Mundos Virtuais, Riscos Reais:

Fundamentos para a definição de uma Estratégia da Informação Nacional

TCor Tm (Eng) Paulo Viegas Nunes
pfvnunesam@gmail.com

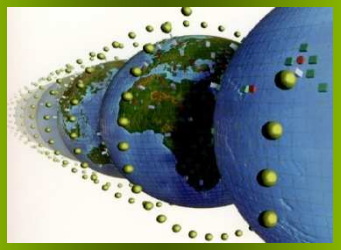
CIIWAC

Sumário

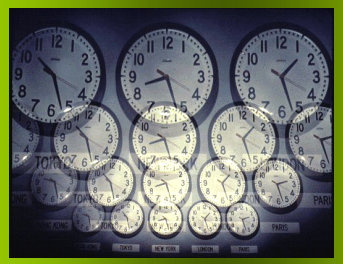
- Introdução
- Análise e Gestão do Risco Social no Ciberespaço
- Desenvolvimento de Cenários e Análise Estratégica
- Estratégia da Informação Nacional (EIN)
  - Enquadramento e Definição
  - Modelo de Implementação
  - Componente Operacional, Estrutural e Genética
- Aplicação e Validação do Modelo
- Conclusões

Introdução

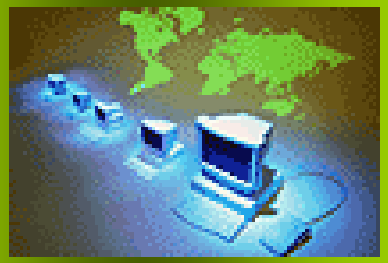
Internet e a Sociedade Global em Rede



Novos Parâmetros de Competitividade das Nações

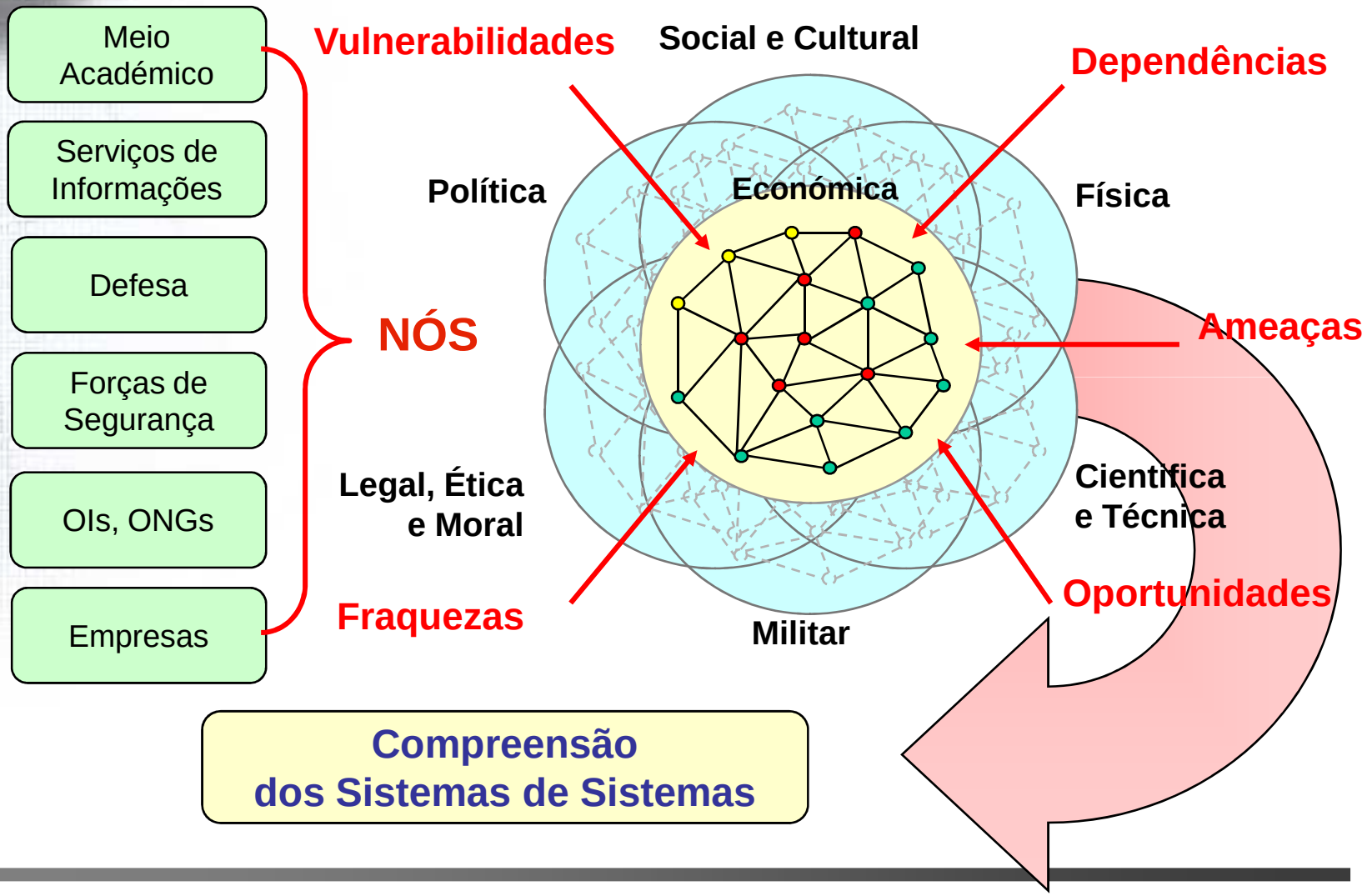


Infra-estruturas de Informação e a Soberania dos Estados



Conflitualidade da Informação

Sociedade em Rede:
um Sistema de Sistemas



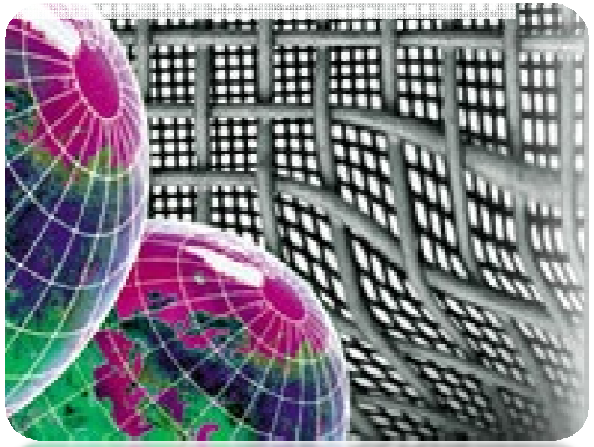
Fonte: Grossman-Vermaas (2004)

Compreensão dos Sistemas de Sistemas

Estudo do Ciberespaço

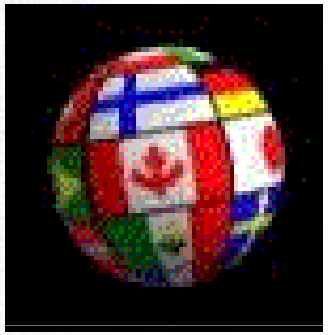
Estudo do Ciberespaço pode ser sistematizado segundo duas perspectivas:

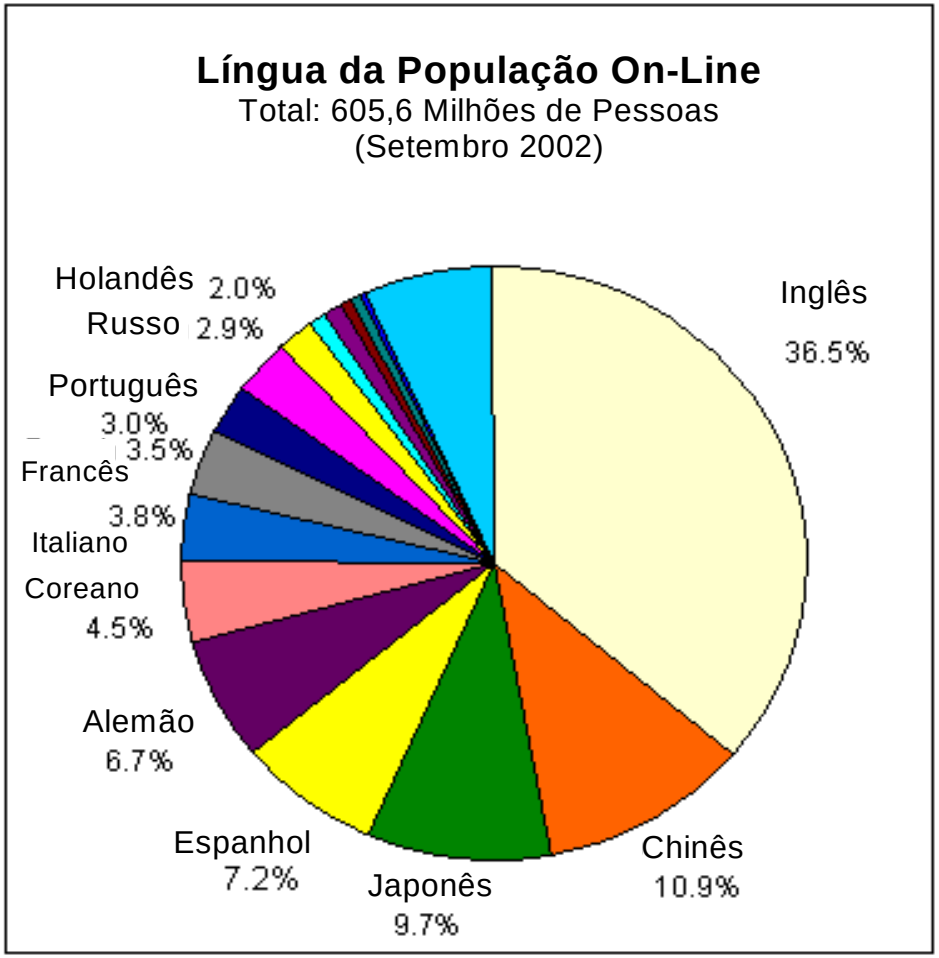
- **Espaço Virtual**
  (interacções sociais, económicas, políticas e culturais);
- **Infra-estructura Tecnológica da Informação**
  (Internet).



Evolução do Pensamento Geopolítico:

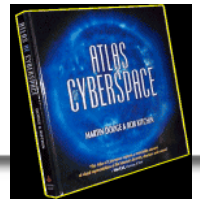
Os Interesses Nacionais



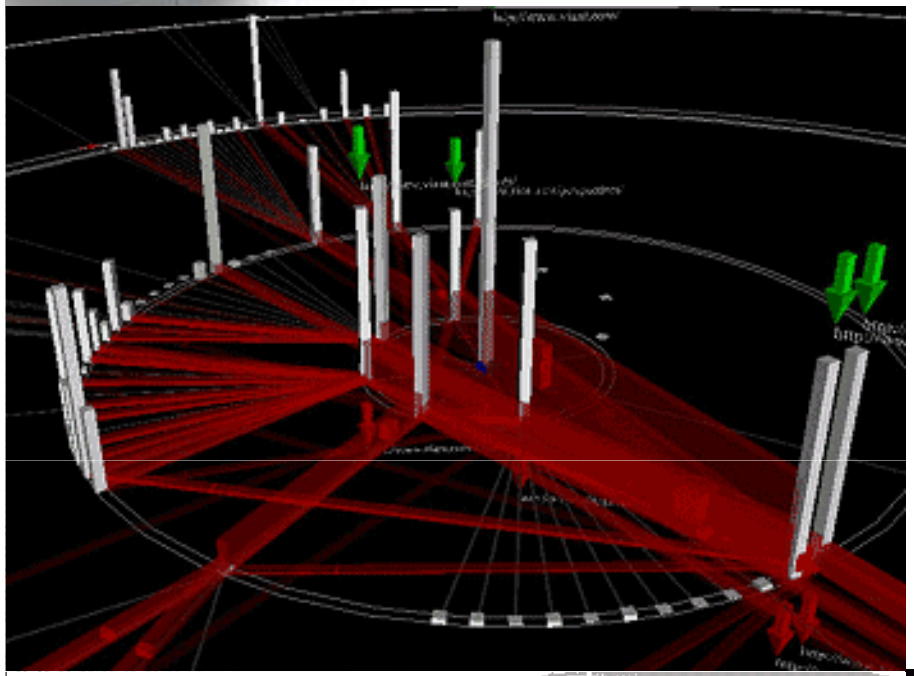


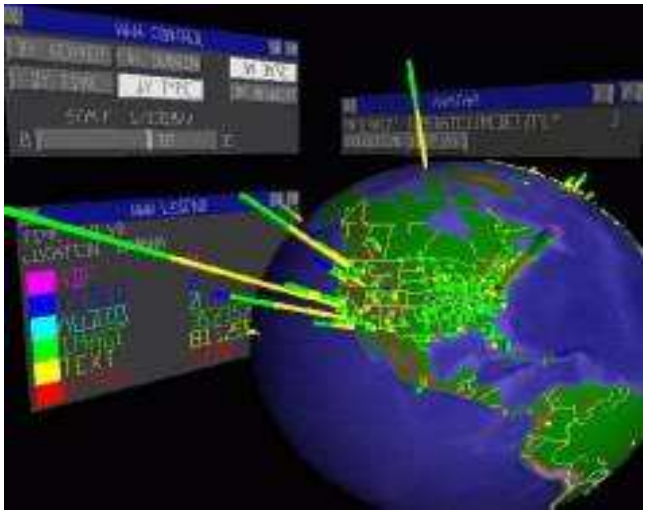
O Alargamento do espaço de influência dos Estados passa pelo desenvolvimento de uma Política para a Internet, palco de uma constante **Competição** e "**Guerra Cultural**".

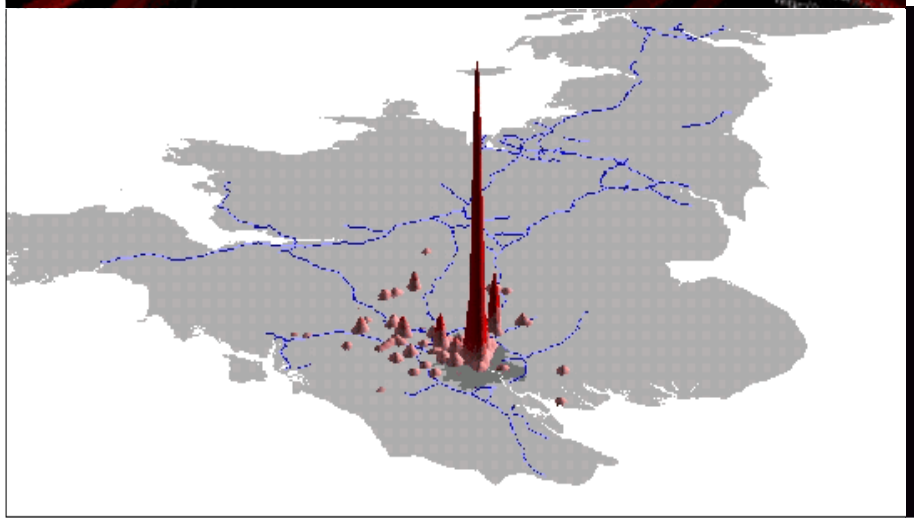
Registo de Actividade da Internet

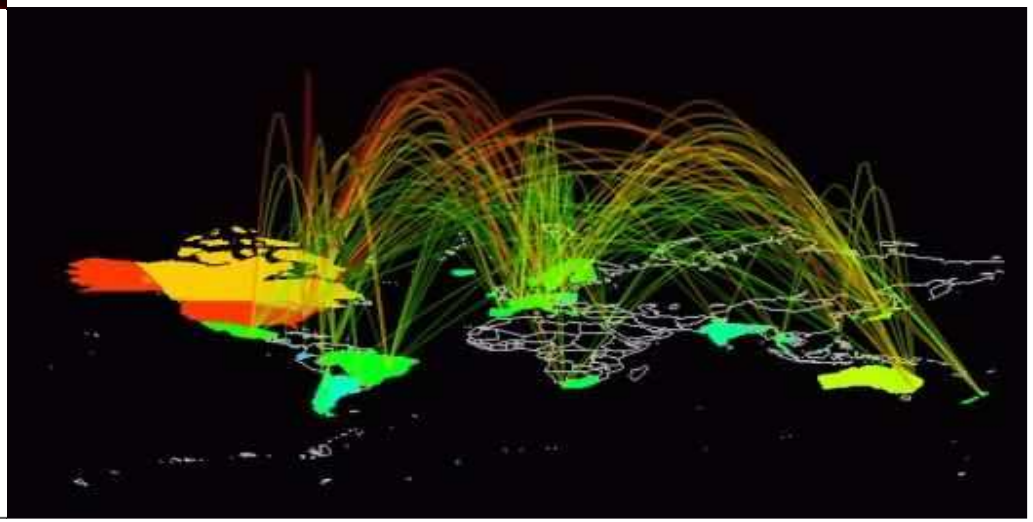


Fonte:

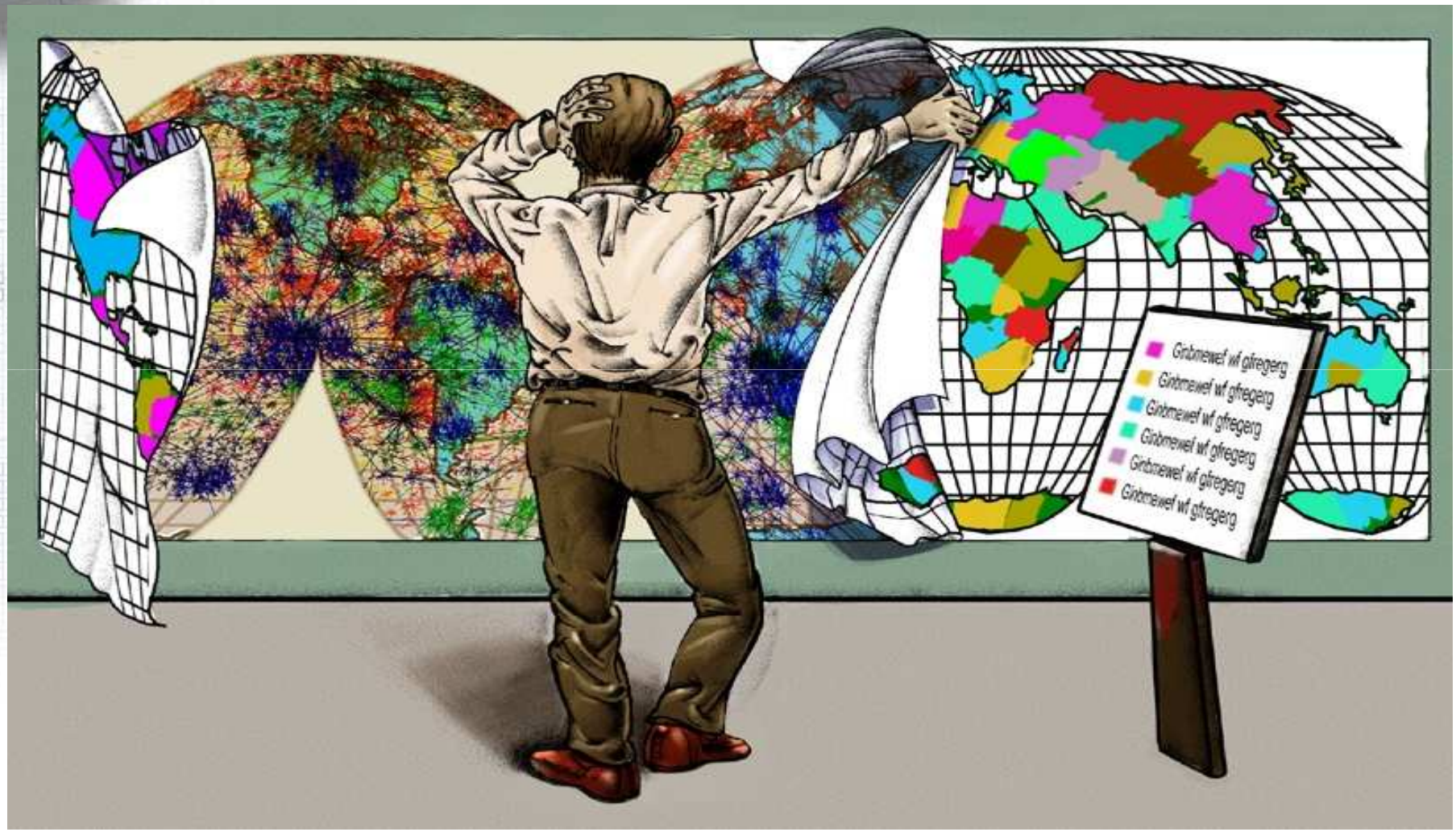








Infra-estrutura Nacional de Informação



Infra-Estruturas Críticas Nacionais:
Modelo de Interdependências

Rede Eléctrica Nacional

Redes de Telecomunicações

Transportes
(ex: Controlo Trafego Aéreo, Ferroviário, Metro, etc.)

Defesa
(ex: Sist. C3I, Radares, Mísseis, etc.)

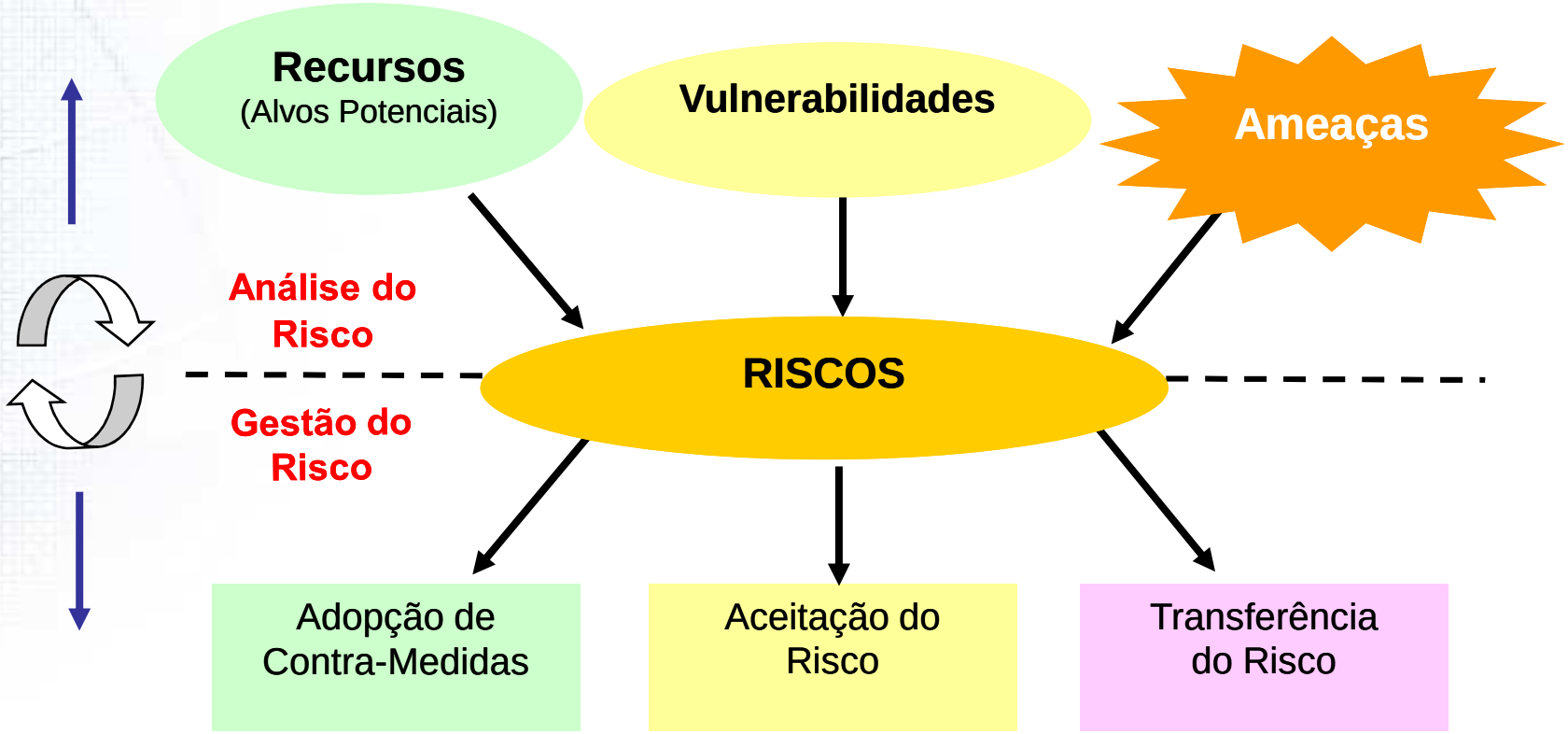
Sist. Financeiro
(ex: Banca, Bolsa, Multibanco, etc.)

Protecção Civil
(ex: Bombeiros, 112, Forças Seg., etc.)

Outras Infra-estruturas Críticas
(ex: Governo, Saúde, Sist. Distrib. Água, etc.)

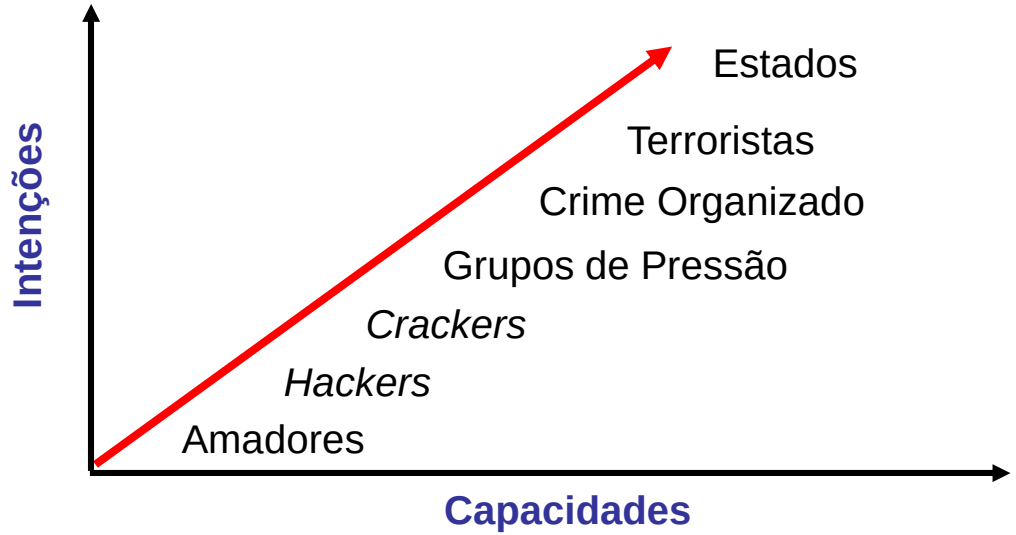
Fonte: Adaptado Gen Pinto Ramalho (2003); Eng. Sousa Cardoso (2003).

Modelo de Análise e Gestão do Risco



Fonte: Adaptado de Cardoso (2003)

Nível da Ciberameaça



Fontes: Martin Libicki (1996);
Morris (1995)

Ataque de Informação

Probabilidade X

Capacidades
vs
Intenções

Nível do Ataque

Importante
vs
Nível
Estratégico

Poder Disruptivo

Armas da
Guerra de Informação

podem ser
consideradas

Armas de
"Disrupção Massiva"

Desenvolvimento de Cenários e Análise Estratégica

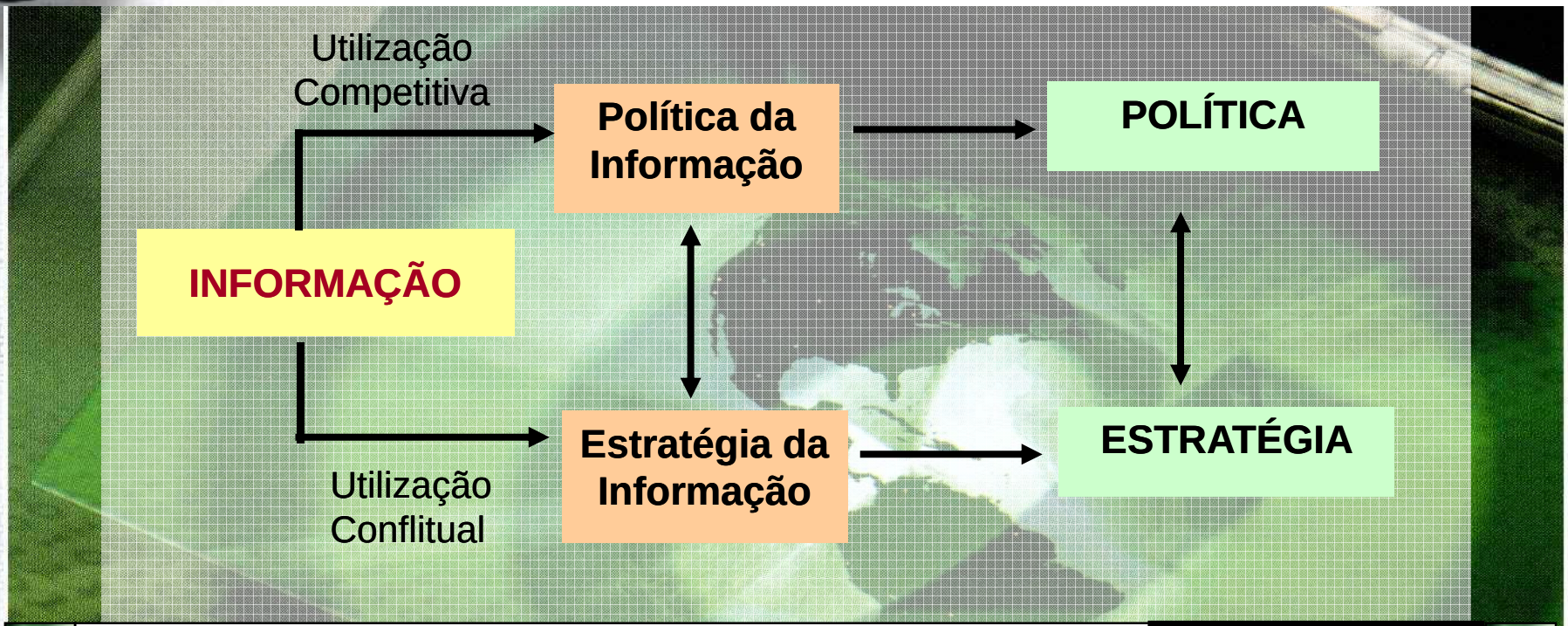
Parâmetros da Complexidade do Problema

Gama de Variação de cada Parâmetro

Vectores de Poder do Estado	Infra-estruturas Críticas Atacadas	Efeitos das Armas de Guerra de Informação	Probabilidade de Ataque	Tipo de Actores Hostis
Político/ Diplomático	Rede Eléctrica	Físicos	Muito Elevada	Amadores
Informação	Redes de Telecomunicações	Sintaxe	Elevada	*Hackers*
Militar	Sistemas de Transporte	Semânticos	Moderada	*Crackers*
Económico	Sistema Financeiro		Reduzida	Activistas
	Defesa		Nula	Crime Organizado
	Serviços de Emergência			Terroristas
	Outras Infra-estruturas Críticas			Estados

Matriz de Suporte à Análise Morfológica do Risco Social no Ciberespaço

Estratégia da Informação Nacional
Enquadramento e Definição



Estratégia da Informação Nacional

A ciência e a arte de desenvolver capacidades e explorar a informação (recurso/arma), com vista à consecução dos objectivos fixados pela Política.

Estratégia da Informação Nacional: Finalidade

- **Garantia da Informação**
  "Information Assurance"

.

- **Superioridade da Informação**
  "Information Superiority"

- **Domínio da Informação**
  "Information Dominance"

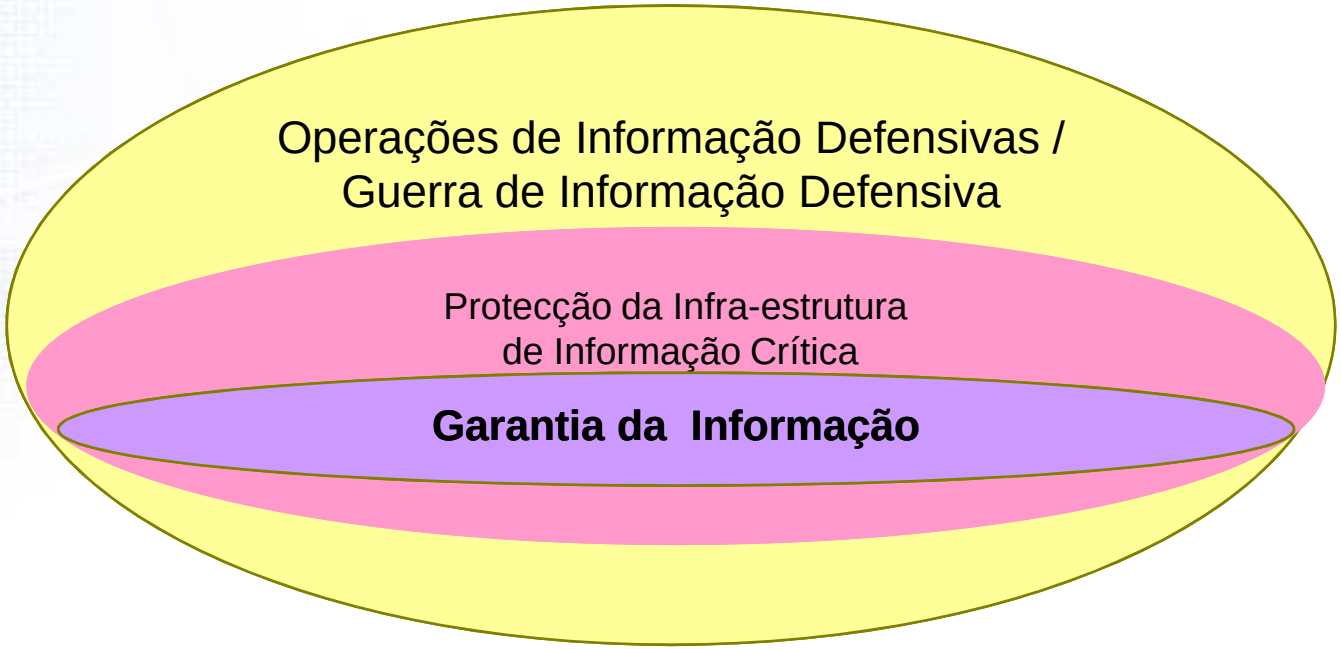
Finalidade da Estratégia da Informação Nacional :

- **Assegurar a Garantia da Informação (1ª Fase);**
- **Perspectivar a Superioridade da Informação (2ª Fase).**

Estratégia da Informação Nacional:
Domínios de Competência

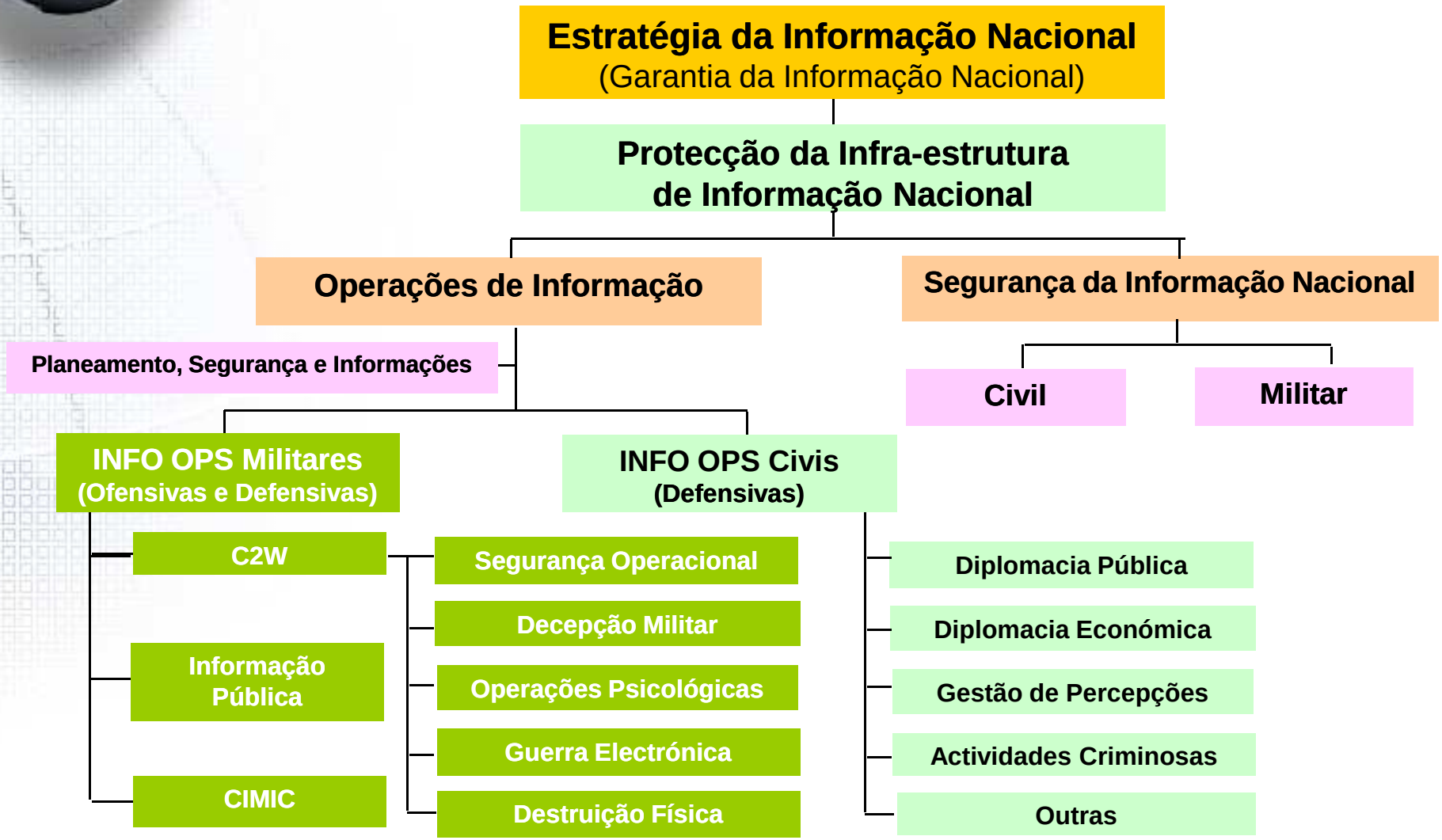
Preocupações Nacionais:

- Disponibilidade e integridade da informação de interesse Nacional;
- Eficiência com que o País processa e utiliza a informação.



Fonte: Adaptado de *National Office of IO/CIP Studies in Swedish National Defence College* (Nicander, 2001).

Estratégia da Informação Nacional
Modelo de Implementação

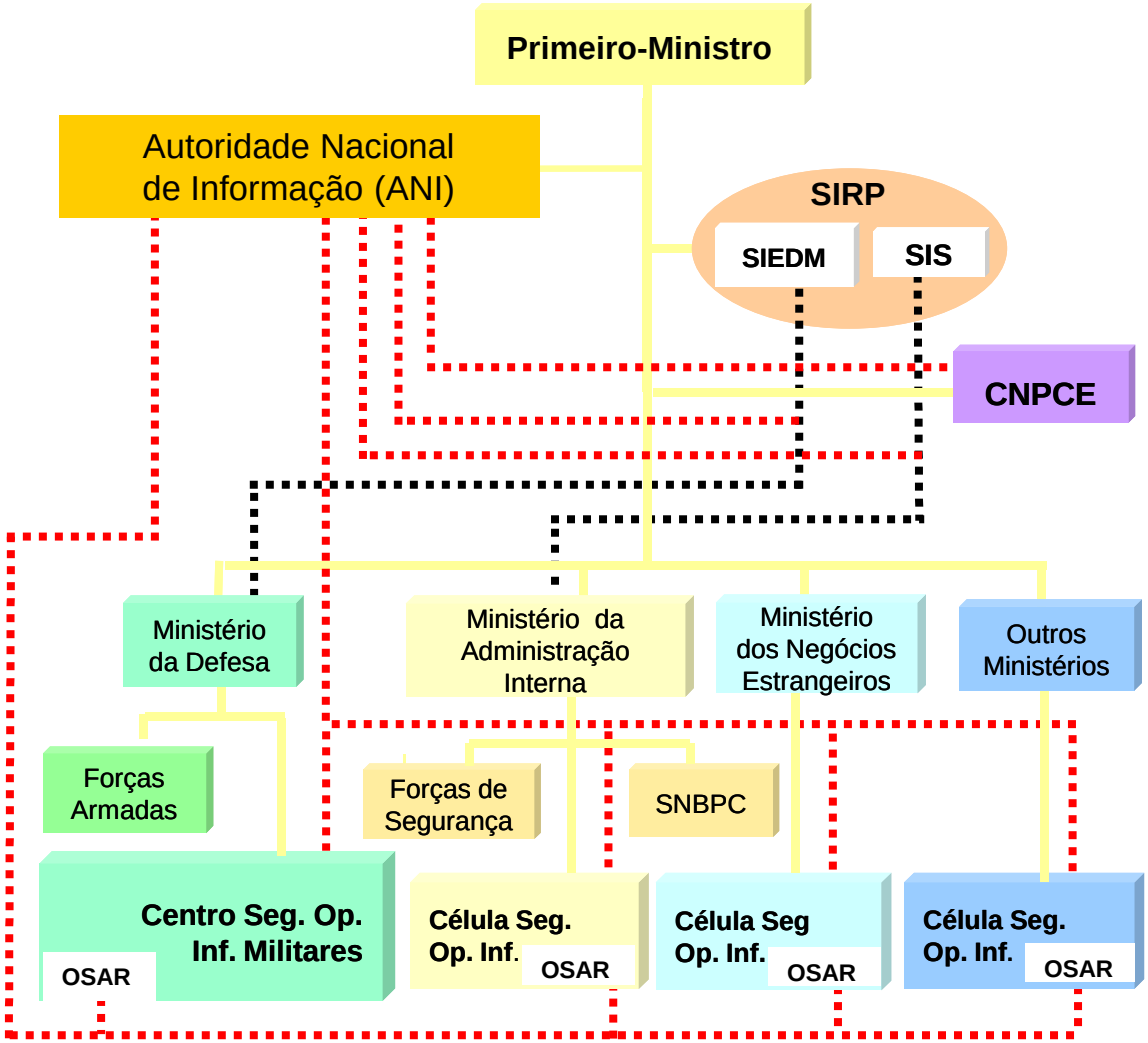


Estratégia da Informação Nacional

Estrutura do SPIIN: uma solução …

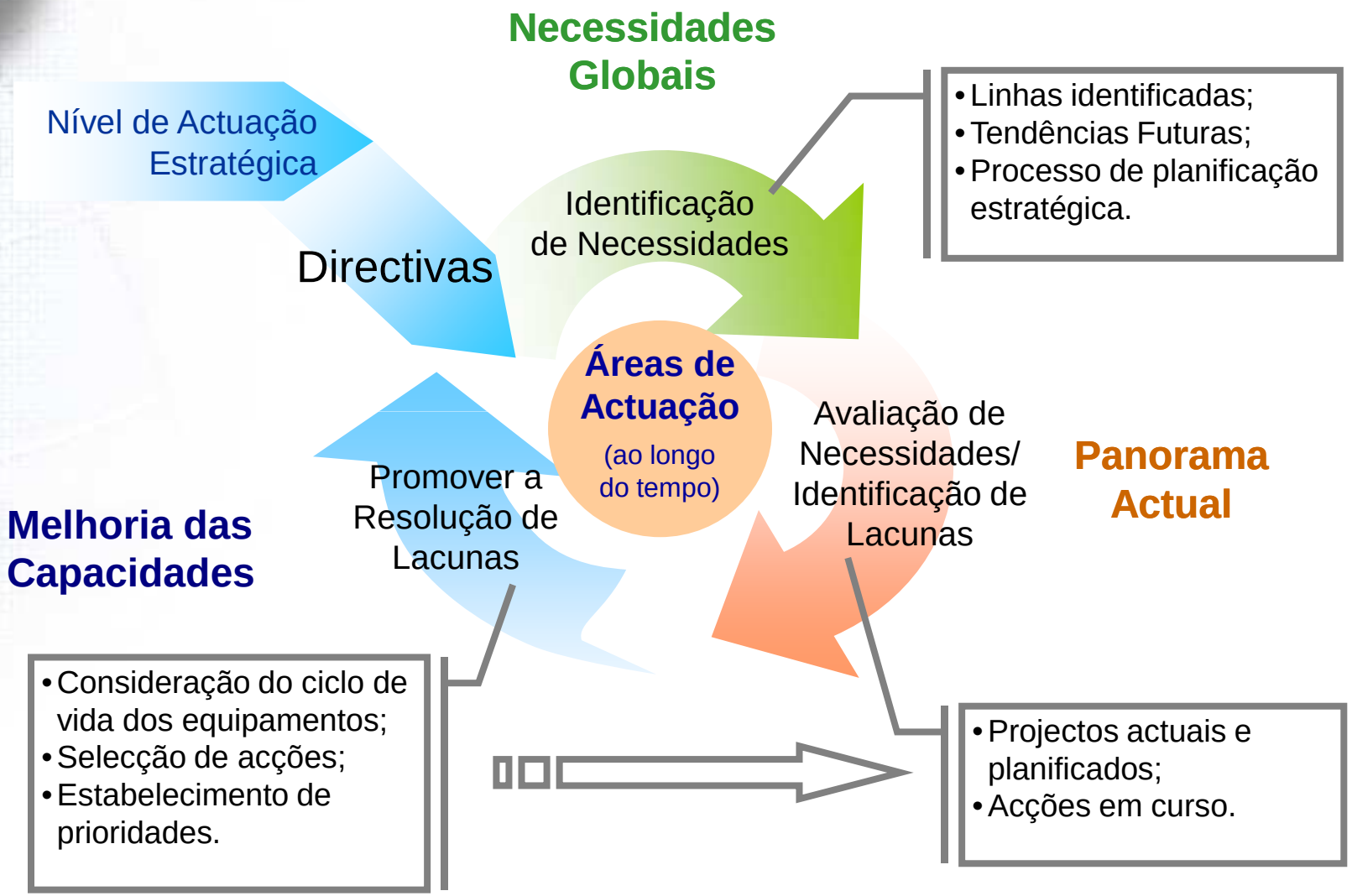
OBJECTIVO

Assegurar a protecção das infra-estruturas e recursos de informação nacionais contra eventuais ataques, de âmbito nacional ou internacional, que, afectando a Infra-estrutura de Informação Crítica Nacional, ponham em causa a consecução dos interesses nacionais e afectem a Sociedade Portuguesa



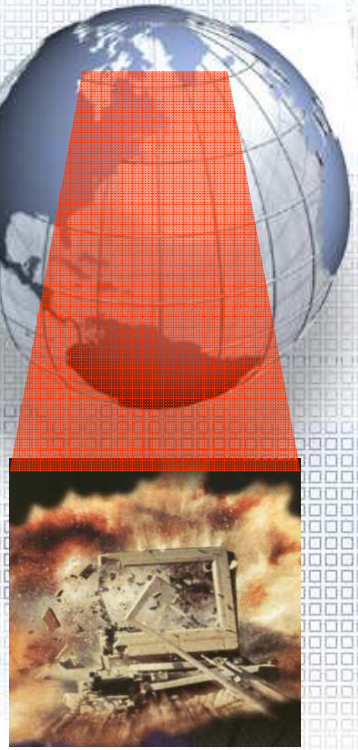
Legenda
Relação Hierárquica
Relação Funcional

Desenvolvimento de Capacidades: Processo Genérico



Fuente: CDP (2004)

Aplicação e Validação do Modelo



- Exercício “O dia Seguinte … no Ciberespaço”;
- Adaptação e desenvolvimento de ferramentas de análise e apoio ao planeamento da Gestão de Crises no Ciberespaço;
- Duas fases :
  - **“Tomada de Consciência”:** implicações do surgimento de uma Crise no Ciberespaço (acções de curto prazo);
  - **“Realismo e Pragmatismo”:** Visão político-estratégica da gestão do risco social (propostas e iniciativas I&D para reduzir as vulnerabilidades nacionais).
- Estruturação de um Exercício Nacional

Conclusões

- Desenvolvimento da Sociedade em Rede e do Ciberespaço marcam um salto na evolução da realidade Geopolítica e Geoestratégica;
- Infra-estruturas de Informação nacionais apresentam **grandes vulnerabilidades, aumentando o risco social**;
- Natureza dos desafios e a emergência de conflitos de informação (Guerra de Informação) impõem a **necessidade de desenvolver uma visão estratégica** ampla, integrada e coerente da realidade;
- Revisão do actual **quadro legal**, criação de **doutrinas**, **estruturas** e **meios** para implementar a Estratégia da Informação Nacional;
- Este modelo apresenta um enquadramento para a concepção e implementação da Estratégia de Informação Nacional.

Mesmo uma viagem de 10.000 Km ...

tem início com um simples passo ...

Questões

Mundos Virtuais, Riscos Reais:

Fundamentos para a definição de uma Estratégia da Informação Nacional

TCor Tm (Eng) Paulo Viegas Nunes
pfvnunesam@gmail.com

CIIWAC