A Segurança nas Redes de Telecomunicações

e a doutrina "pressure point warfare"

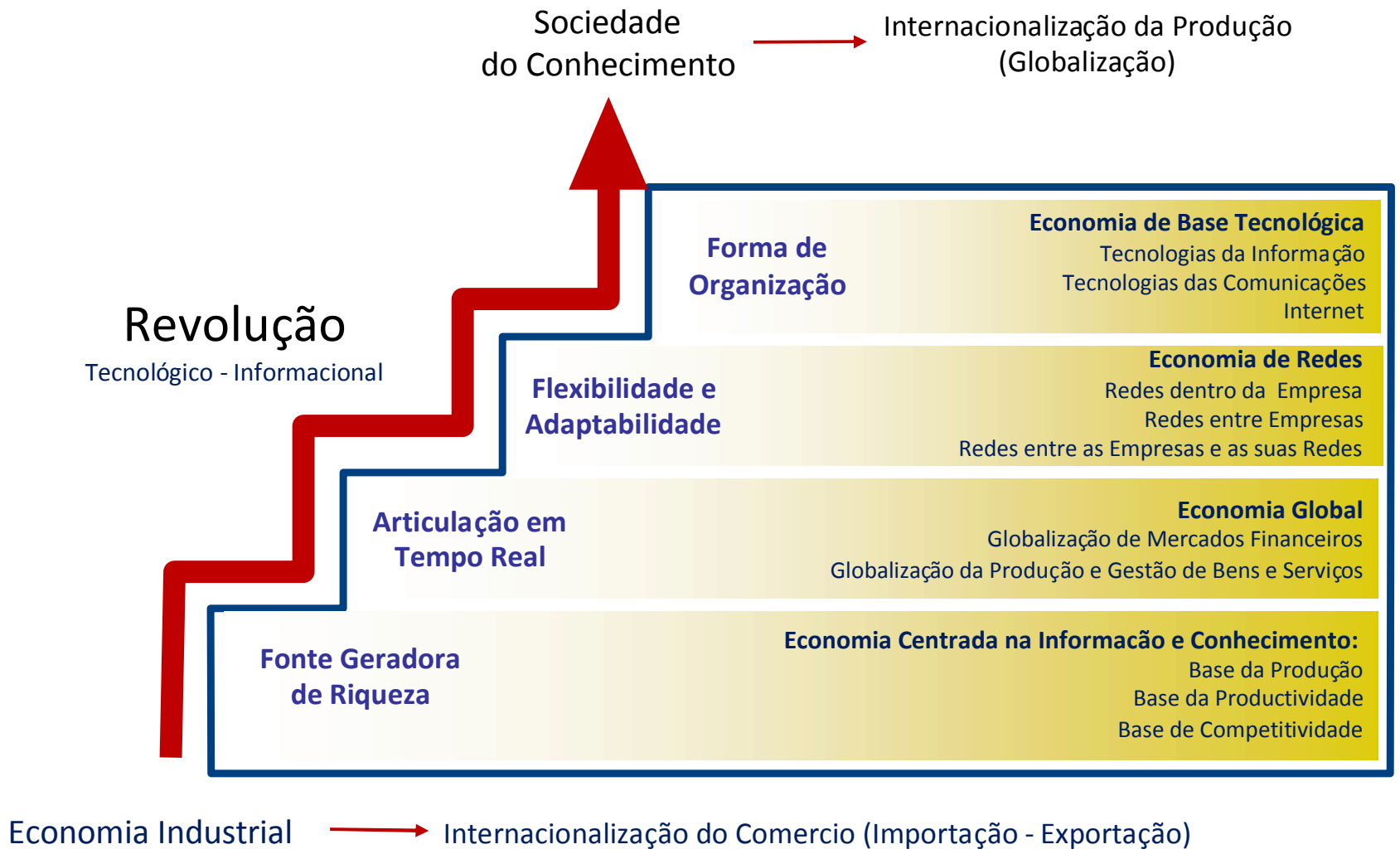
Luis Sousa Cardoso
FIINA Presidente
QSDG/ITU Chairman

A Caminho

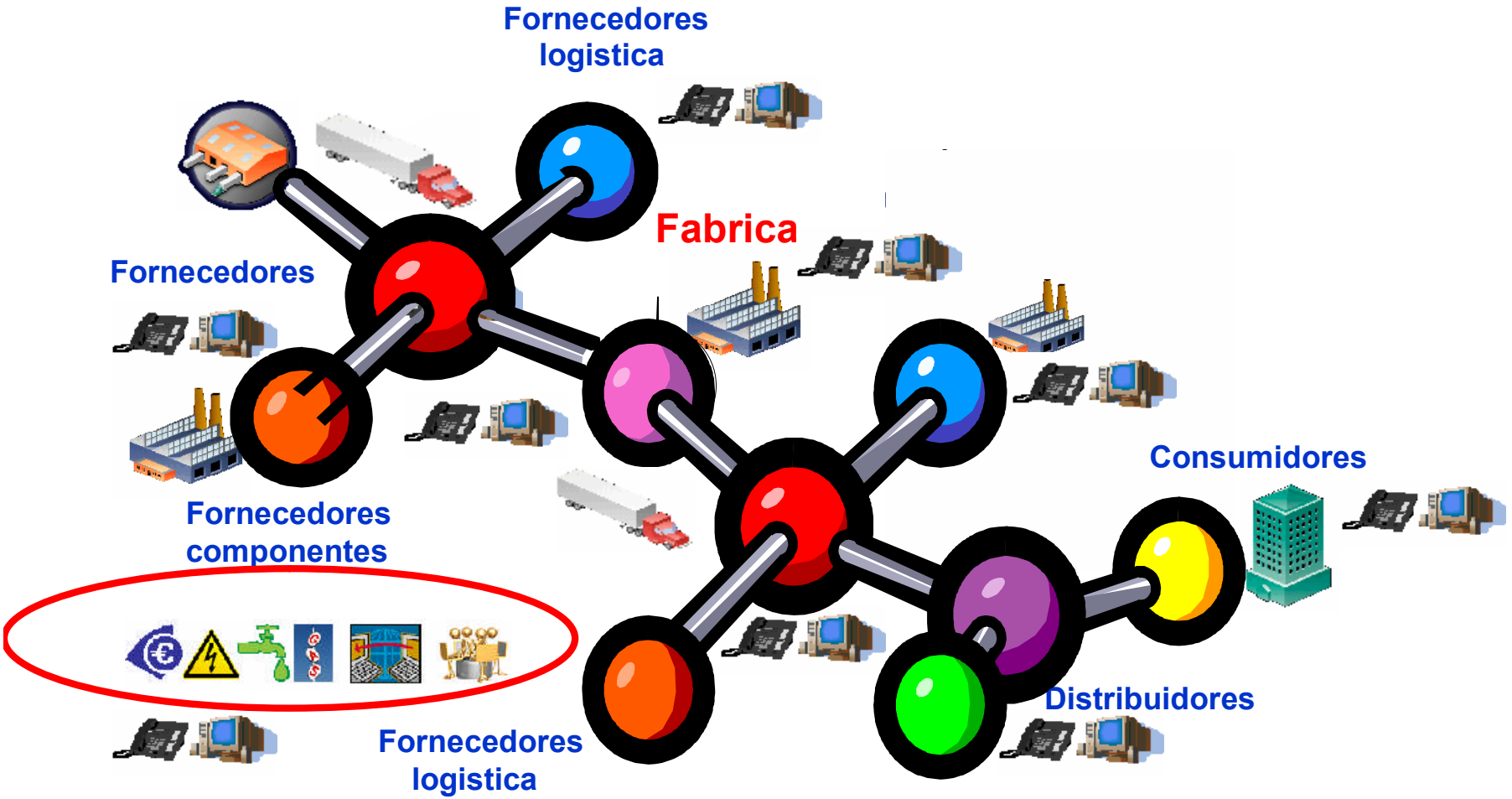
da

Sociedade do Conhecimento

A Caminho da Sociedade do Conhecimento

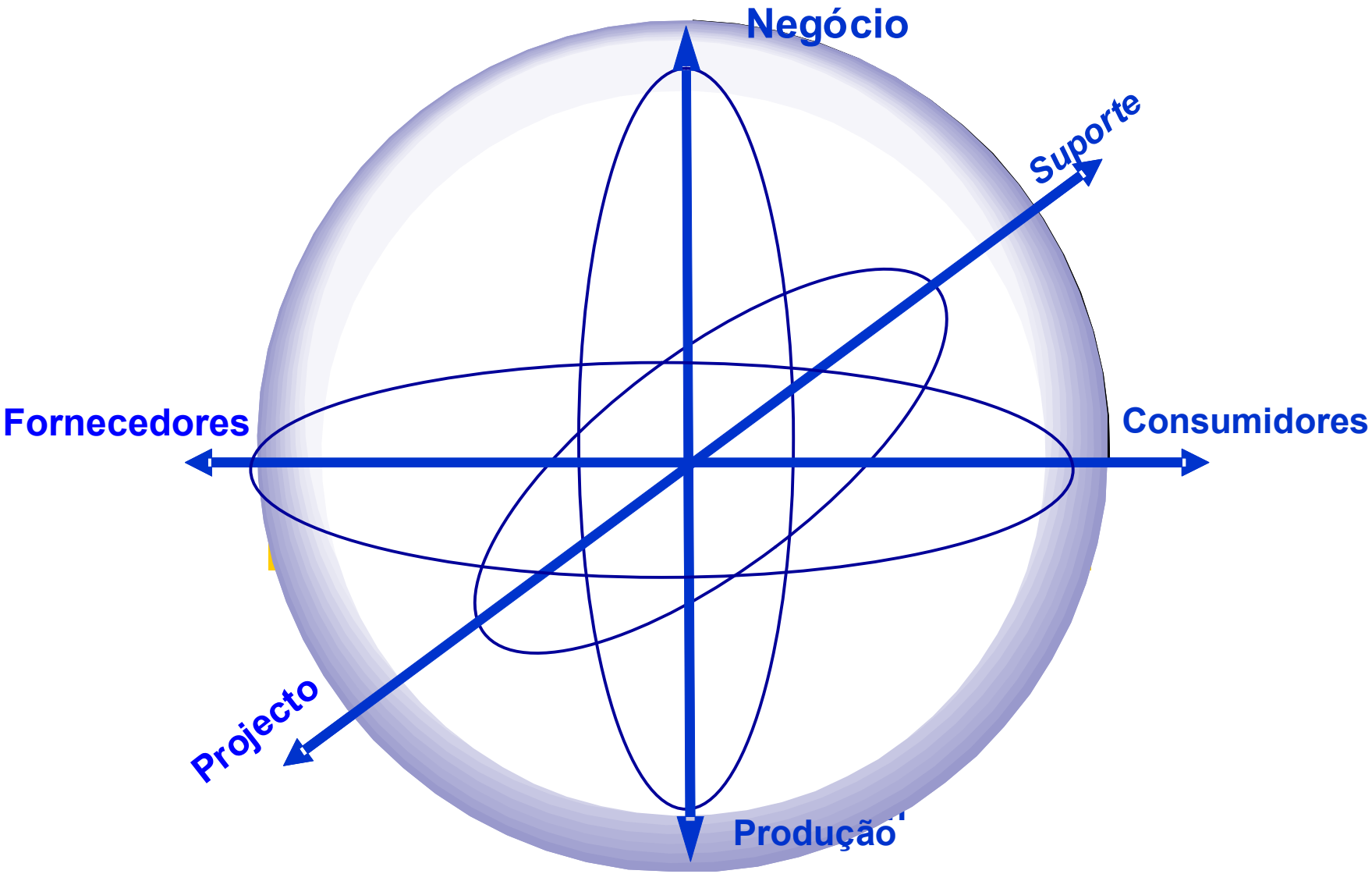


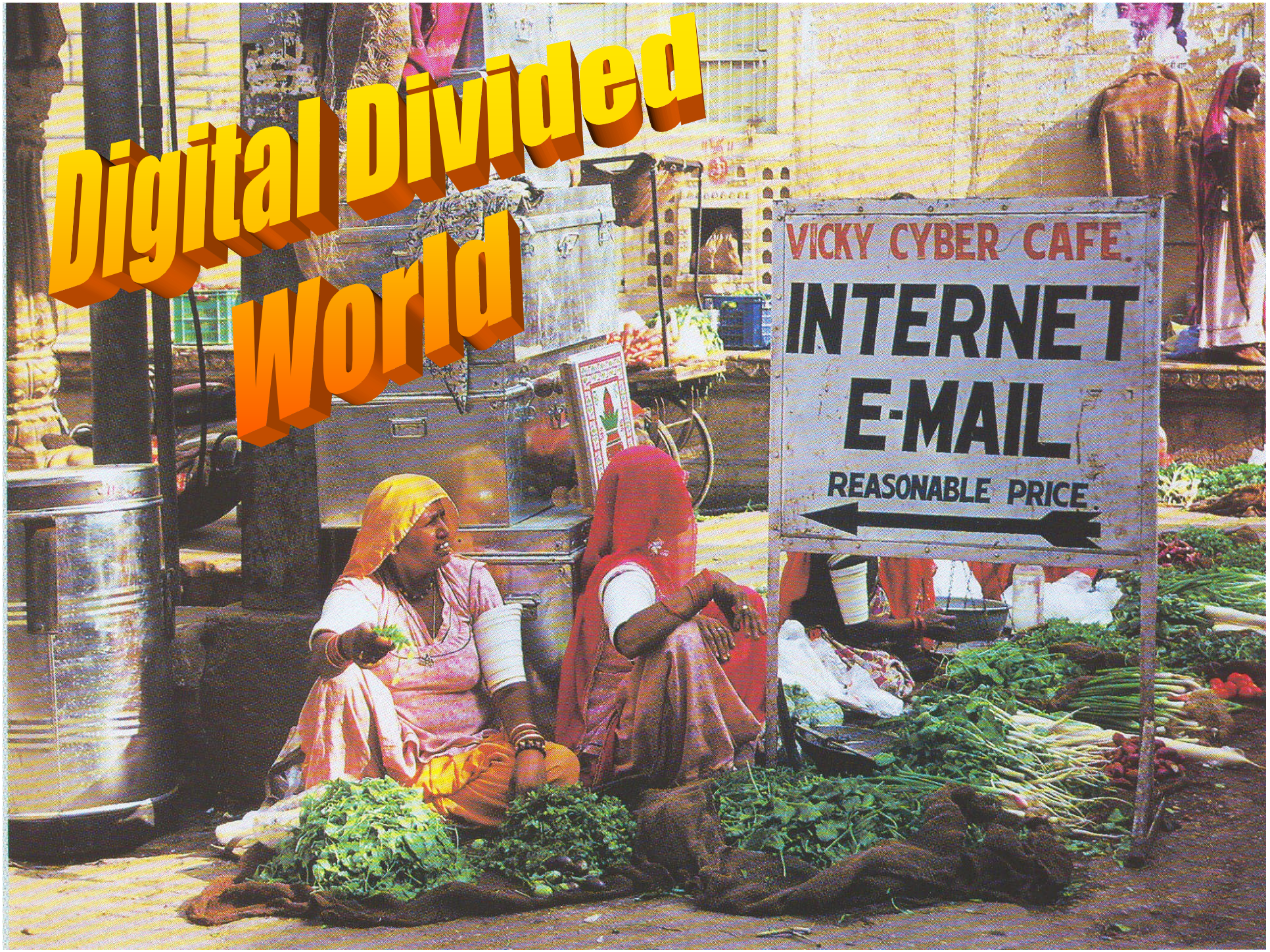
Cadeia de Valor e Interdependências



Fornecedores podem sofrer ciber-ataques com o objectivo de afectar a fábrica.
Estes ciber-ataques podem paralizar a fábrica

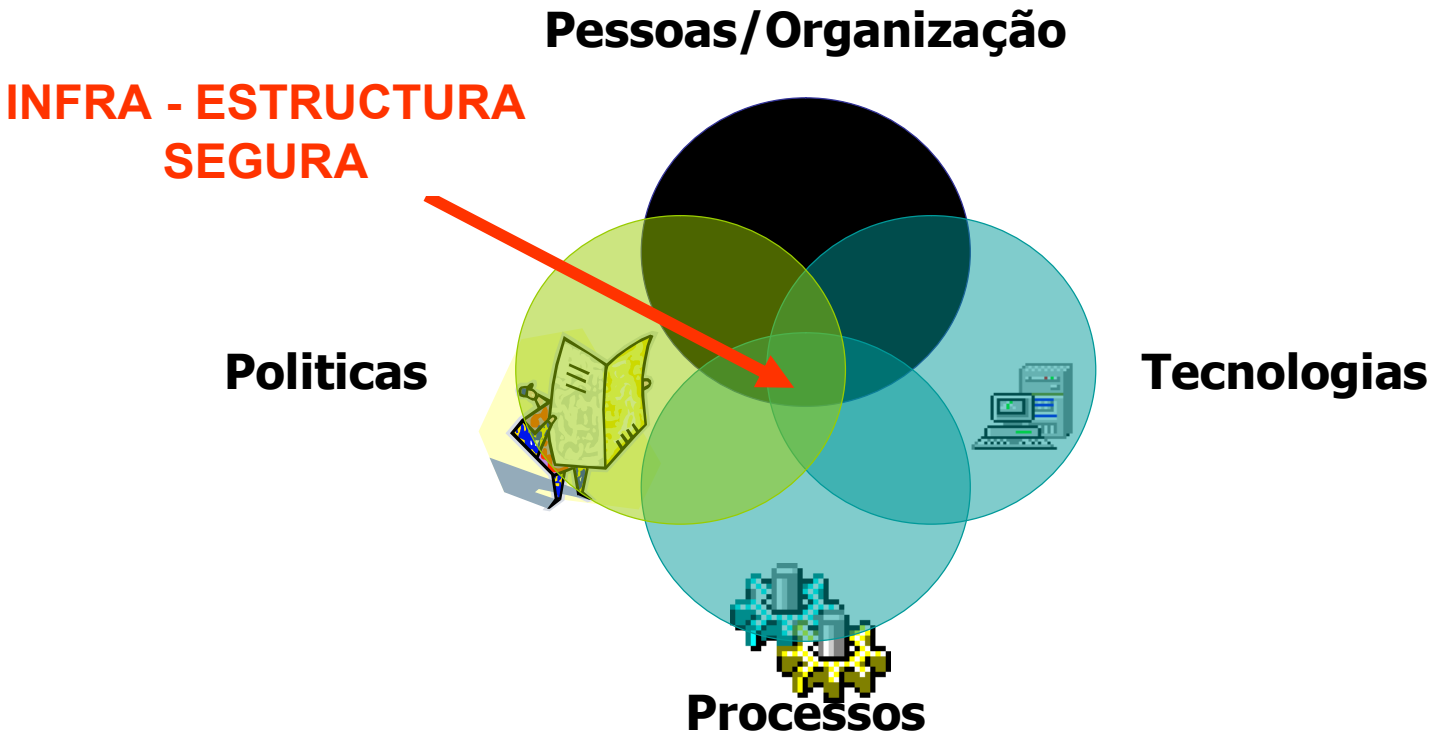
Panorama da Ciber-Segurança




Digital Divided World
VICKY CYBER CAFE.
INTERNET
E-MAIL
REASONABLE PRICE.

Disponibilidade e Fiabilidade

Desafios da Segurança



A protecção da infra-estrutura de informação (CIIP) é hoje em dia entendida como um elemento chave da segurança nacional em muitos países

As infra-estruturas críticas são as instalações físicas e de tecnologia de informação, redes, serviços e bens, os quais, se forem interrompidos ou destruídos, provocarão um sério impacto na saúde, na protecção, na segurança ou no bem-estar económico dos cidadãos ou ainda no funcionamento efectivo dos governos nos Estados

INFRA-ESTRUTURAS CRÍTICAS

- Instalações e redes de energia
- Tecnologia da informação e comunicação
- Finanças
- Cuidados de saúde
- Alimentação
- Água
- Transportes
- Produção, armazenamento e transporte de mercadorias perigosas
- Administração (por exemplo, serviços de base, instalações, redes de informação, bens, sítios e monumentos de importância nacional).

DEPENDÊNCIA

- "…a tecnologia da informação constitui o enlace de controle (*control loop*) de praticamente todas as infraestruturas críticas…"

FONTE: Making the Nation Safer (NCR 2002)

- Essa dependência torna-se tão forte que o que acontece a um sistema pode afetar outros sistemas não diretamente inter-relacionados.

No entanto, em muitos casos, os efeitos psicológicos podem agravar acontecimentos que em si mesmo seriam de menor importância.

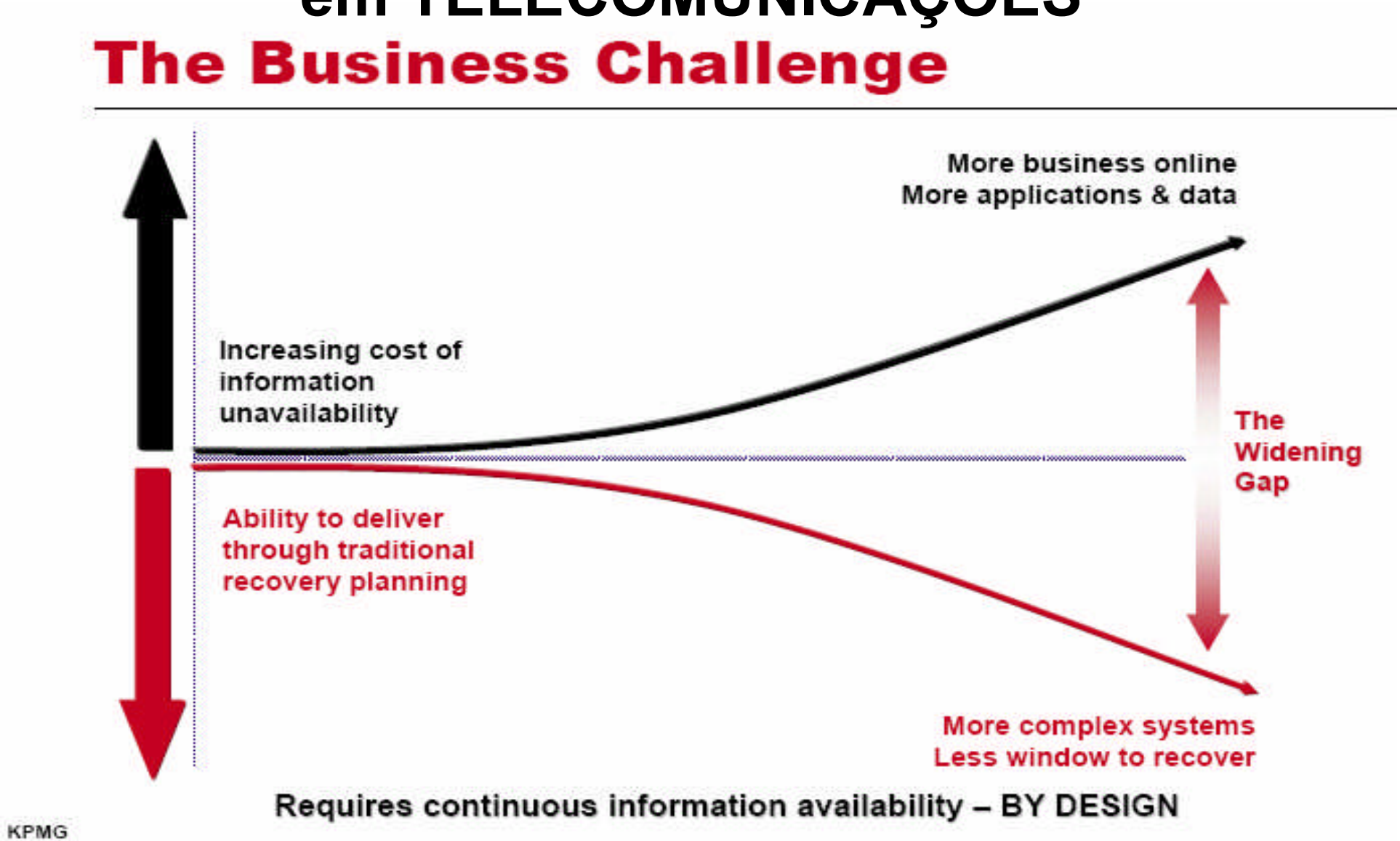
Quais os Riscos de uma Rede menos Segura e a evolução da guerra

QUANTAS REDES DE TELECOMUNICAÇÕES EXISTEM NO MUNDO ?

Uma!

(E ESTE É O PROBLEMA!!)

COMPLEXIDADE DO RISCO em TELECOMUNICAÇÔES



NÍVEL DE AMEAÇA

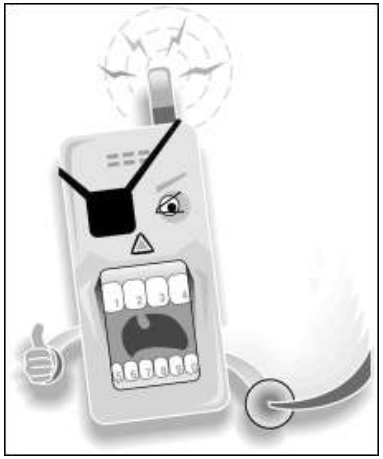
ESTADOS

CRIME ORGANIZADO??

TERRORISTAS

GRUPOS DE PRESSÃO

CRACKERS



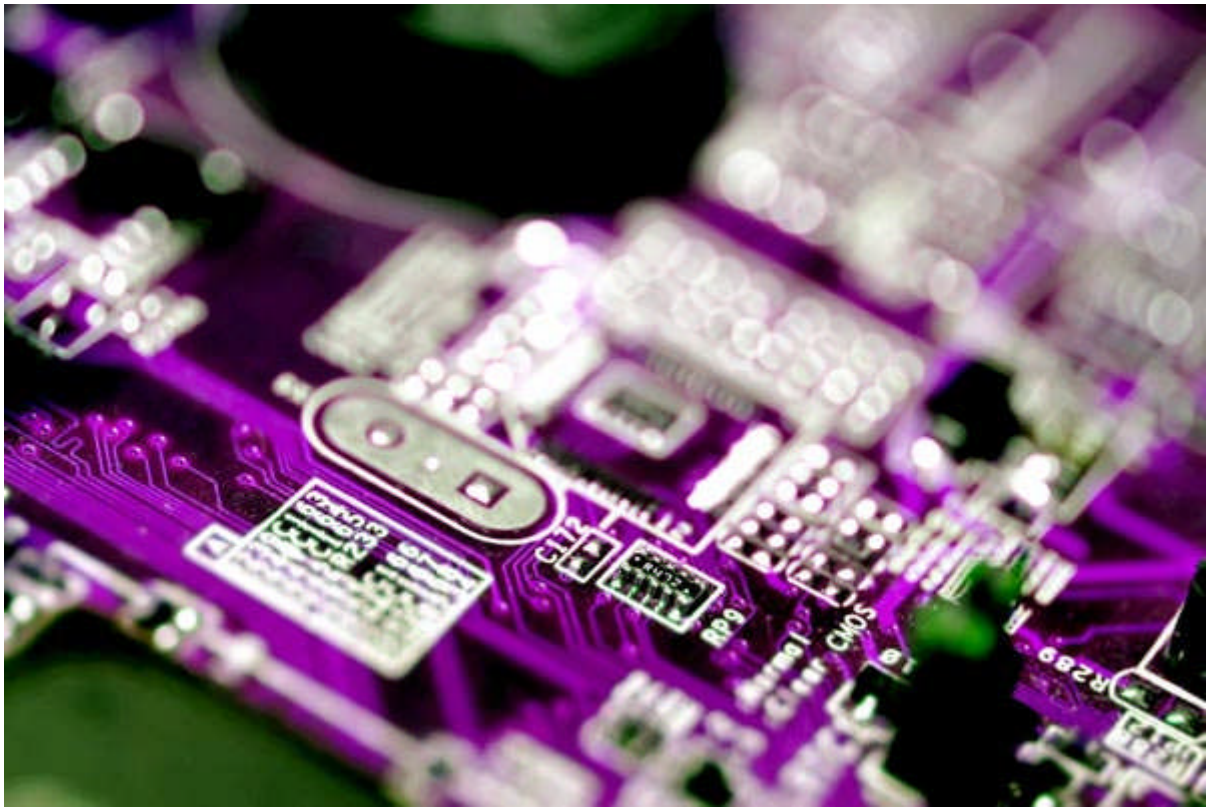
HACKERS

INTENÇÕES

CAPACIDADE

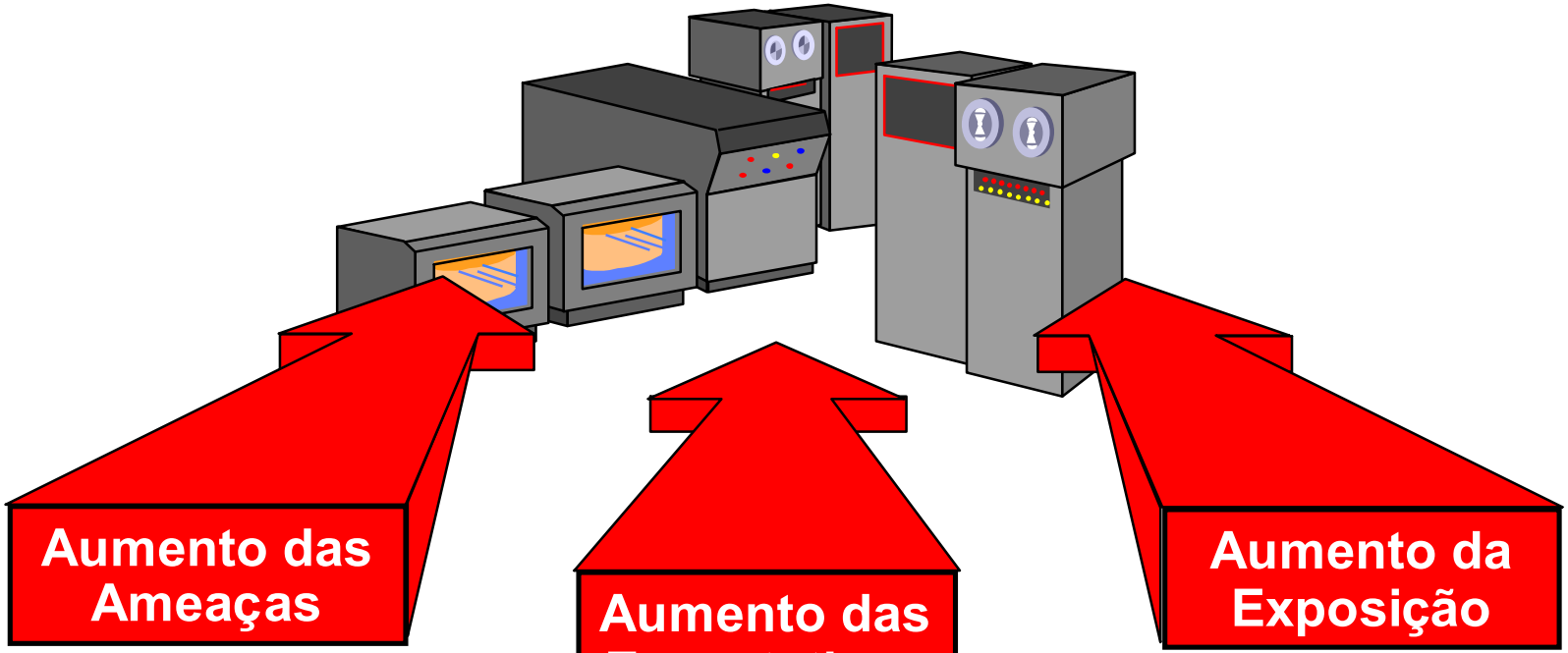
A informação não é mais uma função de suporte; é uma função Operacional.

Pode ser tão mortal quanto é útil



A realidade tem sido sempre pequena demais para a imaginação humana

Necessidade de incrementar a Segurança da Informação



Viroses, hackers, fraude, espionagem DDoS

Utilizadores assinantes, parceiros, auditores, reguladores

Dependencia das IT, Aumento da conectividade

Cibercrime e Segurança da Informação

e-Training

Base de Dados

SCM

Marketing

Produção

Estratégia

Negócio e Inteligencia competitiva

Ciclo do Negócio

Tactical

Publicidade

Vendas

CRM

Análise e Investigação

KB

Gestão do Conhecimento

Analise de conteúdos

Filtragem de dados

Data Mining

Area de informação não estructurada

Area de informação mal estructurada

Area de informação bem estructurada

Dados Padrão

Internet

Organizações de criminosos transnacionais cada vez mais utilizam sistemas de informação para apoiar suas operações.

A Junta Internacional de Controle de Narcóticos das Nações Unidas expediu um relatório em que declarava que os traficantes de narcóticos de todo o mundo vêm cada vez mais utilizando TIs e a Internet para supervisionar operações de fiscalização, para se comunicarem entre si e para facilitar o transporte e a venda de drogas ilícitas.

A EVOLUÇÃO

- **A ciber - guerra está a mudar os seus contornos e a defesa da rede e das infra-estruturas tem de adaptar-se.**
- **Os autores dos ciber - ataques alteraram. Em vez de hackers procurando notoriedade passaram a células (estruturas) de crime organizado com objectivos financeiros e de características hostis.**
- **Incrementou-se a actividade com origens de carácter politico.**
- **Igualmente os Estados passaram a desenvolver actividade nesta área.**

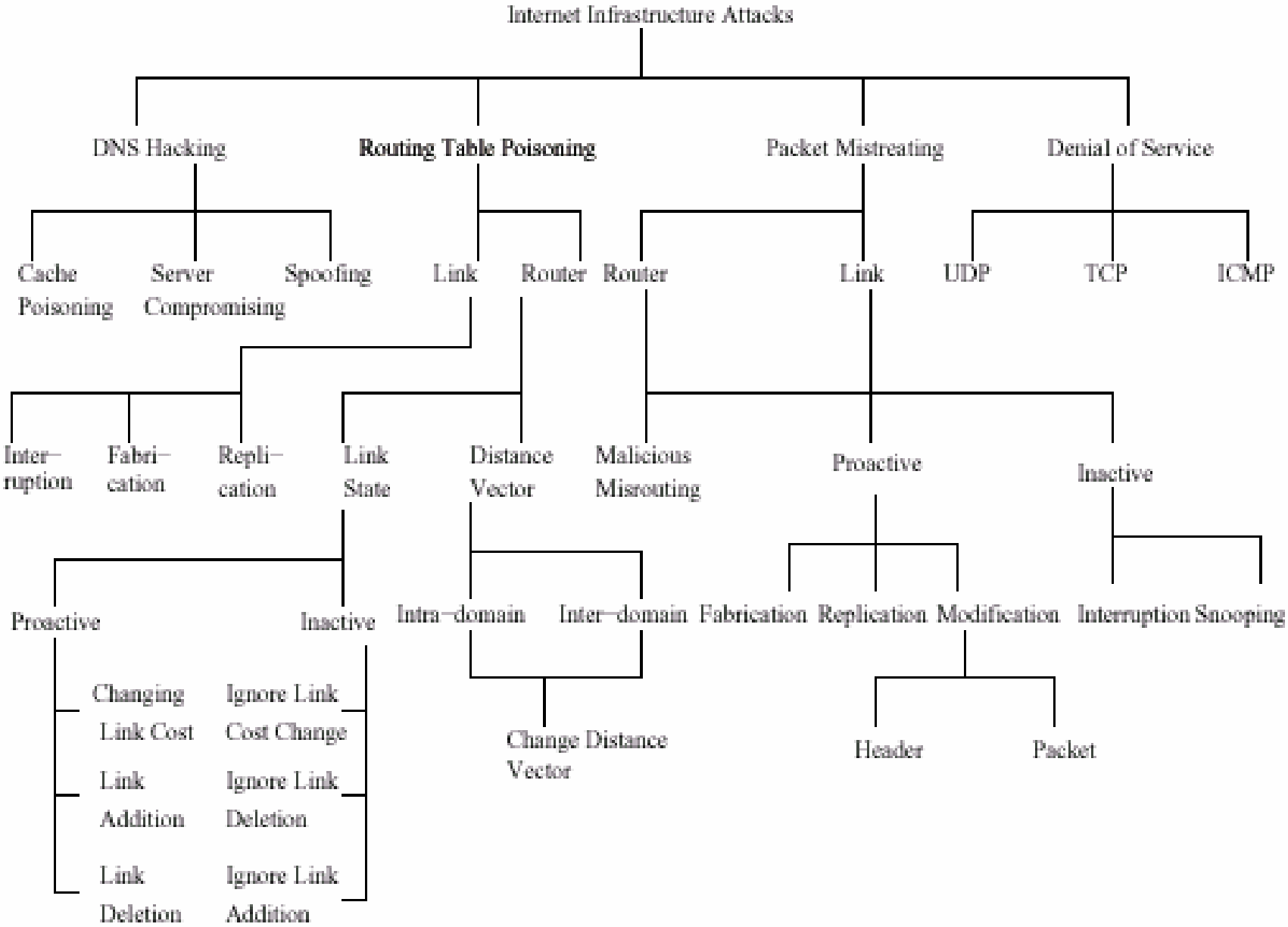
A Globalização da Ciber-guerra

- **É um conflito assimétrico, sem fronteiras e com aspectos globais**
- **Interesses privados ou de estado são por vezes impossiveis de distinguir**
- **Cidadãos do País X podem decidir combater pelo País Y**
- **Qualquer indivíduo, em qualquer lugar, pode ser voluntário em qualquer altura.**
- **Corporações são participantes activos, quer como alvos quer como combatentes**

A Guerra nas Redes de Telecomunicações

Escuela de Terroristas de Afganistan

INTERNET INFRASTRUCTURE ATTACKS



putting the TEA back into CYBER TERRORISM

Grupos Organizados

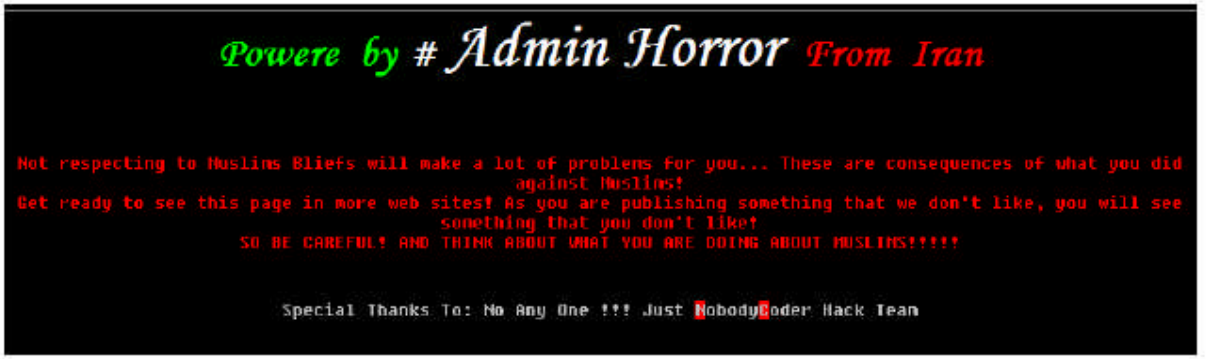
- **Existem Grupos Organizados unidos por uma ideologia comum, seja ela religiosa, politica ou mesmo uma crença (por exemplo a libertação dos animais), ou ainda motivados pelo aspecto financeiro.**
- **Os membros destes Grupos coordenam os seus conhecimentos e actividade para levar a cabo actividades nas redes de telecomunicações, as quais podem ter caracter ilícito.**
- **Existe a necessidade de diferenciar entre os Grupos que apenas teorizam acerca das suas ideologias e cuja actividade reside apenas na publicação e divulgação das suas ideias e os outros que exercem actividade na rede para "demontrar" as suas ideias e "forçar os seus objectivos" levando a acções que criam danos na normal actividade da rede ou de terceiros.**

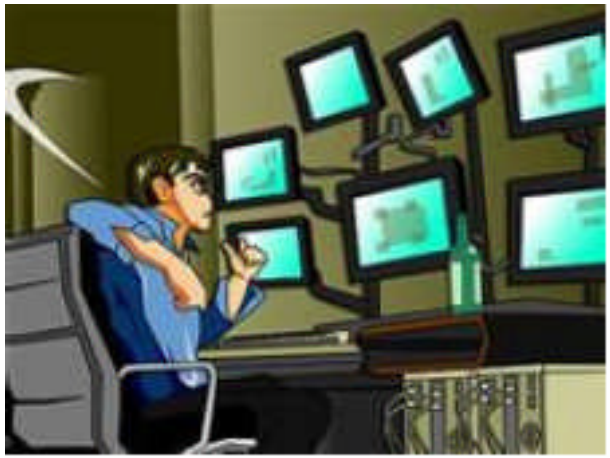
rm -rf /capitalism

killall state

apt-get install anarchism

(hackmeeting[arroba]listas.sindominio.net)





- **Em 1999 os grupos de hackers 2600, Chaos Computer Club, the Cult of the Dead Cow (cDc), !Hispahack, L0pht Heavy Indusries, Phrack , Pulhas y T0xyn emitiram um comunicado anunciando a associação num unidade designada por "Legion of the Underground" (LoU) onde se podia ler:**

  "Los firmantes piden a todos los hackers del planeta ***que rechacen todo aquello relacionado con dañar las infraestructuras de información de cualquier país****. No deis soporte a NINGÚN acto de"Ciberguerra"; mantened las redes de comunicaciones vivas: son el sistema nervioso de nuestro planeta"*

- **Nas economias mais dependentes das tecnologias de informação, o trabalho de peritos em redes de comunicações, computadores e sistemas de segurança passaram a ter uma extrema importância para as diferentes actividades de uma Nação, nomeadamente no respeitante às Forças Armadas.**

Eventos na Internet

- **Espionagem industrial realizada por "hackers" para as empresas ou para o seu próprio proveito;**
- **Sabotagem de sistemas via bombardeamento eletrónico, Todavia, apesar de ser uma prática extremamente destruídora, nem sempre, não é necessariamente ilegal;**
- **Sabotagem e vandalismo de dados;**
- **Terrorismo**

“Podem terroristas usar um computador ligado a uma rede e criar desordem e destruição num ponto distante do mundo?”

“Podem os terroristas, sem recorrerem ao uso de bombas ou explosivos, afectarem um sector da economia, ou, por exemplo, quebrarem o fornecimento de energia eléctrica?”

Um caso….

- **No ano 2000, um Australiano usando um computador ligado à Internet, provocou o despejo de milhões de litros de produtos dos esgotos não tratados ao longo da Queensland's sunshine coast como retaliação pelo facto de ter sido despedido pelo Governo.**

- **Quando a detido pela polícia, esta verificou que ele tinha trabalhado anteriormente na empresa que desenvolveu o software de controlo das instalações de tratamento do conteúdo dos esgotos."**

Um Caso…

- **Neste caso o perpetrador não era um terrorista, mas sim um simples Australiano, com conhecimentos especiais, que estava revoltado pelo seu despedimento.**

- **Também é difícil afirmar-se que o acto foi uma acção de ciber-terrorismo.**

- **Mas o facto é que levanta a possibilidade de ele ser alíciado por terroristas para um futuro ataque de ciber-terrorrismo.**

EM JUNHO 2001 FOI NOTICIADO QUE UM HACKER QUEBROU OS DOIS WEB SERVERS DO COMPANHIA ISO-CALIFORNIA QUE FORNECE 75% DA ENERGIA ELECTRICA DAQUELE ESTADO. PARA O EFEITO USOU UM BUG DOS SERVERS SOLARIS QUE TINHA SIDO REPORTADO EM MARÇO

Operação Sunrise

- **Em 1998, regista-se nos Estados Unidos um incidente posteriormente denominado *Solar sunrise*. Durante esse incidente, os sistemas militares do país foram alvo de ataque electrónico, aparentemente por parte de alguém que operava um computador no Médio Oriente.**

- **Os ataques eram perpetrados no mesmo momento em que se considerava a acção militar contra o Iraque. A escolha do momento dos ataques suscitou suspeitas de que essa fosse a primeira etapa de um grande ataque cibernético por parte de uma nação hostil.**

- **Segundo se comprovou, dois adolescentes da Califórnia, sob a direcção de um sofisticado *hacker* israelita, também um adolescente, haviam orquestrado os ataques tentando simular seu envolvimento dirigindo seu ataque através de computadores em vários países.**

- **Tratou-se de uma real operação militar**

Outros Casos....

- **2 Novembro 2007. Uma série de ataques DoS originou a interrupção do serviço de Internet no Kurgyzstan durante mais de 7 horas. O ataque ocorreu exactamente 5 horas antes de uma manifestação nacional em Bishkek exigindo a demissão do Presidente Kurmanbek Bakiev**

- **No Nepal, em Janeiro de 2006, o Rei Gyanendra, em ordem a fazer face às constantes manifestações e tumultos, ordenou à United Telecom Ltd o corte de todas as linhas telefónicas fixas e móveis no país. As comunicações foram repostas dois dias depois. O mesmo já tinha acontecido em Fevereiro de 2005.**

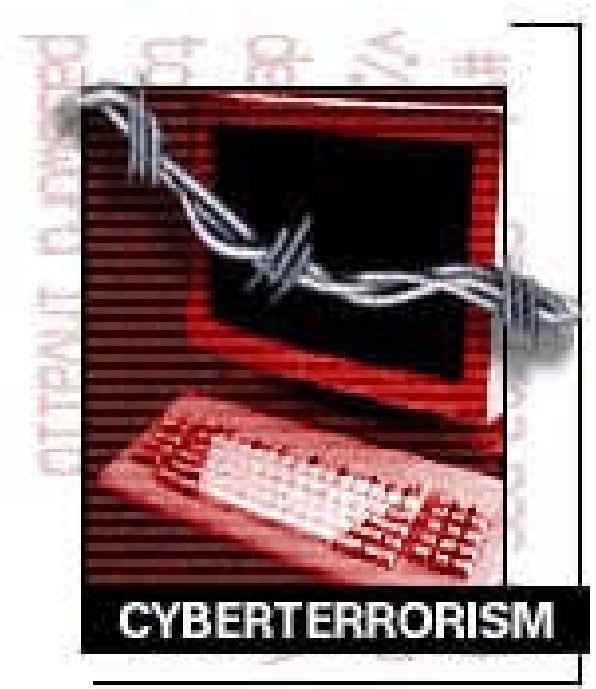
Outros Casos....

- **Em Abril 2001, foi publicado no Japão um novo livro sobre a história daquele país em que as atrocidades cometidas pelas suas forças de ocupação na China e Coreia do Sul eram praticamente apagadas. Como reacção hacker's pro-Coreanos atacaram os servidores da entidades responsáveis pela publicação do referido livro. Foram, nomeadamente afectados o Ministério da Educação, O Partido Democrático Liberal (LDP) e a Empresa Editora.**
- **Em Agosto 2001, após a visita do PM Japonês a um controverso "Memorial de Guerra" – Yasukuni Shrine, hacker's pro-Chineses atacaram múltiplos sites pertencentes a Empresas e Institutos de Investigação Japoneses. O ataque durou cerca de 20 dias.**

Outros Casos....

- Dezembro 1989 o Trojan Horse “AIDS” apagou na Universidade de Bolonha, Itália, 10 anos de investigação. Os dados não foram recuperados.
- 15 Janeiro 1990, um erro de software, causou a interrupção de comunicações da rede da ATT durante 9 horas.
- No início de 1994 verifica-se a quase total interrupção dos computadores da Base da Força Aérea de Roma (NY) nos USA durante um período de 18 dias.
- Entre 1992 e 1994 software malicioso foi colocado nos STP (rede sinalização SS7) da MCI, possibilitando a obtenção ilegítima de mais de 100000 números de calling cards e respectivos PINs, os quais foram depois vendidos por todos os USA e Europa. Desta acção resultou o valor estimado de $50 milhões de perdas por uso não autorizado de comunicações de longa distância.

Outros Casos....



MARÇO 10, 1998

Um jovem de Massachusetts desactivou a torre de control do aeroporto e outras facilidades do aeroporto durante seis horas e interrompeu todo o serviço telefonico em Rutland, Massachusetts.

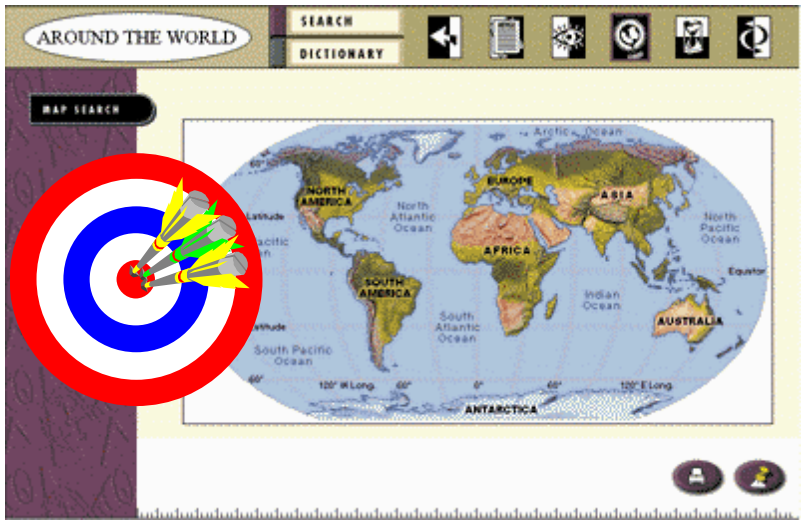
O ataque tambem desactivou a transmissão de rádio do aeroporto e o sistema de aproximação e respectivas luzes de pista.

Outros Casos....

“METAL ATTACKS”

Um jovem romeno Calin Matias, alias “metal”, de 17 anos, entrou nos sistemas do Pentagono, da Força Aérea dos USA e destruiu as paginas web do FBI

FRANCE TELECOM, BRITISH TELECOM, DEUTSCH TELECOM, FORAM IGUALMENTE AFECTADAS PELAS ACTIVIDADES DO “METAL”



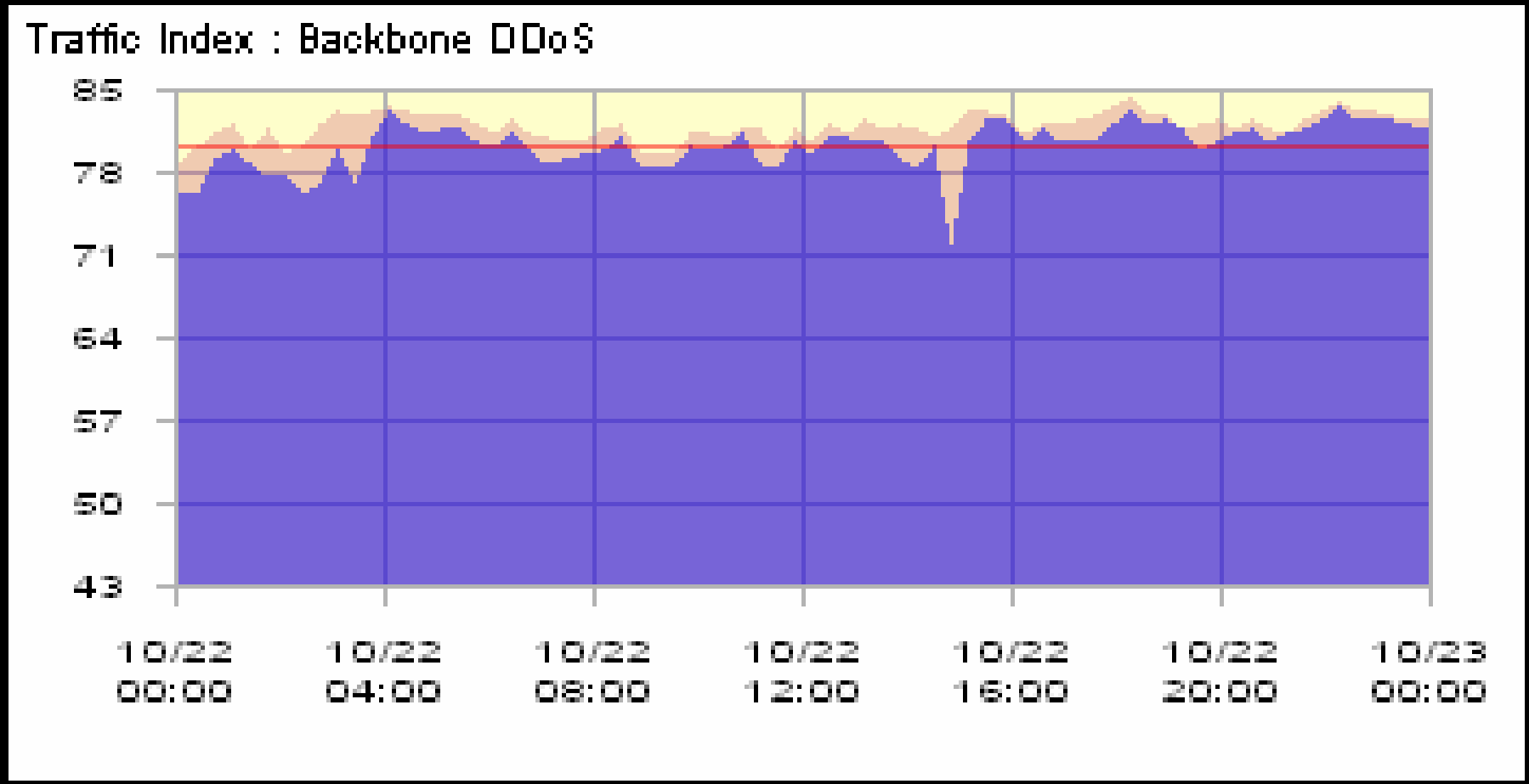
ATAQUES A SERVIDORES ROOT

Uma série de ataques distribuídos de negação de serviço foram dirigidos aos treze "servidores raiz" – os principais computadores que administram o tráfego global da Internet.

- **O ataque teve duração relativamente curta, em parte porque se recorreu a medidas de segurança adequadas, mas também porque o desconhecido perpetrador subitamente decidiu suspendê-lo.**

Esses ataques demonstram que as ameaças podem visar nervos centrais especialmente críticos da rede global de informação e continuam a ser extremamente difíceis de serem rastreadas. Tivessem seus autores tentado paralisar a Internet, independentemente de quem fossem, provavelmente teriam conseguido, e usaram uma forma bem conhecida de ataque.

MAPA DOS SERVIDORES ROOT

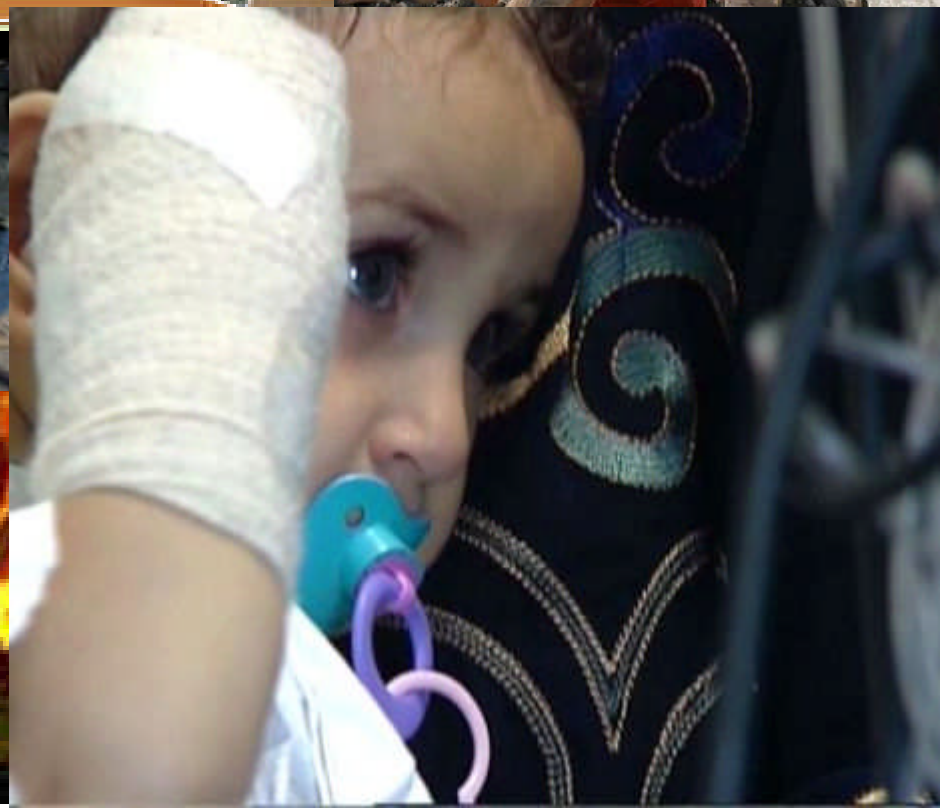

Traffic Index : Backbone DDoS
85
78
71
64
57
50
43
10/22 00:00
10/22 04:00
10/22 08:00
10/22 12:00
10/22 16:00
10/22 20:00
10/23 00:00

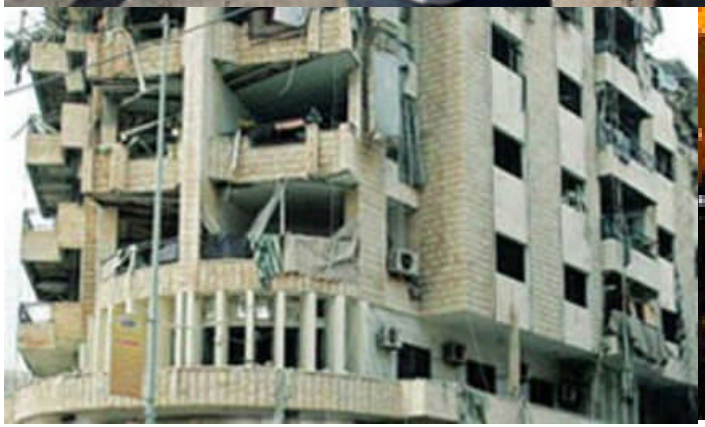
Outros Incidentes…

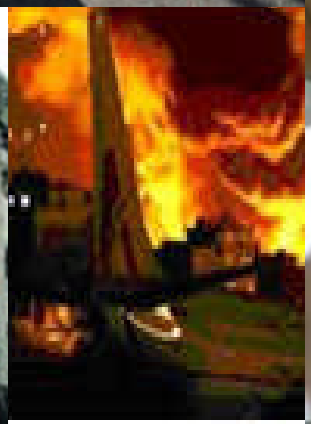
- **Em Jan 2003 o serviço de Internet sofre uma quebra devido ao virus Slammer lançado a partir da Coreia do Sul.**
- **Em Ago 2003 Blackout na América do Norte**
- **Em Ago 2003 grande confusão no Japão criada pelo virus Blaster**
- **Em Ago 2004 os sistemas de emergência do Japão foram afectados devido a um incidente com um operador de telecomunicações.**

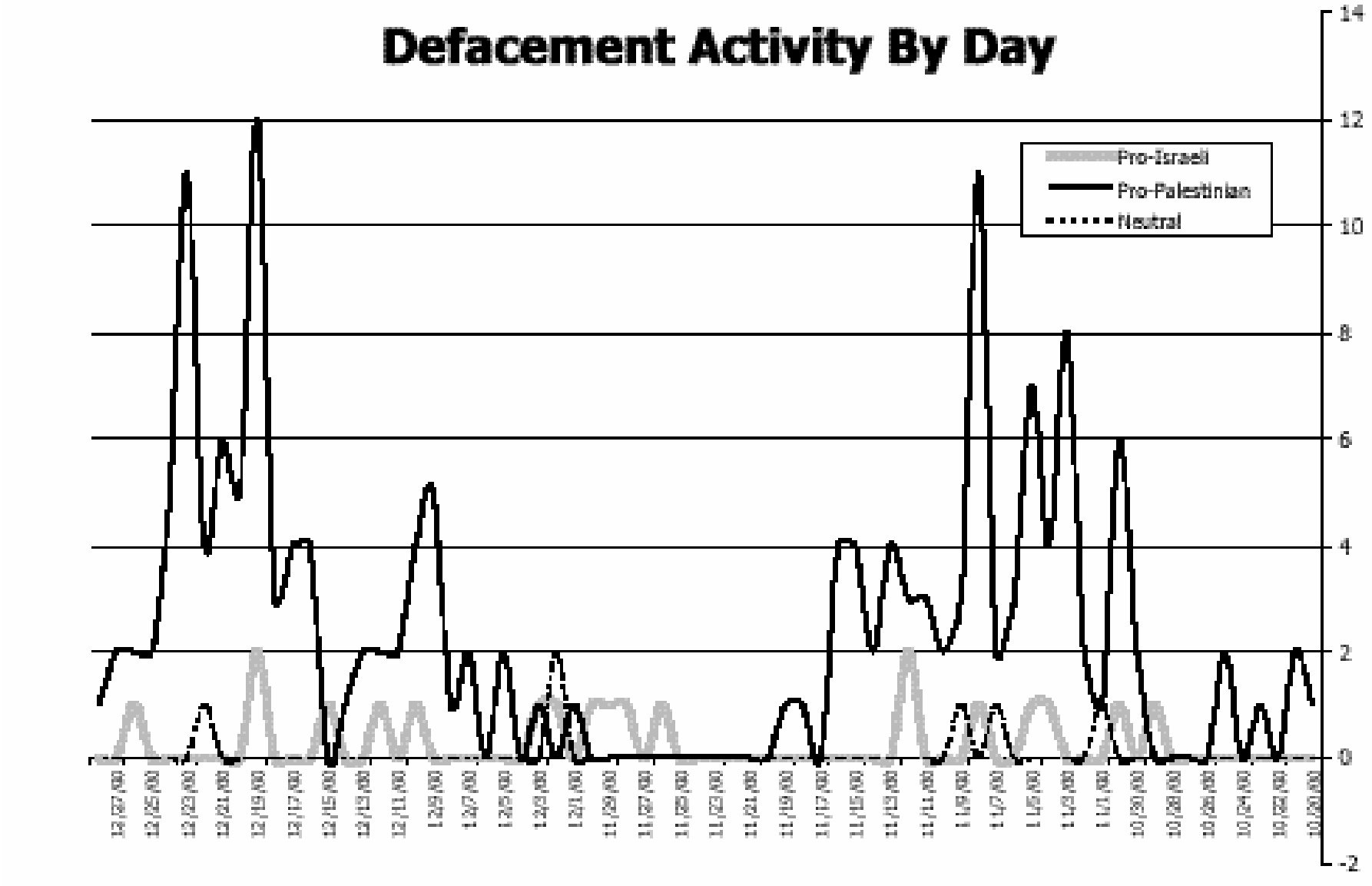
Ciber-Guerra no Medio Oriente

De Outubro 2000
a Janeiro 2001



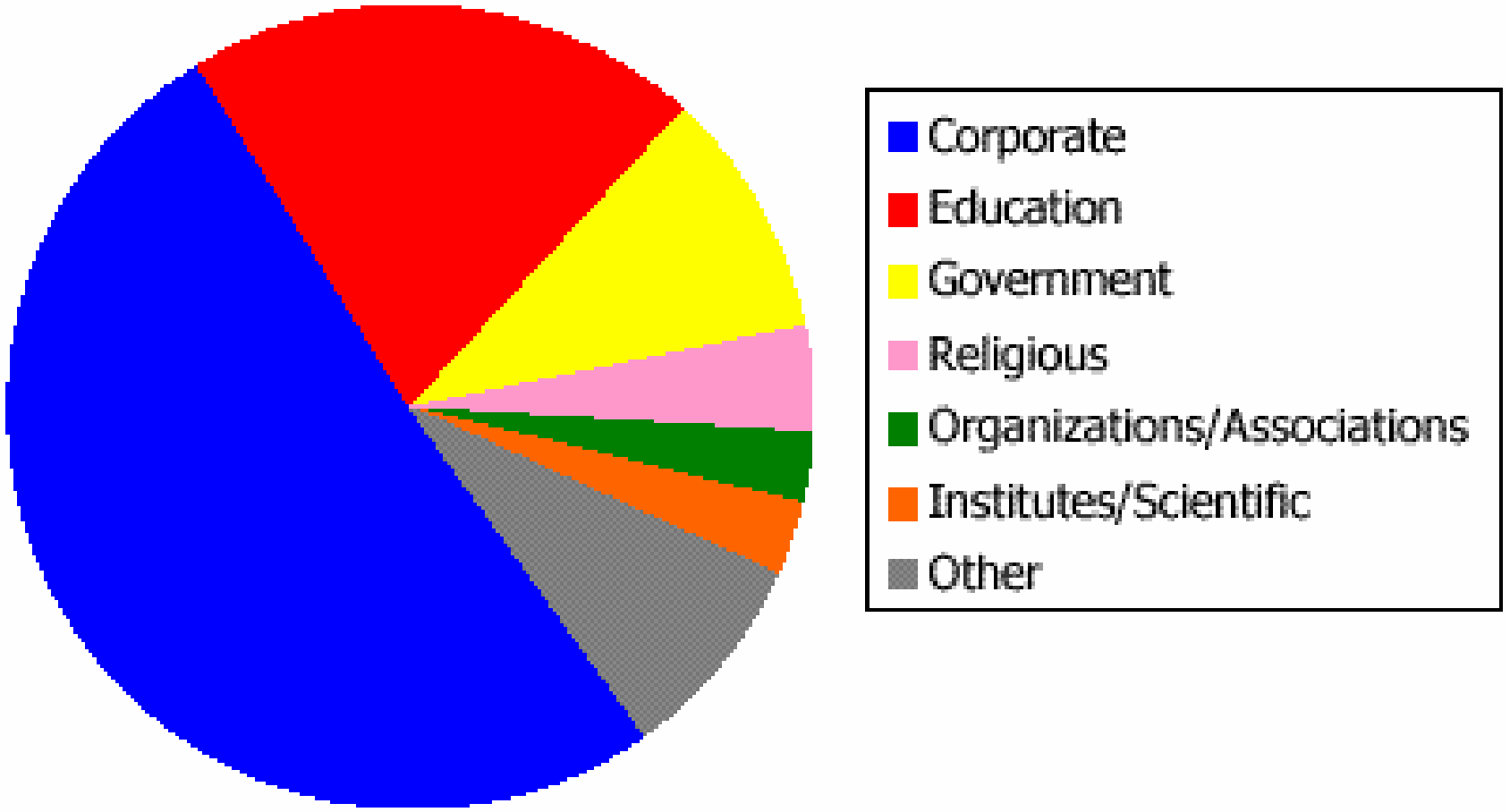




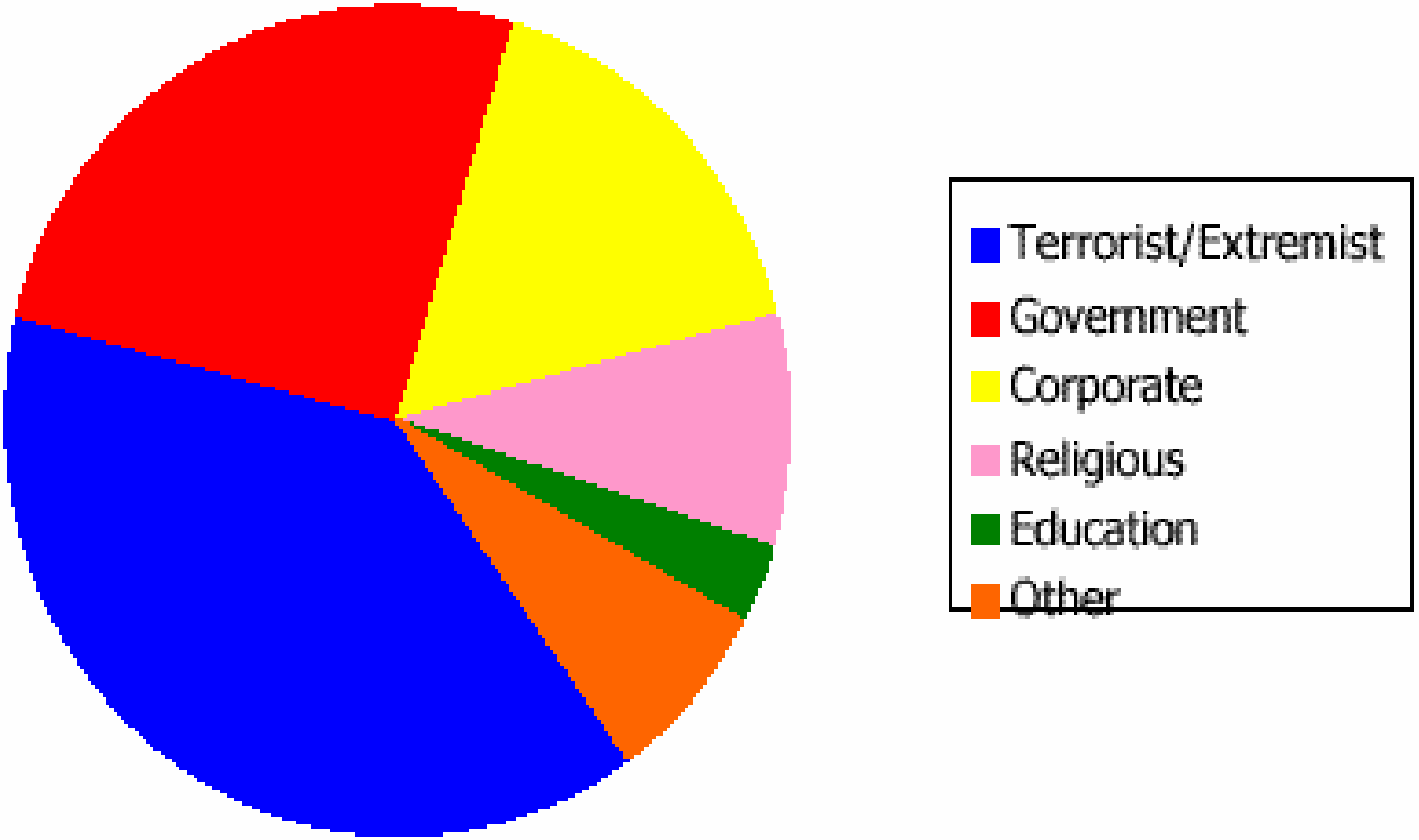


PERIODO 20out2000 A 27dez2000

Pro-Palestinian Attacks by Sector



Pro-Israeli Attacks by Sector



Ciber-Guerra no Kosovo (1999)

Ataques ao sistemas governamentais e militares dos USA conduzida por “Hackers” da Servia como retaliação da guerra movida contra a Servia e que foram intensificados quando os bombardeamentos começaram.

- **Grupo de “hackers” "Black Hand"**
- **Hackers "Serbian Angel"**

❖ **Desfiguração do site da White House**

» **Letras vermelhas "Hackerz wuz Here“**

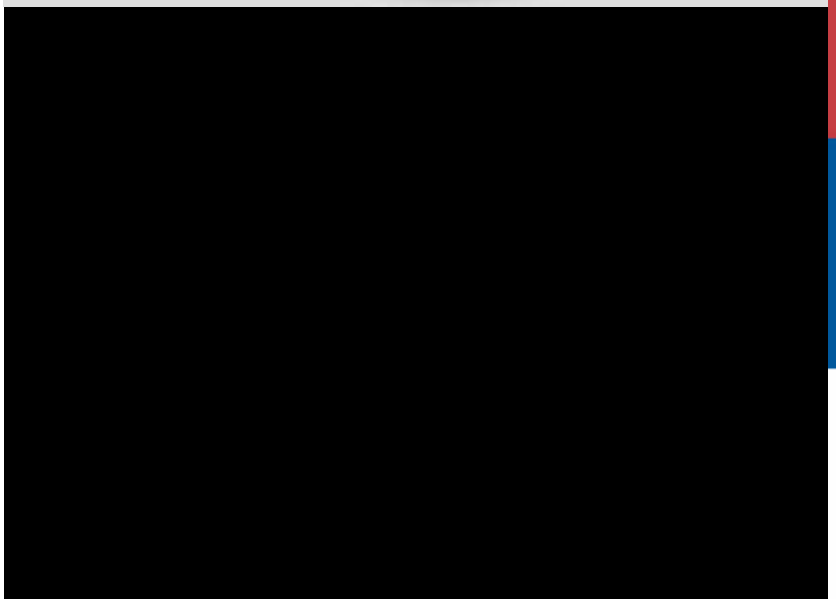
Outros Casos.....

- **Em Janeiro de 1999 os computadores do US Air Intelligence computers sofreram um ataque coordenado. Aparentemente tal ataque tinha origens na Russia**

Primavera 1999

- **A Embaixada Chinesa em Belgrado é bombardeada.**
- **Retaliação: Hackers Chineses atacaram sites governamentais nos USA e entraram no sistemas da White House, do Departamento de Energia, e do Serviço Nacional de Parques**


www.khg-crew.ws - për të gjithë! - Kosova Hackers Group
copyright 1998-2008 by KHG (eliani)



cracked by dodi - Netscape

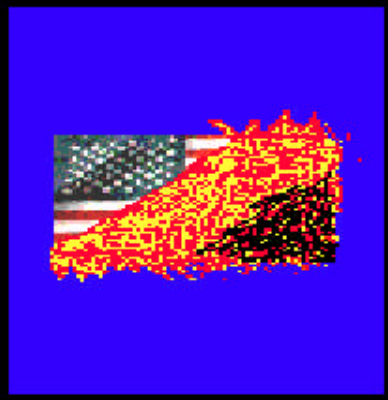
File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security Shop Stop

Bookmarks Location: http://www.attrition.org/mirror/attrition/2000/11/04/www.cognifit.co.il/ What's Related

jihad

Islamic unity



I see at last I am no longer on my own in the cyber war against the jews.
(notice how i didn't say israel ? well I don't recognise Israel as a country)
I am pleased to see my Muslim brothers in Gforce and PHC contributing to the destruction of jewish internet sites.

Today is Friday 3rd Novemeber:

Netvision.net.il's backbone was held down for another hour leaving many .gov. web sites inacessible. Expect more in the coming weeks.
This time even the uunet peering router was badly lagged.

As for www.idf.il I don't care where you move your propaganda machine I will to take it out

Document: Done

Jihad Sites

- Sites do *jihad* aparecem e desaparecem constantemente, às vezes tirados do ar pelos provedores para reaparecerem em qualquer outro lugar, às vezes deliberadamente retirados para continuarem à frente dos investigadores.
- O número de sites extremistas vem crescendo de forma exponencial – de uma meia dúzia no ano 2000 para alguns milhares em 2008.
- Muitos dos sites do *jihad* colocam suas informações e discussões mais inflamadas em áreas protegidas por senhas.


English Site
الصفحة العربية
فان حزب الله هم الغالبون
فإن حزب الله هم الغالبون
Central Press Office الوحدة الإعلامية المركزية

"Irhabi007"

- Foi o responsável pelo *jihad* na internet
- Foi uma figura central para possibilitar a reconstituição da al-Qaida após a queda do Taliban e a fuga do Afeganistão.
- Os seus seguidores transferiram-se para o ciberespaço, definitivamente um território sem governo, no qual os adeptos do *jihad* criaram escolas virtuais para treinamento ideológico e militar e uma intensa propaganda armada.
- Foi pioneiro em muitas das técnicas. Apropriou-se, por exemplo, do site do Departamento de Estradas e Transporte do Estado do Arkansas – para distribuir arquivos de grande dimensão com vídeos e ensinava seus companheiros ciber-jihadistas a proteger o anonimato online.
- Vivia na zona oeste de Londres, chamava-se Younis Tsouli, filho de um representante do Turismo de Marrocos, tinha 22 anos, e era estudante de tecnologia de informática quando foi detido pelas autoridades inglesas. Utilizava numeros de cartões de credito roubados para a criação dos diversos websites que utilizou.


معا من أجل هزيمة الاعلام الصليبي الكاذب
الله أكبر
لا إله إلا الله محمد رسول الله
لا عزة إلا بالجهاد
سوف نعيد حكم الله في الأرض ونمضي على درب الجهاد
HaCKErS aL-AnSaR
لا إله إلا الله محمد رسول الله
هاكرز أنصار الجهاد
لا إله إلا الله محمد رسول الله
كتيبة القاعدة الإعلامية

OBL Crew

In the Name of Allah, Most Beneficent, Most Merciful

All Praise is for Allah, and may Prayers and Peace be upon the Messenger of Allah and upon his Family, Companions, and whoever is guided by his guidance.

What is eJIHAD ?

JIHAD is the term used for struggle against evil. Electronic jihad or simply , E - JIHAD , is the jihad in cyberspace against all the propagandas and false allegations against the message of truth . E-JIHAD is the struggle in cyber space against all false and evil disciplines, ideology and forces of evil .

What is the need of eJIHAD ?

Have you ever think what is the need of army? To defend the freedom and liberty of a territory and defend it from the attacks of evil intruders. similarly , E-jihad is the battle in the field of cyber space, against all false believes, and to defend the truth against the false and mean propagandas and cults. It is as necessary as a regular army, to defend the ideological borders of a nation.

It is said, " **it is not the gun, it is man behind the gun** ". Do you ever think what makes a "man "? Nothing, but just the faith and ideology. Without faith and ideology, there is no r then have gun , but without any man .

Why should we join eJIHAD ?

The Muslims in general and the scholars in particular are commanded to call people to Islam, as Allah says (interpretation of the meaning):

"Let there arise out of you a group of people inviting to all that is good (Islam), enjoining Al-Ma'roof (i.e. Islamic Monotheism and all that Islam orders one to do) and forbidding Al-M disbelief and all that Islam has forbidden). And it is they who are the successful"[Aal 'Imraan 3:104]

The Prophet (peace and blessings of Allah be upon him) said: "Convey from me even if it is (only) one aayah." (Narrated by Al-Bukhaari, 3461)

Calling people to Allah is an important task and a glorious mission, because it means calling people to worship Allah alone. It means bringing them forth from darkness to the light, pl place of evil and truth in the place of falsehood. Hence whoever does this needs to have knowledge, understanding, patience, forbearance, gentleness and kindness. He needs to give c himself, and he needs to understand people's circumstances and habits.

Allah says (interpretation of the meaning):

"Invite (mankind, O Muhammad) to the way of your Lord (i.e. Islam) with wisdom (i.e. with the Divine Revelation and the Qur'aan) and fair preaching, and argue with them in a way th your Lord knows best who has gone astray from His path, and He is the Best Aware of those who are guided" [Al-Nahl 16:125]

Allah Subhanu Wata'Allah also orders us to do good deeds as :

" I swear by the time, Most surely man is in loss, Except those who believe and do good, and enjoin on each other truth, and enjoin on each other patience. " (AL-ASAR 103:1 – 103:

that means if we dont want not to be among losers , we have to follow the HOLY teachings of Allah as well as we have to try to spread the DIVINE TEACHINGS to every human being.

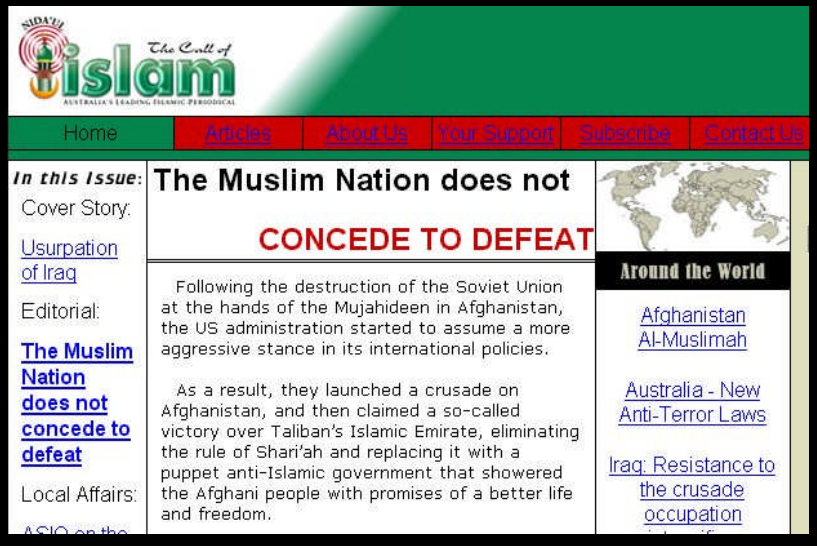
How can we participate?

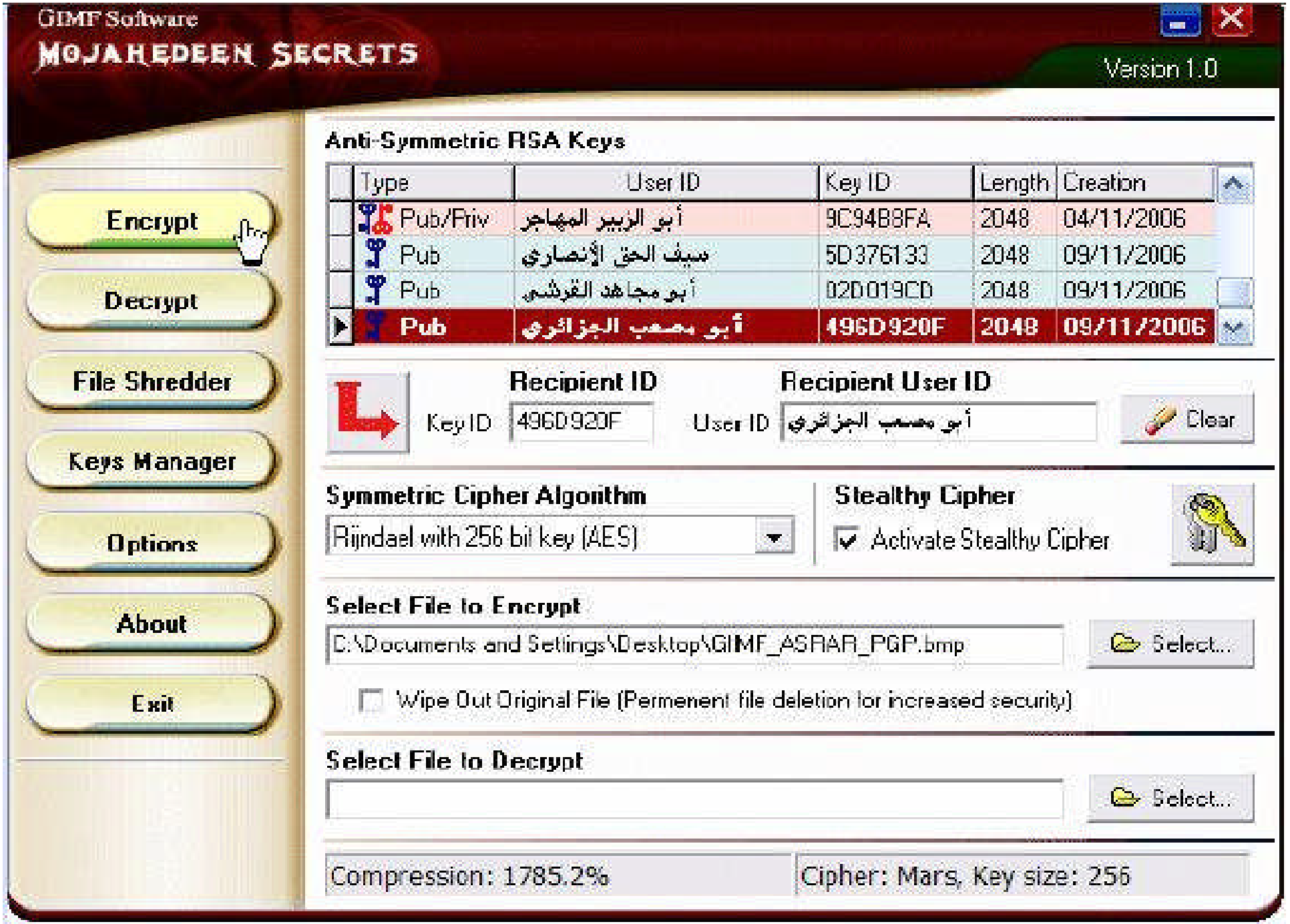
Very simple, just believe that you are a cyber soldier to defend your religion, to defend your faith, to defend your HOLY TEACHINGS OF HOLY QURA'AN AND SUNNAH, and you will **MUJAHID** " the very next moment.

After all , it is very inexpensive and time convenient and we dont have to go anywhere and not to spent anything. all we need is a PC connected to internet and it is available in nearly getting this message because you have already access to computer and internet .

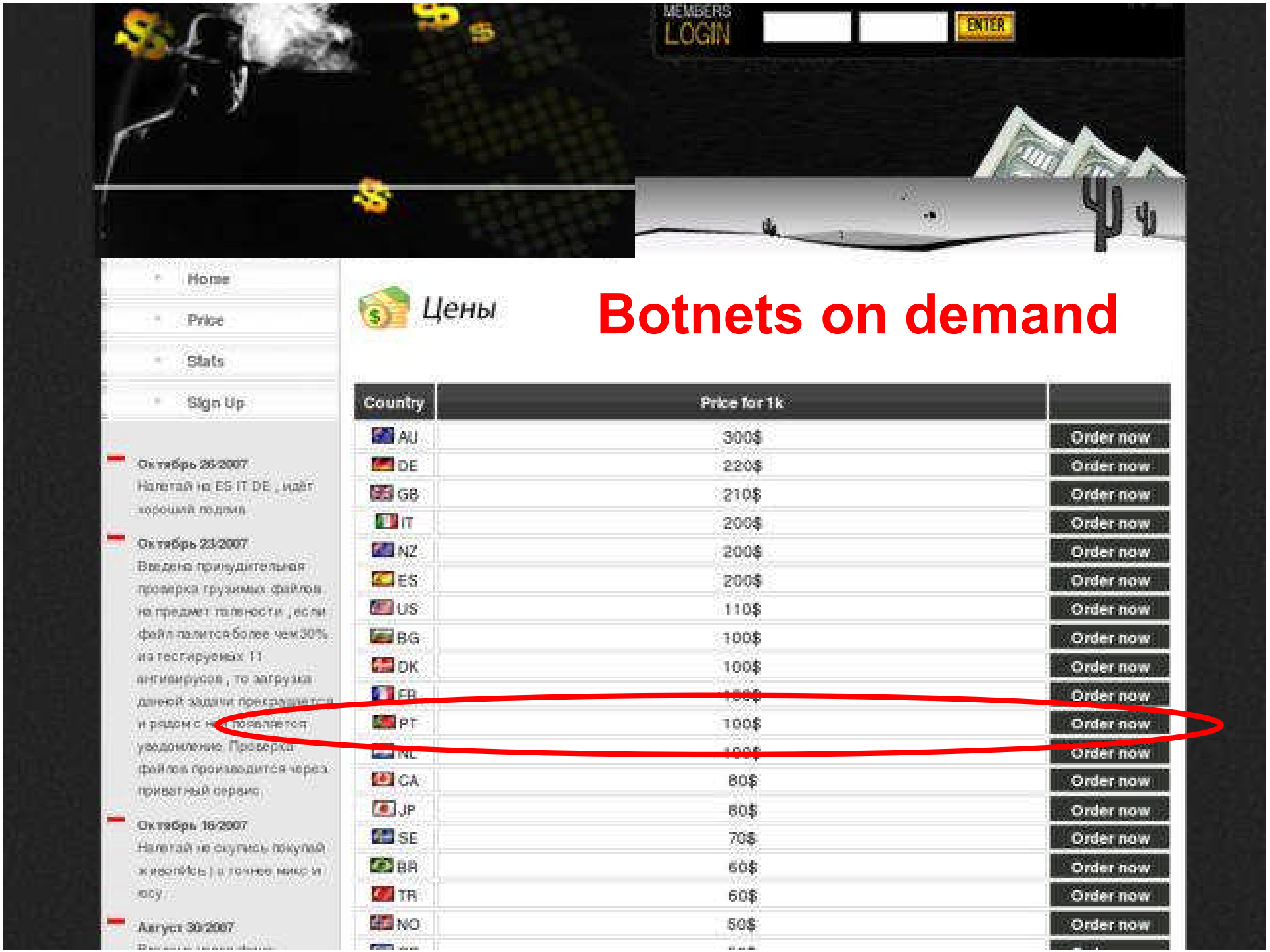
REMEMBER, you dont have to do any extra arrangements for "E - JIHAD " , it has no cost but it gives piles of sweet fruit of success in this life as well as life after death

MANUAIS DE CIBER - GUERRA





رسم 1: الواجهة الرئيسية لبرنامج أسرار المجاهدين من إنتاج سرية الأمن التقني في الجبهة الإعلامية الإسلامية العالمية


MEMBERS
LOGIN
ENTER
Home
Price
Stats
Sign Up
Цены
Botnets on demand
Country
Price for 1k
AU 300$ Order now
DE 220$ Order now
GB 210$ Order now
IT 200$ Order now
NZ 200$ Order now
ES 200$ Order now
US 110$ Order now
BG 100$ Order now
DK 100$ Order now
PT 100$ Order now
CA 80$ Order now
JP 80$ Order now
SE 70$ Order now
BR 60$ Order now
TR 60$ Order now
NO 50$ Order now
Октябрь 26/2007
Октябрь 23/2007
Октябрь 16/2007
Август 30/2007

Irhabi007 pode estar desconectado da internet, mas outros continuam ligados. Entre os mais engenhosos está uma pessoa que navega pela rede com o nome – é verdade – de Irhabi11

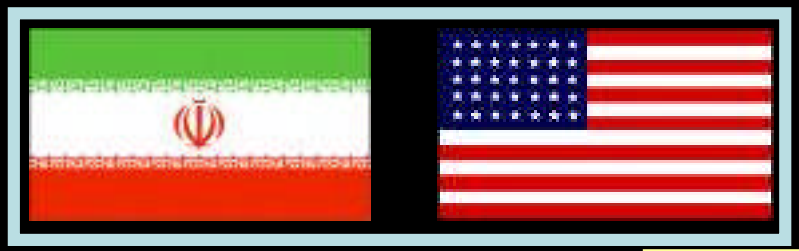
A Unidade 121 – Ciber-Guerra Coreia do Norte

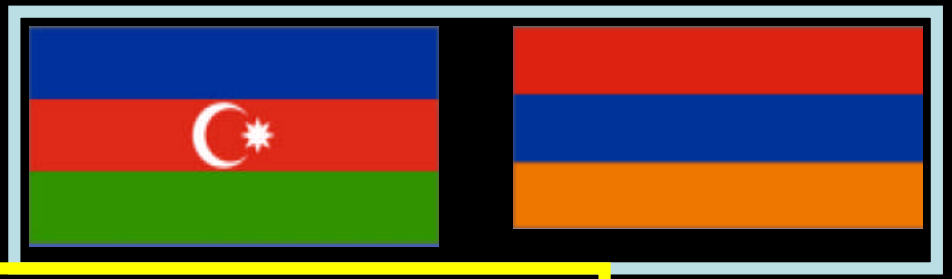
- **A Coreia do Norte tem operado uma unidade de Ciber-guerra tentando infiltrar-se na rede de comunicações da Coreia do Sul. Esta unidade está operacional desde 1998 e está localizada na região montanhosa de Hyungsan.**

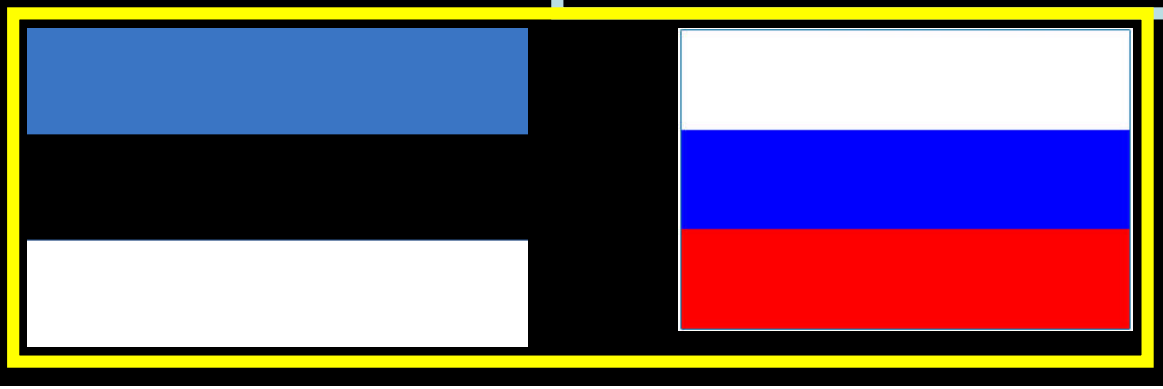
Guerra do Golfo

Durante a Guerra do Golfo em 1991, “hackers” holandeses obtiveram informação, através dos computadores do Departamento de Defesa dos USA, sobre os movimentos das tropas dos USA e tentaram vender essa informação ao Iraque. Estes pensaram tratar-se de uma operação de despistagem

Alguns ciber-conflitos







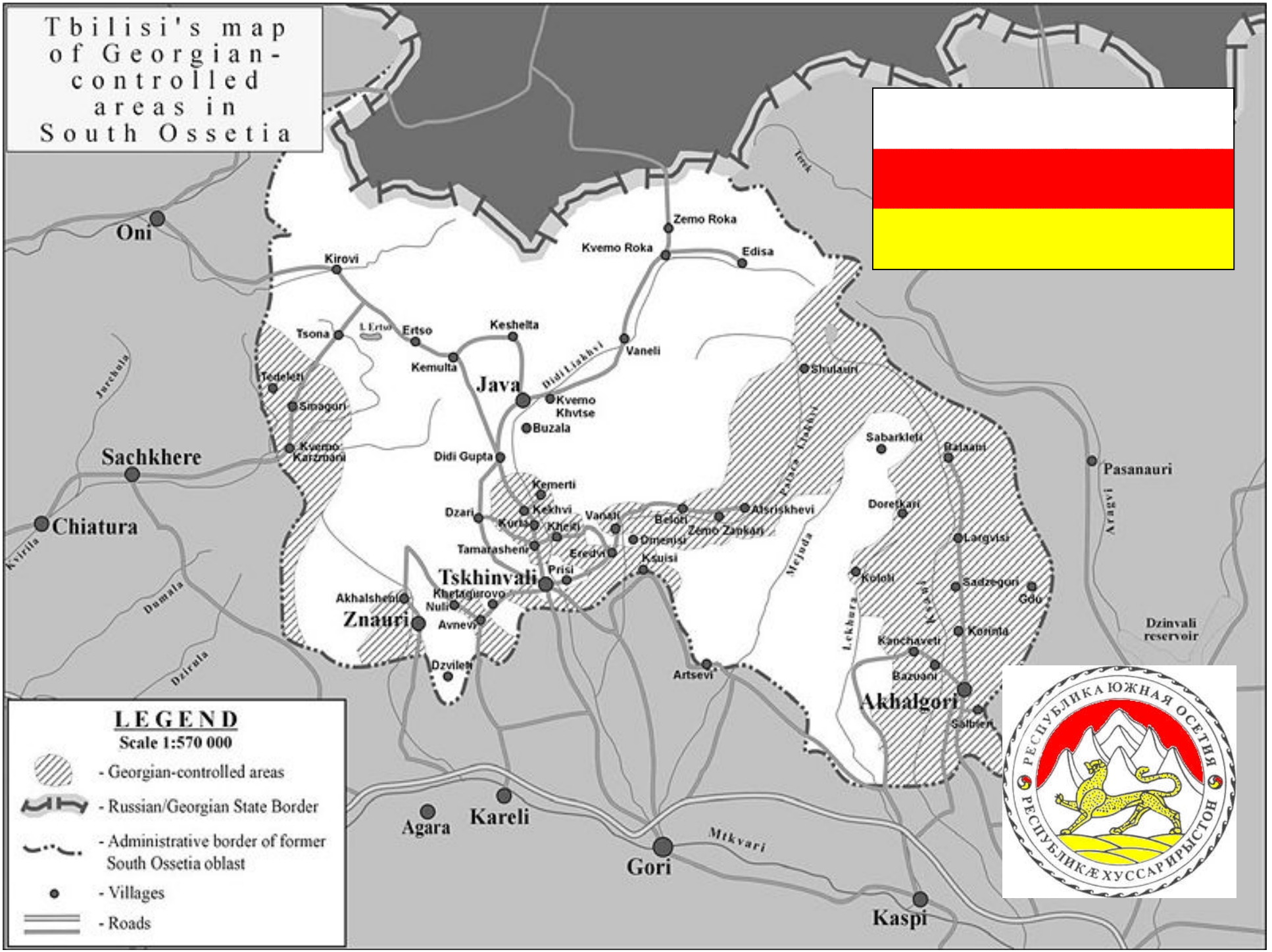
Site: www9.50megs.com/gforce/mirror.htm
Members: sniper, heataz, Rsnake, instinct, miller, rave, nicks xtremist

Turkish Hacktivists

Ataque à Lituânia

JULHO 2008

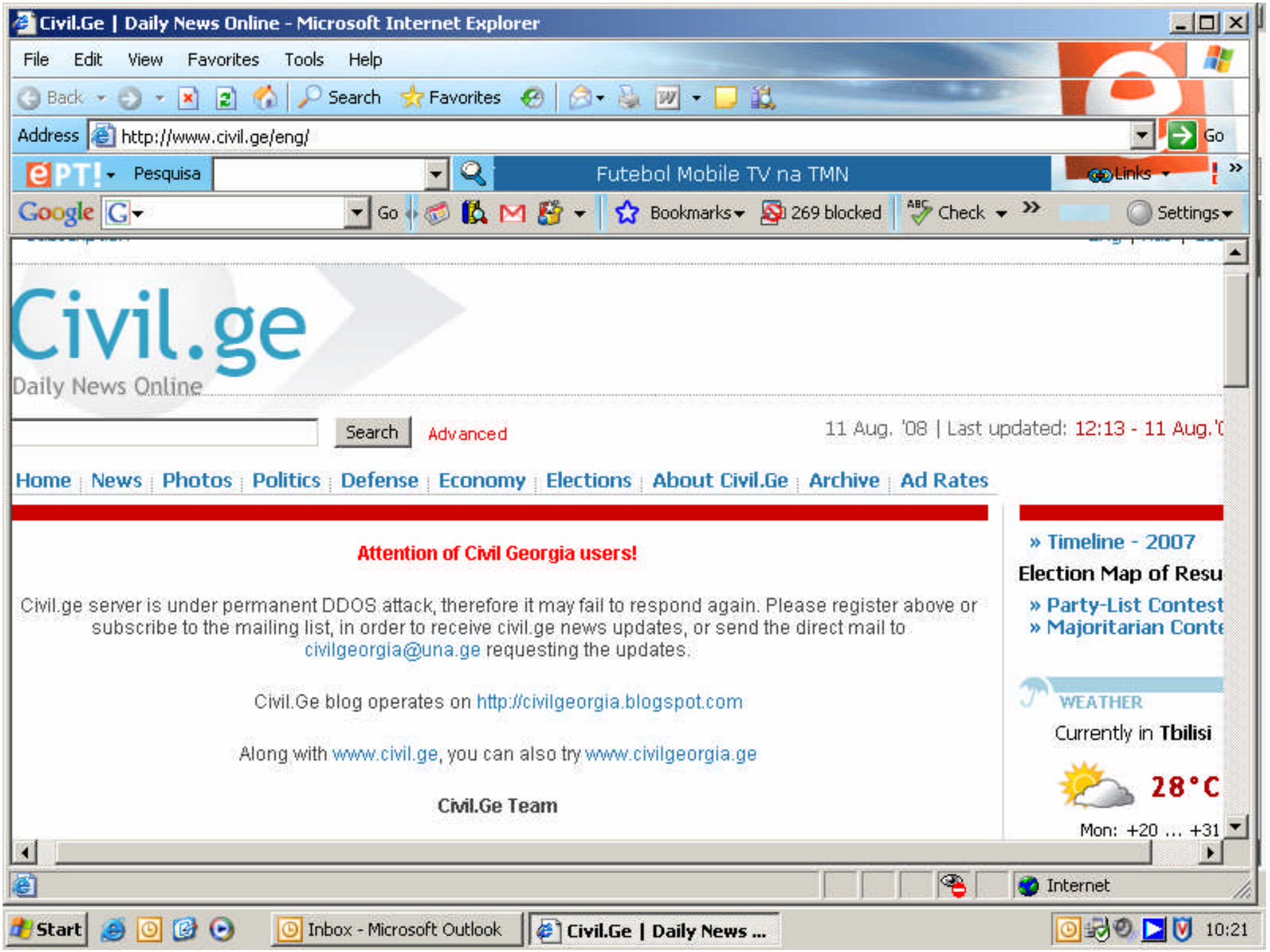
- **Hackers atacaram mais de 300 sites do governo da Lituânia. Os 300 sites eram todos do mesmo ISP. O ataque teve início numa Sexta-Feira e só na Segunda-Feira alguns sites foram restaurados.**
- **Hackers invadiram centenas de páginas do governo da Lituânia num ataque coordenado lançado a partir de um lugar não identificado no exterior do país. Os invasores publicaram símbolos soviéticos numa ampla gama de páginas, desde a da Comissão de Valores Mobiliários à do Partido Social Democrata.**
- **O ataque veio na sequência de uma decisão legislativa da Lituânia banindo os simbolos comunistas espalhados pelo país e coincidiu com a visita do PM da Lituânia aos Estados Unidos.**

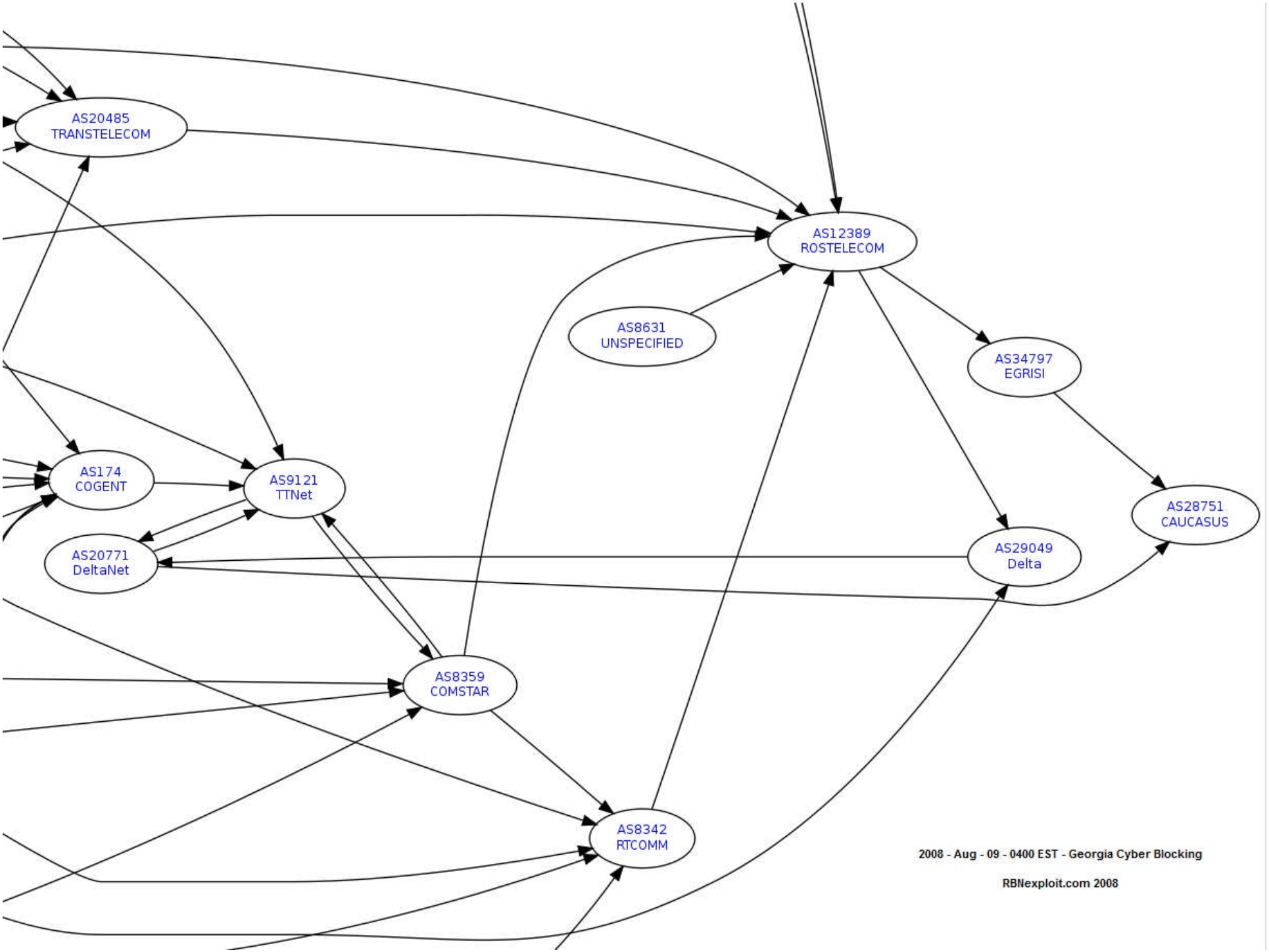

Tbilisi's map of Georgian-controlled areas in South Ossetia
Oni
Kirovi
Zemo Roka
Kvemo Roka
Edisa
Tsona
Ertso
Keshelta
Kemulta
Java
Didi Liakhvi
Vaneli
Shulauri
Tedeleti
Simagori
Kvemo Khvtse
Buzala
Jurcbula
Sachkhere
Kvemo Karzmani
Didi Gupta
Patsa Liakhvi
Sabarkleti
Bajaani
Pasanauri
Kemerti
Chiatura
Dzari
Kekhvi
Kurta
Kheiti
Varsati
Beloti
Zemo Zankari
Alsrishkevi
Dimenisi
Doretkari
Largvisi
Kvirila
Tamarasheni
Eredvi
Ksuisi
Tskhinvali
Prisi
Mejuda
Aragvi
Dumala
Akhalsheni
Khetagurovo
Nuli
Znauri
Avnevi
Koloti
Sadzegori
Gdo
Dzinvali reservoir
Dzirula
Dzvileti
Artsevi
Lekhura
Kornisi
Kanchaveti
Bazuani
Akhalgori
Salbieri
Agara
Kareli
Mtkvari
Gori
Kaspi
LEGEND
Scale 1:570 000
- Georgian-controlled areas
- Russian/Georgian State Border
- Administrative border of former South Ossetia oblast
- Villages
- Roads
РЕСПУБЛИКА ЮЖНАЯ ОСЕТИЯ
РЕСПУБЛИКÆ ХУССАРИРЫСТОН

Guerra na Ossétia do Sul

AGOSTO 2008

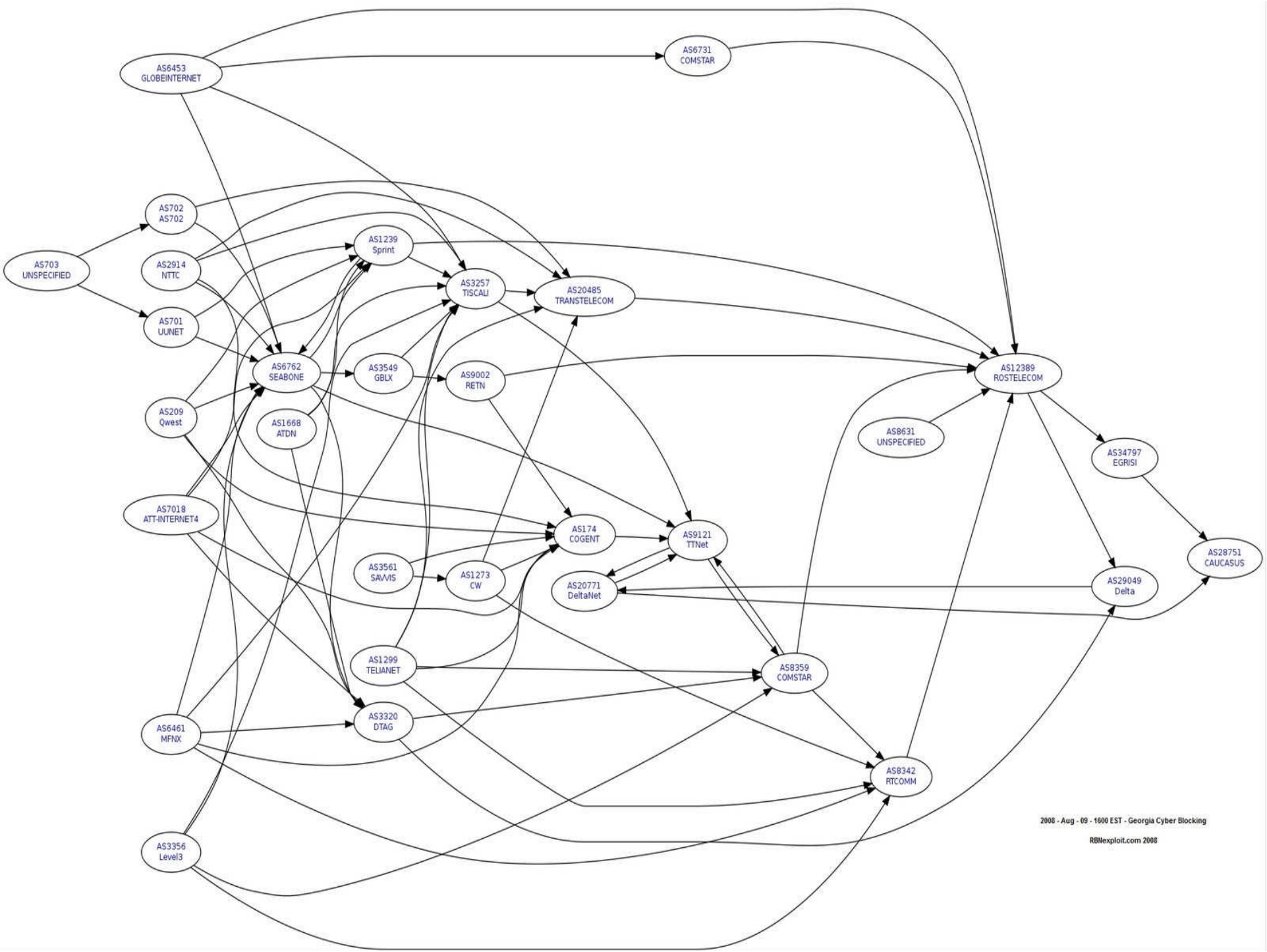
- **Desde que a guerra teve início, as redes, *sites* e infra-estruturas de comunicações georgianas têm sido atacadas insistentemente por piratas ou especialistas alegadamente russos. Vários sites do Governo da Geórgia ficaram inperativos e têm sido forçados a permanecer offline devido a ataques provocados por supostos hackers russos**
- **O website do presidente da Geórgia, ficou inoperativo depois de ataques DDOS. O comando e controle do servidor que realizou o ataque localiza-se nos Estados Unidos e entrou para a rede poucas semanas antes do conflito.**
- **Dois sites, president.gov.ge e rustavi2.com, o site de uma proeminente emissora de TV georgiana, foram transferidos para Atlanta (empresa Tulip Systems Inc). Peritos de segurança de computadores disseram que apesar disso esses sites de notícias novamente foram atacados.**
- **Os «hackers» trabalharam de forma coordenada nos ataques ao Governo da Geórgia, aos média, aos bancos e aos transportes. Os ataques online passavam pela sobrecarga dos sistemas com milhares de pedidos.**
- **A rede Caucasus Network Tbilisi – que contem os servidores comerciais da Internet na Georgia ficou, por longo tempo, debaixo de um ataque realizado por milhares de Computadores comprometidos (botnet)**


Civil.Ge | Daily News Online - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.civil.ge/eng/
Go
Pesquisa
Futebol Mobile TV na TMN
Links
Google
Go
Bookmarks
269 blocked
Check
Settings
Civil.ge
Daily News Online
Search
Advanced
11 Aug. '08 | Last updated: 12:13 - 11 Aug.
Home News Photos Politics Defense Economy Elections About Civil.Ge Archive Ad Rates
Attention of Civil Georgia users!
Civil.ge server is under permanent DDOS attack, therefore it may fail to respond again. Please register above or subscribe to the mailing list, in order to receive civil.ge news updates, or send the direct mail to civilgeorgia@una.ge requesting the updates.
Civil.Ge blog operates on http://civilgeorgia.blogspot.com
Along with www.civil.ge, you can also try www.civilgeorgia.ge
Civil.Ge Team
» Timeline - 2007
Election Map of Resu
» Party-List Contest
» Majoritarian Conte
WEATHER
Currently in Tbilisi
28°C
Mon: +20 ... +31
Internet
Start
Inbox - Microsoft Outlook
Civil.Ge | Daily News ...
10:21


AS20485
TRANSTELECOM
AS12389
ROSTELECOM
AS8631
UNSPECIFIED
AS34797
EGRISI
AS174
COGENT
AS9121
TTNet
AS28751
CAUCASUS
AS20771
DeltaNet
AS29049
Delta
AS8359
COMSTAR
AS8342
RTCOMM
2008 - Aug - 09 - 0400 EST - Georgia Cyber Blocking
RBNexploit.com 2008

ping: president.gov.ge

location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	50.7	51.6	52.2
New York, U.S.A.	Okay	29.5	30.6	31.6
Stockholm, Sweden	Okay	123.3	125.4	130.3
Copenhagen, Denmark	Okay	109.4	109.8	110.6
Austin1, U.S.A.	Okay	56.9	60.5	63.8
Amsterdam2, Netherlands	Okay	107.0	109.2	128.6
Paris, France	Okay	102.1	102.3	102.4
Madrid, Spain	Okay	126.7	129.3	147.4
Amsterdam, Netherlands	Okay	98.1	105.4	140.3
Munchen, Germany	Okay	117.5	118.3	120.0
Hong Kong, China	Okay	254.0	256.8	279.4
Vancouver, Canada	Okay	79.3	84.9	132.9
Zurich, Switzerland	Okay	119.5	126.4	178.7
Austin, U.S.A.	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Shanghai, China	Okay	265.9	266.2	266.6
Sydney, Australia	Packets lost (100%)			
Melbourne, Australia	Packets lost (100%)			
Singapore, Singapore	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			


AS6453
GLOBEINTERNET
AS6731
COMSTAR
AS702
AS702
AS703
UNSPECIFIED
AS2914
NTTC
AS1239
Sprint
AS3257
TISCALI
AS20485
TRANSTELECOM
AS701
UUNET
AS6762
SEABONE
AS3549
GBLX
AS9002
RETN
AS12389
ROSTELECOM
AS209
Qwest
AS1668
ATDN
AS8631
UNSPECIFIED
AS34797
EGRISI
AS7018
ATT-INTERNET4
AS174
COGENT
AS9121
TTNet
AS28751
CAUCASUS
AS3561
SAVVIS
AS1273
CW
AS20771
DeltaNet
AS29049
Delta
AS1299
TELIANET
AS8359
COMSTAR
AS6461
MFNX
AS3320
DTAG
AS8342
RTCOMM
AS3356
Level3
2008 - Aug - 09 - 1600 EST - Georgia Cyber Blocking
RBNexploit.com 2008

ping: mfa.gov.ge

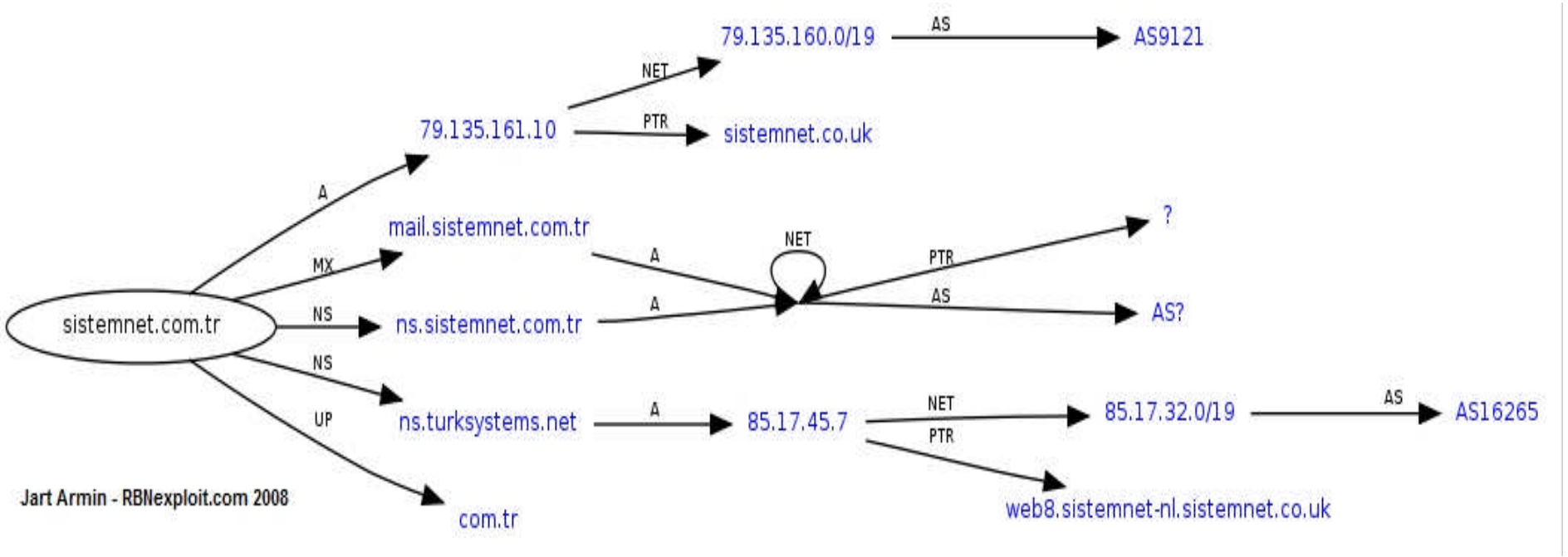
location	result	min. rrt	avg. rrt	max. rrt
Florida, U.S.A.	Okay	59.4	59.9	60.5
Amsterdam, Netherlands	Okay	149.3	164.6	275.4
Melbourne, Australia	Okay	173.8	174.5	175.0
Singapore, Singapore	Okay	208.5	214.0	238.6
New York, U.S.A.	Packets lost (100%)			
Amsterdam2, Netherlands	Packets lost (100%)			
Austinl, U.S.A.	Packets lost (100%)			
London, United Kingdom	Packets lost (100%)			
Stockholm, Sweden	Packets lost (100%)			
Cologne, Germany	Packets lost (100%)			
Chicago, U.S.A.	Packets lost (100%)			
Austin, U.S.A.	Packets lost (100%)			
Amsterdam3, Netherlands	Packets lost (100%)			
Krakow, Poland	Packets lost (100%)			
Paris, France	Packets lost (100%)			
Copenhagen, Denmark	Packets lost (100%)			
San Francisco, U.S.A.	Packets lost (100%)			
Vancouver, Canada	Packets lost (100%)			
Madrid, Spain	Packets lost (100%)			
Shanghai, China	Packets lost (100%)			
Lille, France	Packets lost (100%)			
Zurich, Switzerland	Packets lost (100%)			
Munchen, Germany	Packets lost (100%)			
Cagliari, Italy	Packets lost (100%)			
Hong Kong, China	Packets lost (100%)			
Johannesburg, South Africa	Packets lost (100%)			
Porto Alegre, Brazil	Packets lost (100%)			
Sydney, Australia	Packets lost (100%)			
Mumbai, India	Packets lost (100%)			
Santa Clara, U.S.A.	Packets lost (100%)			

- **O indivíduo com directa responsabilidade em conduzirem os ataques cibernéticos à Georgia foi operativos da RBN (Russian Business Network) identificados como Alexandr A. Boykov de St Petersburg, Russia. Envolvidos nos ataques esteve também um programador e spammer de St Petersburg chamado Andrew Smirnov.**

- **Mr. Boykov é conhecido por estar envolvido em actividades criminais desde há longo tempo. Ele é conhecido por distribuir o malware VirusIsolator (que provoca o download de Trojans que tomam o controlo do computador das vitimas). Ele está igualmente envolvido em fraudes financeira operando sites para "vigarices" incluindo: Harbor Lending, Oakwood Lending, e Capital Lending. Mr Boykov é igualmente um distribuir de spam de caracter porno.**

- **Mr. Smirnov é conhecido por operar um diverso numero de sites dedicados a vigarices incluindo canadian-pharmacy-support e canadiandiscountmeds. Mr. Smirnov é conhecido pelas suas ideias nacionalistas sobre a Russia e suporta as ideias de cortar o abastecimento de gás à Ucrania.**

- **Mr. Boykov operata um serviço de host na Class C Network 79.135.167.0/24. Deve ser notado que os ataques pré-invasão foram emanados de 79.135.167.22. Nas semanas a seguir à invasão existiu uma grande campanha de spam, supostamente com notícias originadas na BBC, acusando o Presidente da Georgia de ser “gay”. Quando alguem carrega no link do email um virus é download a partir de 79.135.167.49. (Sistemnet Telecom - AS9121 TTNet (Turkey) associada com AbdAllah_Internet)**



Sistemnet Telecom - AS9121 TTNet (Turkey) associada com AbdAllah_Internet

Título em Jornal

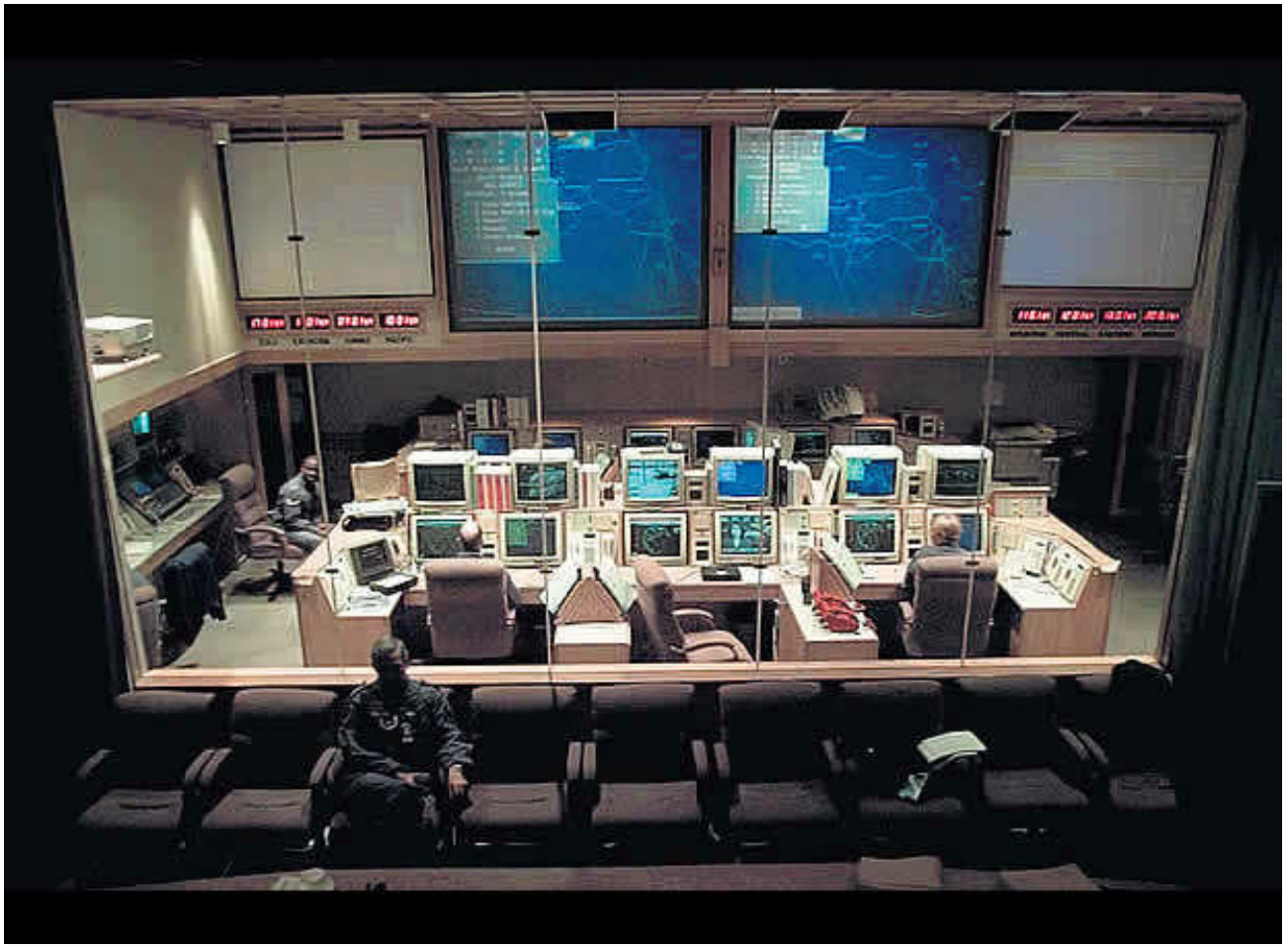
Militares Georgianos observam avanço das tropas russas

Título em Jornal

NATO exige retirada das tropas Russas

ou

Os cães ladram e a caravana passa



Mando de Defensa Aeroespacial en Colorado

Terrorist use of GPS and SATCOM, Internet financial transactions by adversaries, radar and navigational jamming, and attacking American servers are just a few examples of operations that involve cyberspace.

Em 12 Agosto 2008 os 8000 que compõem a força do Cyber Comand receberam ordens para parar toda a actividade.

Outros Casos...

- Fevereiro 2007 200000 registos médicos foram “roubados” da base de dados dos Anthem Blue Cross e Blue Shield no UK.
- No mesmo período o Johns Hopkins University Hospital informou que os registos de mais de 80000 doentes timham sido “roubados”.
- Ainda no mesmo período a empresa americana WellPoint informou que os registos de maiss de 196000 doentes tinham sido ilegalmente copiados.
- De acordo com os média os registos continham informação detalhadas sobre os doentes e os seus registos médicos.
- Porquê??
- ……...
- ……...
- Cenário ENISA

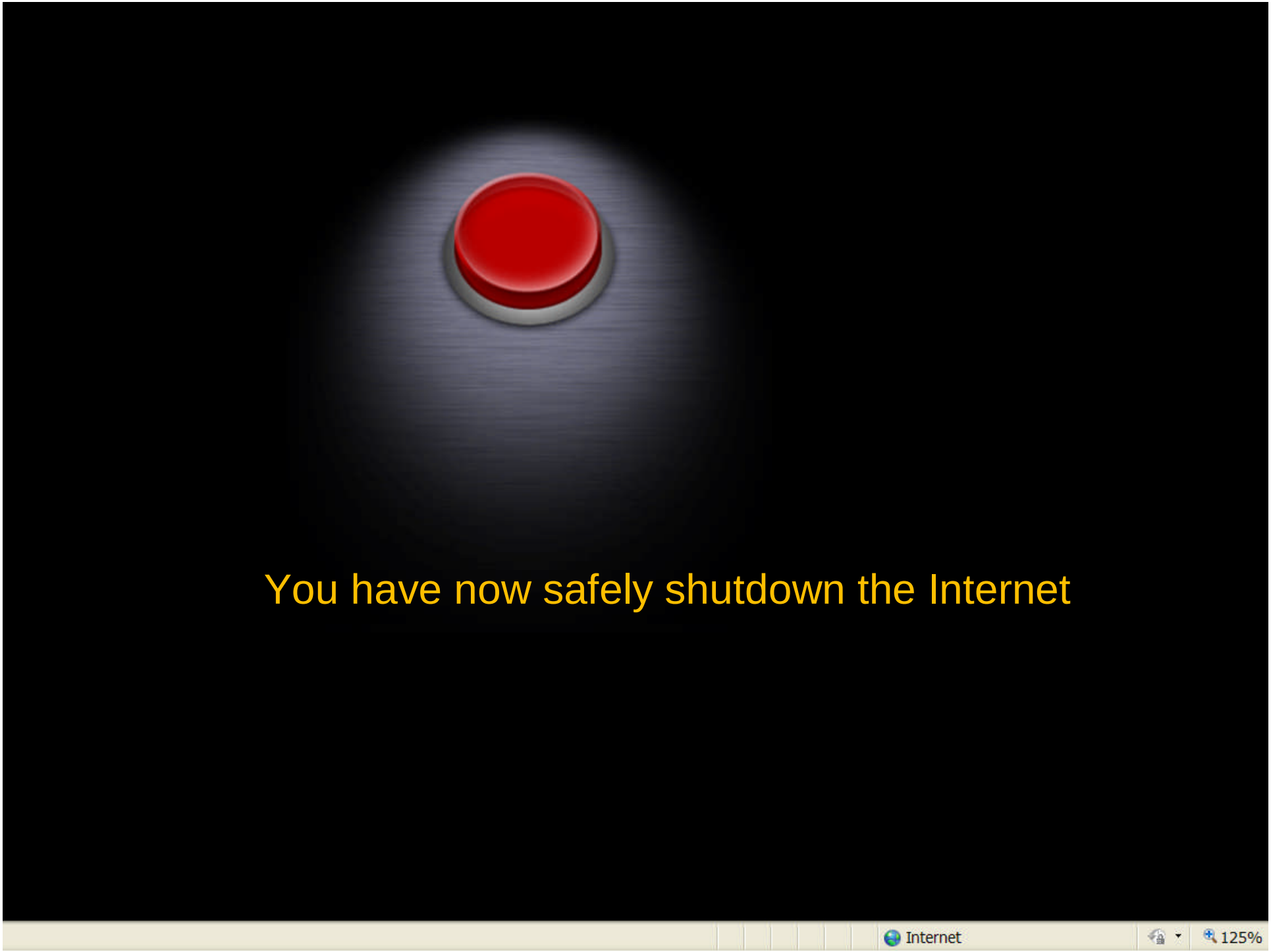
Egyptian Internet blackout

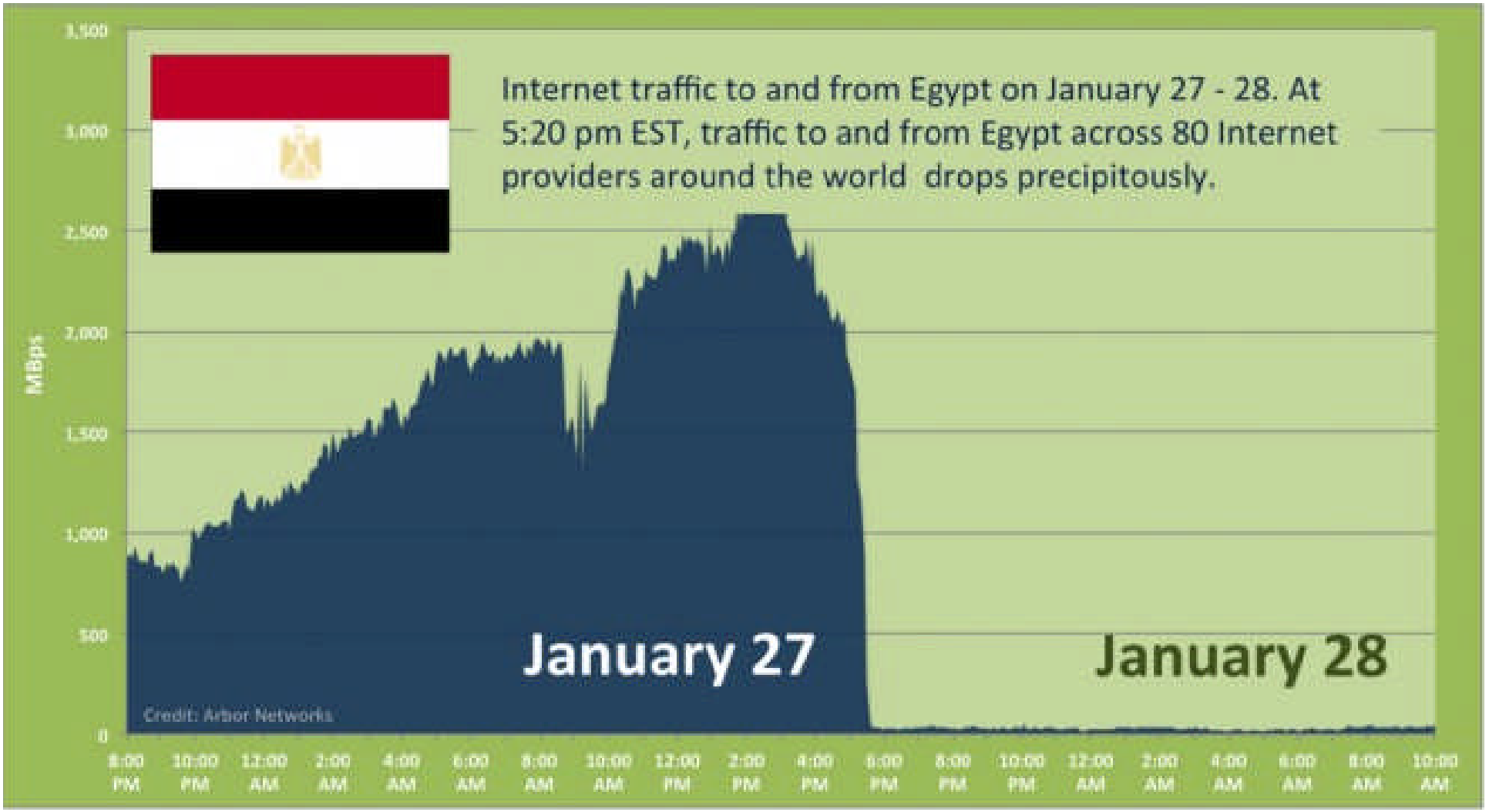
- On January 2011, The Egyptian government ordered service providers to shut down all international connections to the Internet.
- This was faced as an attempt to prevent the protests from gaining momentum by censoring social networking Web sites. This behavior isn't new or extraordinary; repressive regimes have long resorted to Internet censorship to protect their positions. Egypt took a much more extreme step.
- However, Critical European-Asian fiber-optic routes through Egypt appear to be unaffected for now. The majority of Internet connectivity between Europe and Asia actually passes through Egypt. The Gulf states, in particular, depend critically on the Egyptian fiberoptic corridor for their connectivity to world markets.
- But every Egyptian provider, every business, bank, Internet cafe, website, school, Embassy, and Government office that relied on the big four Egyptian ISPs for their Internet connectivity was cut off from the rest of the world. Link Egypt, Vodafone/Raya, Telecom Egypt, Etisalat Misr, and all their customers and partners are, for the moment, off the air.

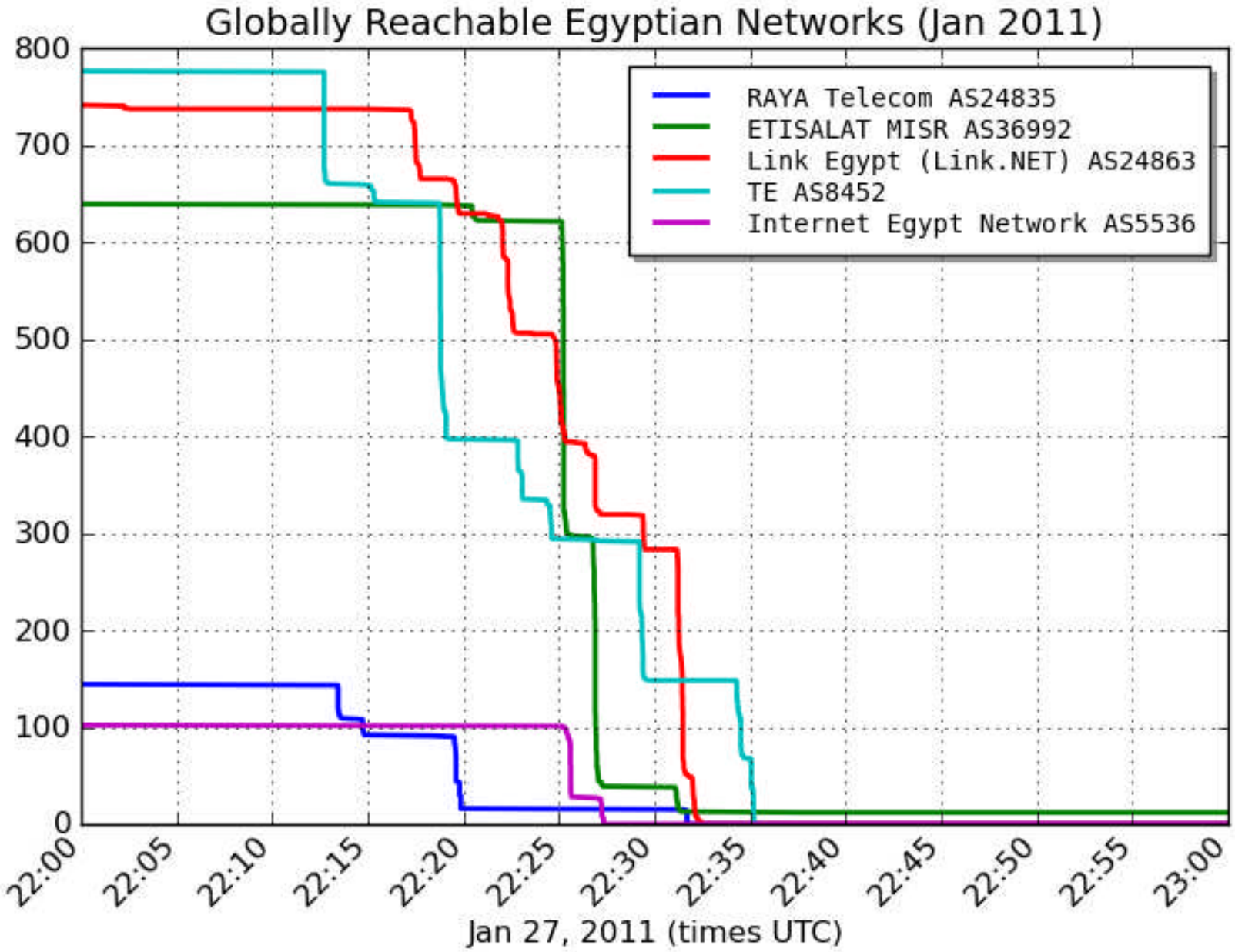
O Apagão da Internet no Egipto

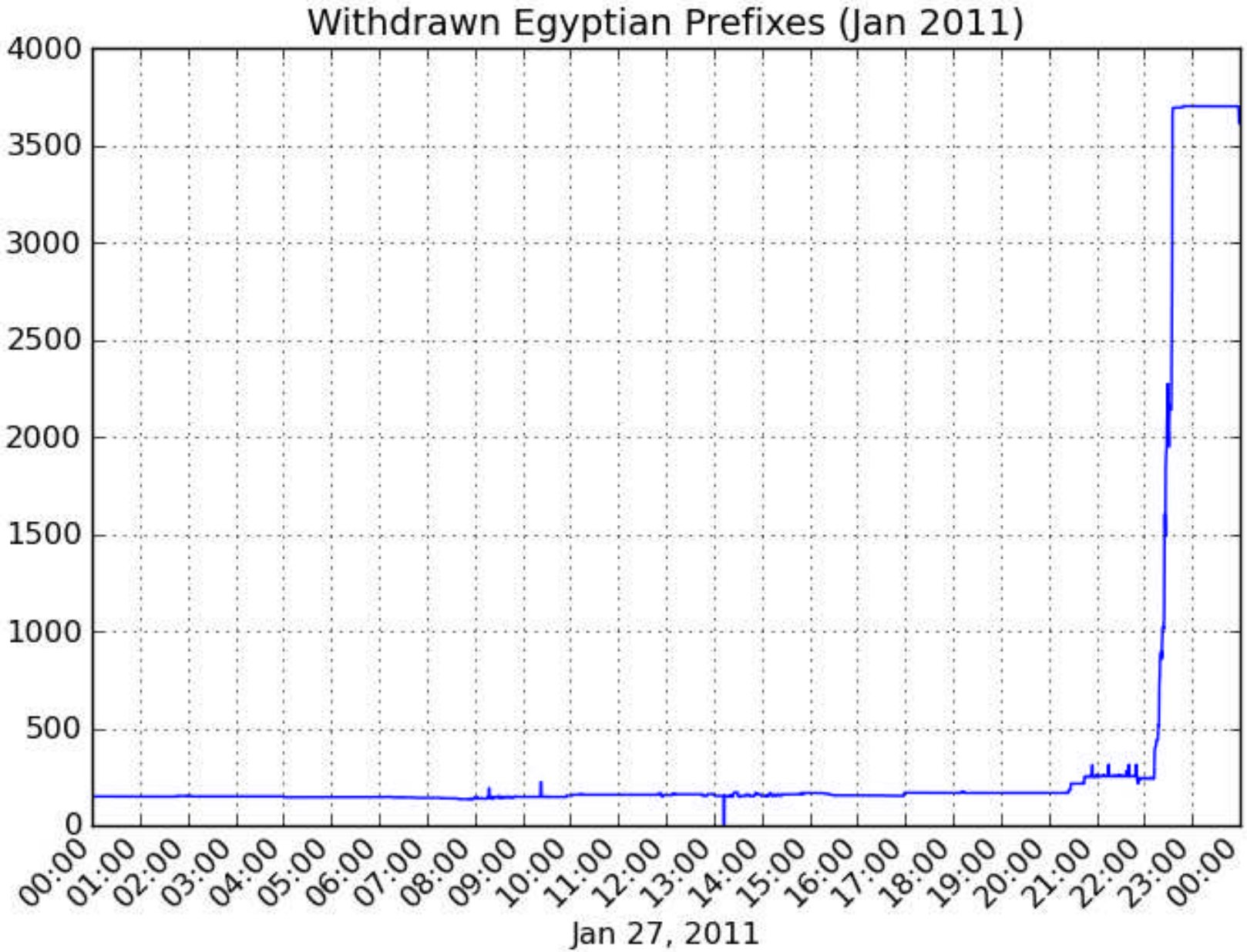
- Em Janeiro 2011, O governo do Egipto ordenou a diversos ISP para fecharem as suas ligações Internacionais da Internet.
- Este movimento foi encarado como uma tentativa para evitar os protestos que na altura se registavam nas diferentes cidades do Egipto. Deste modo a actividade das redes sociais era bloqueada. Com esta medida os egipcíos ficavam com dificuldade em coordenar novos protestos e enviar para o resto do mundo imagens da repressão a que estavam a ser sujeitos.
- Contudo a infra-estructura crítica de sistemas de fibra optica não foi afectada. De notar que a maioria das ligações enter a Europa e a Asia usa estes sistemas de fibra optica. Os Estados do Golfo em particular dependem de modo critico destes corredores de fibra oprica.
- Mas todos os provedores de serviços do Egipto, todos os Bancos, Internet cafés, escolas, Embaixadas, e Departamentos Governamentais foram desligados do resto do mundo dado que estavam dependentes dos maiores 4 ISP do Egipto: Link Egypt, Vodafone/Raya, Telecom Egypt, Etisalat Misr, os quais ficaram “fora do ar”.

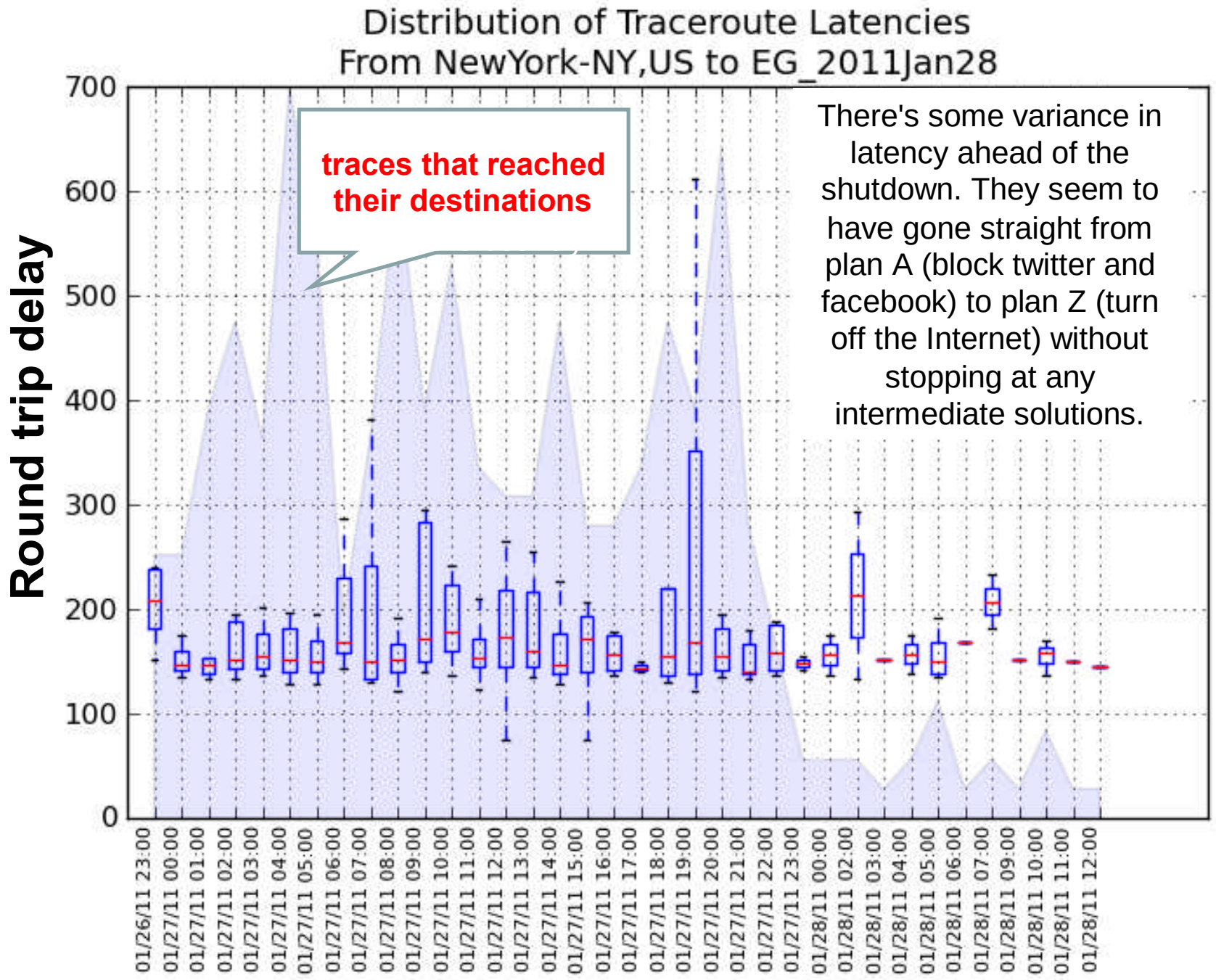

To stop
internet
press
firmly.

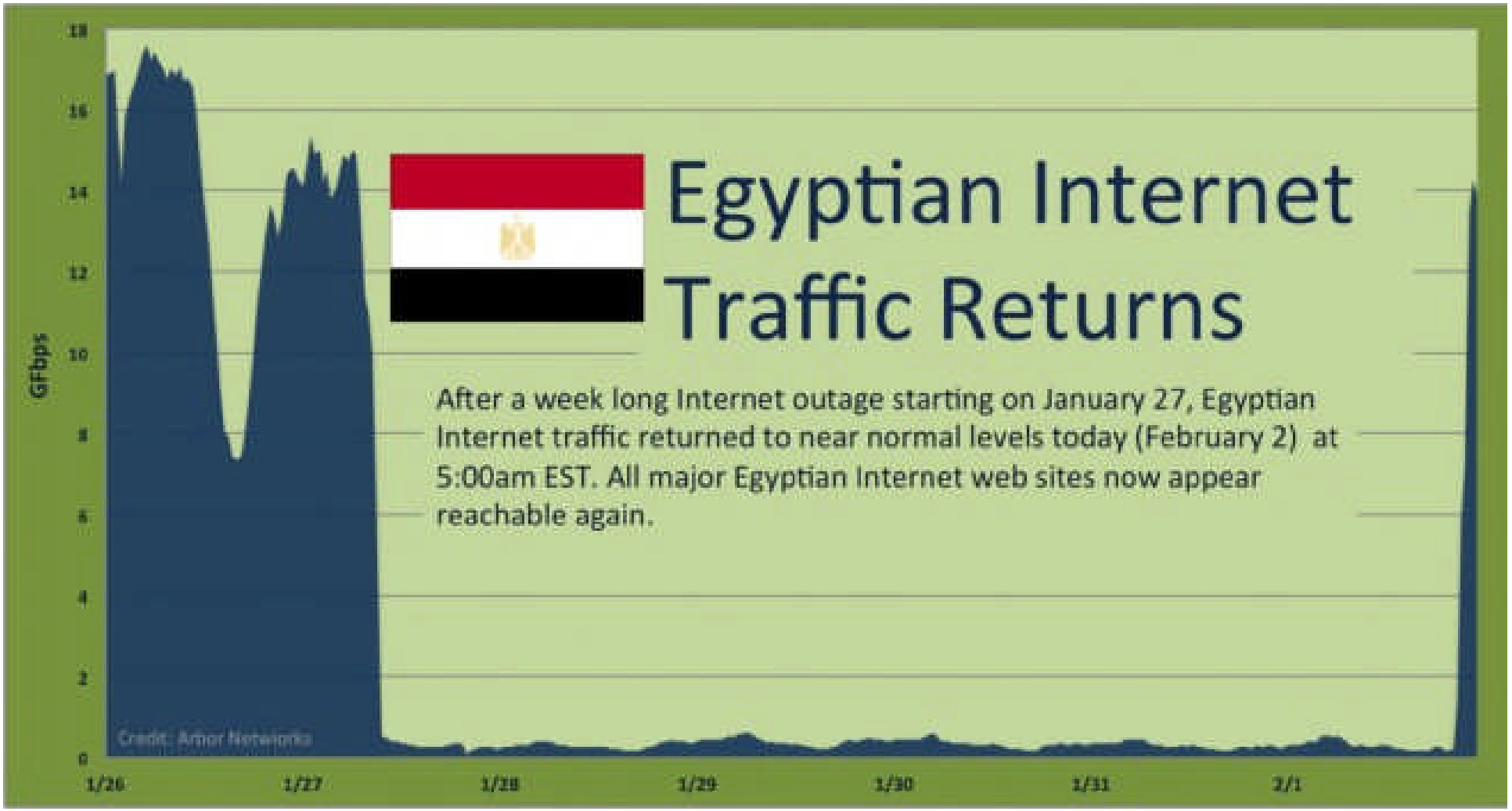

You have now safely shutdown the Internet
Internet
125%

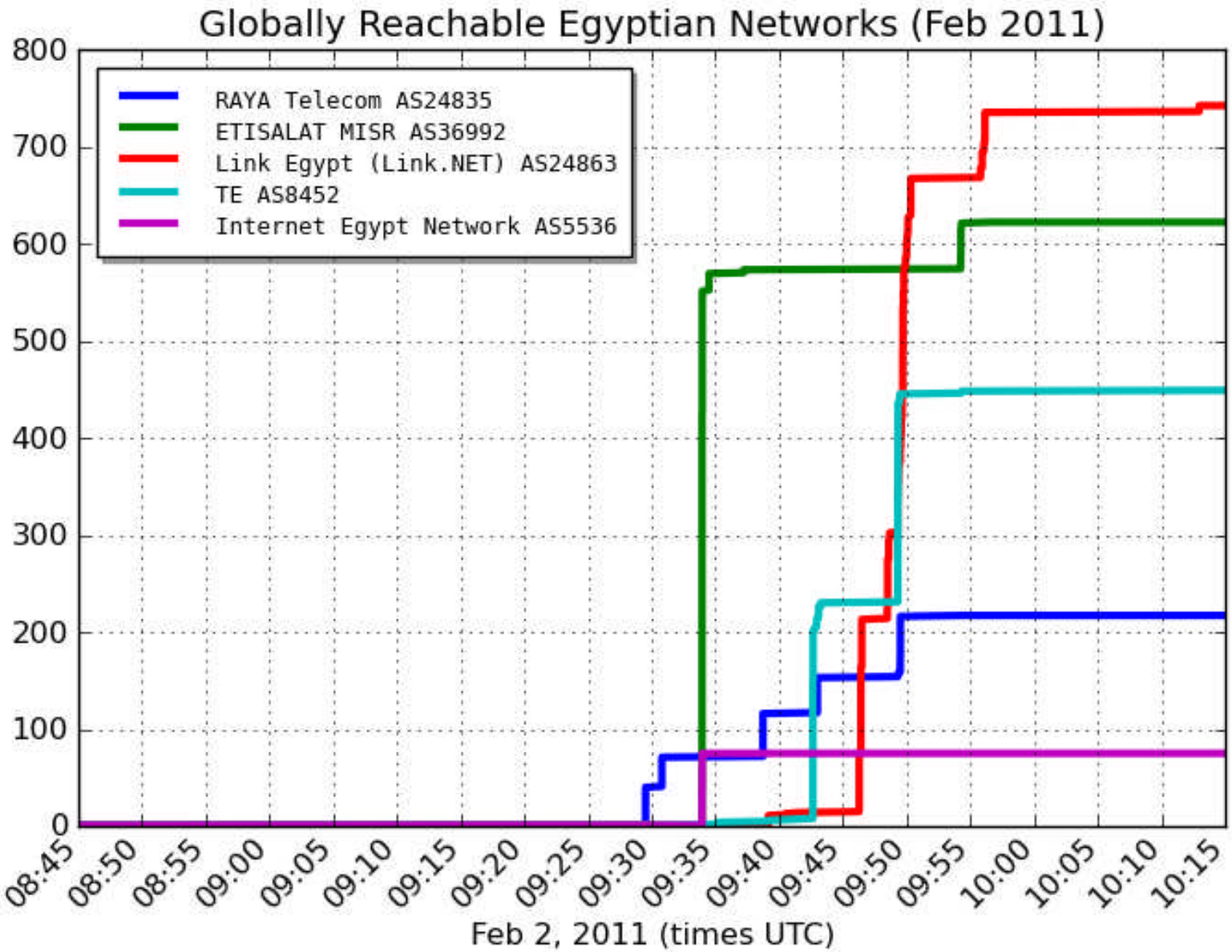

Internet traffic to and from Egypt on January 27 - 28. At 5:20 pm EST, traffic to and from Egypt across 80 Internet providers around the world drops precipitously.
MBps
3,500
3,000
2,500
2,000
1,500
1,000
500
0
January 27
January 28
Credit: Arbor Networks
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
8:00 PM
10:00 PM
12:00 AM
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM

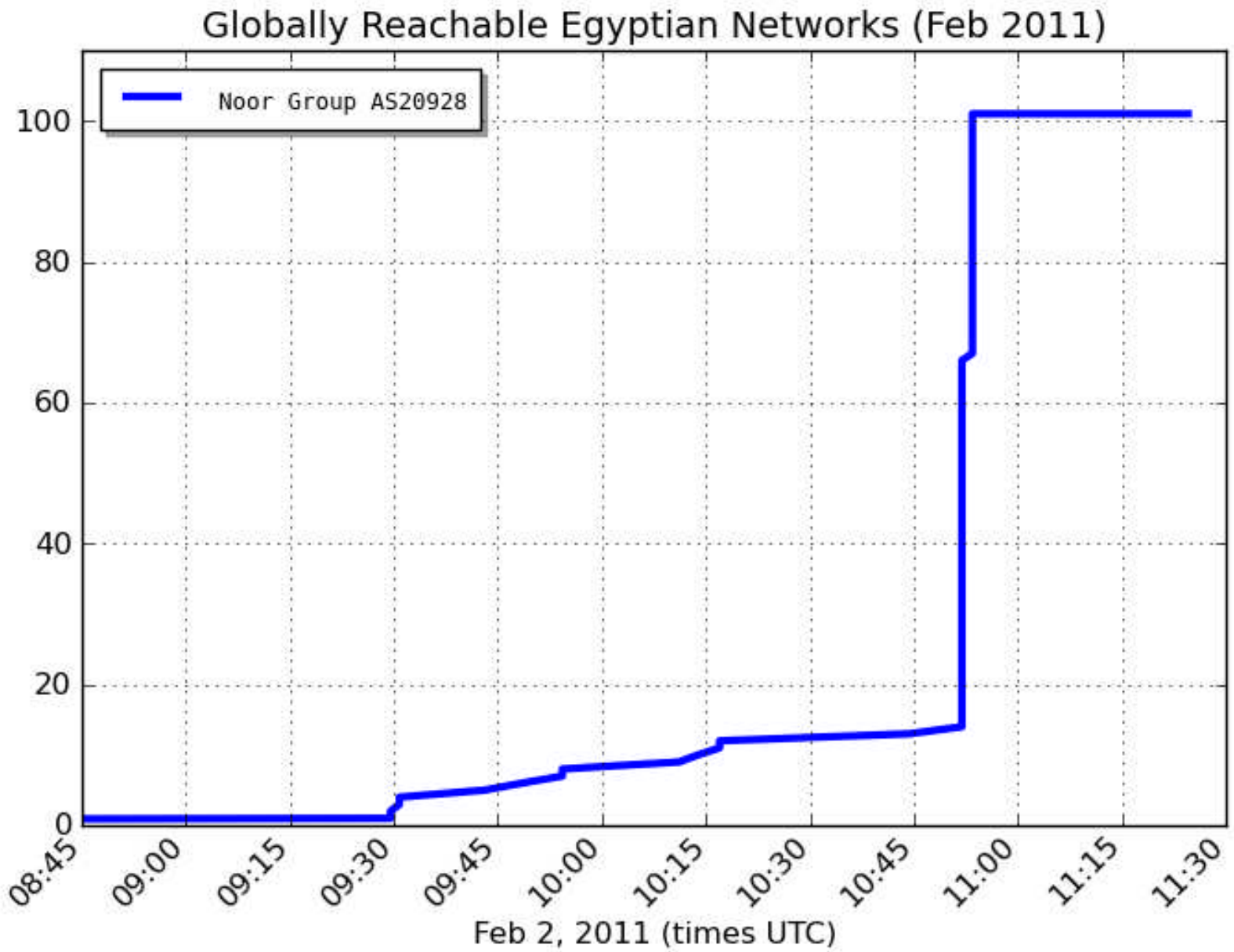

Globally Reachable Egyptian Networks (Jan 2011)
RAYA Telecom AS24835
ETISALAT MISR AS36992
Link Egypt (Link.NET) AS24863
TE AS8452
Internet Egypt Network AS5536
800
700
600
500
400
300
200
100
0
22:00
22:05
22:10
22:15
22:20
22:25
22:30
22:35
22:40
22:45
22:50
22:55
23:00
Jan 27, 2011 (times UTC)

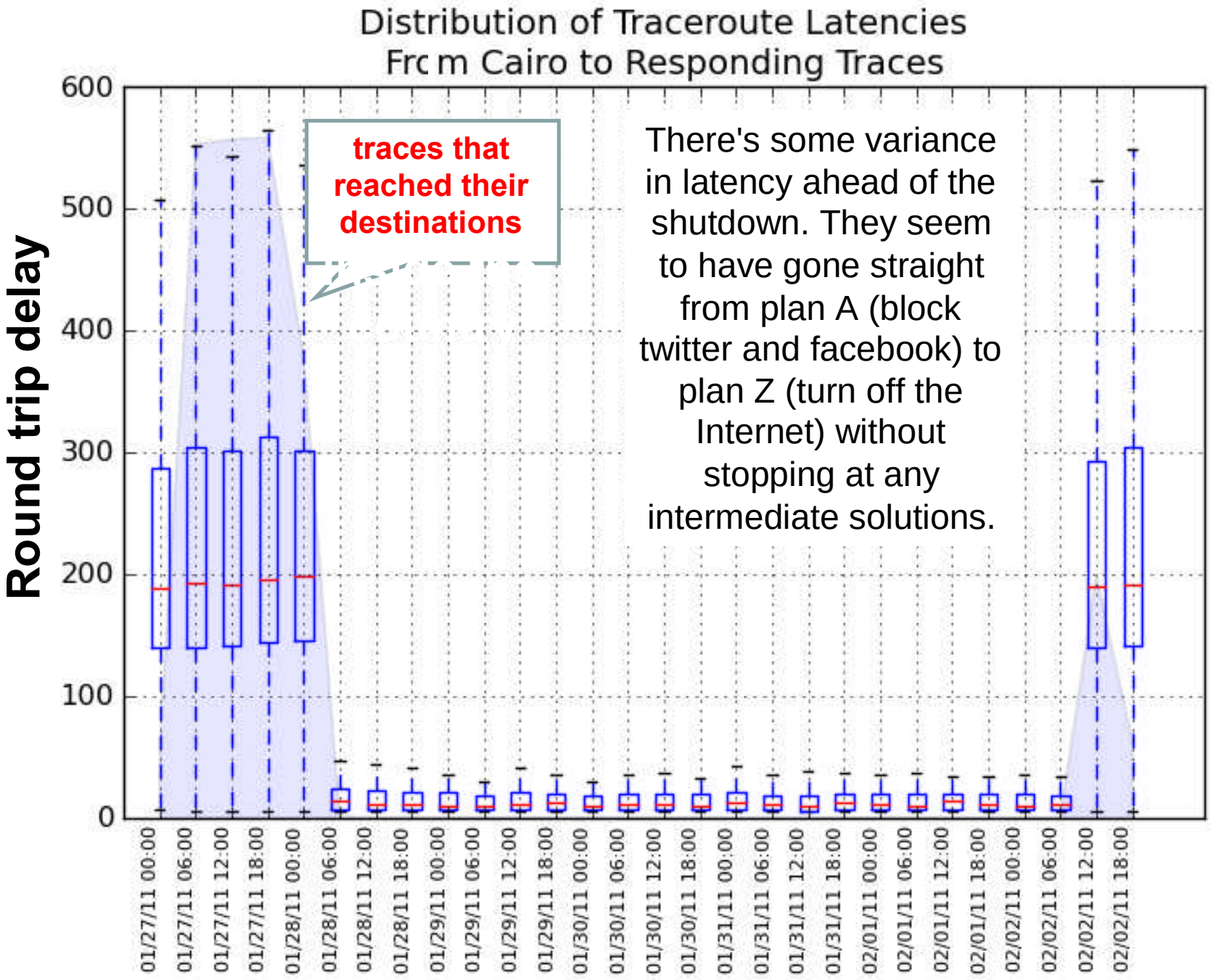

Withdrawn Egyptian Prefixes (Jan 2011)
4000
3500
3000
2500
2000
1500
1000
500
0
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
08:00
09:00
10:00
11:00
12:00
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00
00:00
Jan 27, 2011


Distribution of Traceroute Latencies
From NewYork-NY,US to EG_2011Jan28
Round trip delay
700
600
500
400
300
200
100
0
traces that reached their destinations
There's some variance in latency ahead of the shutdown. They seem to have gone straight from plan A (block twitter and facebook) to plan Z (turn off the Internet) without stopping at any intermediate solutions.
01/26/11 23:00
01/27/11 00:00
01/27/11 01:00
01/27/11 02:00
01/27/11 03:00
01/27/11 04:00
01/27/11 05:00
01/27/11 06:00
01/27/11 07:00
01/27/11 08:00
01/27/11 09:00
01/27/11 10:00
01/27/11 11:00
01/27/11 12:00
01/27/11 13:00
01/27/11 14:00
01/27/11 15:00
01/27/11 16:00
01/27/11 17:00
01/27/11 18:00
01/27/11 19:00
01/27/11 20:00
01/27/11 21:00
01/27/11 22:00
01/27/11 23:00
01/28/11 00:00
01/28/11 02:00
01/28/11 03:00
01/28/11 04:00
01/28/11 05:00
01/28/11 06:00
01/28/11 07:00
01/28/11 09:00
01/28/11 10:00
01/28/11 11:00
01/28/11 12:00


Egyptian Internet Traffic Returns
After a week long Internet outage starting on January 27, Egyptian Internet traffic returned to near normal levels today (February 2) at 5:00am EST. All major Egyptian Internet web sites now appear reachable again.
GFbps
18
16
14
12
10
8
6
4
2
0
1/26
1/27
1/28
1/29
1/30
1/31
2/1
Credit: Arbor Networks


Globally Reachable Egyptian Networks (Feb 2011)
RAYA Telecom AS24835
ETISALAT MISR AS36992
Link Egypt (Link.NET) AS24863
TE AS8452
Internet Egypt Network AS5536
800
700
600
500
400
300
200
100
0
08:45
08:50
08:55
09:00
09:05
09:10
09:15
09:20
09:25
09:30
09:35
09:40
09:45
09:50
09:55
10:00
10:05
10:10
10:15
Feb 2, 2011 (times UTC)


Globally Reachable Egyptian Networks (Feb 2011)
Noor Group AS20928
100
80
60
40
20
0
08:45
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
11:15
11:30
Feb 2, 2011 (times UTC)


Distribution of Traceroute Latencies
Frc m Cairo to Responding Traces
Round trip delay
600
500
400
300
200
100
0
traces that reached their destinations
There's some variance in latency ahead of the shutdown. They seem to have gone straight from plan A (block twitter and facebook) to plan Z (turn off the Internet) without stopping at any intermediate solutions.
01/27/11 00:00
01/27/11 06:00
01/27/11 12:00
01/27/11 18:00
01/28/11 00:00
01/28/11 06:00
01/28/11 12:00
01/28/11 18:00
01/29/11 00:00
01/29/11 06:00
01/29/11 12:00
01/29/11 18:00
01/30/11 00:00
01/30/11 06:00
01/30/11 12:00
01/30/11 18:00
01/31/11 00:00
01/31/11 06:00
01/31/11 12:00
01/31/11 18:00
02/01/11 00:00
02/01/11 06:00
02/01/11 12:00
02/01/11 18:00
02/02/11 00:00
02/02/11 06:00
02/02/11 12:00
02/02/11 18:00

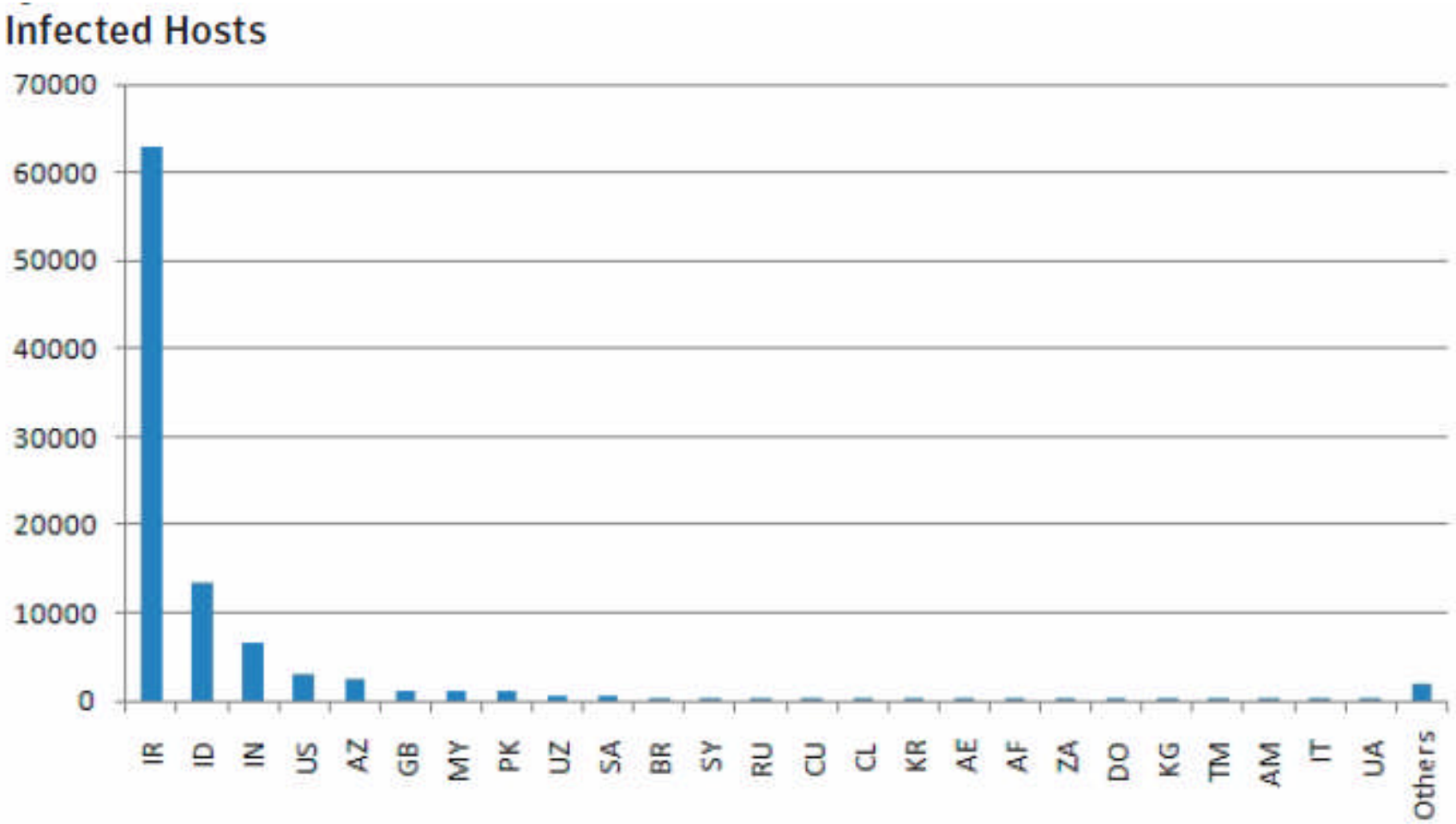
Stuxnet

O Stuxnet foi o primeiro vírus capaz de causar danos no meio físico, o que o torna uma ameaça diferente de tudo o que foi visto anteriormente.

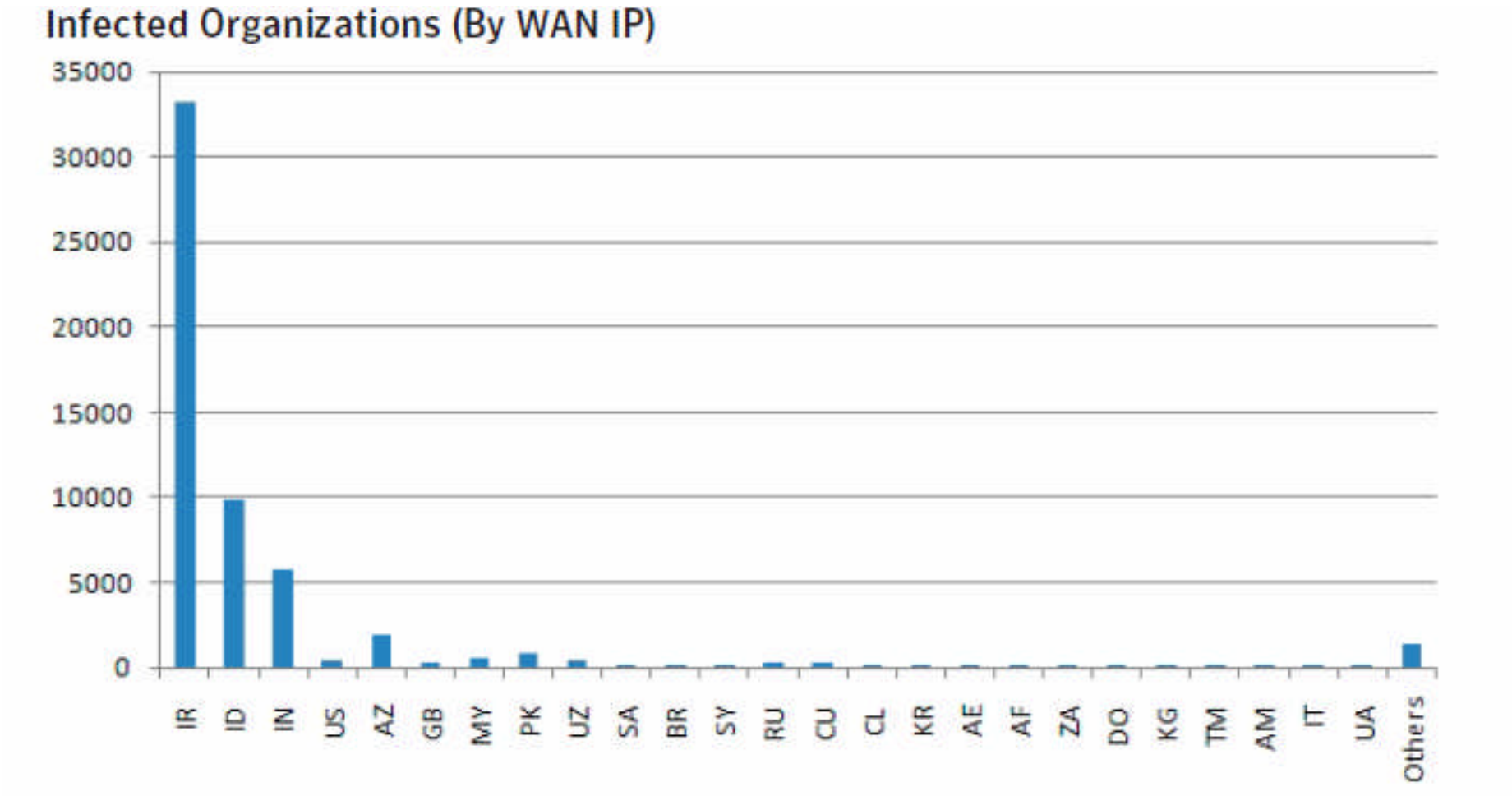
O vírus teve como alvo principal sistemas de controle industriais, que são usados para monitorar e gerir centrais de energia eléctrica, barragens, sistemas de processamento de resíduos e outras operações fundamentais. A partir daí, o malware modifica os códigos existentes para permitir que os atacantes tomem o controle sem que os operadores percebam. Em outras palavras, essa ameaça foi criada para permitir que atacantes manipulem equipamentos físicos, o que a torna extremamente perigosa.

O que também chama a atenção no Stuxnet é que ele foi desenvolvido para atacar um sistema muito especifico de infra-estrutura, infectando um software da Siemens que controla instalações industriais fundamentais.

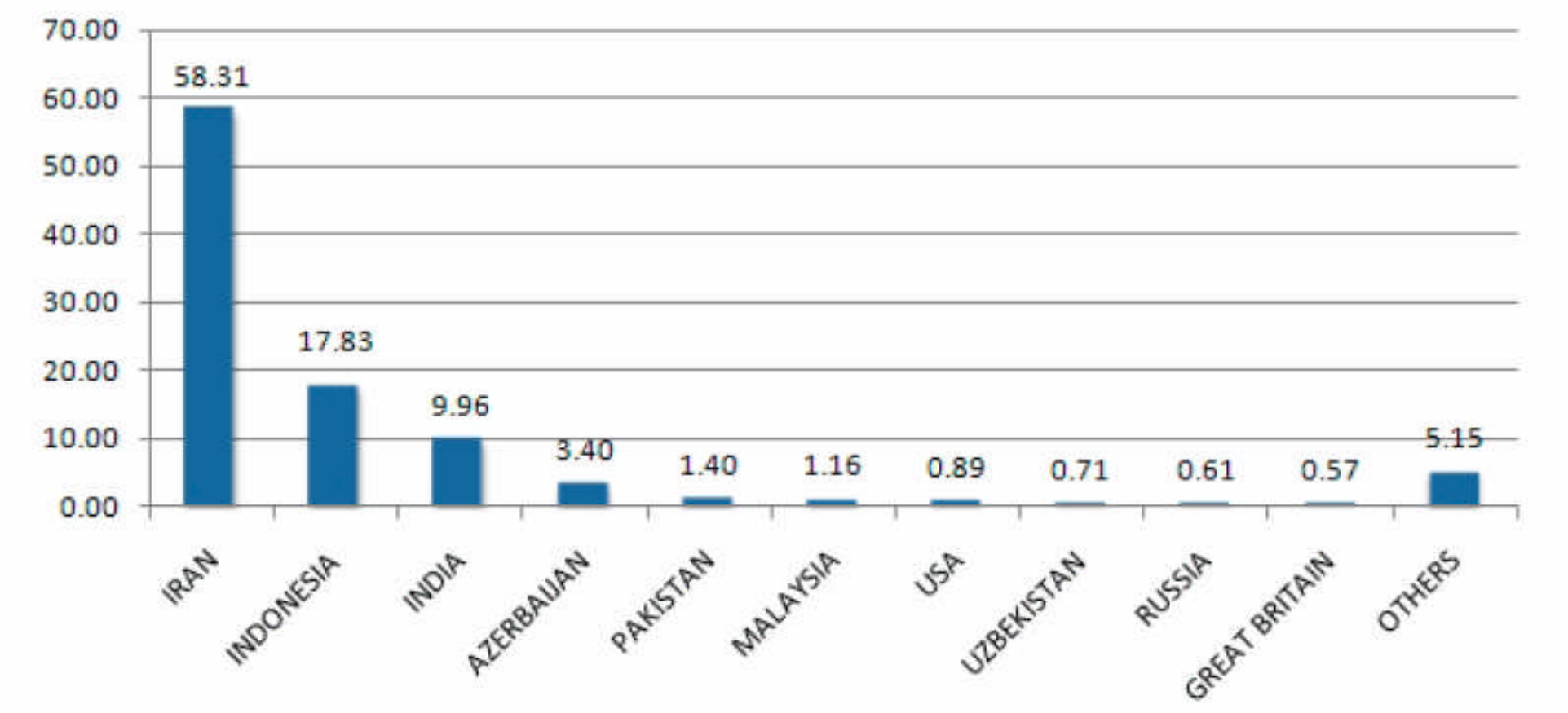
Setembro 29, 2010, numero de hosts unicos infectados por país



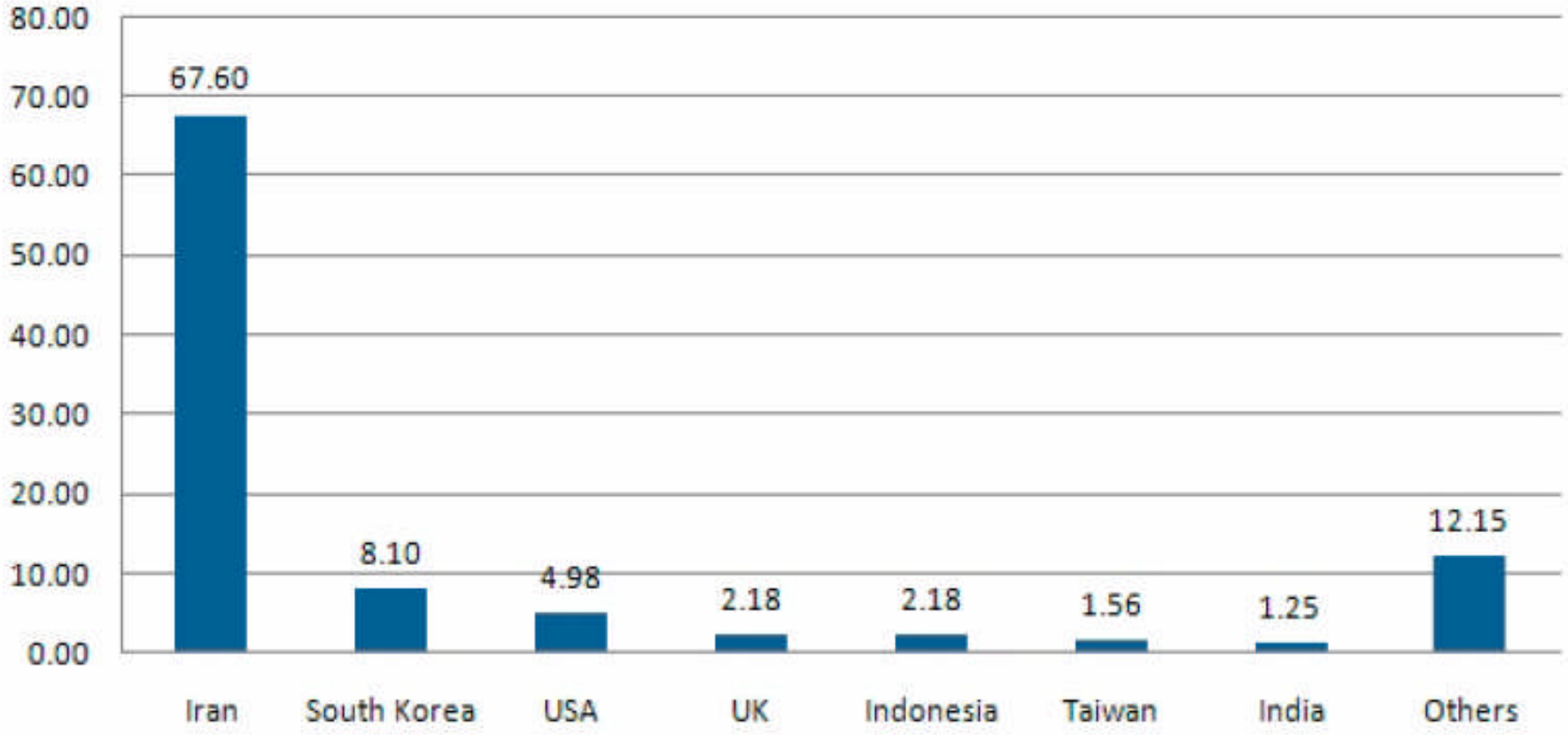
Setembro 29, 2010, numero de organizações infectadas por país com base no endereço WAN IP



Distribuição Geográfica das Infecções



Percentagem de Hosts com Software da Siemens instalado infectados pelo Stuxnet



Stuxnet aims to identify those hosts which have the Siemens

STUXNET CONCLUSIONS

- **A concentração de infecções no Irão indica claramente ter sido este o alvo principal do ataque.**
- **O uso das técnicas de propagação mostra que o Stuxnet se espalhou para além da área alvio inicial**
- **Essa infecções adicionais foram consideradas como danos colaterais These additional infections are likely to be “collateral damage”—(unintentional side-effects).**
- **O virus Stunext (Trojan/Worm) foi apenas o começo de uma nova era em que gerações de viroses podem afectar as nossas vidas for a do espaço designado por ciber-espaço.**

O CRIME ORGANIZADO DECIDE ENTRAR NO JOGO

BotNets

Botnets são redes de máquinas comprometidas e sob o control dos seus atacantes

Estas máquinas podem ser usadas por quem as controla para lançarem ataques ou para serem usadas em actividades maliciosas.

Spammers, hackers, and outros ciber-criminosos estão adquirindo ou alugando botnets — O seu preço situa-se entre os $200 e os $400 por hora.

As botnets tem sido reconhecidas pelos Ciber-criminosos como sendo uma arma de elite para acções de fraude e extorsão

Outros Casos...

FEVEREIRO 2006

Christopher Maxwell, 20, foi indiciado nos EUA por atacar computadores em três universidades (Universidade Estadual da Califórnia, Universidade de Michigan e n Univeridade da Califórnia-Los Angeles) e um hospital (Northwest Hospital em Seattle) , formando uma 'botnet' com mais de 13 000 PCs. Botnets são redes de computadores zumbis que podem ser controlados remotamente pelo dono da botnet.

O Northwest Hospital em Seattle, teve problemas em sua rede quando seus sistemas foram comprometidos. A botnet prejudicou o tratamente de pacientes, atrasou o processamento de exames e desligou computadores em unidades de tratamente intensivo (UTIs).

Os bots de Maxwell deixavam o sistema lento ao instalar pacotes de adware. O cracker teria ganho mais de 100 mil dólares em comissões de desenvolvedores de adwares pela instalação dos programas.

JANUARY 2006

Jeanson Ancheta, de 20 anos, foi considerado culpado pelos tribunais da California, de se ter introduzido em computadores governamentais e tomar o controlo dos mesmos com o proposito de realizar acções de fraude. Ele instalou software Trojan nos sistemas da China Lake Naval Facility no deserto de Mojava, California. Com isso pode controlar remotamente a maior parte dos computadores daquela rede governamental. Ele usou aqueles computadores para gerar "hits" na publicidade de determinados websites, sendo que os anunciantes lhe pagavam conforme o trafego recebido. Ancheta admitiu que a fraude lhe permitiu receber cerca $60,000 de antes de ser detectado.

Além disso, verificou-se que ele controlava 400,000 computadores espalhados por todo o mundo, os quais manipulava remotamente gerando trafego de publicidade, para gerar spam e para infectar outros computadores.


Source: route-views.oregon-ix.net (Mar 2002)
Quem controla a rede de comunicações??
Intelig (17379)
6453
279
TCS (9167)
RNP (1916)
IMPSAT (11415)
Telemar (7738)
11537
Pegasus (19990)
3549
Embratel (4230)
Optiglobe (10685)
1239
IFX (18747)
Registro .br (22548)
701
3561
Metronet (13591)

BotNets

Durante Septembro 2006, Autoridades de Singapura fecharam uma larga rede som mais de 10000 robots, depois de alertada por tecnicos do ISP Telenor ASA que detectou esta rede quando analisava comunicações de Internet Relay Chat (IRC).

OPERAÇÃO ROOTKIT

Em Agosto 2002 - 14 italianos – na maioria profissionais no domínio da segurança da informação foram presos.

Fizeram intrusões abusivas (hacking) entre Setembro 2001 e Agosto 2002 em:

- **Mais de 1000 servidores em todo o mundo**
- **20% pertenciam a Militar/Governo dos USA**
- **20% pertenciam a Militar/Governos Europeus**
- **Várias Universidades e Importantes companhias algumas responsáveis por high-tech**

Sem cooperação internacional seria impossível obter uma boa correlação de eventos que permitisse a identificação dos prevaricadores

A ameaça de virus: todos os tipos?

O crescimento do Outsource

O crescimento do recurso ao Outsourcing dos serviços obriga a um incremento dos diferentes controlos de segurança bem como na sua maior rigorosidade.

Crime Organizado e Call Centres

Tem sido notado que o crime organizado está a infiltrar os seus elementos em call centres com a intenção de obter informação sensível e de caracter privado

- **A Policia de Strathclyde, Escócia, declarou que 10% dos call centres em Glasgow tinham sido infiltrados por gangs ao serviço do crime organizado tentando cometer fraude ou obter informação que a permita realizar. Glasgow tem hoje em dia cerca de 300 call centres empregando mais de 18000 trabalhadores.**
- **Foi reportado que diversa informação de caracter privado foi roubada em call centres em operações na India. (e.g. Doze pessoas foram presas por terem defraudado clientes do Citibank em cerca de $350,000. Três dos homens detidos trabalhavam para Mphasis, a firma offshore firm que opera call centres em Bangalore e Pune).**

DoS

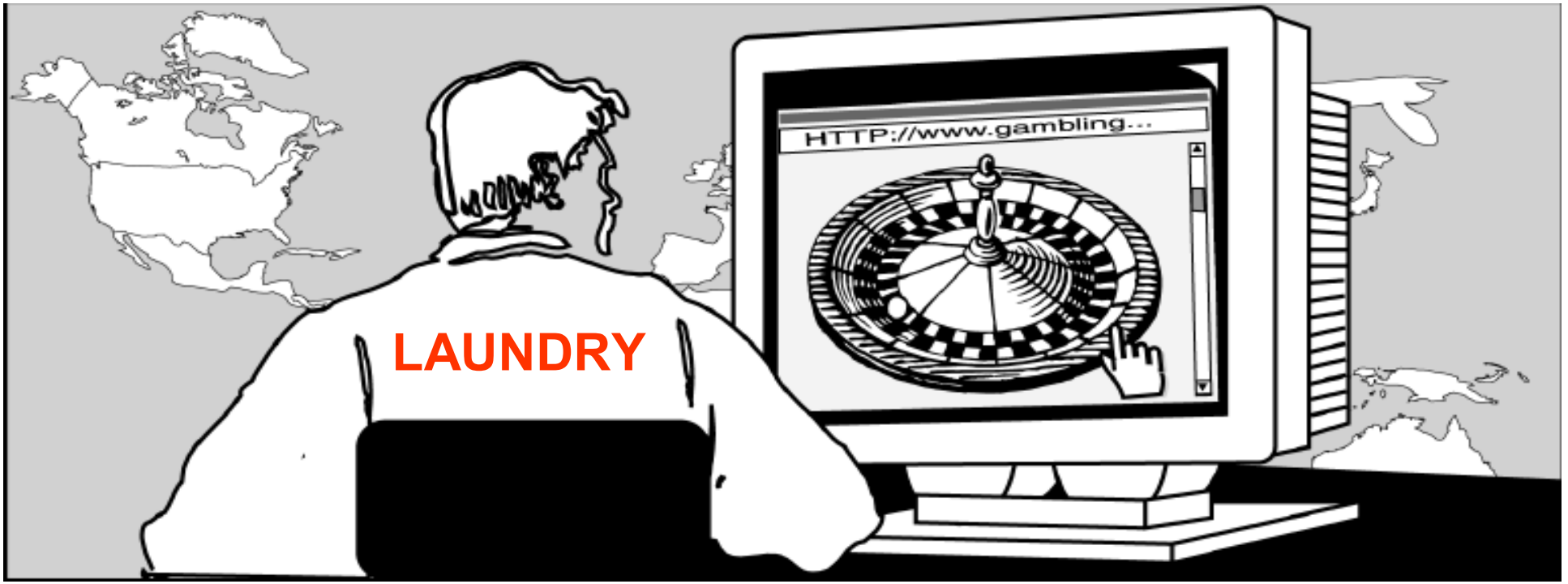
- Transportes
- Comunicações
- Energia
- Financeiro

Chantagem e DoS

On-line gambling é o Oeste selvagem do mundo do jogo.

É uma industria be muitos billions de dollars

De acordo com Autoridades Policiais existe um vário conjunto de reportes de acções conduzidas pelo crime organizado da Russia e Europa de Leste provocando DoS ataques em online gambling sites e e-comerce websites, para criar situações de chantagem e extorsão.



Internet gambling pode igualmente ser um excelente veículo para a “lavagem” de dinheiro.


CRACKDOWN
XBOX 360
Microsoft
realtime
worlds


ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZED TO UNCLASSIFIED LEVEL//ALL INFORMATION SANITIZ
NOAA
ATF
SWO
DCC

MONITORAR


CYBER CRIME
POLICE POST

A Doutrina

“pressure point warfare”

(PPW)

O Templo de Shaolin

Durante este período de tempo o estilo original de artes marciais de Shaolin era o usual na China

O CONCEITO

- **Pontos de pressão são pontos no corpo por onde passam nervos, sangue ou oxigênio e sobre os quais se pode efetuar um golpe para causar um efeito além de simplesmente dor.**
- **Existem centenas de pontos no nosso corpo, e cada um deles tem função específica: alguns, quando atingidos, podem causar inconsciência; outros, dormência e perda momentânea de movimento; e existem até aqueles que podem causar morte.**

空手道

Shashoujian

- **Shashoujian é um termo de origem chinesa com origem no período Tang (618-907 A.D.). Implica uma acção ou qualidade que oferece a vantagem estratégica, quando empregada de um modo particular, num momento crucial de oportunidade para a realização de uma meta específica.**
- **Entre os peritos em computadores é vulgarmente designado por "Killer Application".**
  - **As suas características definidoras são:**
  - **Objectivos limitados em conflitos**
  - **Baseado na doutrina "O inferior derrota o superior"**
  - **Guerras de curta duração**
  - **Pequenos danos**
  - **Grandes campos de batalha com baixa densidade de tropas**
  - **Transparência no campo de batalha**
  - **Luta intensa por superioridade na informação**
  - **Força de integração sem precedentes**
  - **Aumento da necessidade de comando e control**
  - **Objectivos estratégicos obtidos com precisão através de ataques, sem o uso de grandes forças, nas vulnerabilidades das forças de combate do inimigo**

A PPW e a Guerra Assimétrica

- **A Ciber - guerra não é apenas a guerra electrónica ou guerra de informações, mas abrange as operações de guerra psicológica, a teoria da mentira, o terrorismo selectivo ou generalizado, a manipulação do sistema nervoso humano pela aplicação doseada do medo (psicologia do medo).**
- **A Ciber - guerra visa a paralisação de um adversário pela penetração nas redes de computadores que dirigem a maioria das actividades vitais da economia, criando o caos e difundindo um estado de medo generalizado.**
- **Uma Ciber - guerra deverá ser considerada com uma guerra assimétrica conduzindo a uma paralisia estratégica**
- **A doutrina "Pressure Point Warfare" é então um elemento base da Guerra Assimétrica.**
- **Na Ciber - guerra não há linha da frente, não há definições precisas e o próprio conceito de guerra adquire um significado distinto.**

ALVOS PREFERÊNCIAIS

- **Os alvos da ciber-guerra são os computadores, individualmente ou em rede. Trata-se de invadir as redes e programas de controlo de operações. Os alvos preferenciais são:**
  - **Comando das redes de distribuição de energia**
  - **Comando das redes de distribuição de agua potável**
  - **Comando das redes de controlo dos transportes ferroviários**
  - **Comando das redes de controlo de tráfego aéreo**
  - **Comando das redes de emergência: Pronto-socorro, polícia, bombeiros.**
  - **Comando das redes bancárias**
  - **Comando das redes de comunicações**
  - **Comando dos links com sistemas de satélites (sistemas telefónicos, sinais TV, previsões meteorológicas, sistemas GPS)**
  - **Comando das redes governamentais**

- **A guerra de controlo (leitenkrieg ou ciberwar) pode ser implementada pela utilização de acções terroristas.**

A Guerra Irrestrita

Segundo o livro "Guerra Irrestrita" de 1999, e da autoria dos chineses Qiao Liang e Wang Xiangsi (versão em inglês feita pela CIA e publicada em www.defesanet.com.br) é proposta uma guerra assimétrica contra os USA, alinhando com a antiga ideia de paralesia estratégica. Em síntese é dito:

- **A guerra assimétrica não tem regras; nada é proibido**
- **Deve-se atacar as redes de computadores**
- **Deve-se recorrer à sabotagem económica**
- **Espalhar rumores e escândalos que criem tumulto**
- **……**
- **…… (acções terroristas diversas)**

Ciber – guerra / Guerra de Informação

- **É uma guerra de precisão e multifacetada, onde as conferências de imprensa são muitas vezes mais importantes do que os campos de batalha.**
- **É, em certo sentido, a guerra de guerrilhas dos grandes poderes na Idade da Informação, pois aplica os princípios básicos da guerra de guerrilhas, numa base tecnológica e doutrinal muito diferente**
- **A guerra de informação a um nível estratégico, implica um domínio do ciber-espaço, uma vez que não podem ser descurados os ciber-ataques em todos os seus diversificados aspectos.**
- **Nesta nova forma de guerra a supremacia das comunicações é um factor imperioso, sendo que na maior parte dos casos o espaço exterior deve ser entendido como a sua quarta dimensão.**
- **As infra-estruturas de informação constituem nos nossos dias umas das mais valias aportadas pela RMA**

Os Mecanismos…

O transistor, a electrónica, o chip, o computador, a fibra óptica, o satélite, a Internet, são próteses técnicas para a inteligência humana

Neste cenário, a luta pelo poder concentra-se no controle de mecanismos capazes de gerar ou neutralizar assimetrias de informação.
E hoje, não há ferramenta mais eficaz para filtrar, modular, administrar e mesmo neutralizar assimetrias de informação do que as tecnologias da informação

e o seu uso...

As tecnologias de informação, transformam-se, no limite, em infra-estrutura semiótica capaz de minar qualquer hierarquia de controle da difusão do conhecimento. Inclusive aquela cuja origem seu projecto original, o ARPA, pretendia reforçar.

Vemo-la nesta acção - limite em nos recentes casos:

- **Quando, em 1991, Boris Yeltsin subiu num tanque para proclamar ao mundo, diante de câmaras de TV numa praça de Moscovo, o fim da União Soviética, ele conhecia seu "script" e seus riscos. Era o desfecho de um golpe branco que depunha Gorbachev na velocidade da luz e de dedos "teclando" emails. O golpe derramou muitos bits, em vez de sangue.**
- **O mesmo se deu na queda de Suharto na Indonésia, em 1998, e em recentes contra-golpes à mentira oficial deslavada.**
- **Na Venezuela, contra a "quartelada" que tentaria derrubar Chavez, e na Espanha, contra a reeleição de Aznar. Aqui com macabra ironia, pois a mentira era justamente sobre a origem e possíveis causas do ataque terrorista de 11 de Março.**
- **E por último, câmaras digitais de celulares causaram, em Abu Grhaib, mais estragos numa assimetria farisaica do que inúmeros homens - bomba, sem sangue algum a mais.**

CONCLUSÕES

CRIAR CULTURA DE SEGURANÇA

ACÇÕES

- TOMADA DE CONSCIÊNCIA (SECURITY AWEARENESS)
- STANDARDIZAÇÃO
- COOPERAÇÃO INTERNACIONAL
- CAPACIDADE DE INVESTIGAÇÃO
- PROSSECUÇÃO

Protecção das infra-estruturas estrategicamente importantes

OCDE

Ciberguerra é designação exagerada.
A maioria dos ataques de alta tecnologia descritos como actos de ***"ciberguerra"*** *não são merecedores desse nome, segundo considera a Organização para a Cooperação e o Desenvolvimento Económico (OCDE), sublinhando que tal designação é* ***"exagerada"****. A conclusão faz parte de um relatório, no âmbito de uma série de estudos sobre incidentes que podem desencadear uma ruptura global.*

Enquanto as pandemias e a instabilidade financeira podem causar problemas, é pouco provável que os ciberataques possam fazer o mesmo, sendo mais provável que estes ataques tenham efeitos localizados e de curto prazo, refere o documento da OCDE.

UE

Em Novembro 2010, a União Europeia anunciou planos para desenvolver um centro de combate ao cibercrime até 2013, e concordou com os Estados Unidos em estabelecer um grupo de trabalho centrado em cibersegurança. Entretanto, a NATO também adoptou o seu Strategic Concept Charter, documento que esquematiza planos para desenvolver novas capacidades de combate a ataques cibernéticos, a redes militares.

UK

Em Dezembro de 2010 o governo do Reino Unido revelou estar a considerar a venda das competências da GCHQ, o centro de comunicações do Governo britânico, para fechar o hiato de capacidades e competências, entre o sector privado e o público, e assim reforçar as capacidades do país contra ataques cibernéticos

CONCLUSÕES

Ao nível estratégico a guerra de informação implica um domínio do ciber-espaço, pois não podem ser descurados os ciber ataques, com as suas bombas lógicas, vírus e cavalos de Tróia.

Esta diferente forma de guerra implica uma política de segurança e defesa para o ciber-espaço, pois este impôs uma nova dimensão geopolítica, a do próprio o ciber-espaço (Adams, 1993; Nunes, 2003)


Fraude e Segurança
podem afectar
as infra-estrutras

A Questão da Responsabilidade

- **Os Consumidores necessitam saber que podem ser directamente implicados em actividades criminais por actividades efectuadas através de botnets.**

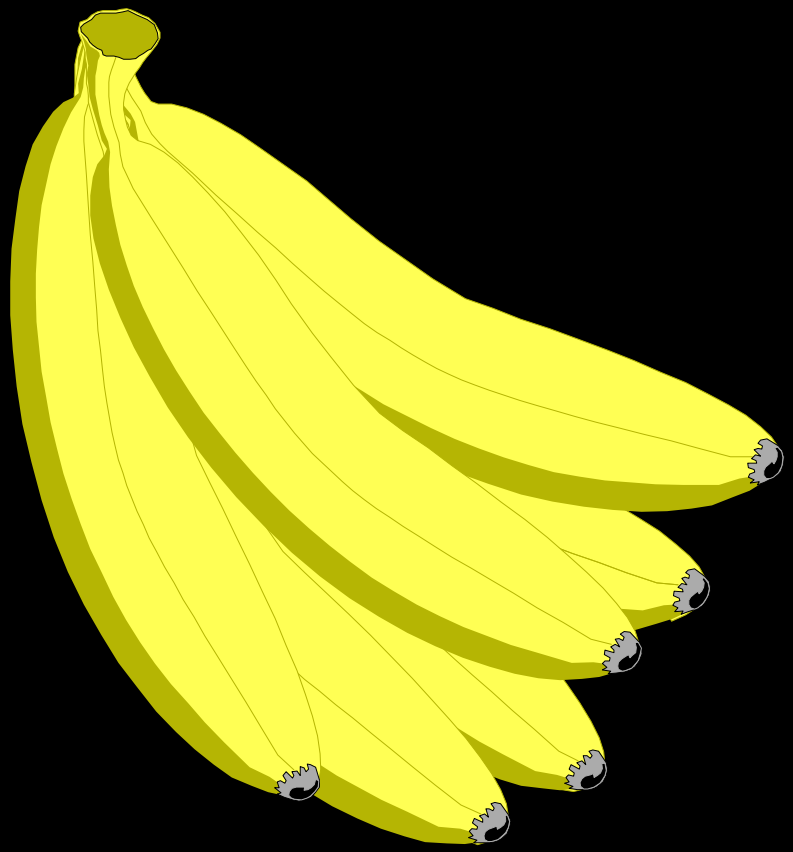
- **Qual a responsabilidades de redes menos seguras e que por isso facilitam actividades criminais com consequências para terceiros ou nas infra-estructuras criticas.** ***(This argument would need to show that the insecure party "had a duty to use reasonable care in securing its computer systems, breached that duty by failing to employ adequate security, and was a reasonably recognized cause of actual damages.“*** - E. Kenneally , "Who's Liable for Insecure Networks? "Computer,June 2002,, pp. 93-94.)

- **Na epoca da banda larga os consumidores domesticos representam a maior fonte de problemas na utilização das redes de telecomunicações. Devem ou não esses consumidores ser responsáveis por certos acidentes ocasionados por não terem tomado medidas mínimas de protecção (exl., aplicando os “patches” de software, instalar uma firewall, usar antivirus) para fazerem a segurança dos seus computadores?**

NÃO DEVERÃO AS EMPRESAS SER RESPONSIBILIZADAS?

AMEAÇA BANANA

BUILD ABSOLUTELY NOTHING ANYWHERE NEAR ANYTHING



NÃO DEVERÃO AS EMPRESAS SER RESPONSIBILIZADAS?

CONCLUSÕES

Para encerrar, uma mensagem de outro físico, talvez o maior cosmólogo vivo, anunciada quando lhe restava o movimento de apenas um único dedo.

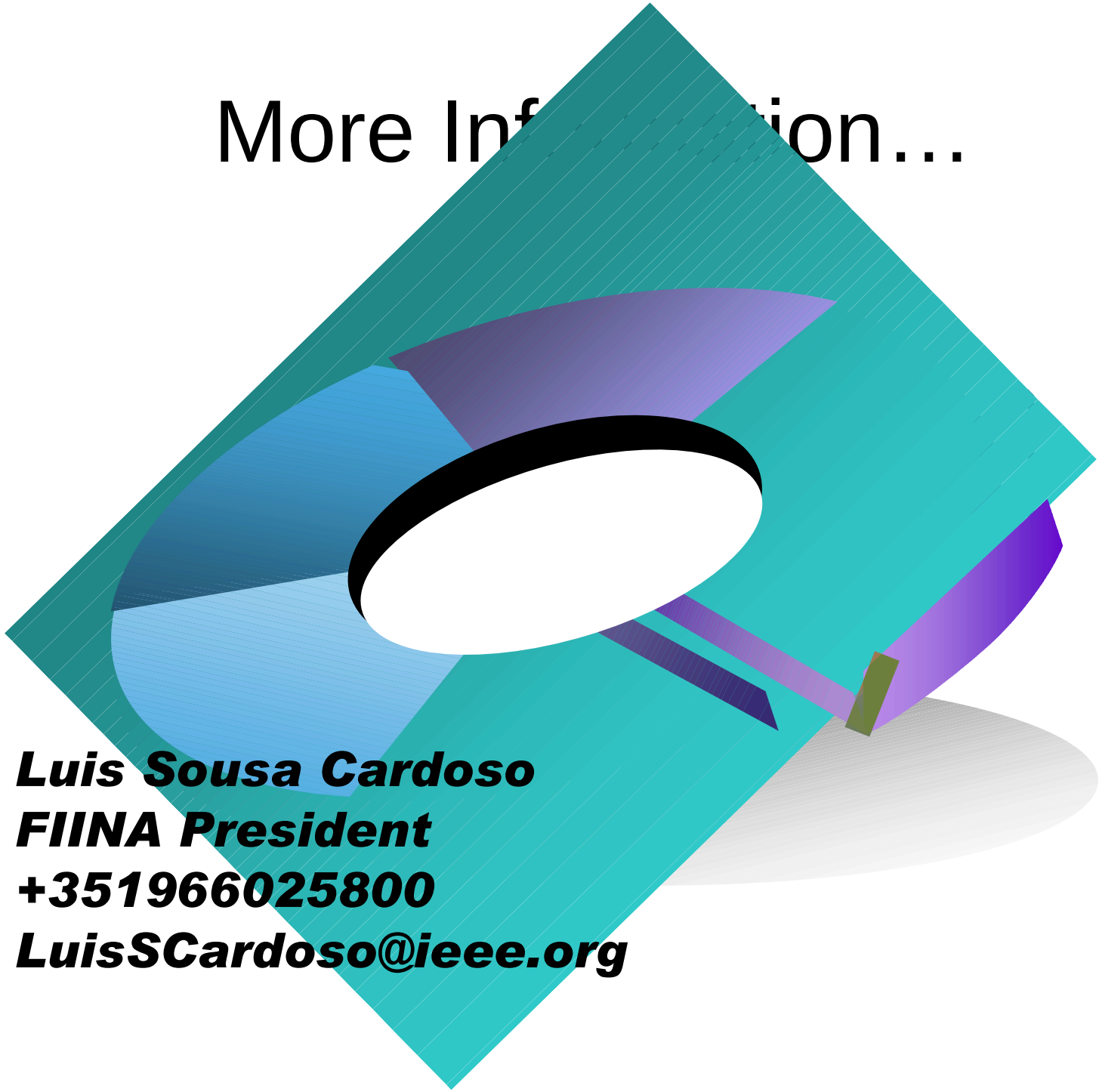
Na verdade, esse recado de Stephen Hawking é o mesmo recado do oráculo de Delfos a Sócrates:

“O maior inimigo do conhecimento não é a ignorância, mas a ilusão do conhecimento".

Peço licença para acrescentar,
a interdição pelos fariseus.


QUESTÕES ???

More Information…



Luis Sousa Cardoso
FIINA President
+351966025800
LuisSCardoso@ieee.org