Notas para Debate: fragilidades na guarda e nos fluxos de informações pela Internet

Gustavo da Gama Torres
Prof. do Depto. de Ciência da Computação da PUC Minas
Pesquisador associado do CEGOV da UFRGS
Agosto de 2013

Retrospectiva

- Denúncias formuladas por Snowden & Greenwald
  - NSA confirma que o Brasil é espionado no programa batizado de X-Keyscore
    - Detecta a atividade de estrangeiros no país através do idioma usado na comunicação, por telefone ou e-mail.
  - Outro programa denominado Prism acessa os servidores de grandes empresas de internet como Google, Facebook e Skype.
    - Nos Estados Unidos, as empresas só fornecem informações ao governo sob ordem judicial.

Segurança Cibernética

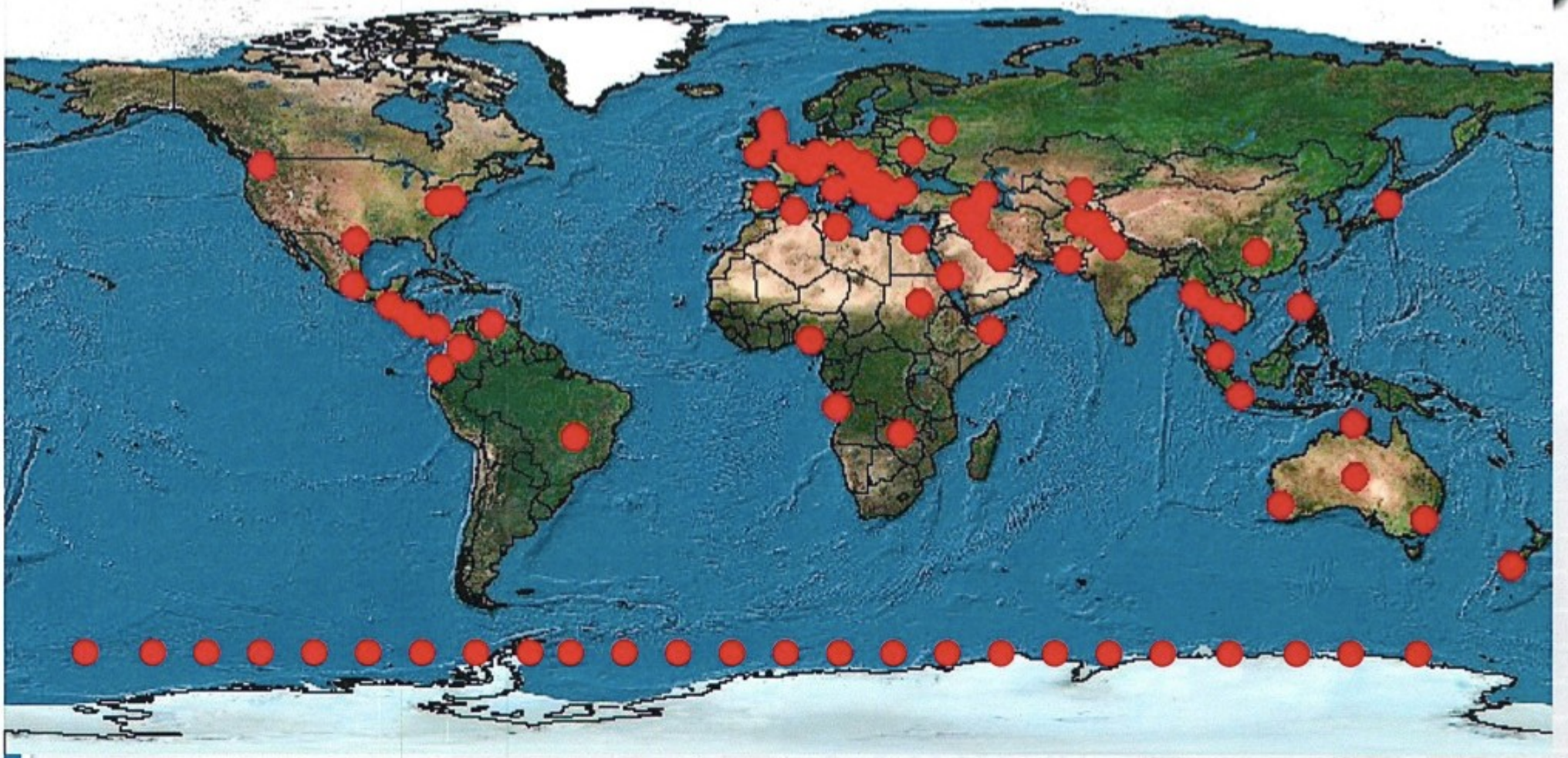
- Proteção e garantia de utilização de ativos de informação estratégicos
  - Baseado em infraestruturas (redes de computadores e sistemas informatizados) que Controlam as sistemas “críticos”
    - Órgãos públicos
    - Serviços públicos
    - Sistemas integrados (financeiro, portos...)

(ver publicações da Secretaria de Assuntos Estratégicos)

Segurança Cibernética

- Militar
  - Defesa cibernética
    - Ações defensivas, de observação, exploratórias, de reconhecimento e inteligência, e ofensivas
      - “...com as finalidades de proteger sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente.” [SAE]

Where is X-KEYSCORE?



Approximately 150 sites

Over 700 servers

What is XKEYSCORE?

1. DNI Exploitation System/Analytic Framework

2. Performs strong (e.g. email) and soft (content) selection

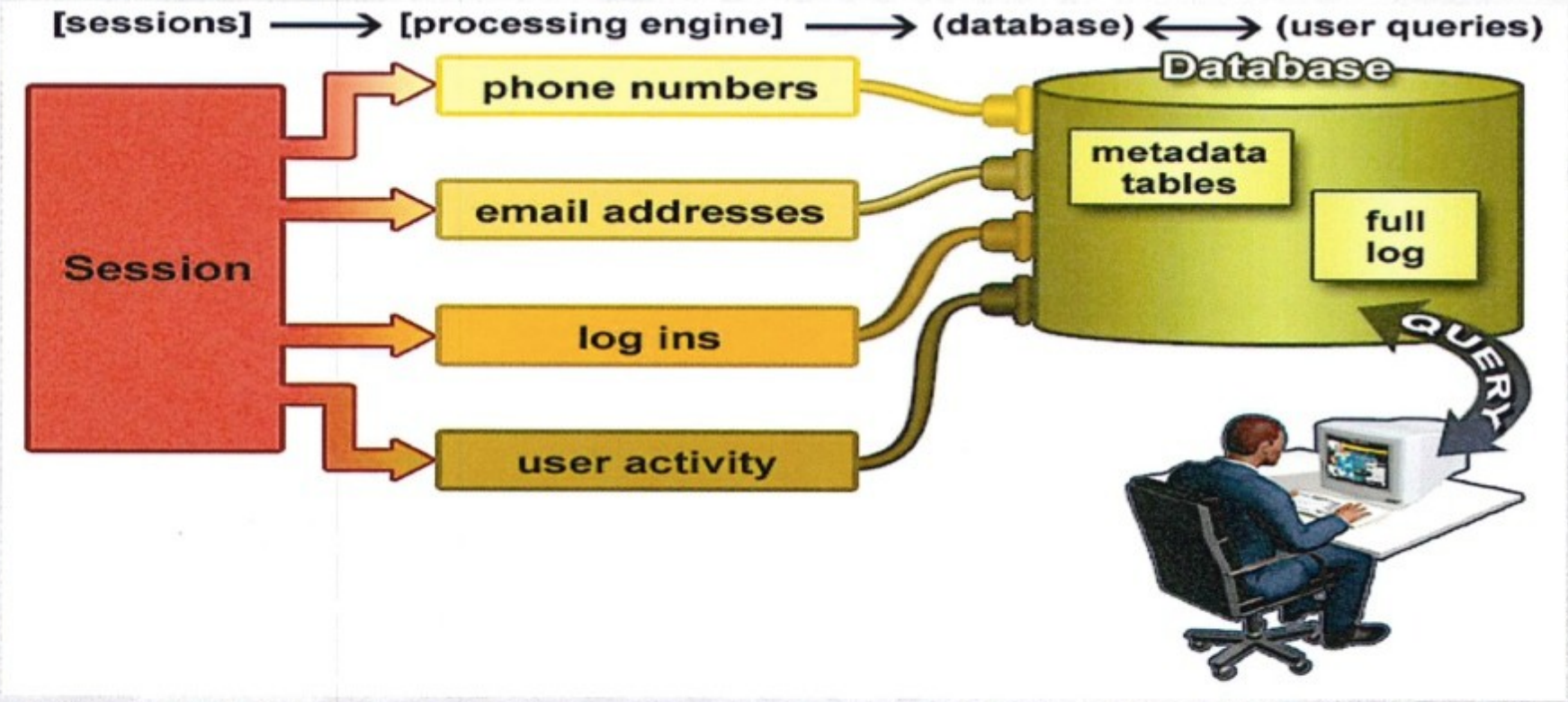
3. Provides real-time target activity (tipping)

4. "Rolling Buffer" of ~3 days of ALL unfiltered data seen by XKEYSCORE:
   - Stores full-take data at the collection site – indexed by meta-data
   - Provides a series of viewers for common data types

1. Federated Query system – one query scans all sites
   - Performing full-take allows analysts to find targets that were previously unknown by mining the meta-data

What XKS does with the Sessions

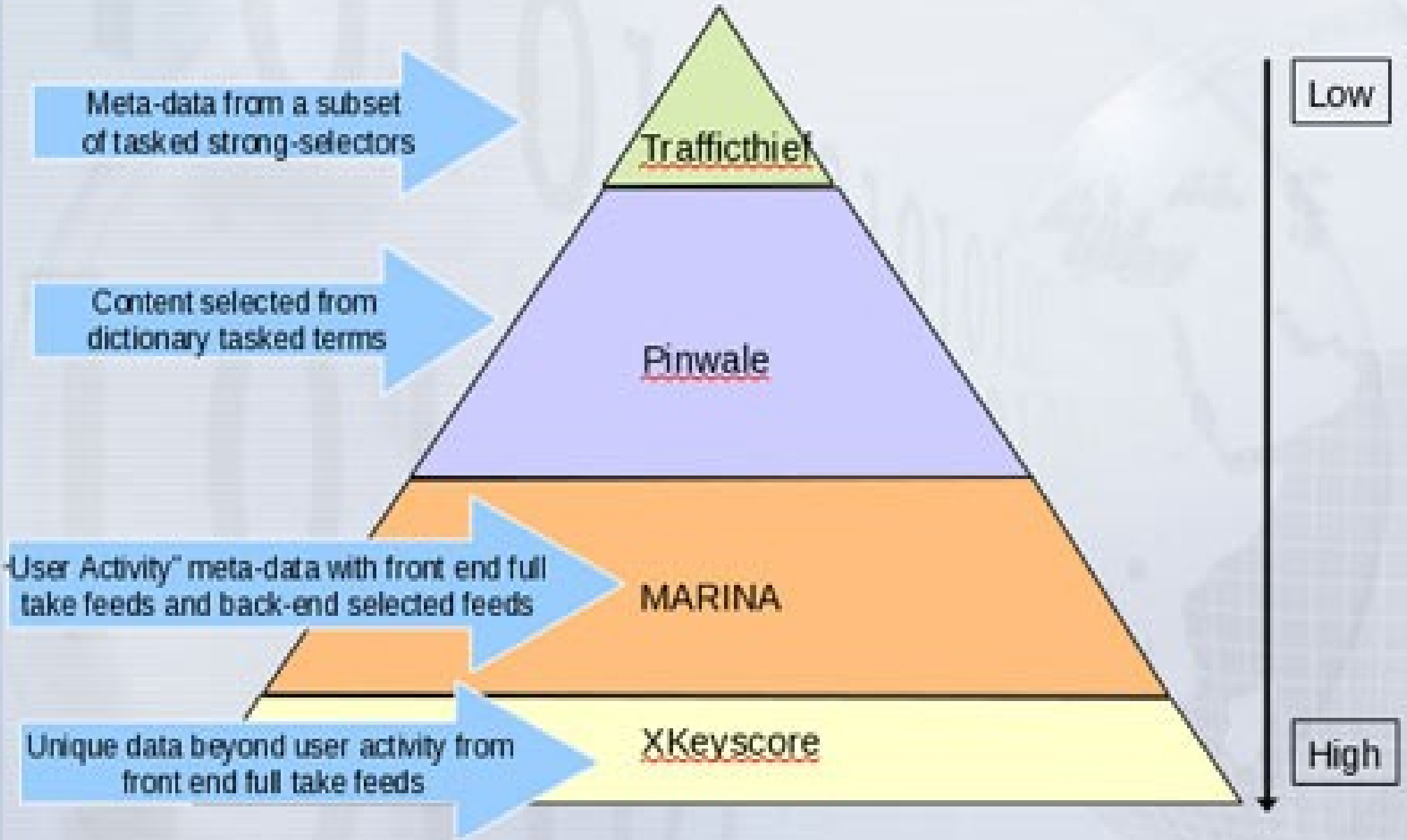
Plug-ins extract and index metadata into tables



Technology Detection

- Show me all the VPN startups in country X, and give me the data so I can decrypt and discover the users
  - These events are easily browsable in XKEYSCORE
    - No strong-selector
  - XKEYSCORE extracts and stores authoring information for many major document types – can perform a retrospective survey to trace the document origin since metadata is typically kept for up to 30 days
  - No other system performs this on raw unselected bulk traffic, data volumes prohibit forwarding

DNI Discovery Options



Information Provided By PRISM

Current Providers

- Microsoft (Hotmail etc)
- Google
- Facebook
- Instagram
- Skype
- Twitter
- AOL
- Apple
- You Tube

Complete list and details on Go PRISMF

Information that can be provided

MICROSOFT
Who's still stuck in 2006
GOOGLE
What idiots have put "Google" into Google
What idiots have searched their own name the most
FACEBOOK
When everyone's birthday is.
What everyone's baby looks like
INSTAGRAM
What everyone's lunch looks like
How New York might look in black and white
SKYPE
How much time people have wasted saying "Can you hear me?"
TWITTER
Which celeb is retweeting praise about themselves
Who's a peddant (they hate it when you spell it like that)
What Samantha Brick's done now
AOL
What your mum and dad's email address is
APPLE
Who prefers under 10 minutes of battery life.
Who hopes they'll contact Steve Jobs by Ouija board
YOUTUBE
Cats! Why always cats?

Segurança Cibernética

- Civil
  - Relacionada à privacidade
    - Direito de recolhimento em relação à vida pública
    - Base de direitos individuais
  - Apesar da importância, a privacidade é confiada a mecanismos informais de proteção
    - Afetados pelas mudanças tecnológicas
    - Internet telefone móvel

Coleta dos Dados (i)

- Os dados de mobilidade são os mais sensíveis
  - Contêm a localização aproximada dos indivíduos, que podem ser usados para reconstruir movimentos no espaço e tempo
  - São usados crescentemente para proporcionar personalização de serviços e recomendação.
    - Movimento da força de vendas de competidores
    - Comparecimento em uma igreja, presença em uma clínica de aborto ou mote
  - Internet das coisas
    - Objetos inteligentesl

Coleta dos Dados (ii)

- A disponibilização de informações pode ser feita de modo bem abrangente com o aparecimento do smartphone.
  - Ex. Apple alterou a sua política de privacidade para permitir o compartilhamento de informações geoespaciais/temporais com “partners and licensees” (Apple Licency Policy, acessada em jul de 2011)
  - (Ver lista de informações pessoais e profissionais sensíveis em Blumberg, A.; Eckerley, P. *On locational privacy an how to avoid losing it forever*. E.F.F. 2009.)

Coleta dos Dados (iii)

- Percepção e contextualização
  - 5w+1
    - Quem (who)
    - O que (what)
    - Onde (where)
    - Quando (when)
    - Como (how)
    - Por que (why)

Engenharia de Confiança

- Segurança
  - Sistemas que mantêm nível adequado de funcionamento, mesmo em situação de falha
- Proteção
  - Em relação a ameaças
    - De confidencialidade
    - De Integridade
    - De disponibilidade

Confiança e Proteção no Contexto (i)

- Uma constatação óbvia
  - O sistema de comunicação brasileiro é aberto à interceptação
- Alguns aspectos
  - Contratos entre concessionárias
  - Disponibilidade e rotas dos cabos
  - Tecnologias adquiridas fechadas

The internet's undersea world

The vast majority of the world's communications are not carried by satellites but an altogether older technology: cables under the earth's oceans. As a ship accidentally wipes out Asia's net access, this map shows how we rely on collections of wires of less than 10cm diameter to link us all together

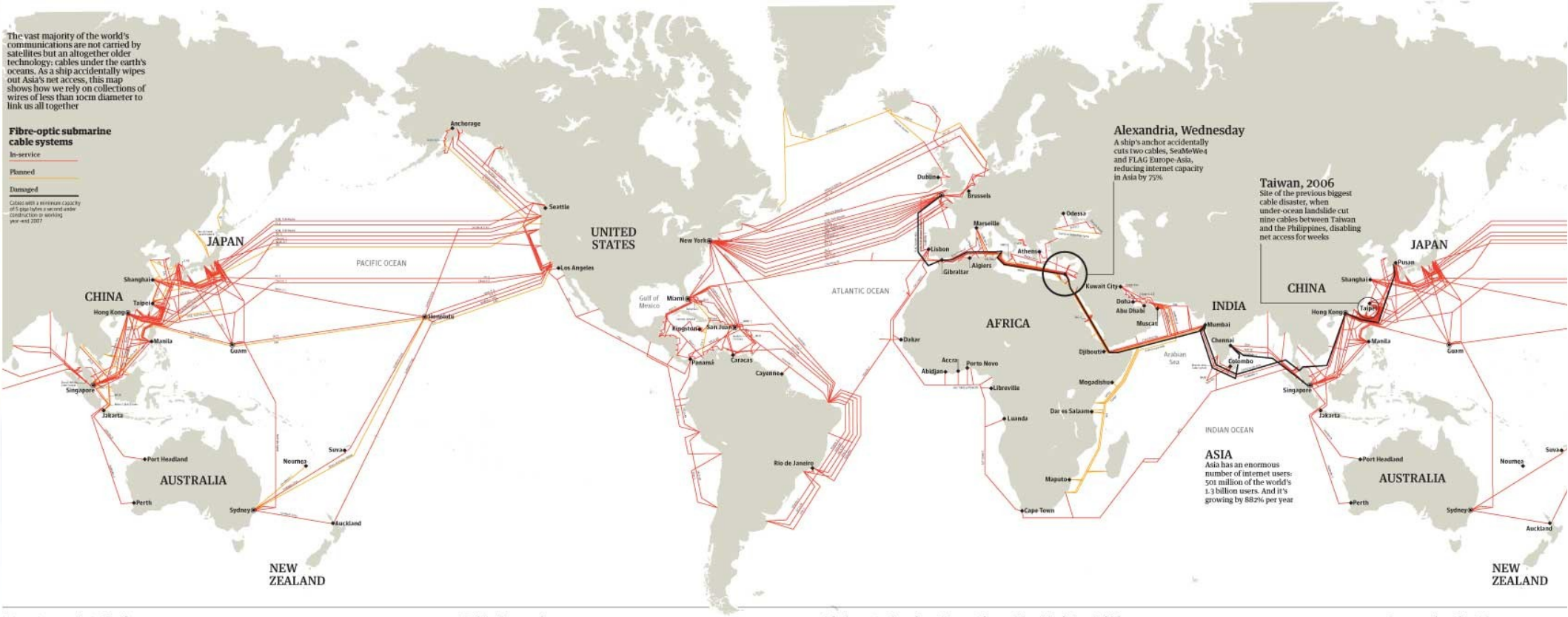
Fibre-optic submarine cable systems

In-service

Planned

Damaged

Cables with a minimum capacity of 5 gigabytes a second under construction or working year-end 2007



Alexandria, Wednesday

A ship's anchor accidentally cuts two cables, SeaMeWe4 and FLAG Europe-Asia, reducing internet capacity in Asia by 75%

Taiwan, 2006

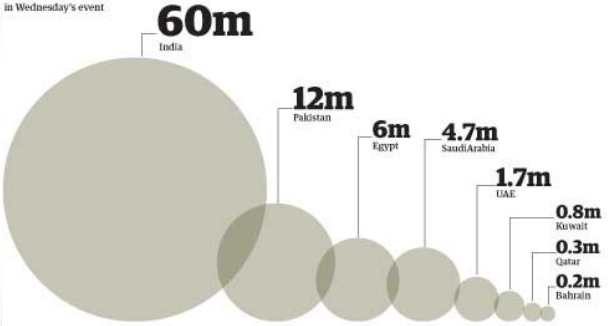
Site of the previous biggest cable disaster, when under-ocean landslide cut nine cables between Taiwan and the Philippines, disabling net access for weeks

ASIA

Asia has an enormous number of internet users: 501 million of the world's 1.3 billion users. And it's growing by 882% per year

Internet users affected by the Alexandria accident

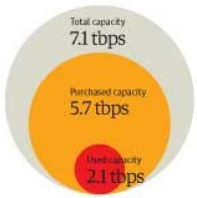
The main countries affected in Wednesday's event



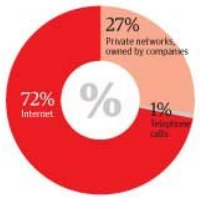
World cable capacity

Submarine cable operators light (turn on) capacity on their systems to sell bandwidth to other carriers. Carriers buy extra capacity, mainly to hold in reserve. On the trans-Atlantic route 80% of the bandwidth is purchased, but only 29% is used

Capacity in terabytes a second



What makes up "used capacity"?



The longest submarine cables

The SeaMeWe-3 system from Norden in Germany to Keoje, South Korea connects 32 different countries with 39 landing points

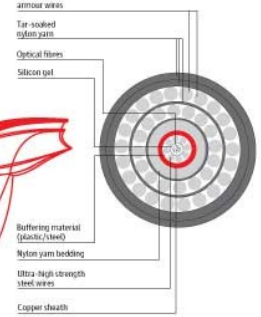
SeaMeWe-3	39,000 km
Southern Cross	30,500 km
China-US	30,476 km
FLAG Europe-Asia	28,000 km
South America-1	25,000 km

The world's cables in bandwidth

The first intercontinental telephony submarine cable system, TAT-1, connected North America to Europe in 1958 and had an initial capacity of 640,000 bytes per second. Since then, total trans-Atlantic cable capacity has soared to over 7 trillion bps

Cross-section of a cable

Cables of this strength are typically 69 mm in diameter and weigh over 10,000 kilograms a kilometer. In deeper waters, lighter and less insulated cables are used



SOURCE: TELEGEOGRAPHY.COM SUBMARINE CABLE MAP 2008. INTERNET STATISTICS FROM INTERNETWORLDSTATS.COM

Confiança e Proteção no Contexto (ii)

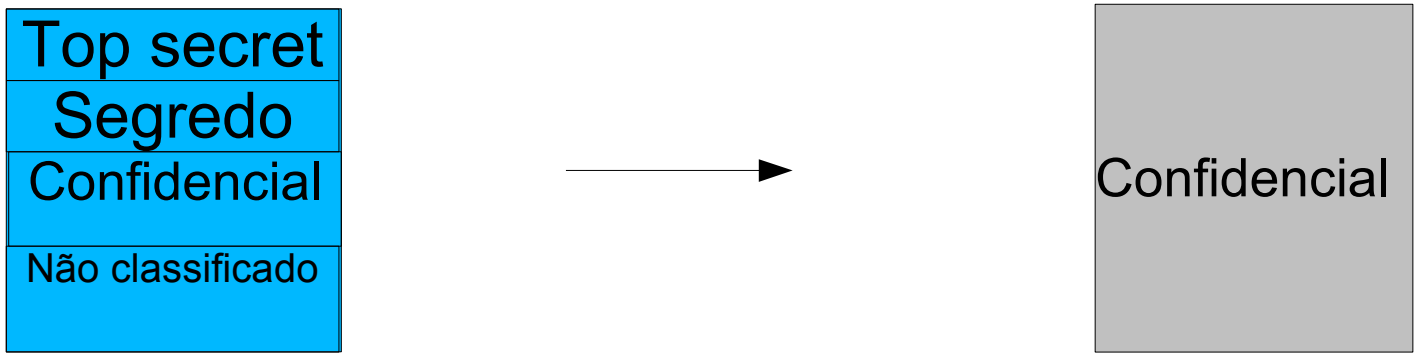
- Aspectos institucionais
  - Controle do regulador
    - “Captura da agência” (George Stigler)
  - Governança da Internet
  - Integração
    - Envolve outros atores além das operadoras
    - Imprecisão de políticas pública
      - Não está claro o mecanismo de coordenação (DSIC/DCI/PR, CERT.br, INFOSEG, CEPESC-ABIN, ITI, CDCiber Ex, SESGE e a CGDEF-SG-MRE, MPOG (e-ping), empresas...)
  - Sistema de inovação

Confiança e Proteção no Contexto (iii)

- Aspectos culturais
  - "ameaças cibernéticas" tratadas de maneira difusa e abstrata
    - Alienação de usuários médios
    - Visão igual para
      - adolescentes “brincando” de “negação de serviço”
      - criminosos que roubam segredos industriais
      - unidades militares dedicadas à guerra

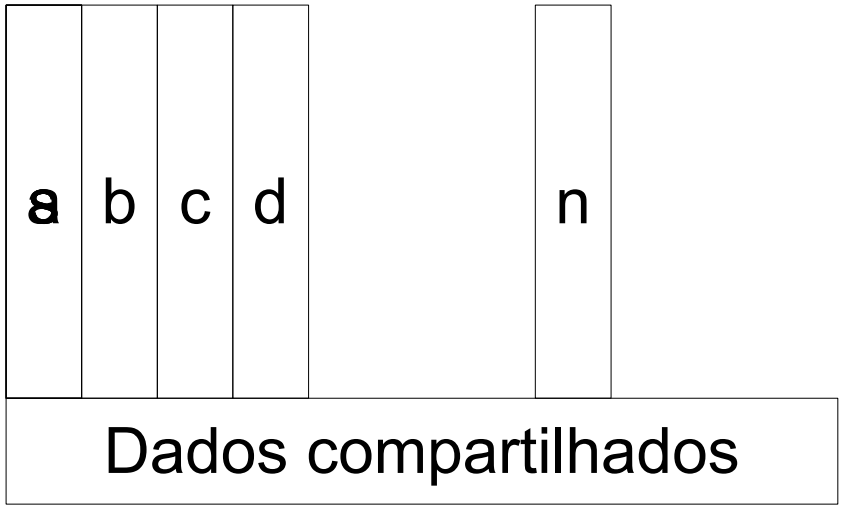
Engenharia de Proteção (i)

- Segurança multinível

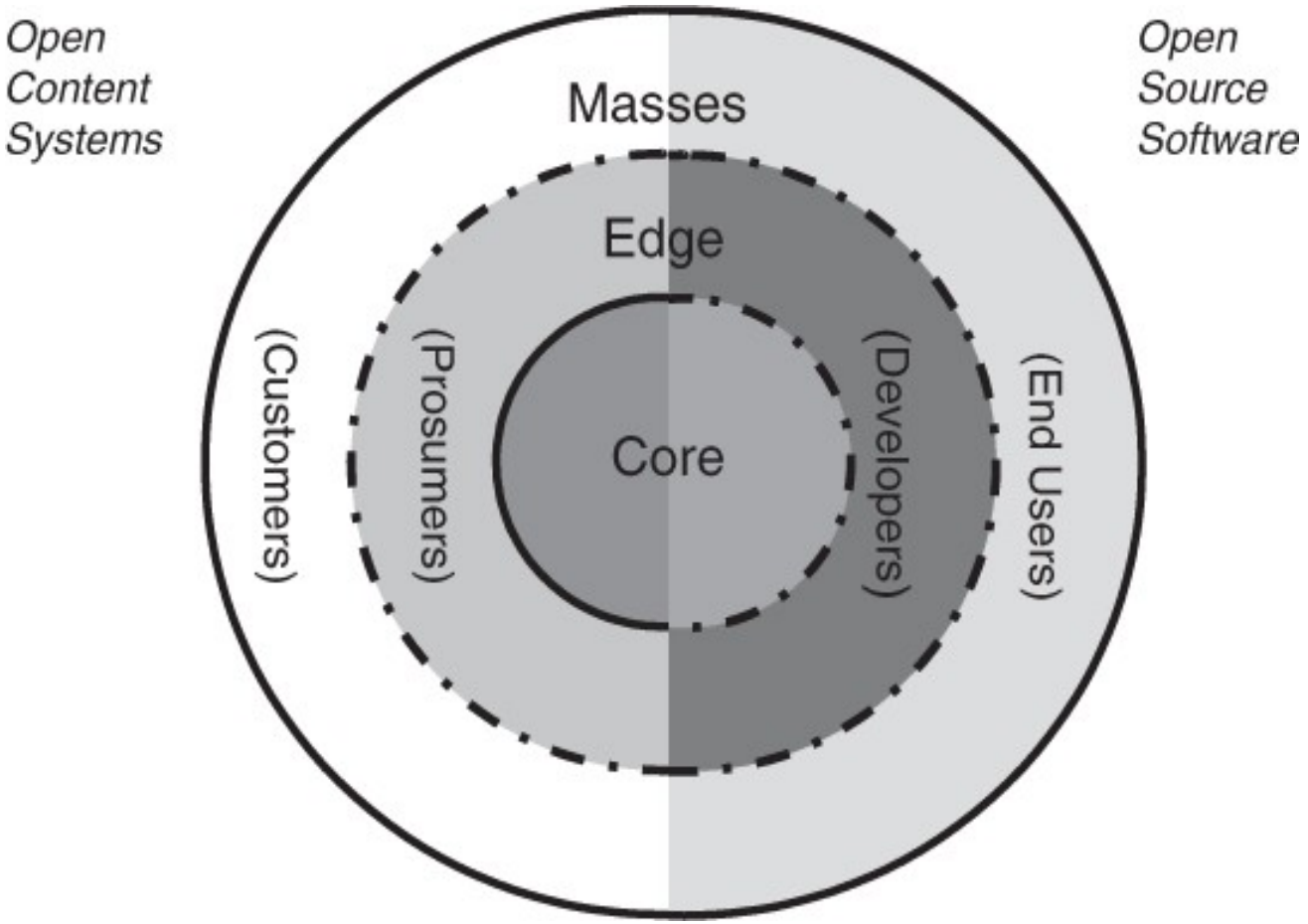


Engenharia de Proteção (ii)

- Segurança multilateral



Sistemas de Borda Dominante



[adaptado de BASS, L.; CLEMENTS, P.; KAZMAN, R.]

Guarda de Informações

- Ativos de informações digitais
  - Valor tangível e intangível
- A preservação considera
  - Disponibilidade, integridade, confidencialidade, autenticidade, proveniência, direitos
- Natureza dos dados
  - Dados privados
    - Sobre pessoas e organizações
  - Dados públicos
    - Abertos ou classificados

Guarda de Informações

- Data center
  - Infraestrutura dos ecossistemas digitais
  - Fatores críticos
    - Custo
      - Saída para a Internet (infraestrutura)
      - Proximidade de fontes e preço da energia
    - Serviço
      - Contratos com cada usuário
      - Contratos corporativos

Conclusão

- Internet como plataforma de inovação
- Não há inovação sem circulação de informação
- Os sistema estão sendo construídos para manter e correlacionar todas as informações
- Nossos sistemas de proteção são, no mínimo, ingênuos
- Nossos *policy makers* desconhecem os limites técnicos das soluções que propõem
- Importância da gestão de pessoas (peopleware) e mobilização social para a cibersegurança

gustavo.gamatorres@pucminas.br

gustavo.gamatorres@gmail.com

Conclusão

- Internet como plataforma de inovação
- Não há inovação sem circulação de informação
- Os sistema estão sendo construídos para manter e correlacionar todas as informações
- Nossos sistemas de proteção são, no mínimo, ingênuos
- Nossos *policy makers* desconhecem os limites técnicos das soluções que propõem
- Importância da gestão de pessoas (peopleware) e mobilização social para a cibersegurança

www.cegov.ufrgs.br

gustavo.gamatorres@pucminas.br

gustavo.gamatorres@gmail.com