Urgente: Hackers causaram a erupção do vulcão Eyjafjallajokull

Anchises M. G. de Paula
iDefense
International Cyber Intelligence Analyst
January 18, 2011

Agenda

<FUD>Volcano hacking</FUD>

Estórias de Cyber Armageddon

Um perfeito incidente SCADA

<real>Incidentes SCADA</real>

Pic. Source: Icelandic Meteorological office

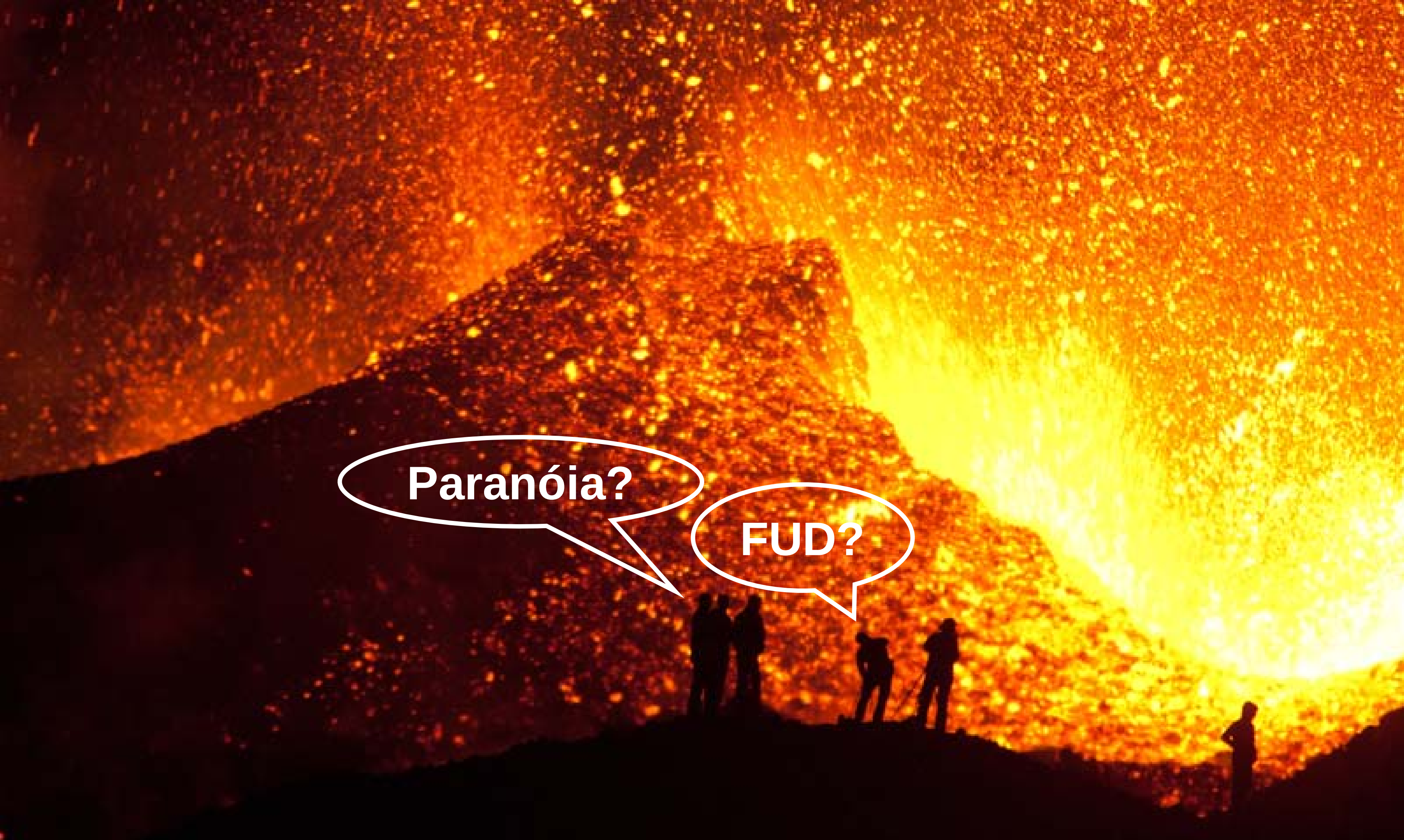
Um FUD perfeito...

EXTRA!!! Cyber attack started Eyjafjallajokull volcano eruption

YourFakeNewsSite.org

“We know that cyber intruders have probed SCADA systems, and that in other countries cyber attacks have started volcano eruptions. Several prominent intelligence sources confirmed that a cyber attack in Iceland in April 2010 that affected several European countries and hundreds of thousands of people. Icelandic Meteorological Office had several plants knocked offline, which indicates that the cyber incident is connected to the explosive activity from the Eyjafjallajökull volcano. It is not clear who did it or what the motive was.”

Pic. Source: The Atmospheres Blog

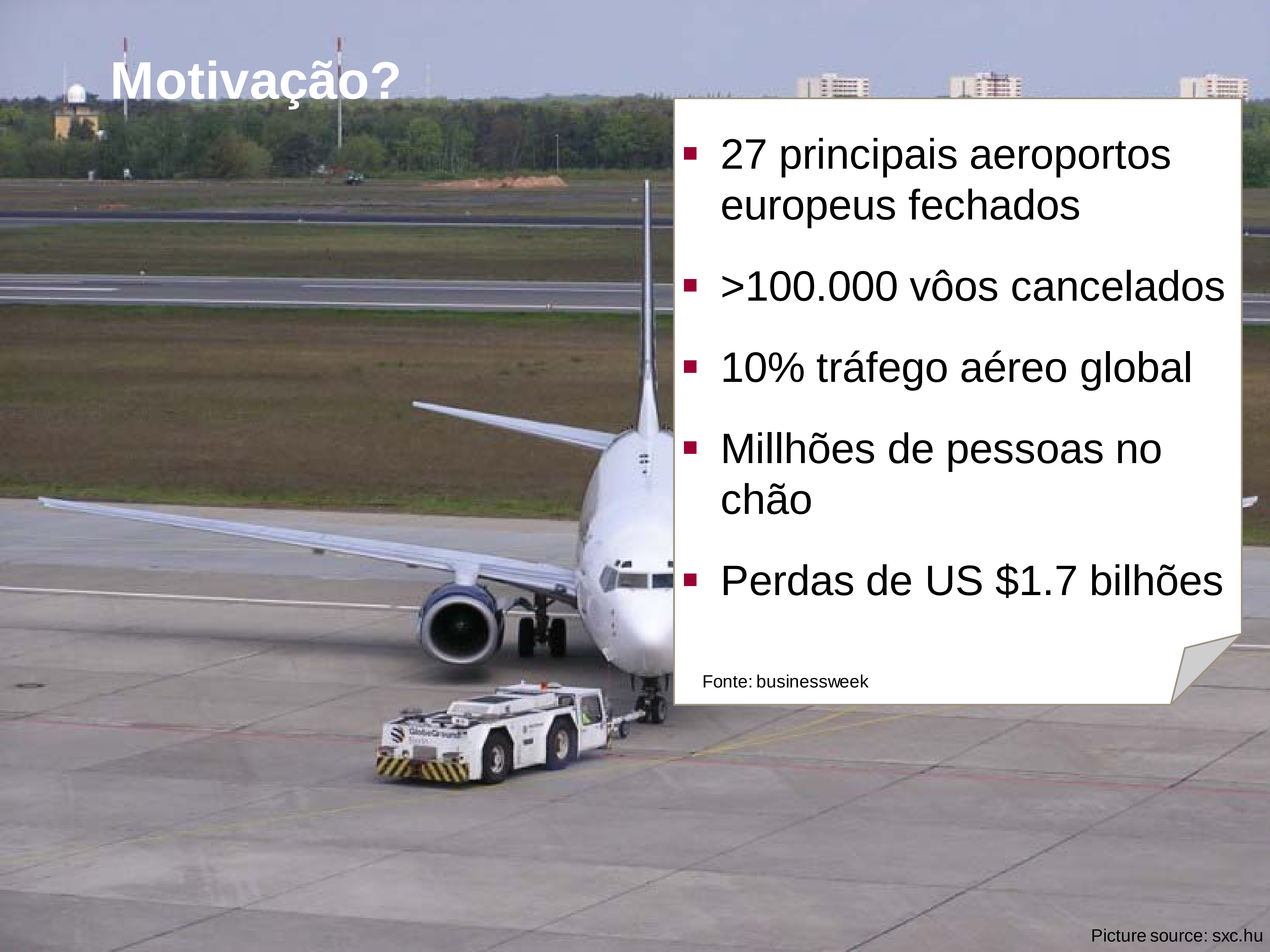


- **Volcano hacking**

(Hipotético)

Pic. Source: The Atmospheres Blog

Motivação?



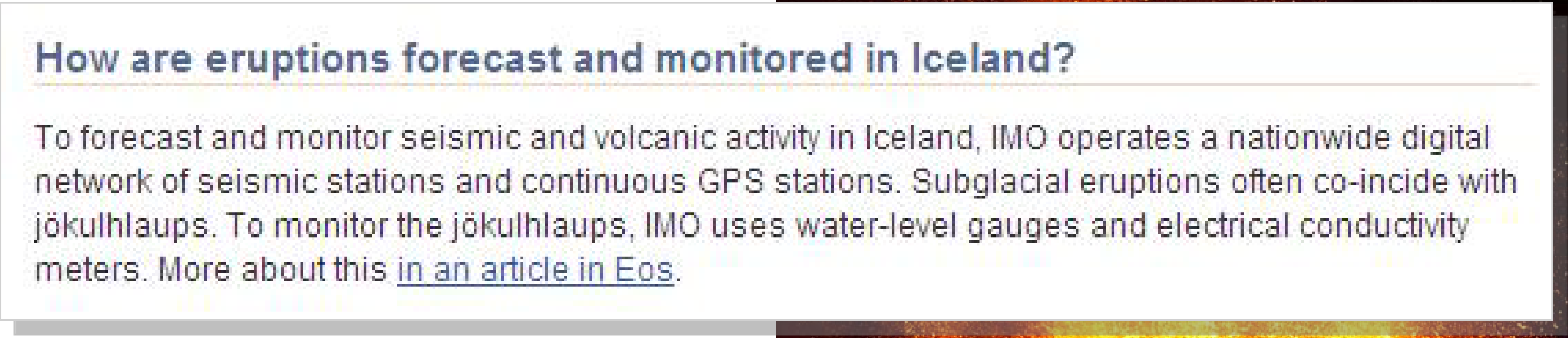
- 27 principais aeroportos europeus fechados
- >100.000 vôos cancelados
- 10% tráfego aéreo global
- Millhões de pessoas no chão
- Perdas de US $1.7 bilhões

Fonte: businessweek

Picture source: sxc.hu

Volcano hacking 101

Icelandic Met Office



How are eruptions forecast and monitored in Iceland?

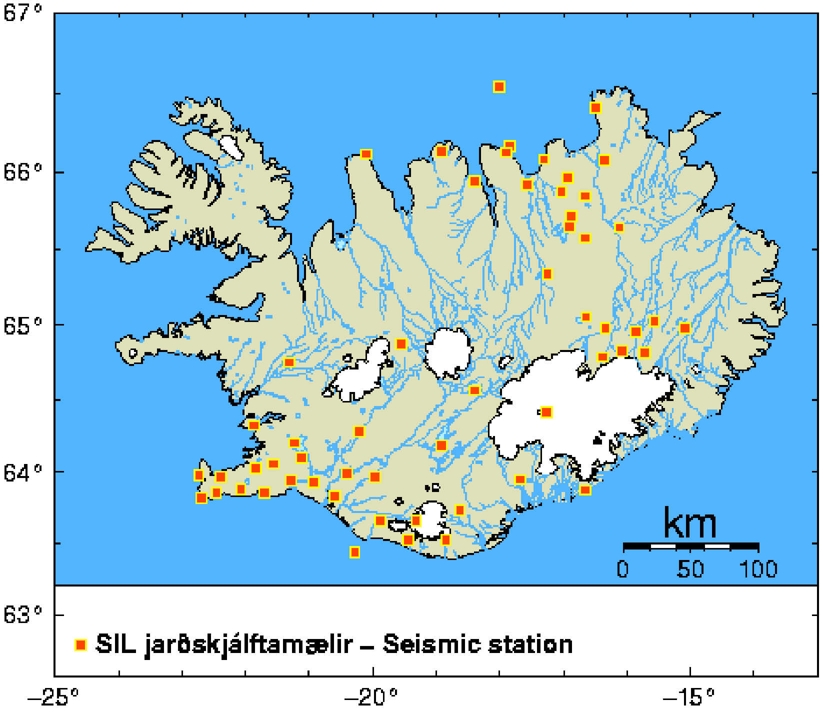
To forecast and monitor seismic and volcanic activity in Iceland, IMO operates a nationwide digital network of seismic stations and continuous GPS stations. Subglacial eruptions often co-incide with jökulhlaups. To monitor the jökulhlaups, IMO uses water-level gauges and electrical conductivity meters. More about this in an article in Eos.

Pic. Source: The Atmospheres Blog

Volcano hacking 101

Icelandic Met Office

- Eles tem sensores !!!
- Eles tem sistema SCADA !?

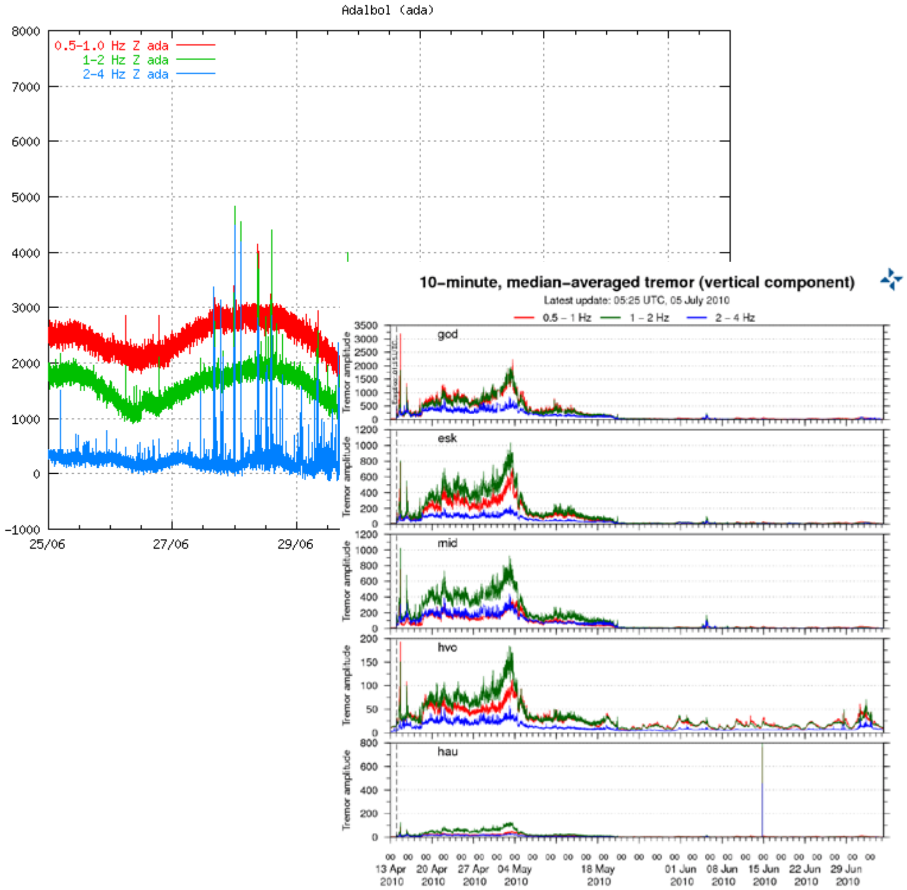


Pic. Source: The Atmospheres Blog

Volcano hacking 101

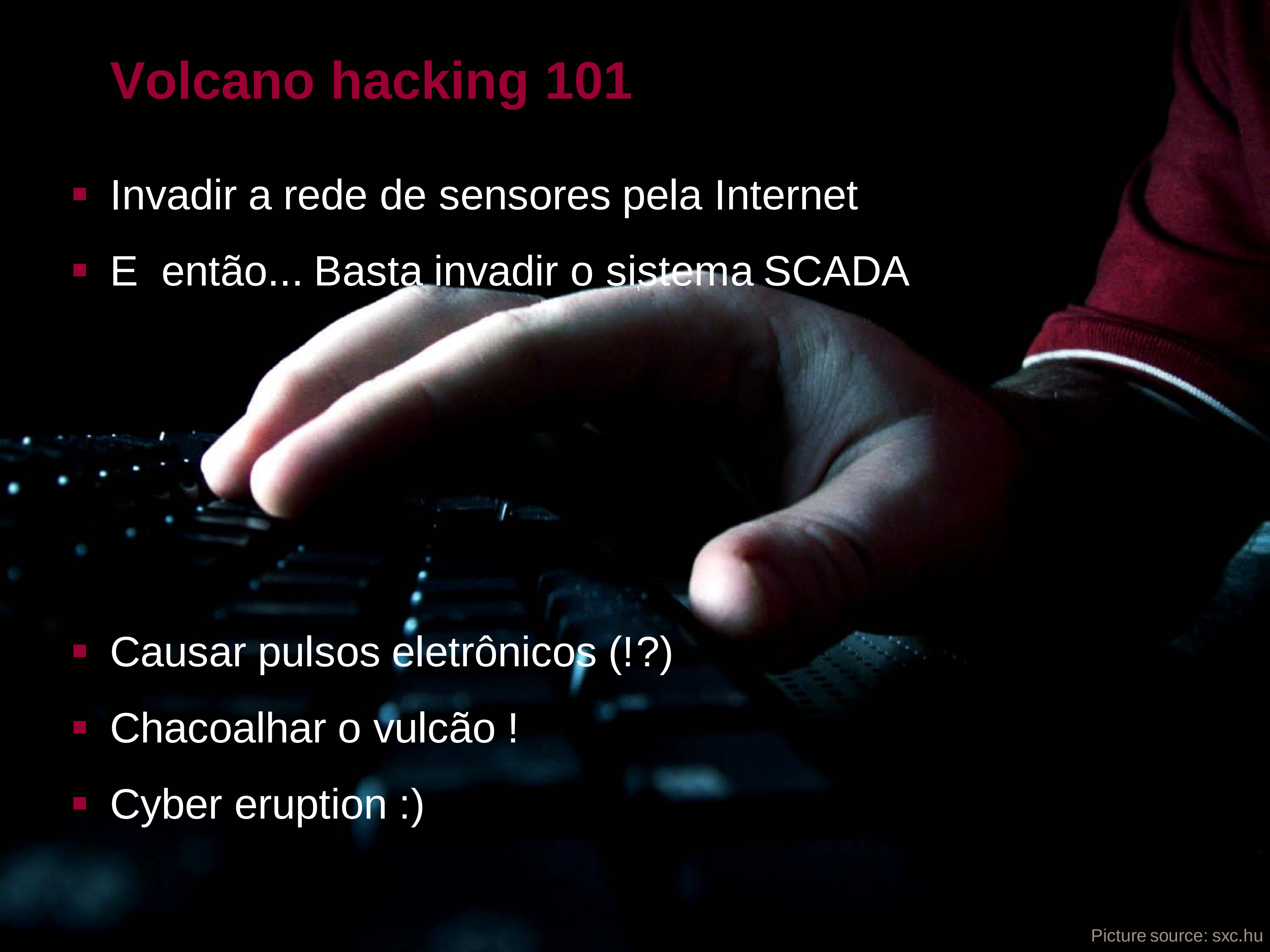
Icelandic Met Office

- Eles têm relatórios online !



Pic. Source: The Atmospheres Blog

Volcano hacking 101



- Invadir a rede de sensores pela Internet
- E então... Basta invadir o sistema SCADA

- Causar pulsos eletrônicos (!?)
- Chacoalhar o vulcão !
- Cyber eruption :)

Picture source: sxc.hu

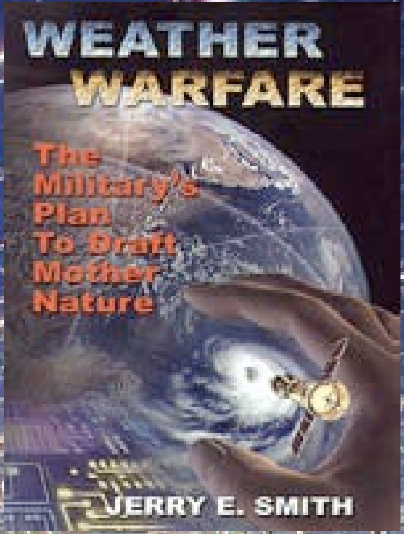
PERAÍÍÍ !!!!

Cyber-eruption?

Cyber-earthquake?

Earthquake HAARP Connection

High-frequency Active Auroral Research Program



09/03/10

US military behind Haiti quake, says Innsbruck scientist.

AustrianIndependent.com

Innsbruck political scientist Claudia von Werlhof has accused the USA of being behind the Haitian earthquake in January, it emerged today (Tues). According to a report on tirol.orf.at, Werlhof said that machines at a military research centre in Alaska used to detect deposits of crude oil by causing artificial earthquakes might have been intentionally set off to cause the Haitian earthquake and enable the USA to send 10,000 soldiers into the country.

Picture source: HAARP

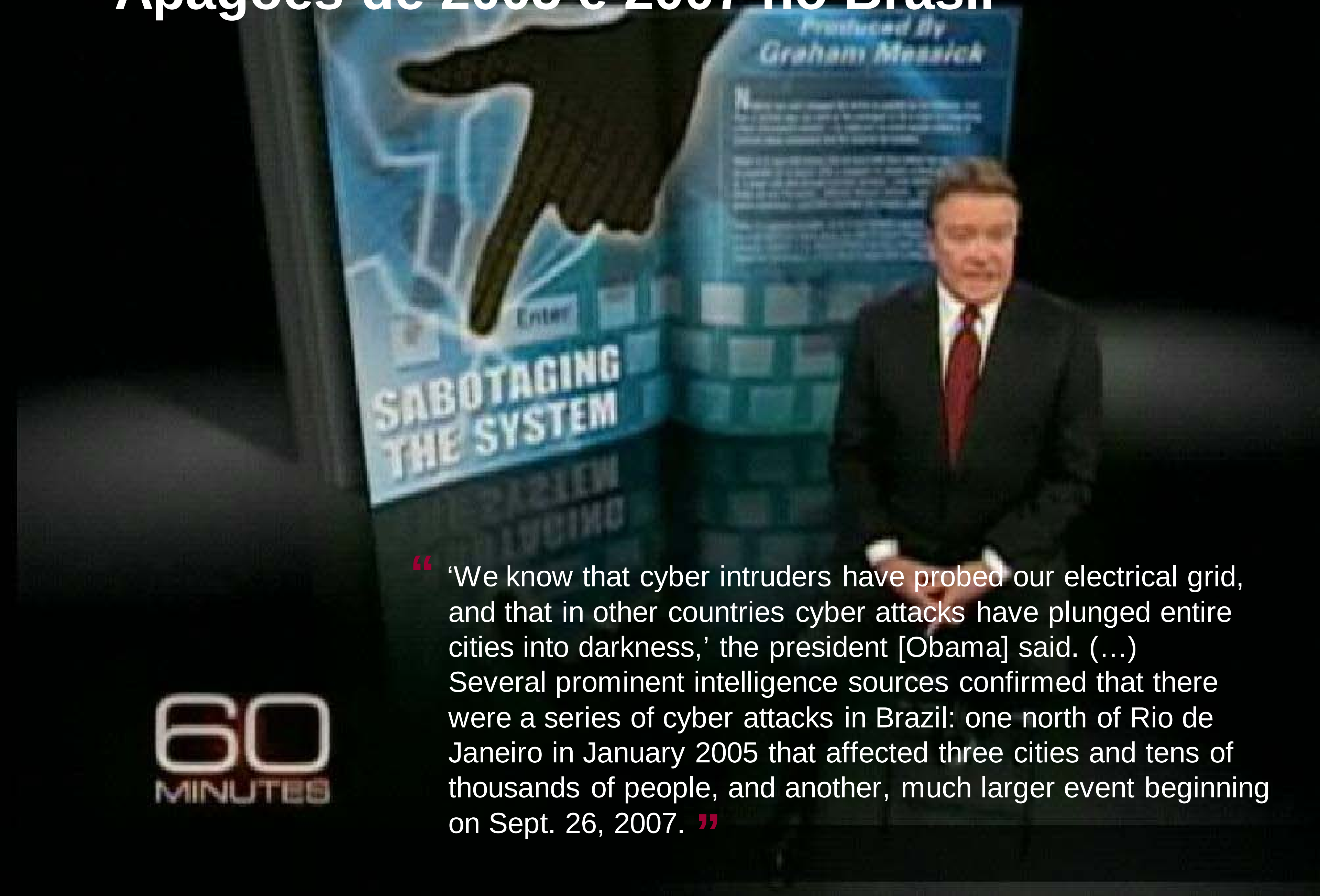
E depois... manda isso para a imprensa !

- Ou tuita ...
- Ou publica em um blog...

Picture source: sxc.hu

O Cyber Armageddon está vindo!

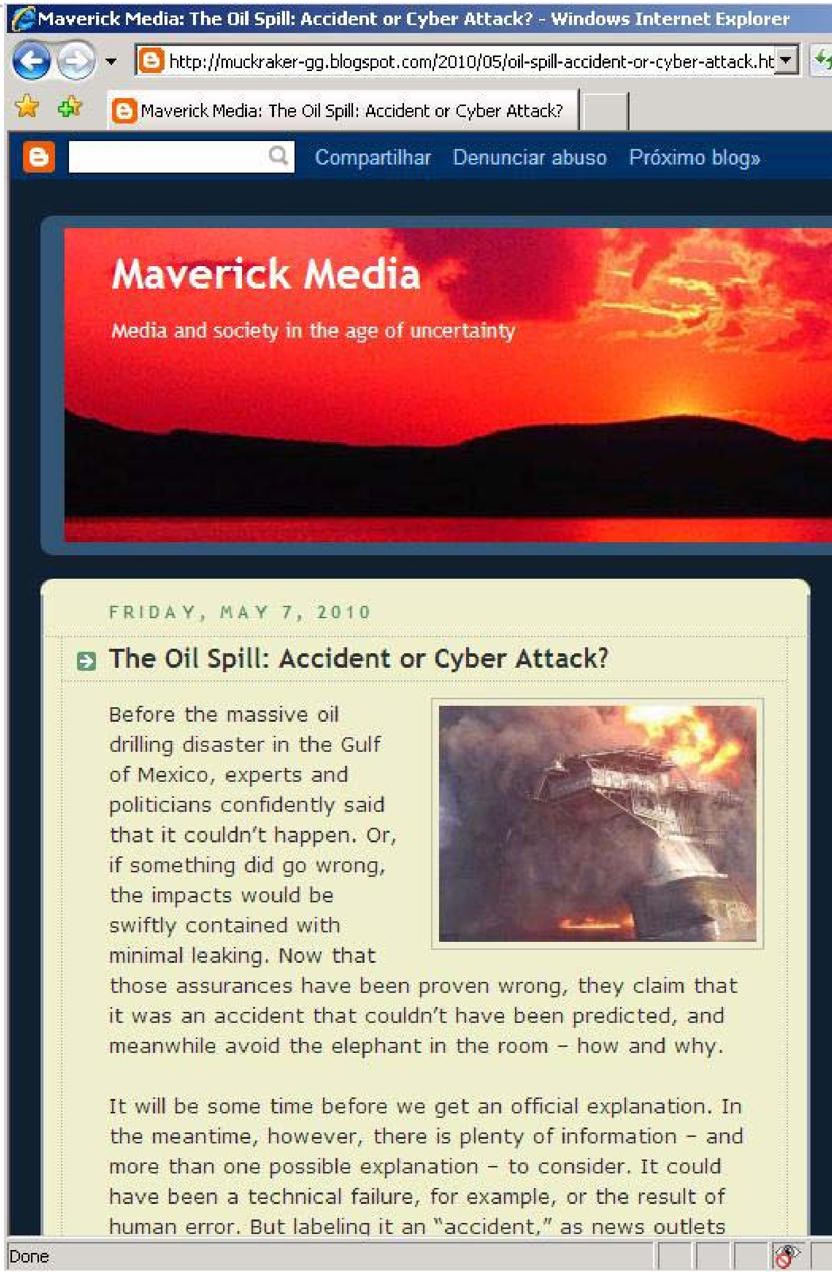
Apagões de 2005 e 2007 no Brasil



> “ ‘We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness,’ the president [Obama] said. (…)
> Several prominent intelligence sources confirmed that there were a series of cyber attacks in Brazil: one north of Rio de Janeiro in January 2005 that affected three cities and tens of thousands of people, and another, much larger event beginning on Sept. 26, 2007. ”

Desastre da BP no Golfo do México Abril/2010

> “ On oil rigs, the advent of robot-controlled platforms has made a cyber attack possible with a PC anywhere in the world. Control of a rig could be accomplished by hacking into the "integrated operations" that link onshore computer networks to offshore ones.”


Maverick Media: The Oil Spill: Accident or Cyber Attack? - Windows Internet Explorer
http://muckraker-gg.blogspot.com/2010/05/oil-spill-accident-or-cyber-attack.ht
Maverick Media: The Oil Spill: Accident or Cyber Attack?
Compartilhar
Denunciar abuso
Próximo blog»
Done

Maverick Media

Media and society in the age of uncertainty

FRIDAY, MAY 7, 2010

The Oil Spill: Accident or Cyber Attack?

Before the massive oil drilling disaster in the Gulf of Mexico, experts and politicians confidently said that it couldn't happen. Or, if something did go wrong, the impacts would be swiftly contained with minimal leaking. Now that those assurances have been proven wrong, they claim that it was an accident that couldn't have been predicted, and meanwhile avoid the elephant in the room – how and why.

It will be some time before we get an official explanation. In the meantime, however, there is plenty of information – and more than one possible explanation – to consider. It could have been a technical failure, for example, or the result of human error. But labeling it an "accident," as news outlets

Caos em Wall Street – Maio 2010

05/09/10

White House: No cyber attack on Wall St.

WashingtonTimes.com

The White House's homeland security and counterterrorism adviser said Sunday there is no evidence that a cyber attack was behind the chaos that shook Wall Street on Thursday.

John Brennan told "Fox News Sunday" that the officials have uncovered no links to cyber attacks in examining the causes of the turbulence that sent the Dow Jones Industrial Average plunging almost 1,000 points before staging a partial recovery at the end of the day.

The market was already weak because of the Greek financial crisis. Beyond that, there was speculation that a typographical error might have triggered the massive computerized sell-off.

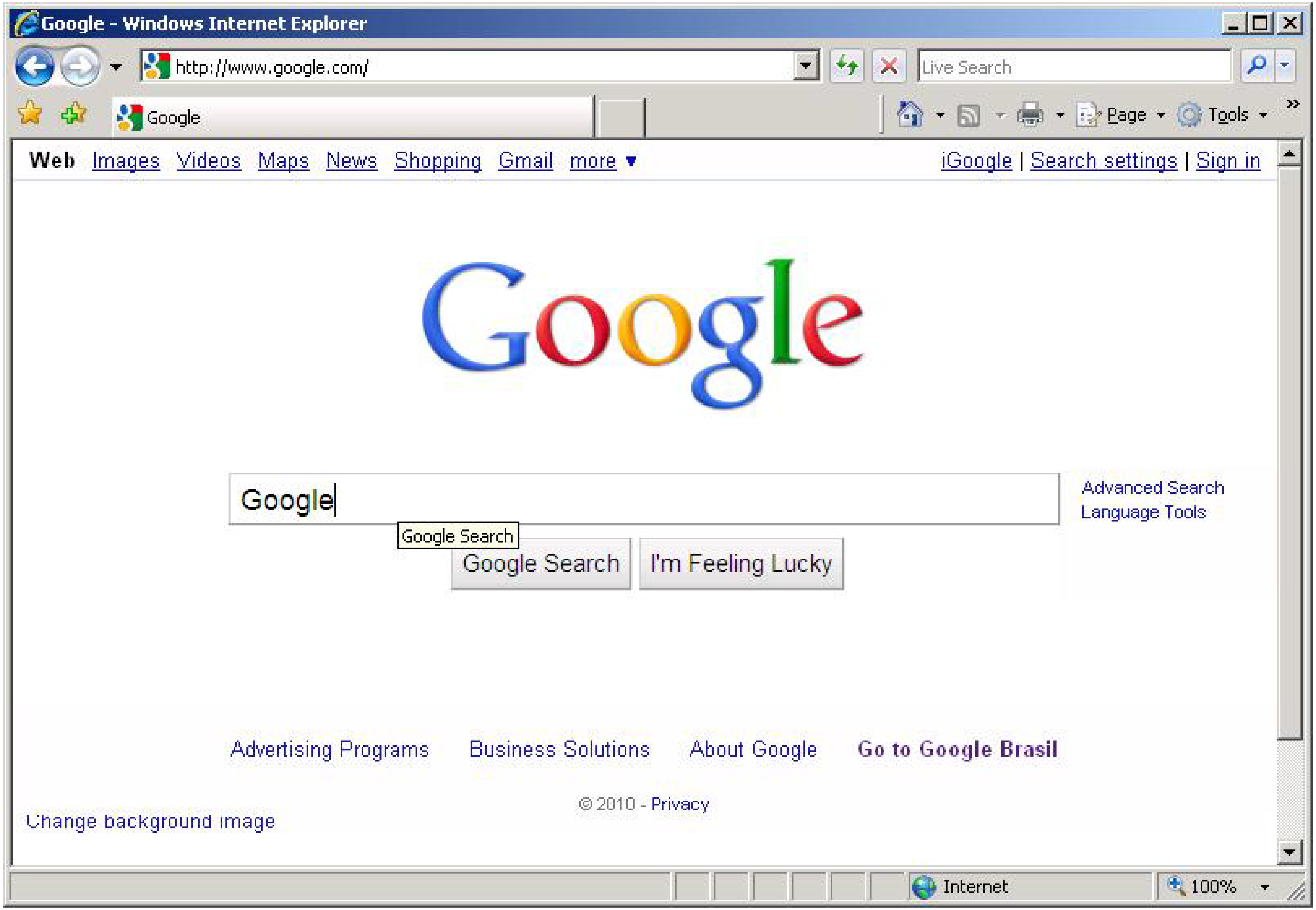
Picture source: sxc.hu

Por que as pessoas acreditam em tudo o que a mídia diz?

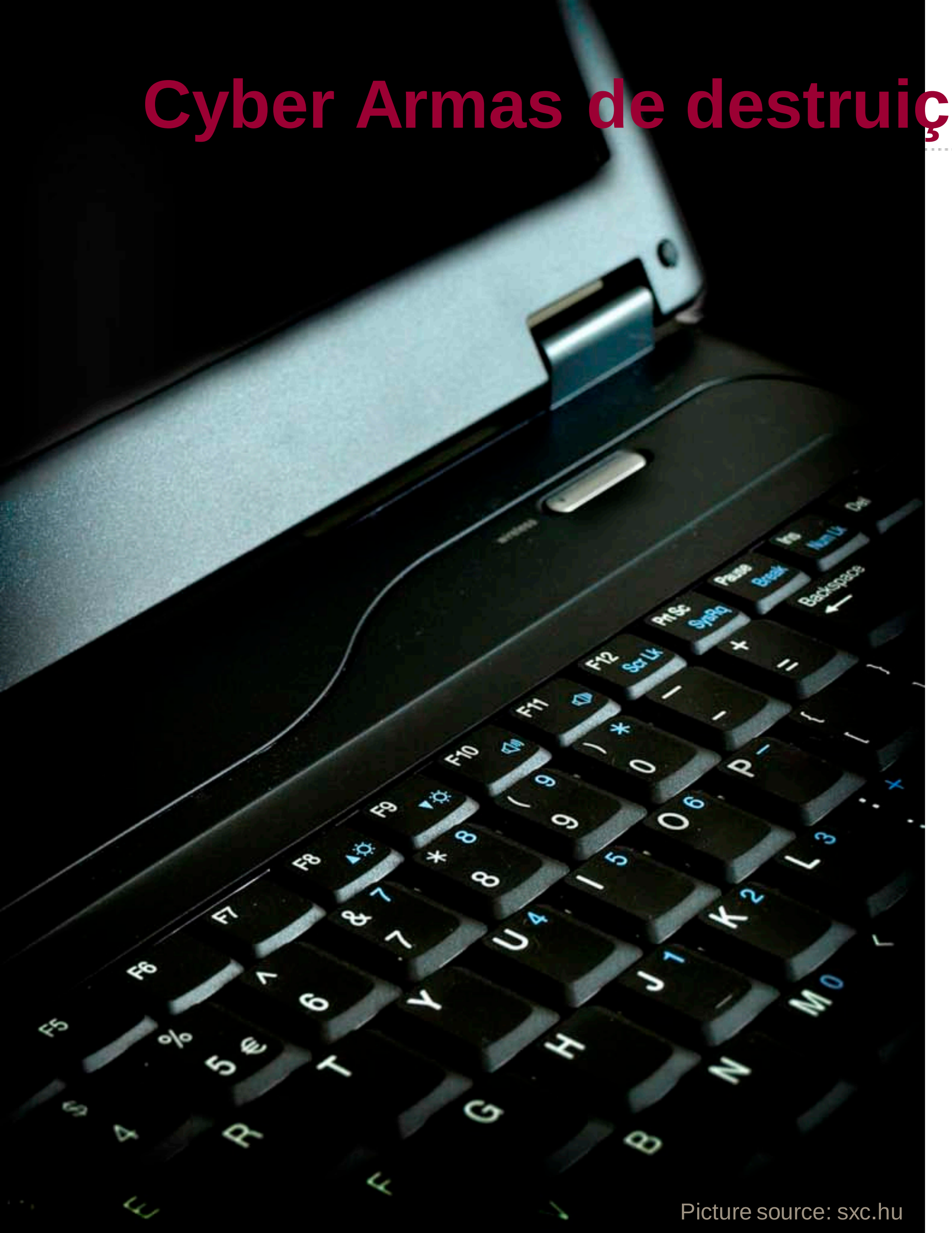
Picture source: sxc.hu

Um perfeito “cyber-termonuclear-global” incidente SCADA

Fato: É fácil destruir a Internet



Cyber Armas de destruição em massa



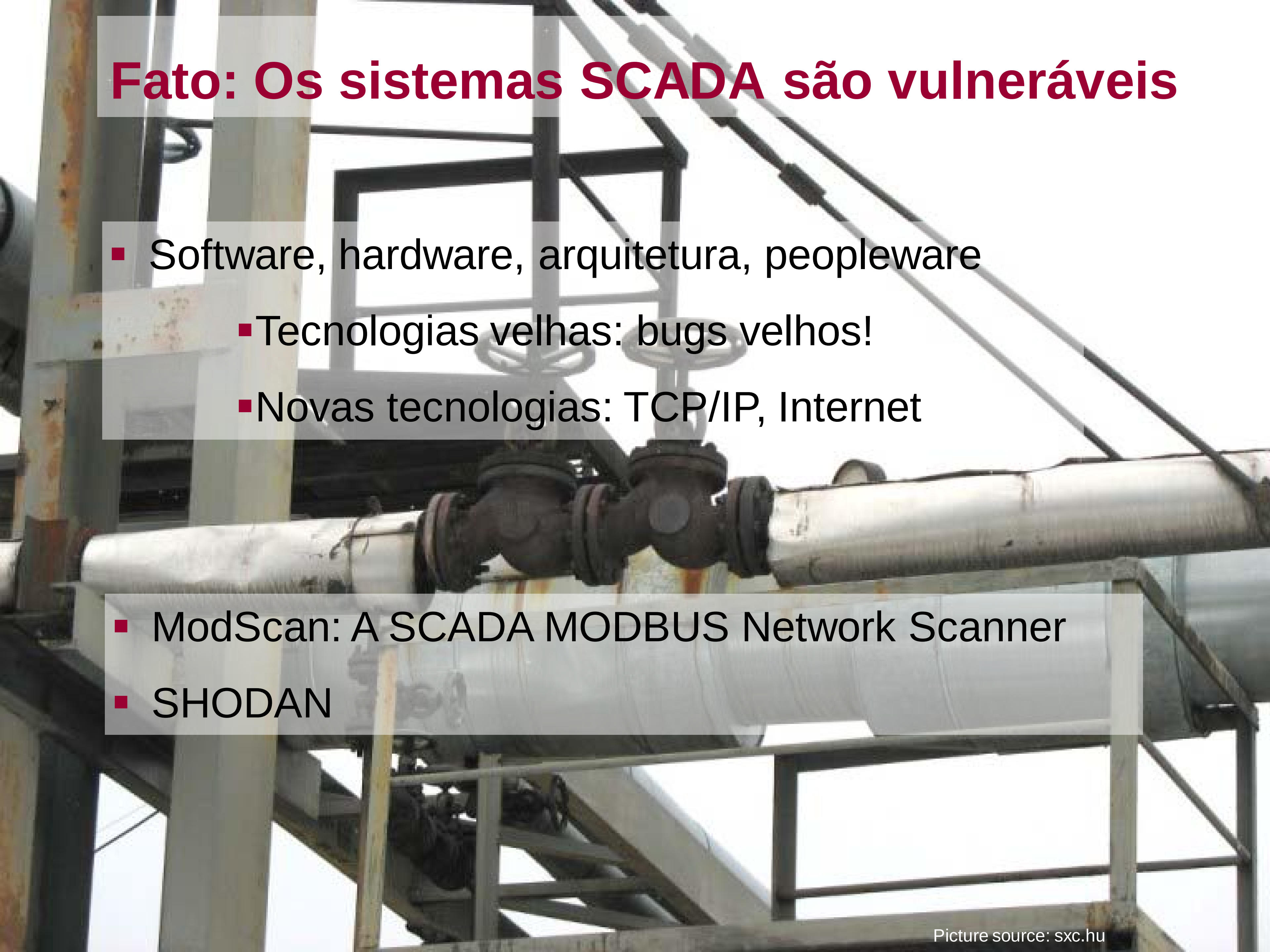
Picture source: sxc.hu

- 0-days
- Malwares
- Trojans
- DDoS
- APT

Fato: Os sistemas SCADA são vulneráveis

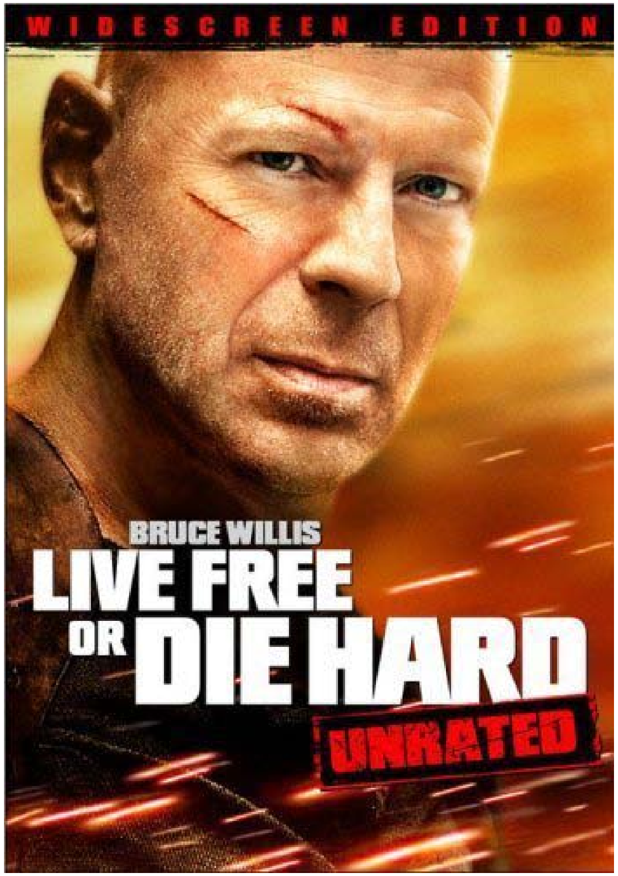
- Software, hardware, arquitetura, peopleware
  - Tecnologias velhas: bugs velhos!
  - Novas tecnologias: TCP/IP, Internet

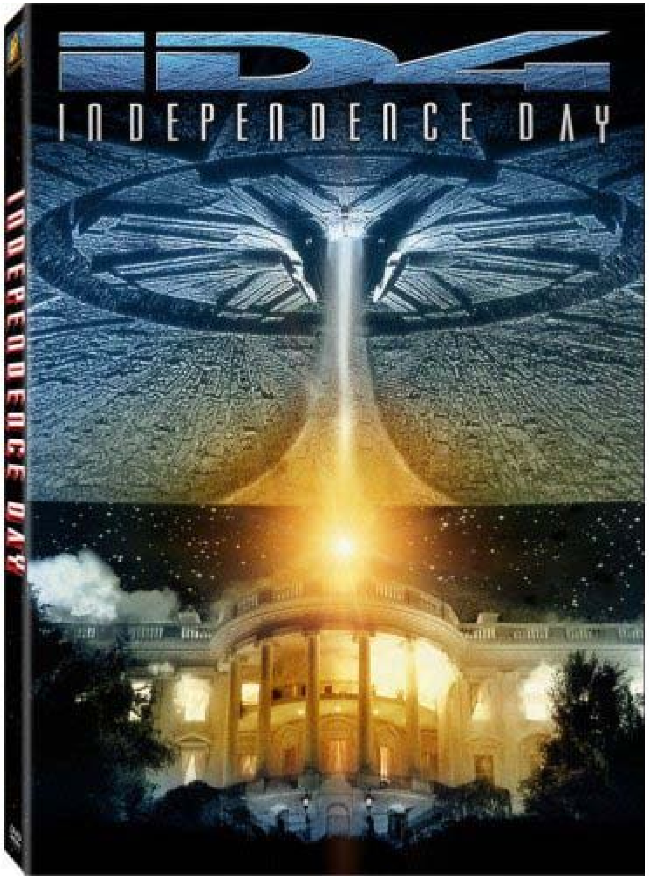
- ModScan: A SCADA MODBUS Network Scanner
- SHODAN



Picture source: sxc.hu

Mito: Hackers podem destruir qualquer coisa





Fato: As pessoas não entendem a tecnologia

Picture source: The IT Crowd

Fato: é fácil colocar a culpa nos Hackers

Fato: “Fontes confidenciais” podem dizer qualquer coisa

- Ninguém pode verificar a história

- Ok, Wikileaks é legal ;)

Picture source: sxc.hu

Fato: As pessoas acreditam em tudo o que a mídia diz

Picture source: sxc.hu

- Poucos jornalistas tem background técnico
- A imprensa quer vender jornal
- A imprensa exagera (as vezes…)

Fato: Agenda Política

- Cyber guerra
  - Cyber Espionagem
  - Critical Infrastructure Protection
- Os Governos precisam de verba

Picture source: sxc.hu

<real>

- Incidentes SCADA

</real>

Picture source: sxc.hu

1999

Rússia: Crackers tomaram o controle de um gasoduto

2001

Austrália: um ex-empregado descontente invadiu o sistema de controle de água e derramou milhões de litros de esgoto

2003

US: verme Slammer afetou a rede corporativa de uma usina nuclear e desabilitou o sistema de monitoramento de segurança

2007

US: Aurora Generator Test (Idaho National Lab.)

http://www.mefeedia.com/news/9316247

2007

US: Operadores desligaram manualmente um reator nuclear da usina Browns Ferry, após os controladores de duas bombas de água terem travado depois de um pico no tráfego de dados

2008

Irlanda: O sistema SCADA de um túnel no porto de Dublin falhou

2009

US: Um erro humano desligou os sistemas de resfriamento de cerca de 18.000 clientes da Duke Energy que participavam de um programa piloto de economia de energia.

2009

US: Um consultor de TI violou um sistema SCADA de uma empresa de exploração de petróleo e gás, depois de uma disputa sobre seu futuro emprego e pagamento.

2010

US: Uma falha do computador interrompe o fluxo de água de uma cidade.

2010

Stuxnet

- Worm que ataca sistemas SCADA
- Quatro zero-days
- Dois certificados digitais
falsos
- Conhecimento do sistema SCADA da Siemens

Picture source: iDefense

Conclusões ?

Um FUD perfeito tem...

Sistemas SCADA

Fontes da inteligência (anônimos!!!)

Hackers

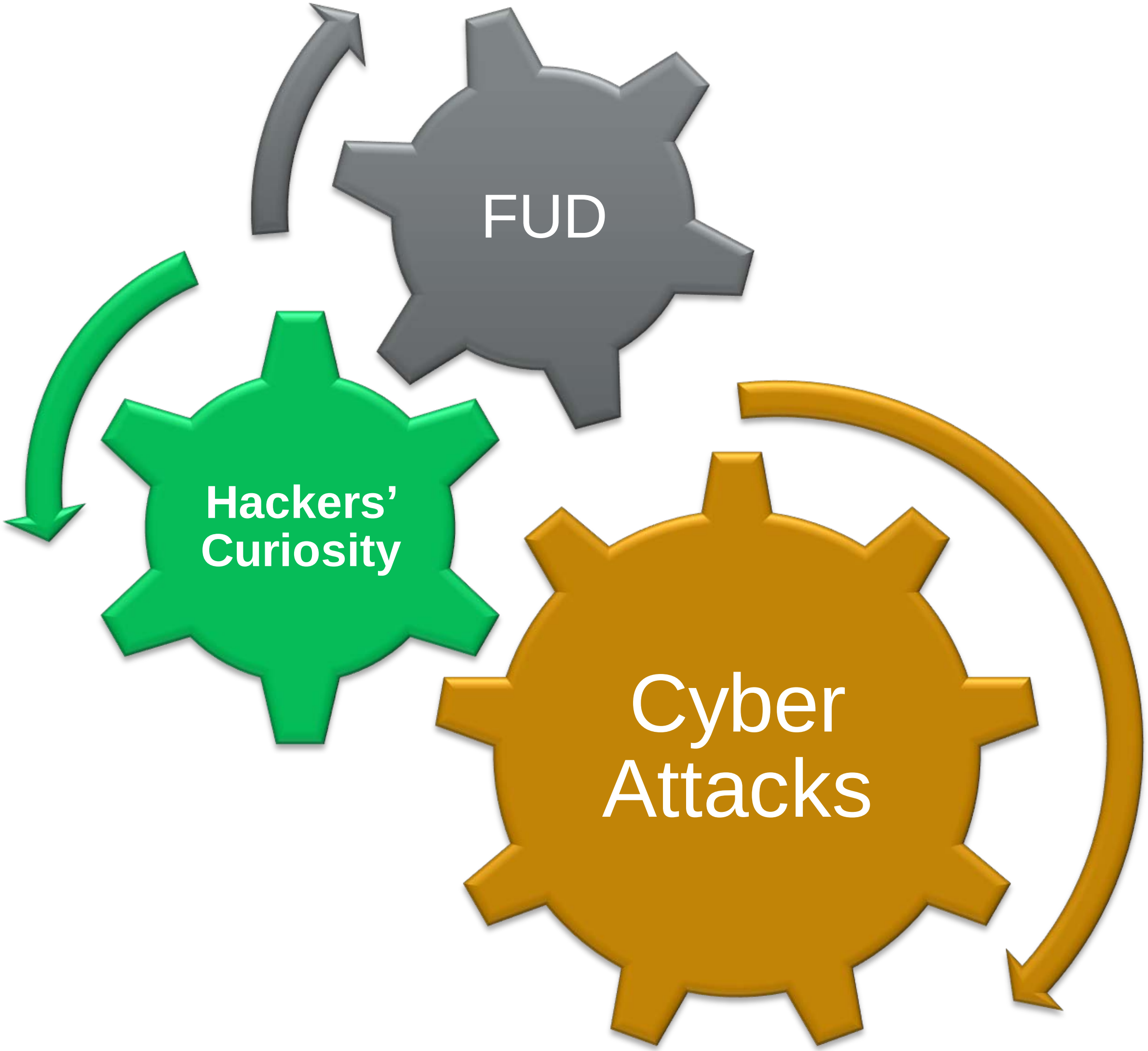
Cyber guerra

Outros países

Cyber ataques

Picture source: sxc.hu

...e suas consequências !


FUD

Hackers' Curiosity

Cyber Attacks

Q&A

Thank You

Anchises M. G. de Paula
iDefense
adepaula@verisign.com
www.verisign.com
@anchisesbr

cloud security alliance℠ CSA Brazil Chapter

GHC

@garoahc

iDEFENSE