Defesa Cibernética: Aspectos Conceituais e Práticos

Painel Terrorismo; Ilícitos Transnacionais e a Defesa Cibernética - Principais ameaças terroristas - Tráfico de pessoas, armas e drogas - Defesa Cibernética

Agenda Rumos da Política Externa Brasileira (2011-2012)

Prof. Dr. Jorge Henrique Cabral Fernandes
Departamento de Ciência da Computação e Faculdade de Ciência da Informação
Universidade de Brasília

9 de abril de 2012

Defesa Cibernética: Aspectos Conceituais e Práticos

1. Transição da Sociedade Analógica para a Digital
2. Organização da Infraestrutura da Sociedade da Informação
3. Segurança e Defesa dos Sistemas de Defesa
4. Temas de Desenvolvimento na Segurança e Defesa Cibernética da Nação Brasileira

1 - Transição da Sociedade Analógica para a Digital

Da Sociedade **Analógica** para a **Digital**

Comércio, Finanças, Transportes, Saúde, Energia, Água, Telecomunicações, Radiodifusão etc

Equipamentos Analógicos

Transição

Equipamentos Digitais Computadorizados

1850´s – 1995´s

1950´s – 1995´s – 2010´s

- **Infraestrutura com Funcionamento Rígido e pré-definido**
- **Baixa Interconectividade**
- **Diversas indústrias atuando em mercados distintos**

*** Baixa inovação e competitividade**

- **Infraestrutura com Funcionamento Flexível e atualizável**
- **Elevada Interconectividade**
- **Indústrias atuando em Mercados convergentes**

*** Alta inovação e competitividade**

Os computadores e o software transformam o mundo real em mundo virtual

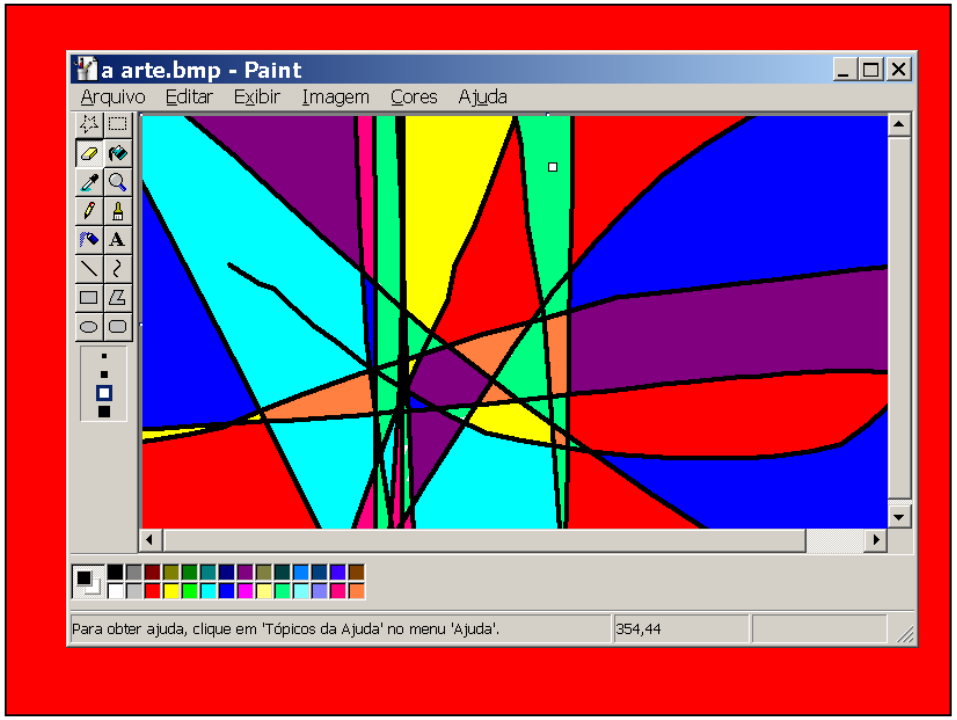
Máquinas de Calcular

Real

Virtual
(Aplicação Computacional)

Máquinas de Desenhar

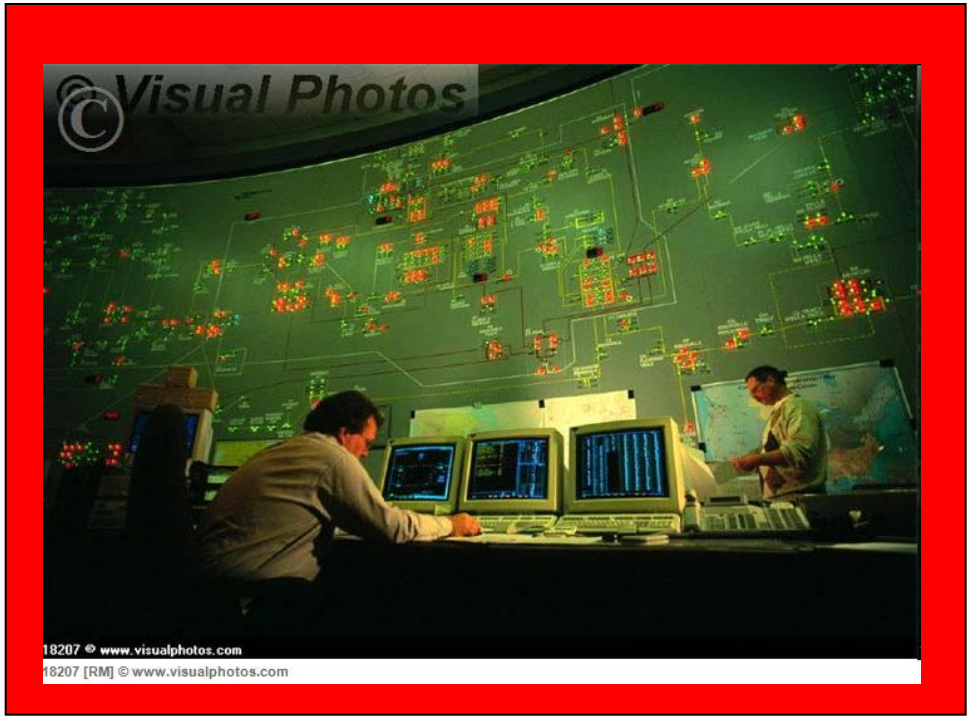
Real



Virtual
(Aplicação Computacional)

Malha de Distribuição de Energia

Real



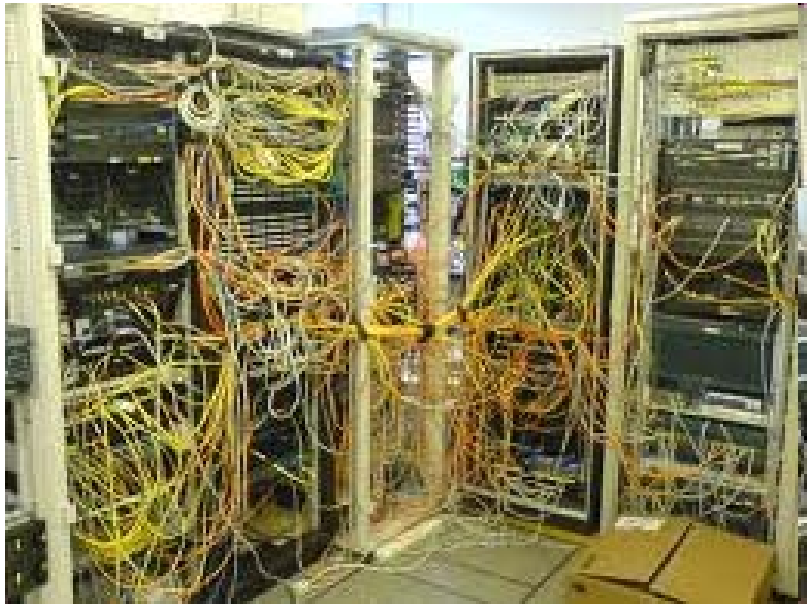
Virtual

Sistemas de Transporte

Real

Virtual
(Aplicação Computacional)

Sistema de Radiodifusão



“Complexidade Real”

Virtual
(Aplicação Computacional)

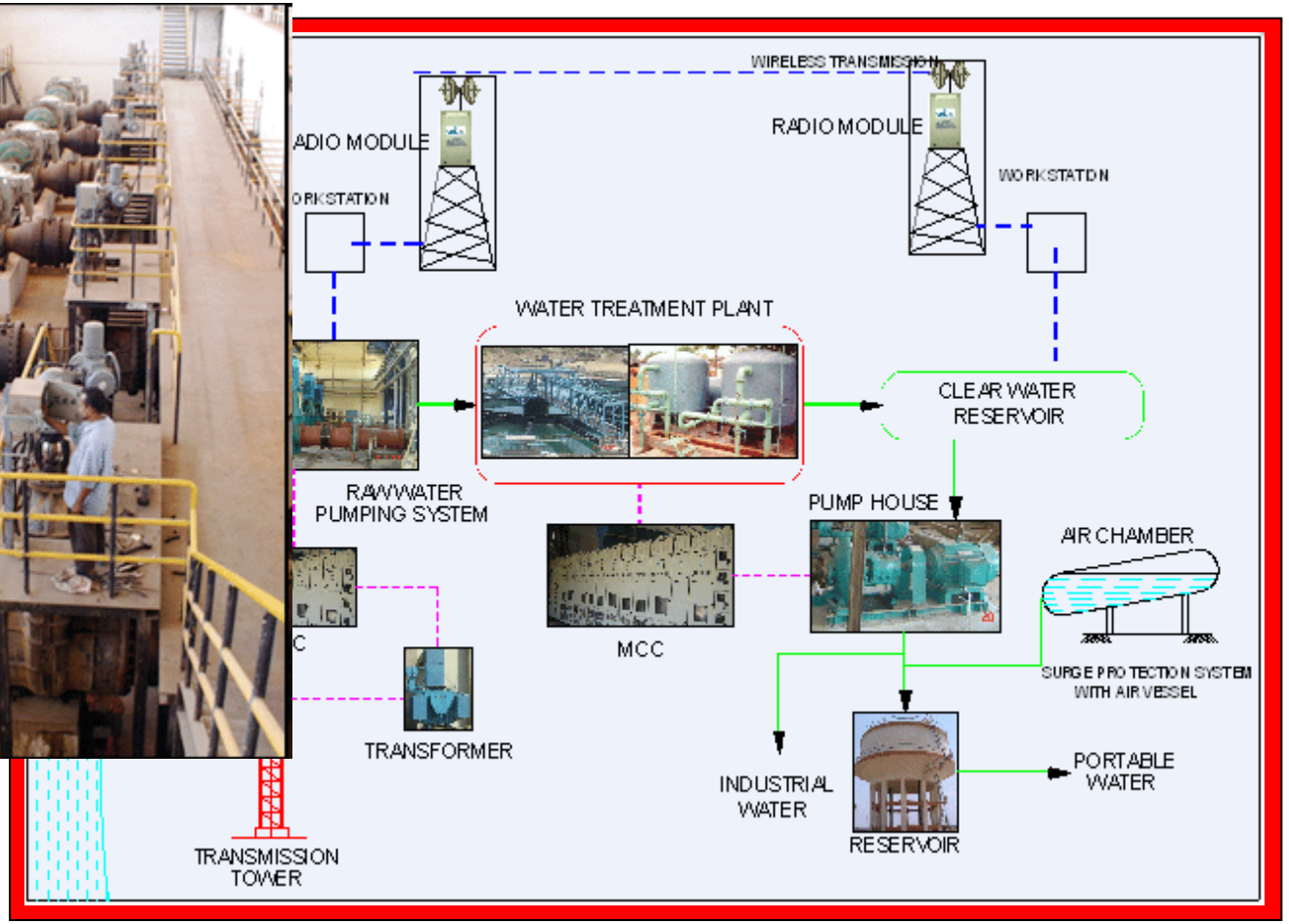
Sistemas de Telecomunicações

Real

Virtual (Aplicação Computacional)

Distribuição de Água

Real



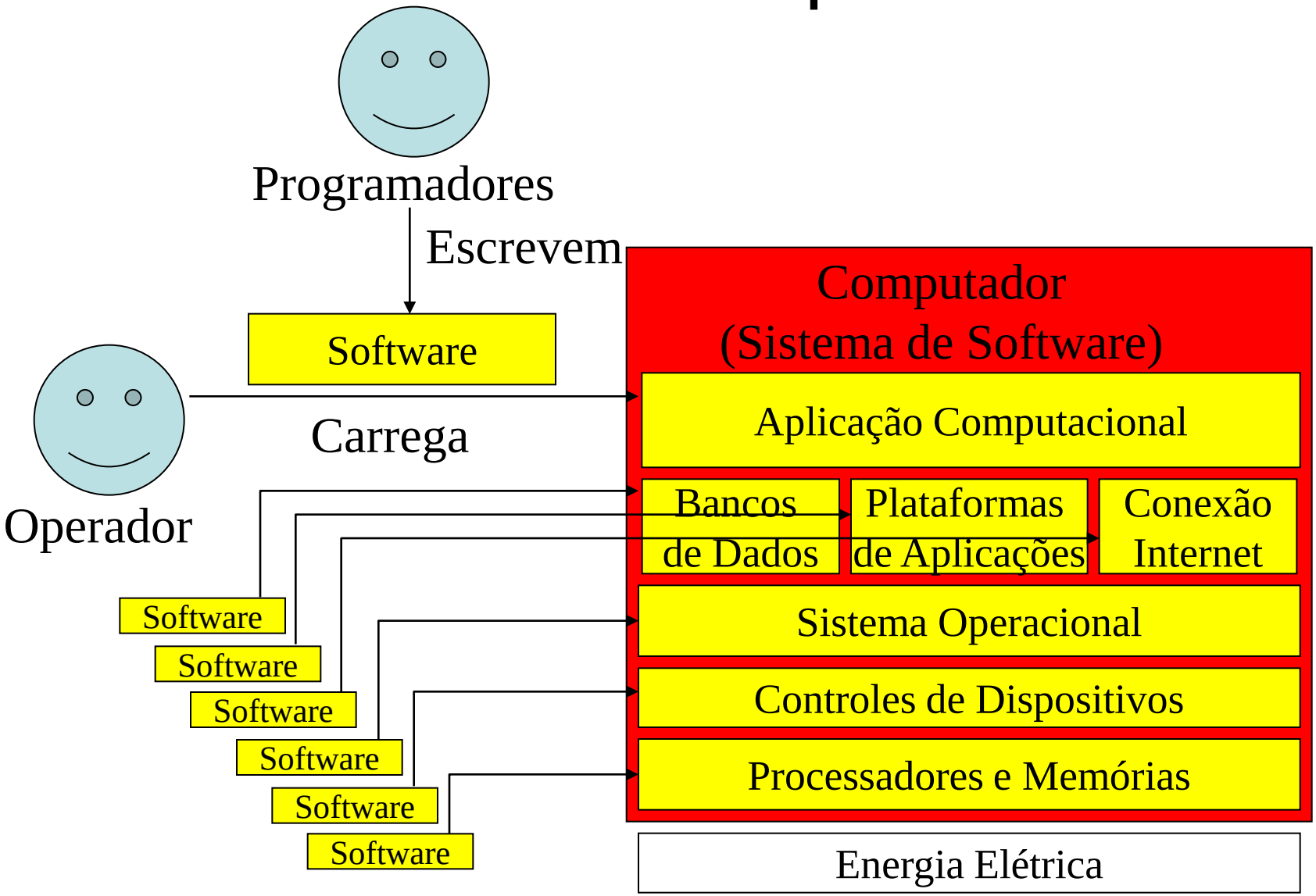
Virtual (Aplicação Computacional)

Conclusões da transição

Desenvolvemos Dependência Crítica de Software e Redes de Computadores

2 – Organização da Infraestrutura da Sociedade da Informação

Papel do Software em um Sistema Computacional

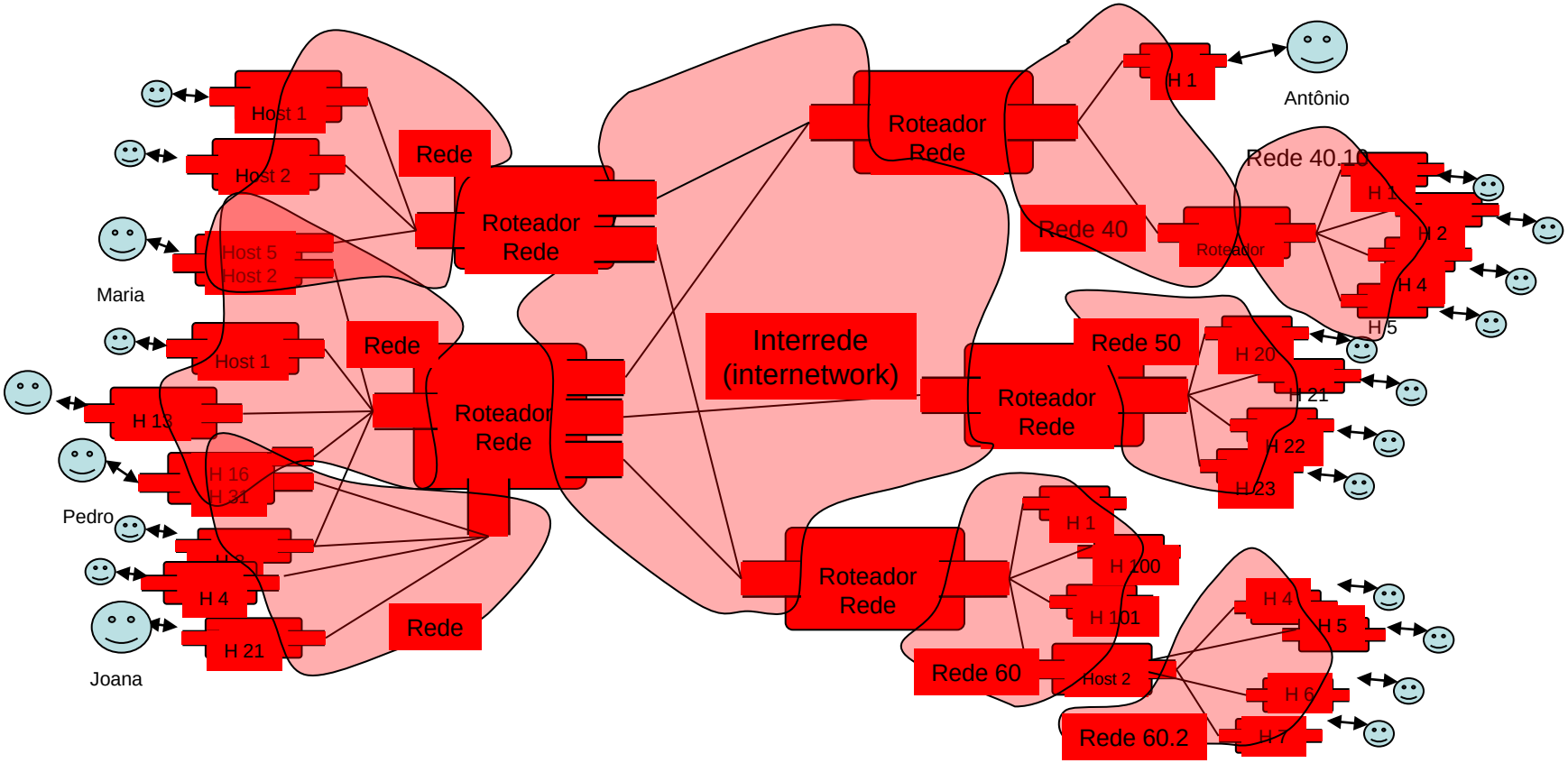


Modos de produção de software e suas consequencias

- Qualquer software
  - É produzido, de forma direta ou indireta
    - Por centenas de pessoas
    - Ao longo de vários anos e versões
    - Com vários bugs que podem produzir falhas de funcionamento
  - Quando funcionando em um computador
    - Possui vulnerabilidades latentes e presentes, que pode ser descobertas por um processo de análise sistemático
    - É vulnerável a ataques por pessoas suficientemente motivadas que tenham acesso ao mesmo

O software é o “cimento” que constitui a infraestrutura da sociedade contemporânea

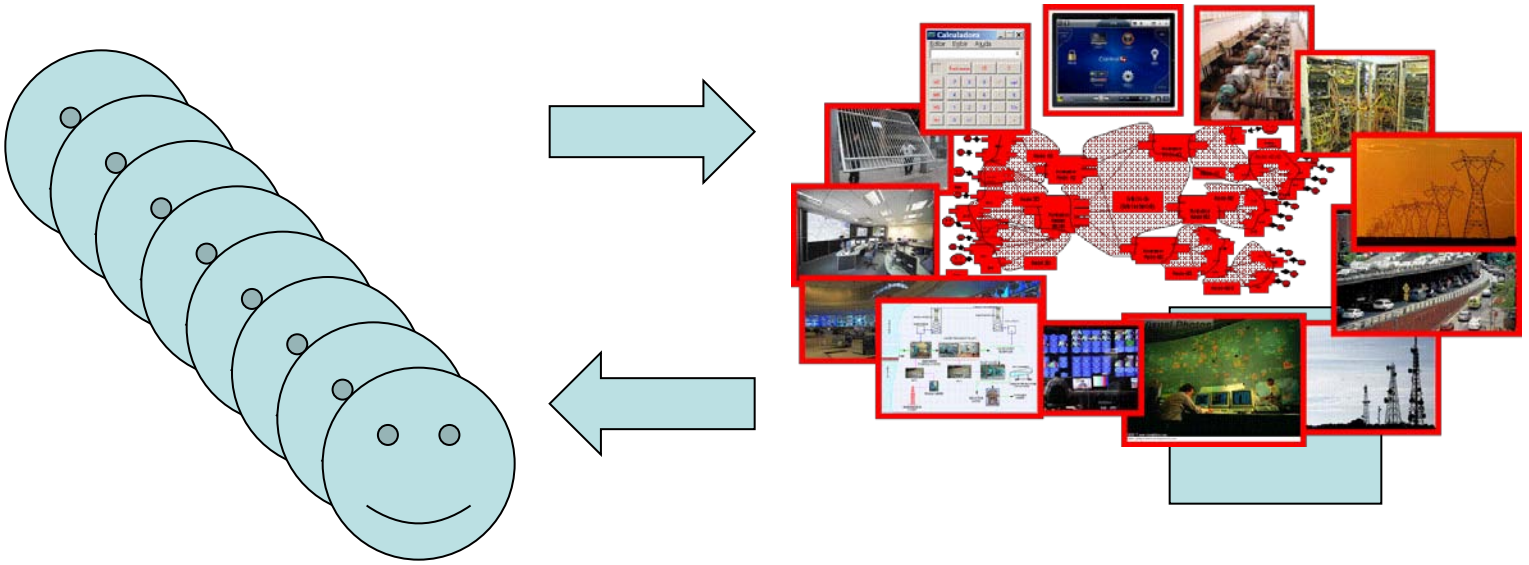
Presença de Sistemas de Software na Rede Mundial de Computadores



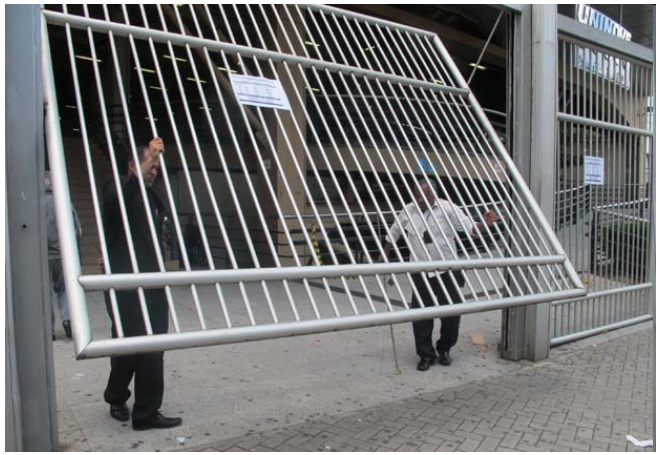
Presença dos Sistemas de Software na Infraestrutura da Sociedade da Informação

A Rede Mundial é o “aço” que dá elasticidade à sociedade da informação

Mas, no final das contas tudo vira informação...e o que importa é o uso que dela fazemos



De modo metafórico, inovamos na forma “abrir portões” e com quem assumimos compromissos ao abrir esses portões...



Manual

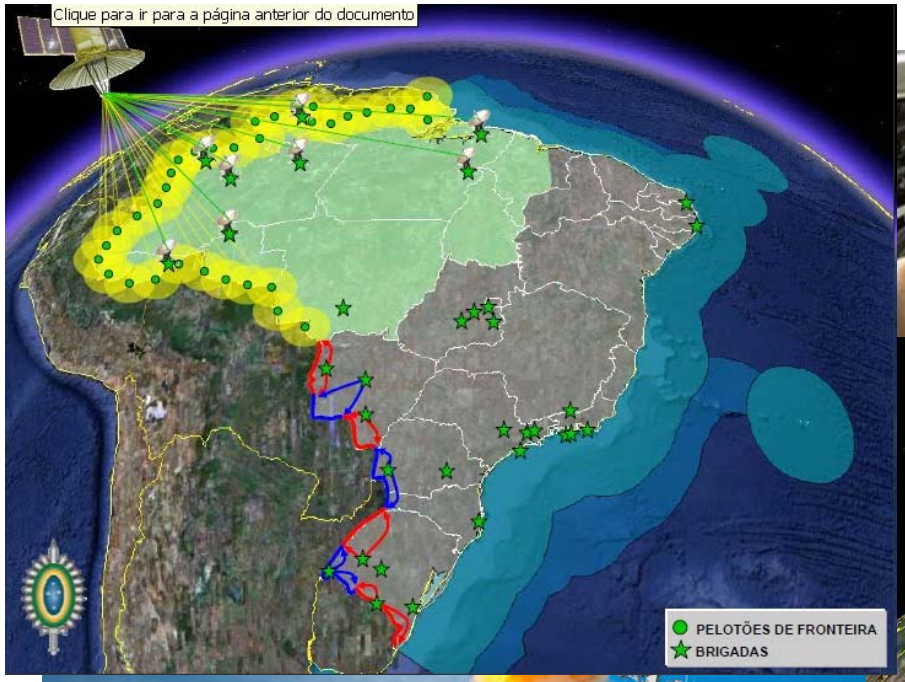
Automatizado

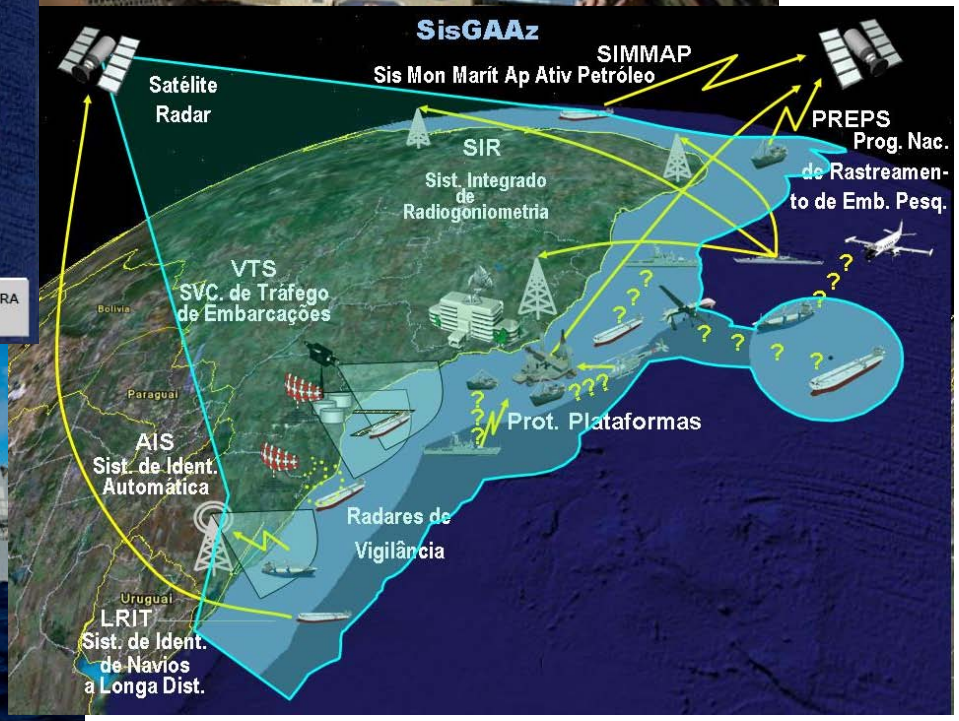
Computadorizado e Através da Internet

O Estado Atual da Sociedade da Informação

- O nosso modo de vida depende, cada vez mais de informação de qualidade
- A informação de qualidade depende do uso inteligente dos sistemas de software, interligados através da Internet, que são inevitavelmente sujeitos a falhas decorrentes de seu modo de produção, causadas por programadores ou por atacantes suficientemente interessados em causar danos ou obter benefícios financeiros ou políticos
- A sociedade tente a desenvolver dependência crítica crescente dos sistemas de computadores para atividades de Comércio, Finanças, Transportes, Saúde, Energia, Água, Telecomunicações, Radiodifusão etc

Problemas similares ocorrem em sistemas militares e de defesa...





3 - Segurança e Defesa dos Sistemas de Defesa

Alguns conflitos Cibernéticos

- Ataques perpetrados por Estados Nacionais?
  - Espionagem cibernética nas redes do Pentágono
  - Ataques à infraestrutura de TIC da Estônia
  - Guerra de informação entre Rússia e Geórgia
  - Ataques e quebra das centrífugas do Iran
- Ataques perpetrados por “Não Estados”
  - “Crimes cibernéticos” e crime organizado
  - Pichação de Sítios de Israel pelo Hamas
- Ataques às infraestruturas críticas
  - Invasão de sistemas de controle de usinas nucleares

Consequencias dos ataques cibernéticos

- Negação de serviços (“fora do ar”)
- Vazamento de informações sigilosas e (ou) proprietárias.
  - Ex: Planos, projetos e produtos
- Adulteração de informações, inclusive de controle
  - Ex: Perda de controle de sistemas
- Roubo de bens e serviços
  - Ex: Roubo de identidade
- Danos materiais e humanos

Existem soluções para o problema da segurança computacional e de rede?

- Soluções para segurança computacional
  - *Trusted Computing Base*
    - Complexo
    - Sem expressividade de mercado
  - *Trusted Platform Module*
    - Vários componentes tecnológicos
    - Em uso no Exército Norte-Americano
    - Problemas com perda de anonimidade, de direitos de usuário e de praticidade
    - Não facilita a competitividade de mercado
- Soluções para segurança de redes
  - A prática indica que, de forma geral, não é possível proteger redes baseadas em sistemas de mercado, inclusive as militares
- Engenharia e Mídias Sociais
  - Muitas vezes é desnecessário explorar vulnerabilidades técnicas de um sistema de software, bastando explorar o uso inadequado de senhas fracas
  - Mídias sociais, como Facebook, são importantes canais de informação e recrutamento de hackers

Testemunho recente no congresso dos EUA

Congress Warned That Foreign Spies Penetrate US Military Networks

March 26, 2012 By Ethical Hacker

(LiveHacking.Com) – It should be assumed that foreign spies have penetrated the US military networks was the message sent to American's politicians last week when security experts testified at hearings held by the US Senate Armed Services Committee on cybersecurity. The committee was told that enforcing a perimeter to keep out spies is unsupportable, and that the US should assume that its networks have already been fully penetrated. Instead, the committee was told, cyberdefence should be about protecting data not controlling access.

> "We've got the wrong mental model here," said Dr James Peery, head of the Information Systems Analysis Centre at the Sandia National Laboratories. "I think we have to go to a model where we assume that the adversary is in our networks."

As part of a prepared statement to the committee Dr. Peery said "A silver bullet for solving the 'cyber problem' for DoD, DOE, dot-gov or the private sector does not exist. **It is impossible to make an absolutely secure information technology (IT) system.**"

Algumas frases....

- Segundo Dr. James Perry, SANDIA Labs
  - “Devemos desenvolver um modelo onde assumimos que o adversário [Espiões Estrangeiros] está em nossas redes.”
- Segundo Dr. Kaigham Gabriel, Defence Advanced Research Projects Agency
  - “Os esforços de segurança cibernética do Departamento de Defesa (DoD) produzem o mesmo efeito de ficar boiando no meio do oceano”.
  - “O DoD supervisiona 15,000 redes de computadores, conectando 7 milhões de dispositivos com numerosos desafios a segurança, como:
    - Com apenas US$18,000 atacantes penetram nossos sistemas de detecção de intrusos
    - Em 48 horas hackers quebram 38.000 senhas, dentre 53.000
    - A cadeia de suprimentos da defesa está em risco. 2/3 dos equipamentos eletrônicos do caça avançado de combate dos EUA são fabricados for a do país
    - ..
    - Os gastos dos EUA com cybersecurity incrementam pouco a nossa segurança: O governo gastou US$ bilhões mas a quantidade de intrusões aumentou.”
- Segundo Dr. Michael A. Wertheimer, da NSA – National Security Agency
  - O governo federal perde seus talentos de TI para a iniciativa privada
  - 10% de saída esperada para 2012

Caminhos da Defesa Cibernética dos EUA

- A DARPA acredita que o DoD deve ter habilidade de conduzir operações ofensivas para defesa da nação, aliados e de interesses
- DoD precisa de “cyber tools” que provenham ao Presidente dos EUA um amplo conjunto de opções para uso na proteção dos interesses do país.
- As ferramentas devem endereçar diferentes escalas de tempo e novos alvos, requerendo trabalho integrado da guerra cibernética com a guerra eletrônica, em níveis sem precedentes.

Fonte: http://www.livehacking.com/2012/03/26/congress-warned-that-foreign-spies-penetrate-us-military-networks/

O Plano Doutrinário da Defesa Cibernética Internacional

- Não há
  - Regulamentação internacional
  - Clareza quanto à finalidade
  - Clareza quanto às respostas possíveis a um ataque cibernético
- Atuação passiva não é suficiente

Como se defender? Como responder aos ataques?

- Princípios e problemas
  - Direito a auto-defesa
  - Problema da atribuição
    - Não é fácil identificar de quem partiu um ataque
  - Ataques de não-estados?
    - Grupos terroristas, organizações internacionais, flash mobs
- Regras de engajamento (Jeffrey Carr)
  - Quando executar um ataque cibernético?
  - Qual o escopo de um ataque cibernético?
  - Duração de um ataque cibernético?
  - Quem deve ser informado quando um ataque estiver em curso?
  - Quais as situações excepcionais às regras de engajamento?

4 - Temas de Desenvolvimento na Segurança e Defesa Cibernética da Nação Brasileira

Qual a finalidade da Defesa Cibernética Brasileira?

1º É a proteção da Internet no Brasil, que constitui a infraestrutura da sociedade da informação?

2º É a proteção das infraestruturas críticas da sociedade brasileira (finanças, transportes, saúde, água e energia), considerando sua dependência da Internet e sua inserção no setor privado?

3º É a proteção dos sistemas de informação e comunicação do Estado Brasileiro?

4º É a proteção da infraestrutura militar nacional?

5º É o emprego de sistemas computacionais e de comunicação no teatro de combate, infringindo danos lógicos e físicos ao adversário e negando-lhe a capacidade de uso da Internet e do Espectro Eletromagnético

Alguns Temas de Desenvolvimento da Segurança e Defesa Cibernética(1/2)

- Aprimoramento de usos da informação e comunicação em todo o Estado e Sociedade Brasileira
  - Formação, debates e discussão de temas estratégicos
  - Popularização do problema da dependência crítica da sociedade nas TICs
  - Serviços de informação estratégicos
  - Fortalecimento da cultura de segurança da informação no Estado
- Desenvolvimento de Inteligência Cibernética
  - Coleta de dados em redes sociais e fontes abertas
  - Monitoramento e correlação de atividades potencialmente hostis
  - Identificação de grupos, intenções e planos
  - Reconhecimento de infraestruturas cibernéticas de potenciais adversários
- Cooperação no combate ao crime organizado cibernético
  - Intranacional
  - Internacional

Alguns Temas de Desenvolvimento da Segurança e Defesa Cibernética(2/2)

- Aprimoramento das segurança nas infraestruturas críticas do Estado
  - Plataformas militares e civis
  - Coleta de dados, resposta, correlação
  - Desenho de soluções técnicas de defesa em profundidade, segmentação, isolamento, diversidade de plataformas
  - Profissionais de segurança bem apoiados, programas de certificação e rede de acreditação
- Pesquisa, Desenvolvimento e Inovação em sistemas e “armas” de defesa e ataque cibernético
  - Pesquisas sobre vulnerabilidades técnicas que podem ser exploradas
  - Honeypots, Botnets, Malwares
- Integração entre setores militar e civil brasileiros
  - Indústria nacional em segurança da informação, segurança e defesa cibernética
  - Maior relacionamento e recrutamento de “hackers”

Referências e Leituras Adicionais

CARR, Jeffrey. Inside Cyberwarfare: mapping the cyber underworld. O´Reilly. 2009.

CLARKE, R.; KNAKE, R. Cyberwar: the next threat to national security and what to do about it. Harper-Collins. 2010.

FERNANDES, Jorge. Gestão da Segurança da Informação e Comunicações. Vol 1. FCU/UnB. 2010.

GRAY, Colin. Another Bloody Century: future warfare. Phoenyx. 2005

HARRIS, Shon. CISSP Exam Guide. Osborne. 2005.

KRAMER, F.; STARR, S.; WENTZ, L. Cyberpower and National Security. National Defense University. 2009.

MANDARINO JUNIOR, Raphael. Segurança e Defesa do Espaço Cibernético Brasileiro. CUBZAC. 2010.

PR; SAE. Desafios Estratégicos para a Segurança e Defesa Cibernética. 1ª Edição. Secretaria de Assuntos Estratégicos. 2011.

RICE, David. Geekonomics: the real cost of insecure software. Addison-Wesley. 2008.