE ANONIMIZAÇÃO
- SEGURANÇA DOS PRODUTOS DIGITAIS

- Produção de informação indesejada: filmagem, foto, redes sociais;
- Posicionamento/localização da tropa e de autoridades;
- Celular infectado no C Op – gravador e câmera.
- Ações de desinformação adversas;
- Ações de Op Psico adversas – Impacto no moral da tropa.

ATUAÇÃO DAS CRI

- **PROTEÇÃO** DAS INFORMAÇÕES OPERACIONAIS CRÍTICAS
- PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO CRÍTICOS
- PROTEÇÃO DO AMBIENTE OPERACIONAL (HIGIENE OPERACIONAL)
- ADOÇÃO DE MEDIDAS DE ANONIMIZAÇÃO
- SEGURANÇA DOS PRODUTOS DIGITAIS

- **OBTENÇÃO DE INFORMAÇÕES** (COLETA E BUSCA)
- IDENTIFICAÇÃO DE LIDERANÇAS “DIGITAIS”
- IDENTIFICAÇÃO DE PERFIS FALSOS
- LEVANTAMENTO E ANÁLISE DE VÍNCULOS
- AVALIAÇÃO DO IMPACTO DAS CAMPANHAS

ATUAÇÃO DAS CRI

- PROTEÇÃO DAS INFORMAÇÕES OPERACIONAIS CRÍTICAS
- PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO CRÍTICOS
- PROTEÇÃO DO AMBIENTE OPERACIONAL (HIGIENE OPERACIONAL)
- ADOÇÃO DE MEDIDAS DE ANONIMIZAÇÃO
- SEGURANÇA DOS PRODUTOS DIGITAIS

- OBTENÇÃO DE INFORMAÇÕES (COLETA E BUSCA)
- IDENTIFICAÇÃO DE LIDERANÇAS “DIGITAIS”
- IDENTIFICAÇÃO DE PERFIS FALSOS
- LEVANTAMENTO E ANÁLISE DE VÍNCULOS
- AVALIAÇÃO DO IMPACTO DAS CAMPANHAS

- ATUAR SOBRE A INFORMAÇÃO - MANIPULAR, CORROMPER e DESTRUIR
- ATUAR SOBRE A INFRAESTRUTURA

- AMPLIFICAÇÃO DA DIFUSÃO NOS MEIOS DIGITAIS
- AMPLIFICAÇÃO DE COMENTÁRIOS

OP INFO

https://ccdcoe.org/.../Ch10_CyberWarinPerspective_Jaitner.pdf

CENTRO DE DEFESA CIBERNÉTICA

RUSSIAN INFORMATION WARFARE: LESSONS FROM UKRAINE

1 - AUTORIDADES UCRANIANAS TIVERAM COMPUTADORES E TELEFONES CELULARES HACKEADOS ('Snake', 'Uroboros' e 'Turla') DESDE 2010

2- O PRINCIPAL CABO DE FIBRA ÓTICA DA Ukrtelecom FOI SABOTADO

- BLOQUEIO ELETRÔNICO NAS COMUNICAÇÕES NAVAIS

4 – CELULARES DE MILITARES UCRANIANOS DENUNCIARAM A POSIÇÃO DAS TROPAS – ALVO DE FOGOS DE ARTILHARIA

5 – PORTAIS DO GOVERNO SOFRERAM ATAQUE DE NEGAÇÃO DE SERVIÇO E DESFIGURAÇÃO.

6 – O GRUPO HACKTIVISTA *Cyberberkut* ASSUMIU A AUTORIA DE VÁRIOS ATAQUES E VAZOU ÁUDIOS DE CONVERSAS E MENSAGENS DE E-MAIL ENTRE OFICIAIS UCRANIANOS COM OS EUA E UNIÃO EUROPEIA.

7 – FORAM CRIADOS CANAIS DEDICADOS NO YOUTUBE

8 – SITES REGISTRADOS EXALTANDO O SEPARATISMO (novorus.info e novorossia.su)

9 – ATENÇÃO DA MÍDIA E DESCRÉDITO DA POPULAÇÃO

CENTRO DE DEFESA CIBERNÉTICA

C D CIBER

PROTEGE E COMBATE