Segurança Cibernética: desafio ou oportunidade?

DISCLAIMER

- **How to write a Disclaimer**
- First things first, You will need to decide what kind of information to include in your disclaimer. A disclaimer is basically just a declaration, so you may just want to declare some or all of the following.
- **Step one** - You will need to convey to your readers that your blog/website is a personal blog/website and that all articles and opinions contained within are your own.
- **Step two** - Explain to your readers that your personal opinions and writings are not meant to defame, purge, humiliate, and or injure anyone should they decide to act upon or reuse any information provided by you.
- **Step three** - Mention the fact that any comments left by any other independant readers or authors are the sole responsibility of that person.
- .
- **Step four** - Include a paragraph or two requesting your readers to contact you directly via email should they wish for you to remove any content that they have identified as being sensitive, harmful, or unnecessary.
- **Step five** - The last thing you may like to include is a legal statement referring to any applicable laws and or regulations pertaining to the country in which you live.
- A legal statement is something that you may need to speak to a lawyer about. I am not a lawyer and therefore can not recommend what you should write. I am also unsure of whether or not a self written disclaimer would stand up in a court of law or not. Again that is something you would have to speak to a lawyer about.
- What I do know, is that writing a disclaimer can be a fun experience. Because they can be made intersting and have the potential to attract readers. I often read blog disclaimers and have found some really well written ones that were great to read.
- So why not write your own disclaimer today.

Fonte: http://lukespook.hubpages.com/hub/how-to-write-a-disclaimer

Sumário

- Introdução
- Resumo Conceitual
- Guerra X Crime
- Ações patrocinadas de Estados-Nação
- Quando um ataque cibernético é considerado um ato de guerra?
- Inteligência Cibernética

Fear, Uncertainty and Doubt

Bons e “velhos”(?) tempos ☺

A control system protected by a real air gap: IBM 360/195 playing chess, November 1974.

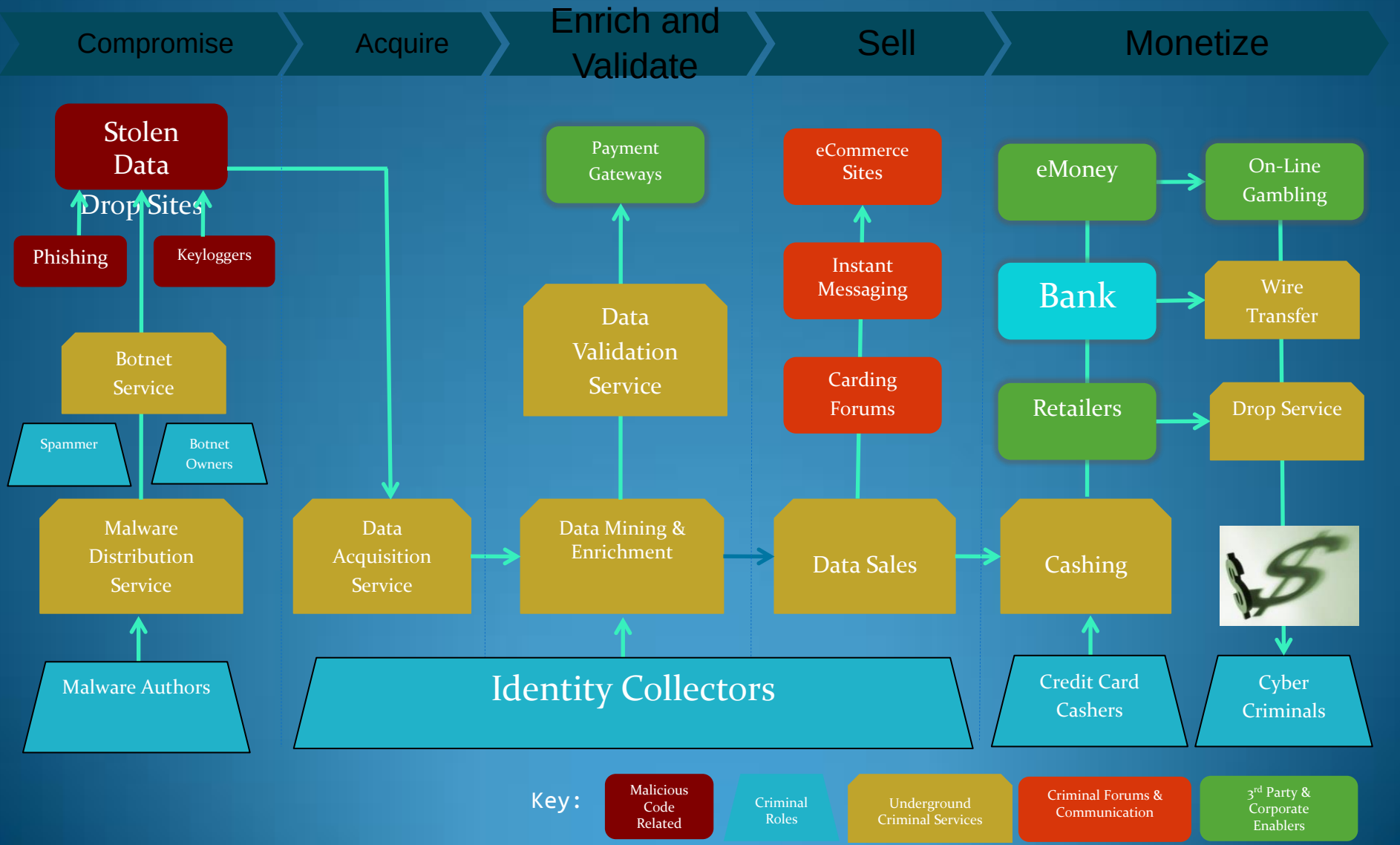
Conceitos

- No contexto das ameaças cibernéticas pode-se elencar quatro domínios de atividade hostil e comportamento:
  - ataques cibernéticos patrocinados pelo Estado,
  - extremismo ideológico e político,
  - a criminalidade organizada e
  - crime de nível/individual.
- Estes domínios são interligados.

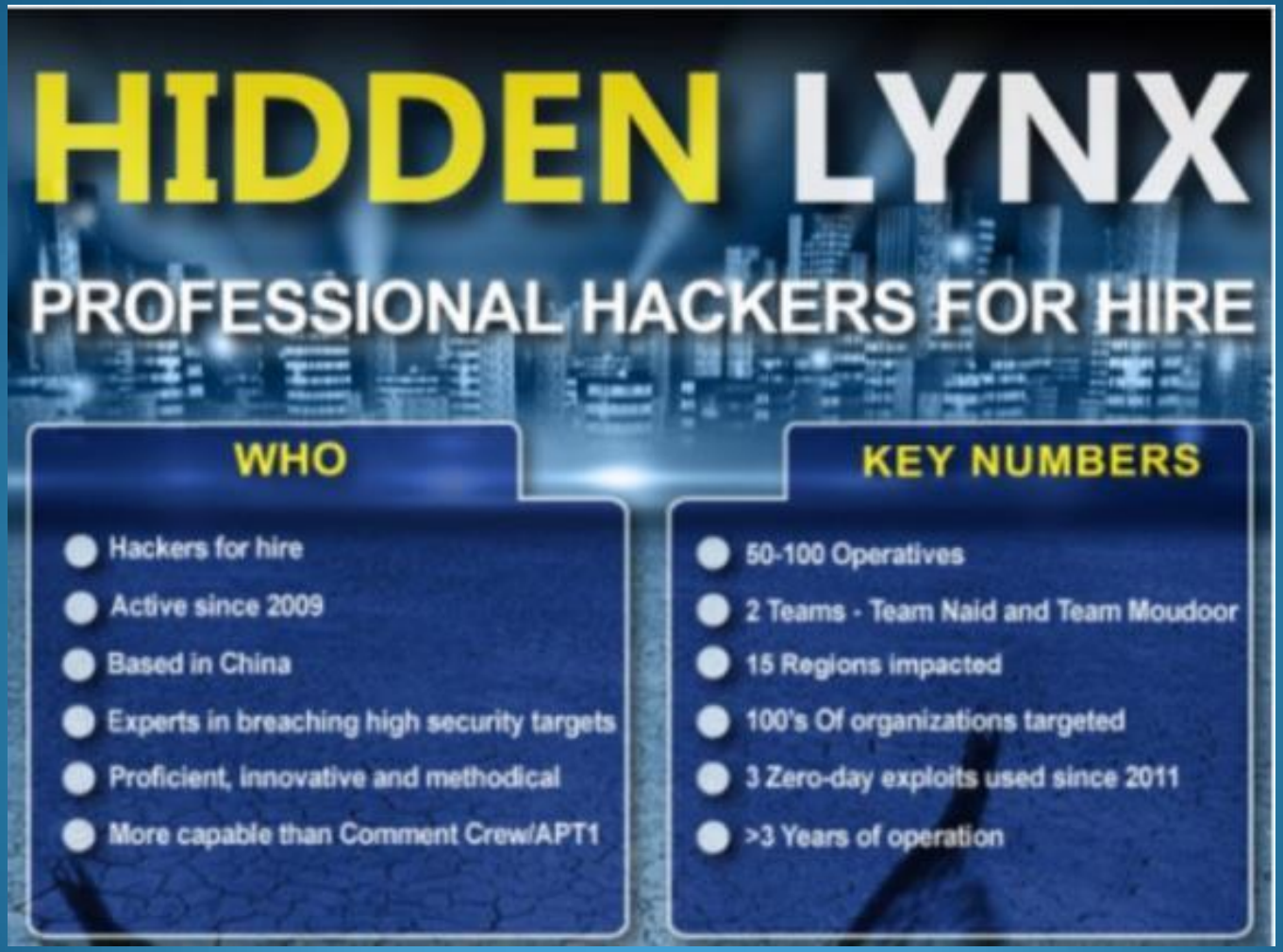
Conceitos

- Tipos de ameaças cibernéticas:
  - Visando diretamente o computador:
    - Botnets
  - Crimes tradicionais que utilizam o computador como uma ferramenta
    - Fraude em internet banking
    - Lavagem de dinheiro cibernética
    - Servidores da economia subterrânea

Economia Subterrânea



Hacker delivery



Guerra x Crime

Guerra x Crime

Guerra

- Governo / Estado
- Sistema financeiro oficial
- Recursos Oficiais
- Financiamento
- Expertise?
- Exploits/Vulns?

Crime

- Privado
- Sistema financeiro semi-oficial (crime organizado)
- Auto financiamento?
- Expertise própria (caseira+ terceirizada)
- Mercado de exploits

Ações patrocinadas por Estados-nação

Atribuição

- é o esforço para identificar o responsável por um ataque cibernético.
- Técnica de atribuição é a capacidade de associar um ataque a um responsável através de meios técnicos, com base nas informações disponibilizadas pelo fato do ataque cibernético em si — isto é, atribuição técnica baseia-se em pistas disponíveis em cena (ou cenas) do ataque.
- As duas questões-chave na atribuição técnica são **precisão** e **exatidão**.

Ações patrocinadas por Estados-nação

- A triste realidade é que a **técnica de atribuição** de um ataque cibernético é muito difícil de ser realizada pois "**bits não vestem uniformes**" e pode ser quase impossível de ser efetivada quando um usuário inconscientemente comprometido ou inocente está envolvido.

Ações patrocinadas por Estados-nação

- **Intenção**
  - Atribuição de um ataque cibernético ajuda, mas se a parte identificada como sendo responsável não é um governo nacional ou outra parte com intenções declaradas na direção do Governo, será praticamente impossível determinar a intenção com alta confiabilidade.
  - Determinações de intenções e atribuição da fonte são muitas vezes complicadas, e inadequadamente tendenciosas, por falta de informação.

USA

- Atividade exaustivamente documentada em torno da preparação para guerra cibernética, bem como agências de governo/militares com capacidades ofensivas prontamente disponíveis.
- Recrutamento maciço de profissional em defesa/ataque para diferentes departamentos:
  - USCC (United States Cyber Command – inclui AirForce, Marines, Navy and Army service components)
- NSA

Rússia

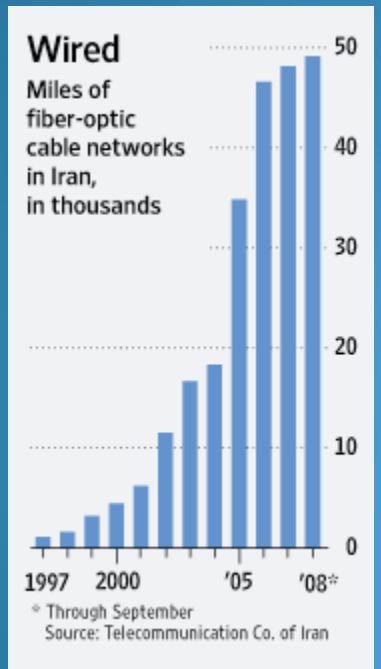
- GRU (Direção principal de inteligência das forças armadas russas)
- SVR (Serviço de Inteligência Estrangeiro)
- **FSB** (Serviços de Segurança Federal)
- Centro de Pesquisa da força militar de países estrangeiros
- Vários “National Youth Associations” (**Nashi**)

China

- PLA (Exército de Libertação do Povo)
- Relatório do Grupo Northrop Grumman
- Departamento 4 – contra-medidas eletrônicas – capacidade ofensiva
- Department 3 – Inteligência de Sinais – capacidade defensiva
- Departamento 7 – cyber ataques.

Iran

- Infraestrutura de Telecomunicações
- Monopólio das tecomunicações pelo Governo.
- Forças Armadas Iranianas.



Israel

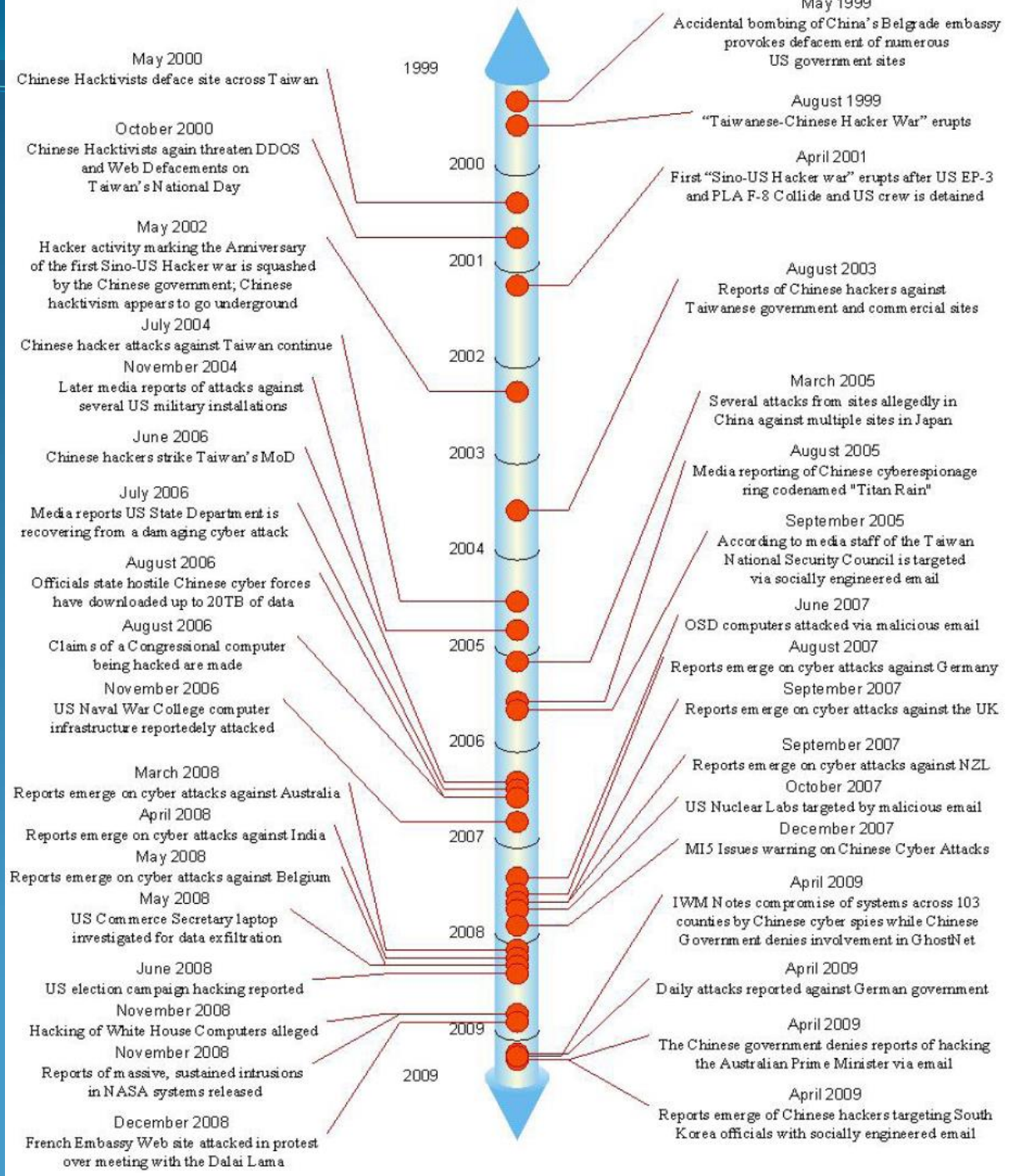
- IDF (Forças de Defesa de Israel):
  - capacidades cibernéticas.
- C4I (Command, Control, Communications, Computers and Intelligence) ramificações na Inteligência e comandos da Força Aérea.
- O pessoal é na sua grande maioria composto de nacionais treinados no exército e outras agências governamentais.
- Mossad? (olhem a seção de empregos no site mossad.gov.il...)

Quando um ataque cibernético é considerado um ato de guerra?

- O conflito cibernético é um **problema estratégico** novo e complicado.
- Não há um **quadro de política** adequada para gerenciar conflitos no espaço cibernético nem um léxico satisfatório para descrevê-lo.
- **Incerteza** é o aspecto mais proeminente do conflito cibernético – na atribuição da identidade de atacantes, o âmbito dos danos colaterais e o efeito potencial sobre o destino pretendido de ataques cibernéticos.
- O conflito cibernético será **parte da guerra no futuro** e as forças armadas avançadas agora têm a capacidade de lançar ataques cibernéticos não só contra as redes de dados, mas também contra a infraestrutura crítica que dependem destas redes.
- O conflito no espaço cibernético **combina** o crime, a espionagem e a ação militar de maneiras que muitas vezes tornam estes elementos indistinguíveis.
- A **utilização de criminosos cibernéticos por Estados** tornou-se um elemento de conflito cibernético, alguns países usam criminosos como agentes ou mercenários contra outros Estados.

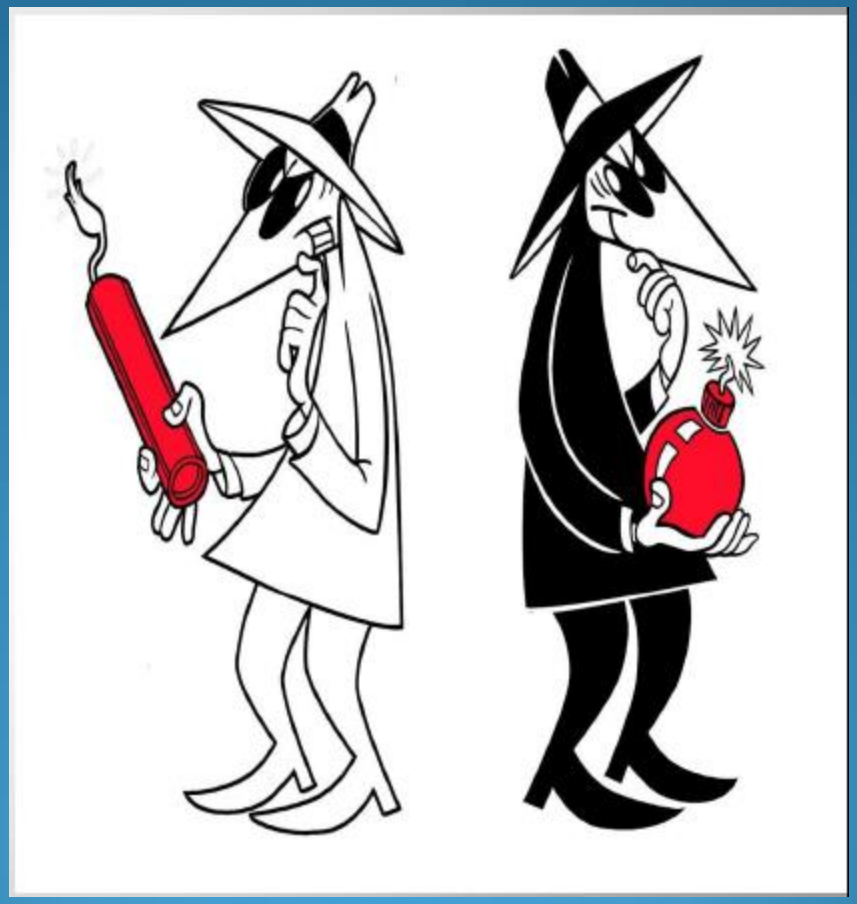
Um foco sobre a China

- Recentes alegações de espionagem cibernética por chineses dependem em grande medida de provas relatadas.
- A prova mais comum prevista pelas vítimas desses ataques consiste em arquivos de log ou malware que mostra conexões feitas por computadores infectados para endereços IP atribuídos da República Popular da China.
- Este tipo de prova é circunstancial na melhor das hipóteses.
- Estatísticas de uso de Internet sugerem que atribuir as ocorrências de guerra da informação na Internet aos chineses pode ser um engano.



Cronologia de eventos cibernéticos significativos relacionados com a China – 1999 a abril de 2009
Fonte: Northrop Grumman Corporation, Information Systems Sector

Inteligência Cibernética



Inteligência cibenética

- Há uma grande suspeita que o exército Popular da Coréia do Norte tenha atuado no background dos ataques de 20 de março e 25 de junho de 2013 ocasionando mais de 25 falhas em sistemas críticos da Coréia do Sul.

Inteligência cibenética

- Durante o primeiro semestre de 2013 as atividades de inteligência cibernética na internet foram sendo divulgadas ao público e com isso a tensão está aumentando em todo o mundo.
- Em janeiro o New York Times anunciou que seu sistemas tinham sido continuamente atacados pelos hackers chineses.
- O New York Times reportou em 19 de fevereiro de 2013 que a Divisão 61398 do Exército de Libertação do Povo chinês estaria secretamente envolvido no incidente da divulgação de informações dos EUA de acordo com o relatório da Mandiant.
- O Departmento de Defesa americano insistiu que o governo chines e o Exército de Libertação do Povo estariam profundamente envolvidos em atividades de inteligência cibernética.
- Como consequência impôs fortes restrições de importação contra equipamentos e dispositivos de redes chineses (Huawei?)

Inteligência cibenética

- O Syrian Electronic Army atacou o programa de previsão do tempo da BBC, o Guardian, e as contas Onion Twitter .
- Especialmente em 23 de abril as cotações das bolsas foram atingidas em função de ataque do Syrian Electronic Army às contas do twitter da AP news que começaram a divulgar mensagens falsas de uma explosão na Casa Branca em Washington,DC.

Inteligência cibenética

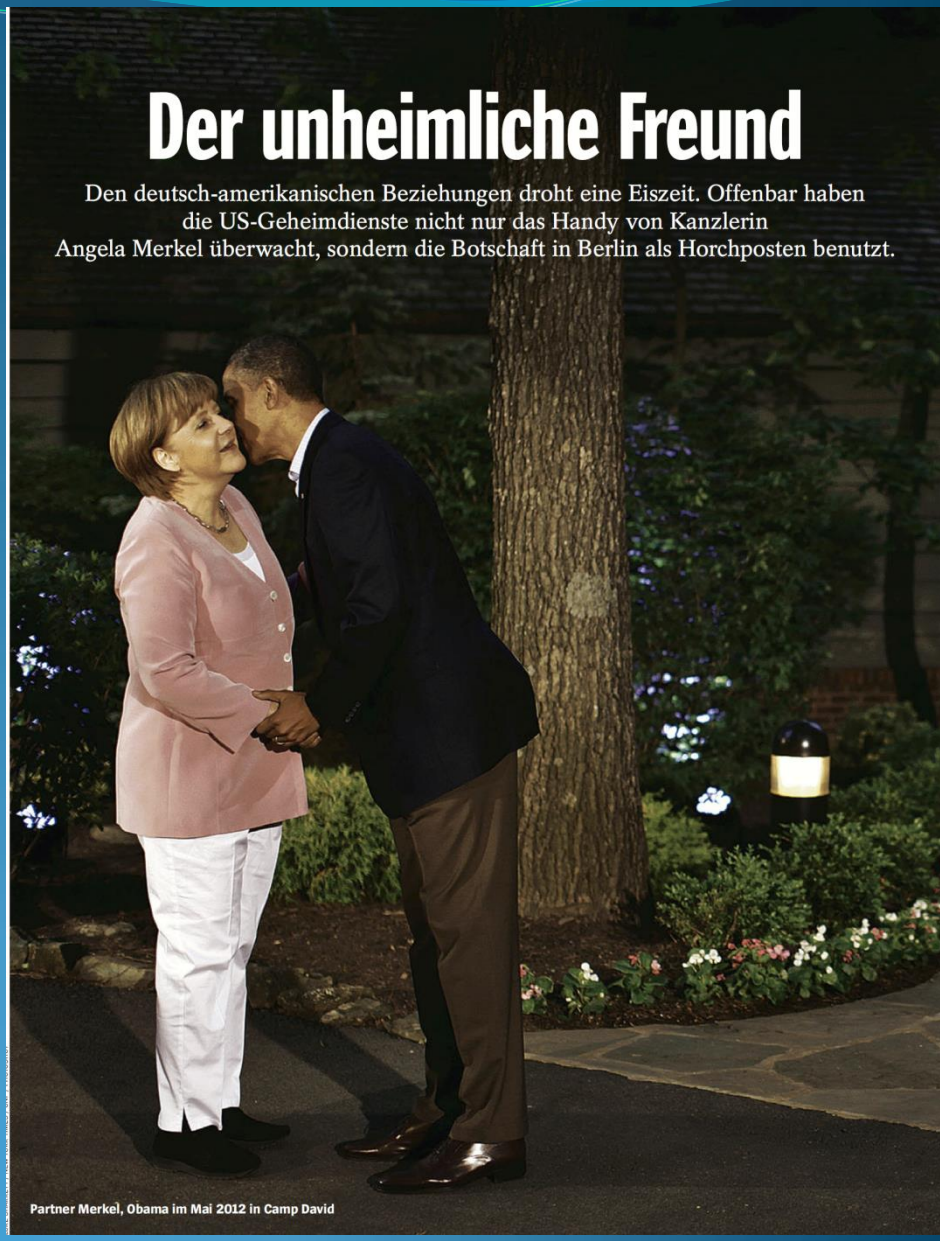
- No início de junho o Guardian expôs o PRISM um programa de coleta massiva de dados para detectar terroristas e prevenir terrorismo.
- Em 10 de junho, o Foreign Policy reportou que a NSA tem uma organização interna responsável por hackear computadores e sistemas chineses.
- Além disso, o Guardian revelou que a agência de inteligência do governo britânico teria hackeado cada delegação durante a reunião de 2009 do encontro do G20.

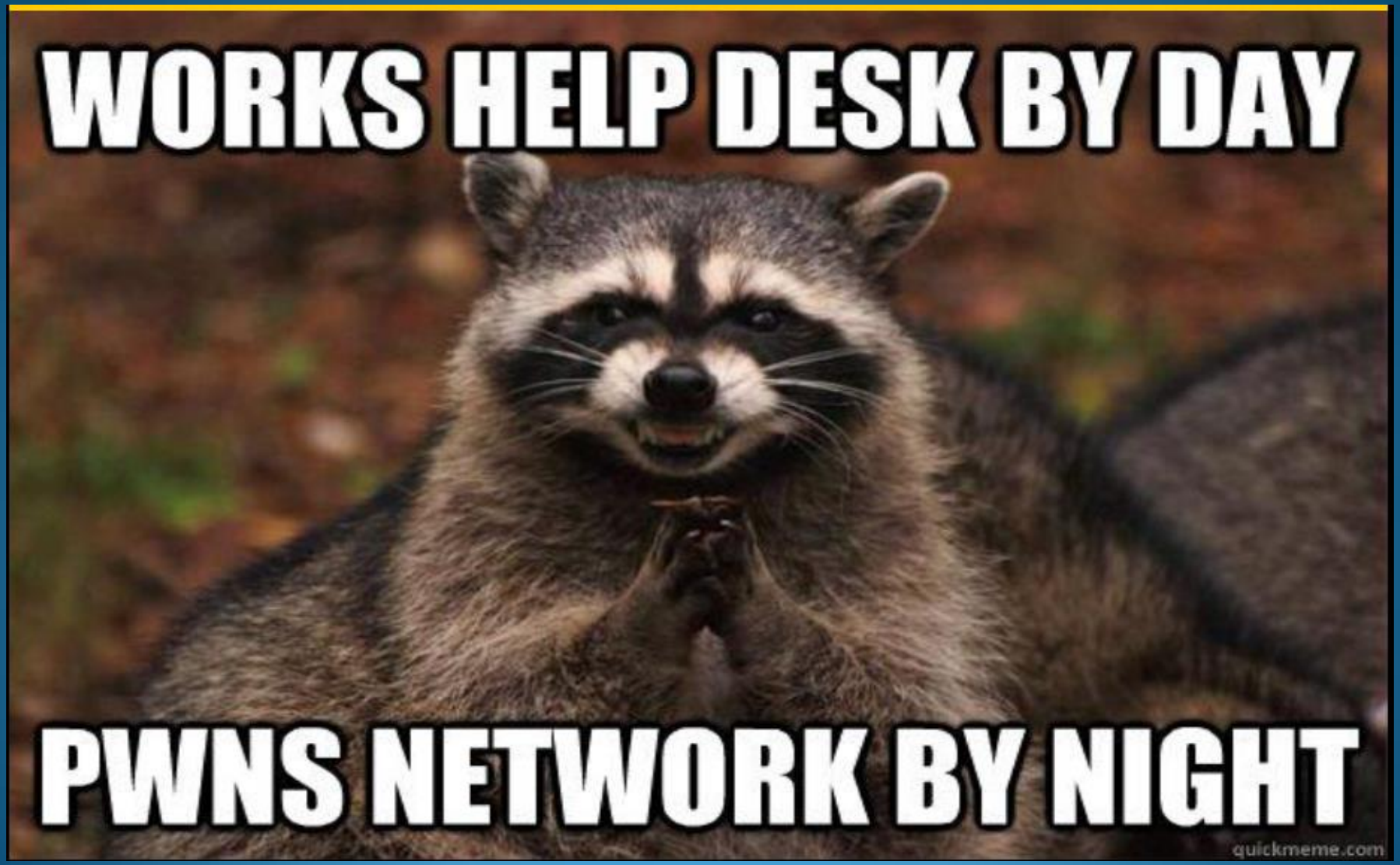
Previsão do Tempo: neve?

O amigo misterioso

Uma era glacial nas relações germano-americanas.

Aparentemente, as agências dos EUA têm monitorado não só o celular pela Chanceler Angela Merkel, mas a embaixada em Berlim, usado como postos de escuta.




WORKS HELP DESK BY DAY
PWNS NETWORK BY NIGHT
quickmeme.com

Inteligência cibenética

- Atualmente, as agências governamentais de cada nação estão fortalecendo seus sistemas de modo a poderem rapidamente responderem às, cada vez mais crescentes, ameaças cibernéticas.
- Há uma grande possibilidade que conflitos diplomáticos venham acontecer em função de atividades cibernéticas no futuro.

Solução?

Russia Finds Chinese Home Appliances Designed for Cyber Espionage

Эксперт: За россиянами шпионят через китайские утюги и чайники

Source: http://www.rosbalt.ru/piter/2013/10/22/1190990.html

Considerações finais

- Questões vitais para os tomadores de decisão quanto ao tratamento das ameaças cibernéticas:
  - atribuição,
  - intenção,
  - marco regulatório e
  - no campo militar as regras de engajamento em caso de um conflito cibernético.
- No espaço cibernético a unidade de tempo é medida em ciclos de máquina portanto os tomadores de decisão devem levar isso em consideração, talvez a máxima:
  - **Quem ataca primeiro tem sempre a vantagem no conflito seja uma verdade, ou não?**

Considerações finais

- A segurança cibernética constitui-se em **assunto complexo e profundo**.
- Sua **análise deve ser executada sob um ponto de vista holístico** levando-se em consideração a multiplicidade de áreas do conhecimento que se fazem necessárias para o tratamento adequado da questão.
- A segurança cibernética é muito mais do que apenas uma questão de segurança nacional ou defesa militar ela é uma **questão integrada** e que para tal necessita de um **esforço integrado** dos setores civil e militar mantidas as suas competências individualizadas.


NO. YOU MAY NOT OUTSOURCE YOUR HOMEWORK TO INDIA.

Muito Obrigado!

Otávio Cunha