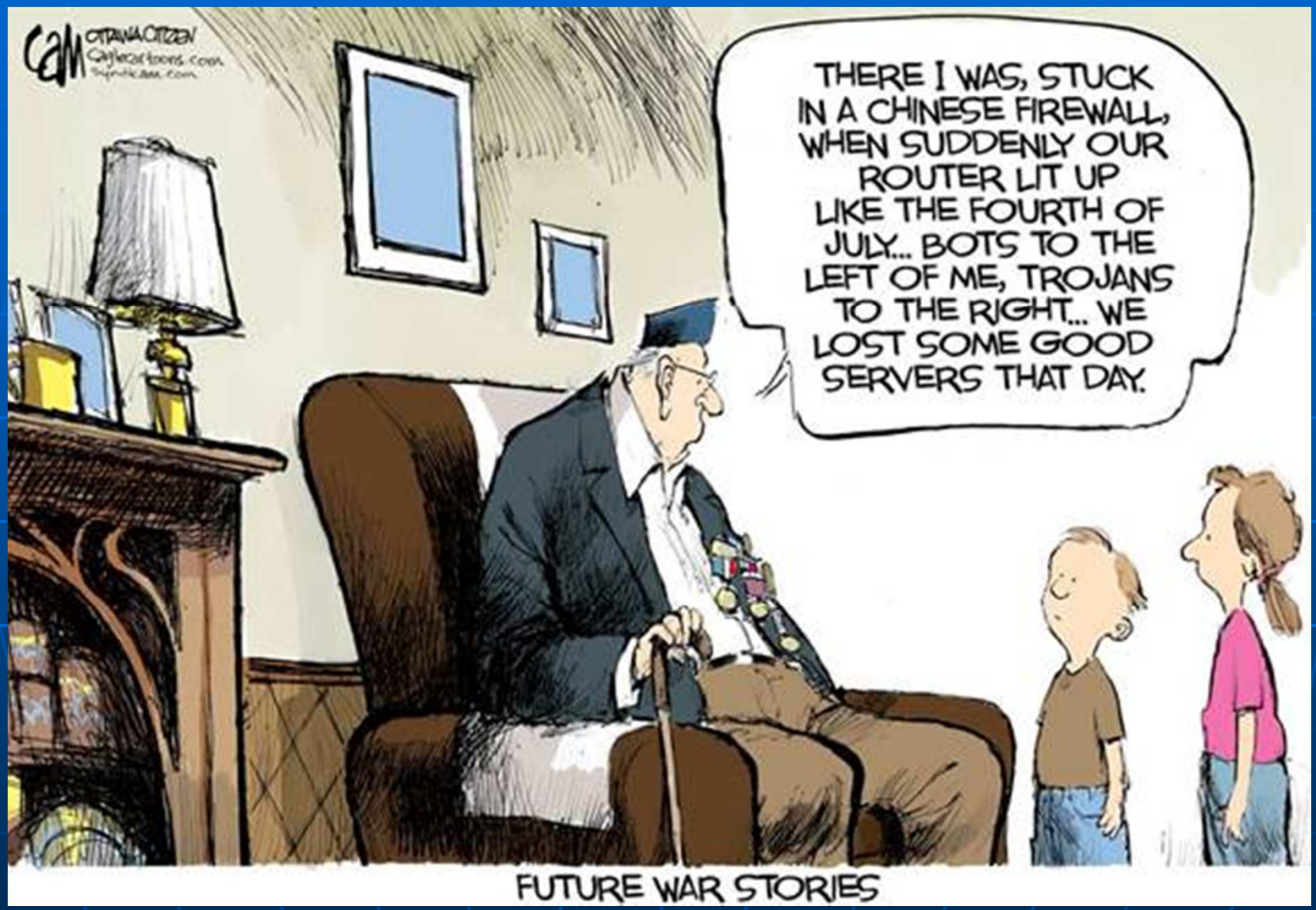
Confraria de Segurança da Informação, 25 Novembro 2015

UNCLASSIFIED

Operações Militares no Ciberespaço

TCOR Paulo Branco

CENTRO DE CIBERDEFESA
ESTADO MAIOR GENERAL DAS FORÇAS ARMADAS
MINISTÉRIO DA DEFESA


CAM OTTAWA CITIZEN
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.
FUTURE WAR STORIES

CRIAÇÃO CENTRO CIBERDEFESA

O atual Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, antecipa como grande tendência no ambiente de segurança global, **o potencial devastador dos ataques cibernéticos**, identificando o ciberterrorismo e a cibercriminalidade como ameaças e riscos prioritários.

RCM 26/2013
Reforma "Defesa 2020"

"*Constituem orientações específicas a ter em consideração no ciclo de planeamento estratégico: (…)*

- ***O levantamento da capacidade de ciberdefesa nacional***"

http://www.defesa.pt/Documents/Linhas Gerais da Reforma Defesa 2020.pdf

CRIAÇÃO CENTRO CIBERDEFESA

Despacho MDN 13692/2013

Orientação política para a Ciberdefesa

São objetivos da Política de Ciberdefesa:

1. Garantir a proteção, a resiliência e a segurança das redes e dos SIC da Defesa Nacional contra ciberataques;
2. Assegurar a liberdade de ação do País no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional;
3. Contribuir de forma cooperativa para a cibersegurança nacional.

CRIAÇÃO CENTRO CIBERDEFESA

Despacho MDN 13692/2013
Orientação política para a Ciberdefesa

O **Centro de Ciberdefesa**, na dependência do CEMGFA, constitui o órgão responsável pela condução de **operações no ciberespaço** e pela resposta a **incidentes informáticos** e **ciberataques**, com responsabilidades de **coordenação, operacionais e técnicas**.

Road Map

Desenvolver capacidade para conduzir operações militares em redes de computadores *(Início Jan2015)*

Implementar a capacidade militar para conduzir todo o espetro de operações no ciberespaço (defensivas, de exploração e ofensivas), ……, constitui a única forma credível de promover uma ciberdefesa eficaz, capaz de constituir um fator de dissuasão a potenciais atacantes.

Despacho MDN 13692/2013

Plano para a Edificação da Capacidade de Ciberdefesa Nacional

Estrutura Orgânica

- Criação do Centro de Ciberdefesa
- Criação de um CIRC no EMGFA e um CIRC em cada ramo

Relações de dependência operacional

DEFINIR

Missão do Centro de Ciberdefesa e dos CIRC.

Patamares de responsabilidade na cooperação entre a Capacidade de Ciberdefesa Nacional e estruturas semelhantes nacionais e internacionais

DIRCSI/EMGFA

Centro de Ciberdefesa → CIRC EMGFA

- CIRC MARINHA
- CIRC EXÉRCITO
- CIRC FORÇA ÁEREA

CIRC – Computer Incident Response Capability

Ciber Responsabilidades

Ministério da Justiça
Cibercrimes

Ministério da Administração Interna
Ciberterrorismo

Serviços de Informações Nacionais (Inteligência)
Ciberespionagem

Forças Armadas Portuguesas
Proteção contra agressão militar externa
(inclui o Ciberespaço)

MISSÕES CIRCs

Garantir a capacidade de deteção e resposta "online" a ciberincidentes

Planear, coordenar e dirigir a investigação de ciberincidentes

Partilhar informação numa estratégia de proteção e resposta defensiva

Participar no trabalho colaborativo e integrado com os restantes Núcleos CIRC

No âmbito das suas possibilidades, contribuir para a condução de CNO

Contribuir para a manutenção de uma carta de situação do ciberespaço, *"situational awareness"*

Participar nos programas de exercícios na área da ciberdefesa

Colaborar nas ações de formação na área da ciberdefesa

CENTRO DE CIBERDEFESA

Propor a doutrina de proteção do Ciberespaço no âmbito da Defesa;

Planear, coordenar e dirigir a investigação de ciberincidentes

Manter uma carta de situação do ciberespaço

Contribuir para as Operações de Informação, na vertente "*Computer Network Operations*" (CNO)

Conduzir operações no ciberespaço (CNA, CNE, CND)

Em coordenação com os Ramos, planear um programa de exercícios na área da ciberdefesa

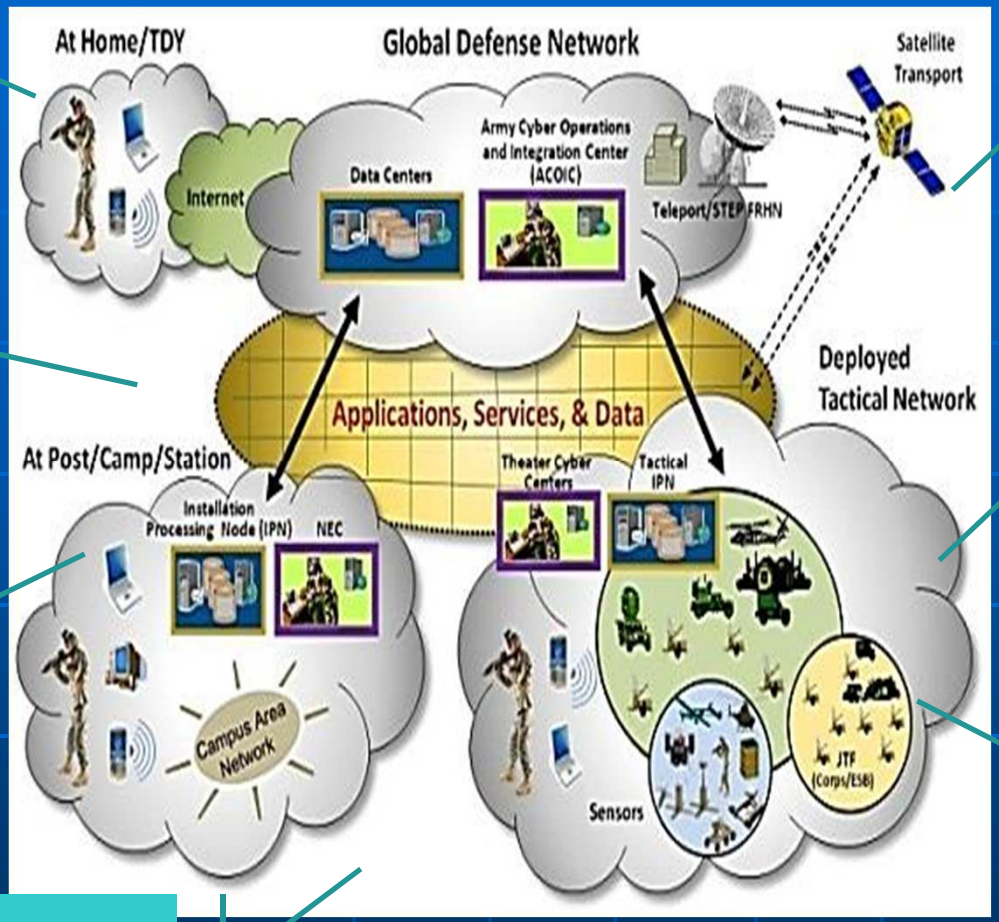
DEFESA DE TODAS AS REDES MILITARES

Providenciar todas as fontes e eventos

Manter uma carta de situação do ciberespaço

Assegurar a integração com as operações de Intel

Treinar e Equipar todas as unidades militares contra ciberataques



Impor e Monitorizar políticas de actuação, níveis de conformidade

Identificar e Proteger "terreno chave" no ciberespaço

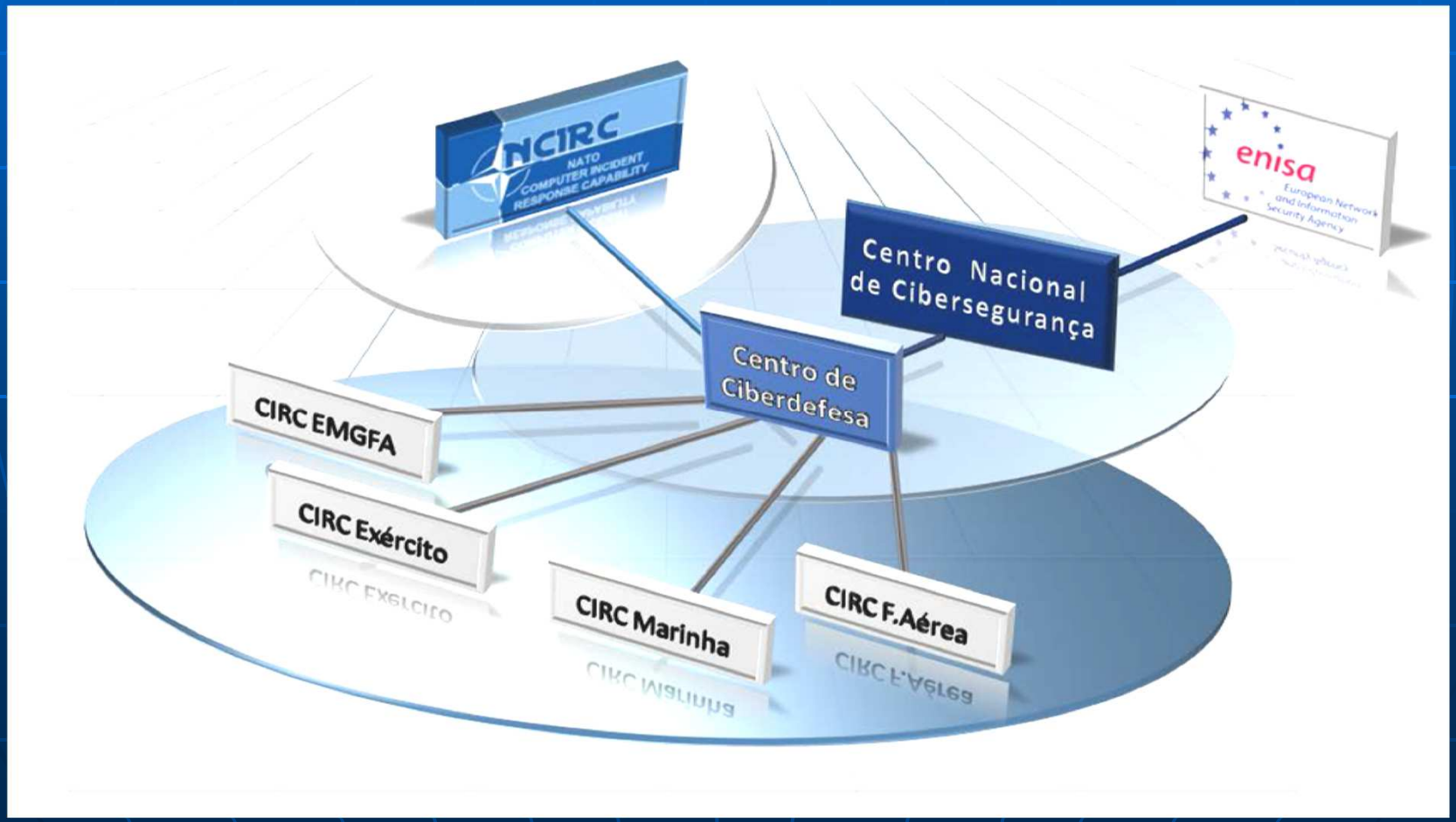
Conduzir análise forense sobre ciberataques

Preciso Dedender para manter a Liberdade para Operar

Governação da Ciberdefesa

CIRC do EMGFA e Ramos partilham informação sobre vulnerabilidades detetadas;

Centro de Ciberdefesa partilha informação com outras organizações nacionais e com as organizações militares internacionais, com destaque para a NATO.

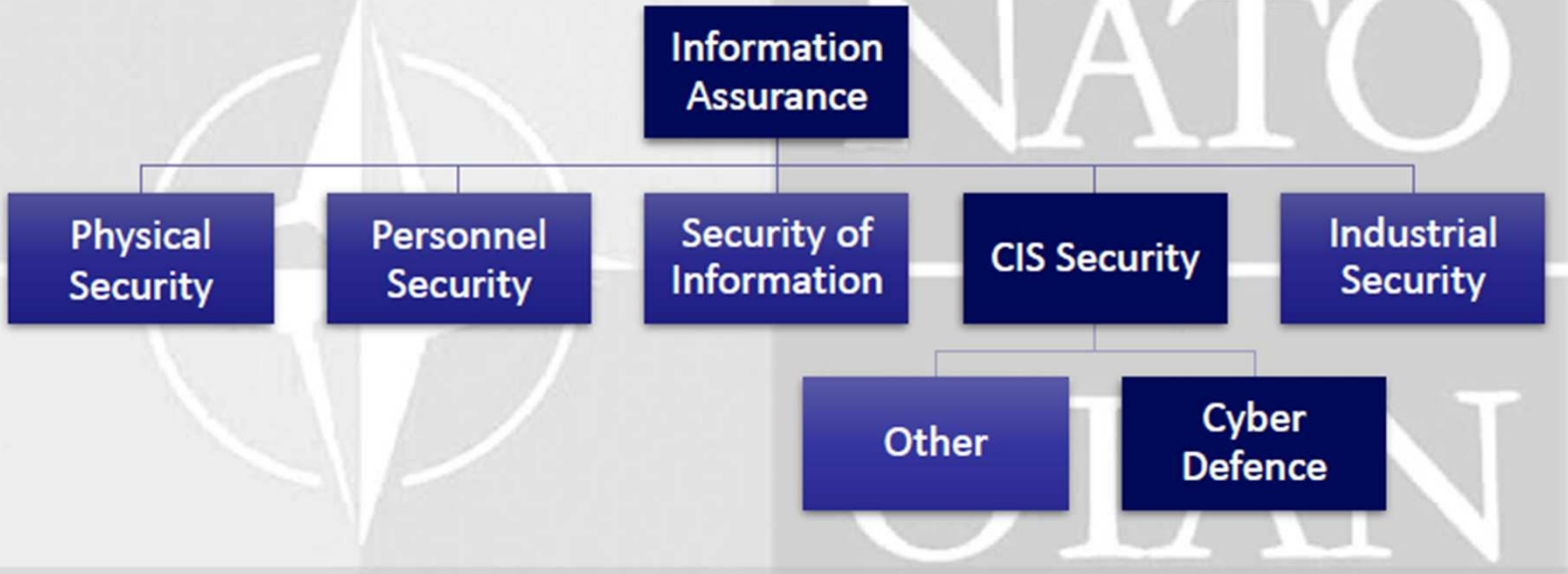


Estratégia Nacional de Cibersegurança

"....potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de todos os cidadãos, das empresas e das entidades públicas e privadas."

RCM nº 36/2015

NATO – ABORDAGEM SEGURANÇA DA INFORMAÇÃO



"**cyber defence**: The means to achieve and execute defensive measures to counter cyberattacks and mitigate their effects, and thus preserve and restore the security of communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems"

JP 3-13, 2012:

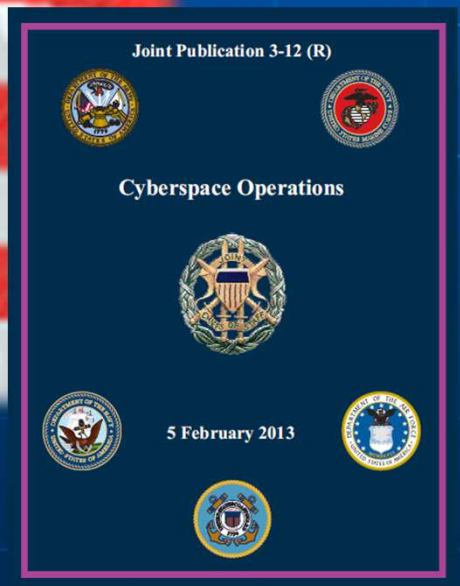
Information Operations → Computer Network Operations

- **Computer Network Attack (CNA)**
- **Computer Network Exploitation (CNE)**
- **Computer Network Defense (CND)**

JP 3-12, 2013:

Cyberspace Operations

- **Defensive Cyberspace Operations (DCO)**
- **Offensive Cyberspace Operations (OCO)**
- **DoD Information Network Operations**



CIBERESPAÇO como um DOMÍNIO

- *Um domínio global dentro do ambiente de informação que consiste numa rede interdependente de infra-estruturas de tecnologias de informação, incluindo a Internet, redes de telecomunicações, sistemas computorizados e processadores e controladores embutidos*. (JP 1-02 – USA DoD)

CIBERESPAÇO como um DOMÍNIO

- Domínio construído pelo homem – em constante mudança
- Interdependente com os tradicionais domínios da guerra
- Não é especial nem isolado – parte integrante do ambiente operacional de cada unidade militar
- Caracteristicas físicas, lógicas(virtuais), e sociais
- Alcance operacional imediato – "global battlefield".

Presença Constante – evolui à velocidade do código!

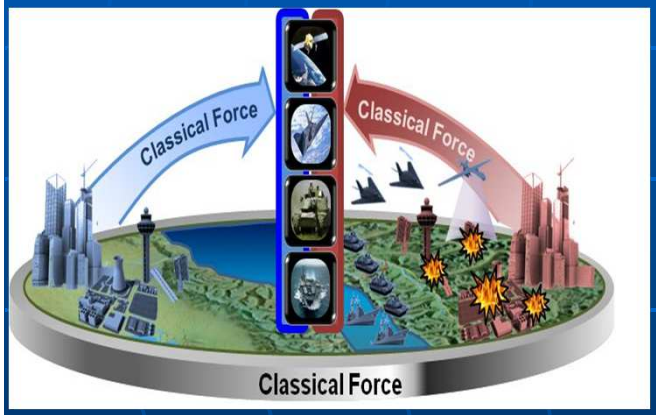
Evolução do Ambiente Operacional

(surgimento do ciberespaço)

Past

Classical

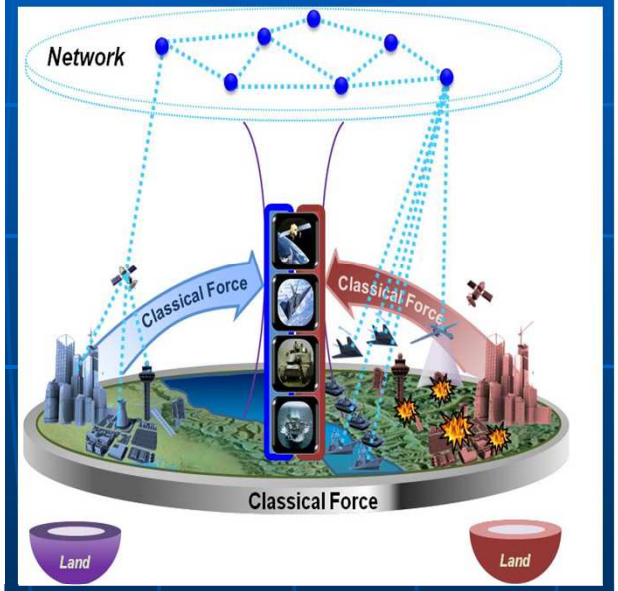
AirLandSea Battle



Today

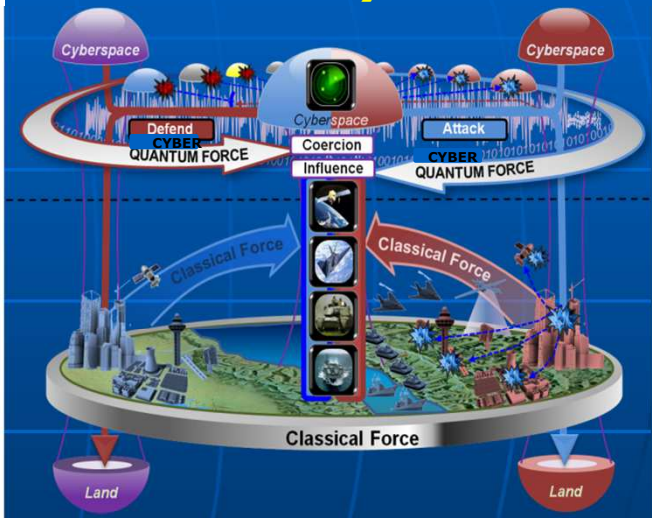
Classical

Network Enabled



Future

Land Cyber



Mass and Velocity of Change in OE

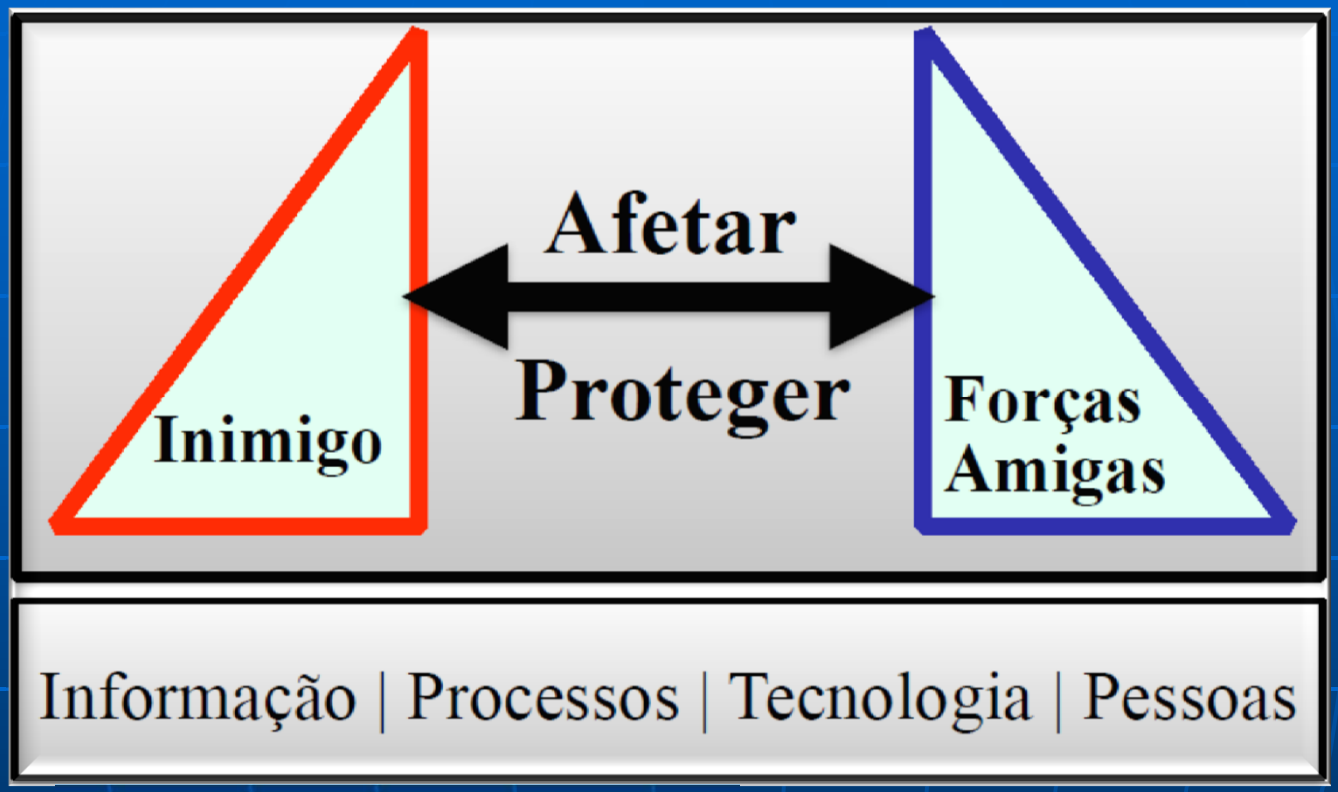
U.S. Army Cyber Command – Dez13

(OE – Operational Enviroment)

Convergência entre domínios clássicos e ciberespaço

O sucesso das operações militares terrestres depende de uma integração perfeita com as operações no ciberespaço.

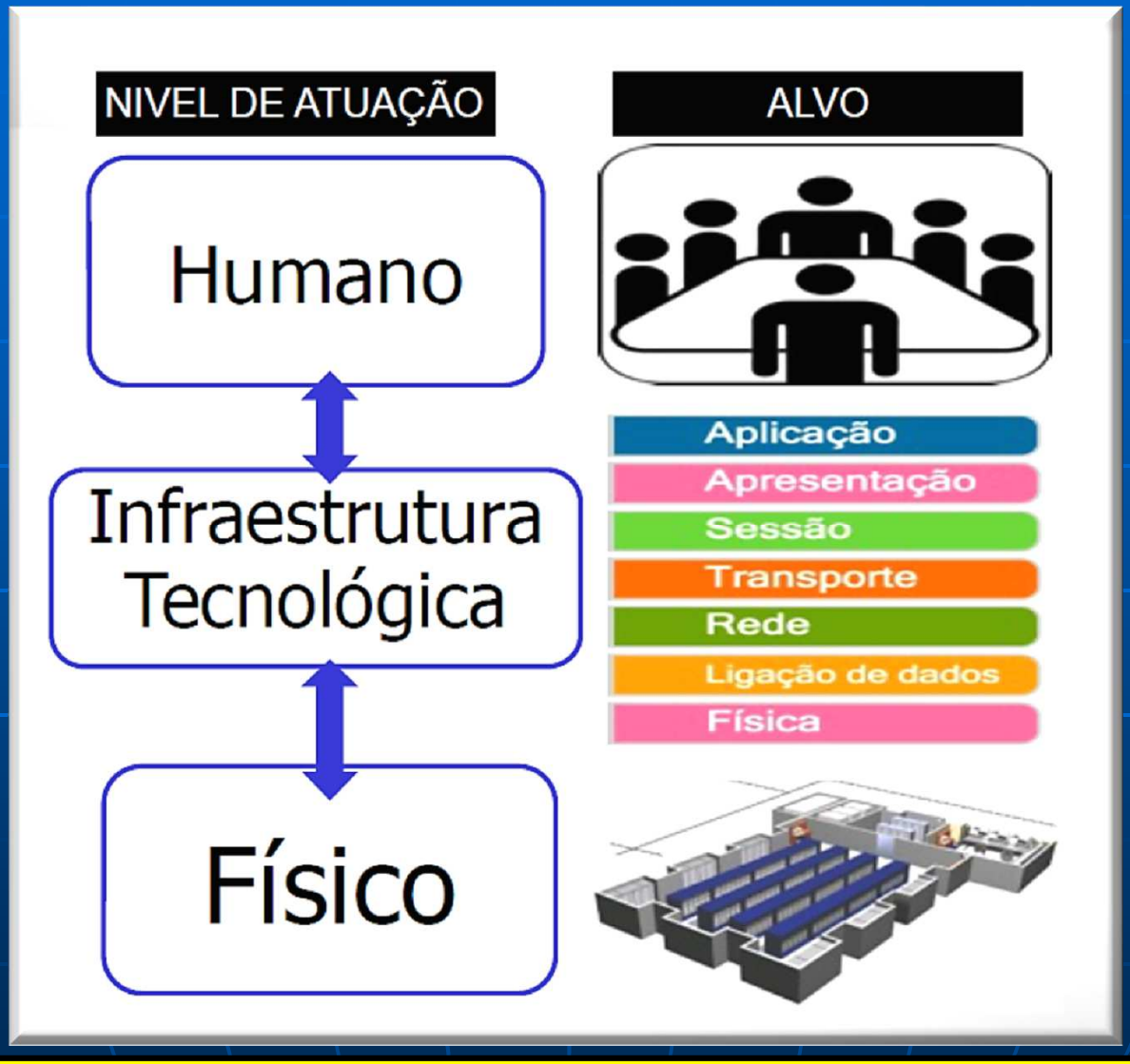
Guerra da Informação



Ataque
Estónia 2007

Ataque
Georgia 2008

VECTORES DE ATAQUE



A chave para as operações no ciberespaço são pessoas, não tecnologia.

Dr. José Carlos L. Martins

AMEÇAS...ambiente hostil

- Sofisticado, evoluído e em crescimento
- Explorado diariamente, aumentando a disrupção e o desenvolvimento de capacidades de destruição (física e lógica)
- Abordagem atual não é defensável ou com custos elevados:
  - Consciência da Situação limitada
  - Redes díspares
  - Defesa reativa (à base de assinaturas e padrões)
  - Conformidade é a nossa primeira linha de defesa

Ameças evoluem mais rápido do que a nossa capacidade de proteção contra as mesmas

CASE STUDY

New Challenges

RUSSIAN AGGRESSION
CRIMEA OCCUPATION

Attempts to get into UKR Secure Communication Network using captured Encryption devices

Network Scans against military networks

E-mail Phishing and Social Engineering

DDoS-attacks against UKR MoD web-portal to support all major occupation events

Captured GSM-base station were used to send fake and demoralizing messages to servicemen in blocked military units

Rapid "Network Enabled" Rearmament of Signal Troops

New Threats and Vulnerabilities (Cyber and TEMPEST)

Immature IA & CD Infrastructure

- Lack of Units
- Lack of FW, IPS, SIEM

Reliable and proven IA procedures don't apply any more.

Underestimation of Cyber threats at Tactical level

Lack of experienced trained technical specialists

End user – weakest link

EXERCÍCIOS MULTINACIONAIS

INTEROPERABILITY with partners

Multinational EXPERIENCE and KNOWLEDGE

Cyber Coalition – 26 nações NATO + PfP (FA + CNCS + PGR)
CWIX – 23 nações NATO + PfP
Locked Shields - Centro de Excelência Estónia "blue teams" vs. "red teams"

Questões?

TCor Paulo Branco
Centro Ciberdefesa
Estado Maior General das Forças Armadas

pjbranco@emgfa.pt