Cibercrimes no contexto da Ciberguerra
4º Cyber Security – 9/12/2014

Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

pedro.jmrezende.com.br/sd.php

Roteiro

1- **Quais Cibercrimes?**

2- **Na Guerra Cibernética ...**

3- **Algumas reflexões**

1. Quais Cibercrimes?

Observações sobre prioridades

Relatório *Trendmicro* - Brasil

www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-brazilian-underground-market.pdf#page=4

CYBERCRIMINAL UNDERGROUND ECONOMY SERIES

* Places in the Internet where cybercriminals converge to sell and buy different products and services exist. Instead of creating their own attack tools from scratch, they can instead purchase what they need from peers who offer competitive prices. Like any other market, the laws of supply and demand dictate prices and feature offerings. But what's more interesting to note is that recently, prices have been going down.

Over the years, we have been keeping tabs on major developments in the cybercriminal underground in an effort to stay true to our mission—to make the world safe for the exchange of digital information. Constant monitoring of cybercriminal activities for

we revisited the Chinese underground and published "Beyond Online Gaming: Revisiting the Chinese Underground Market [3]." We learned then that every country's or region's underground market had distinct characteristics. So this year, we will add another market to our growing list, that of Brazil.

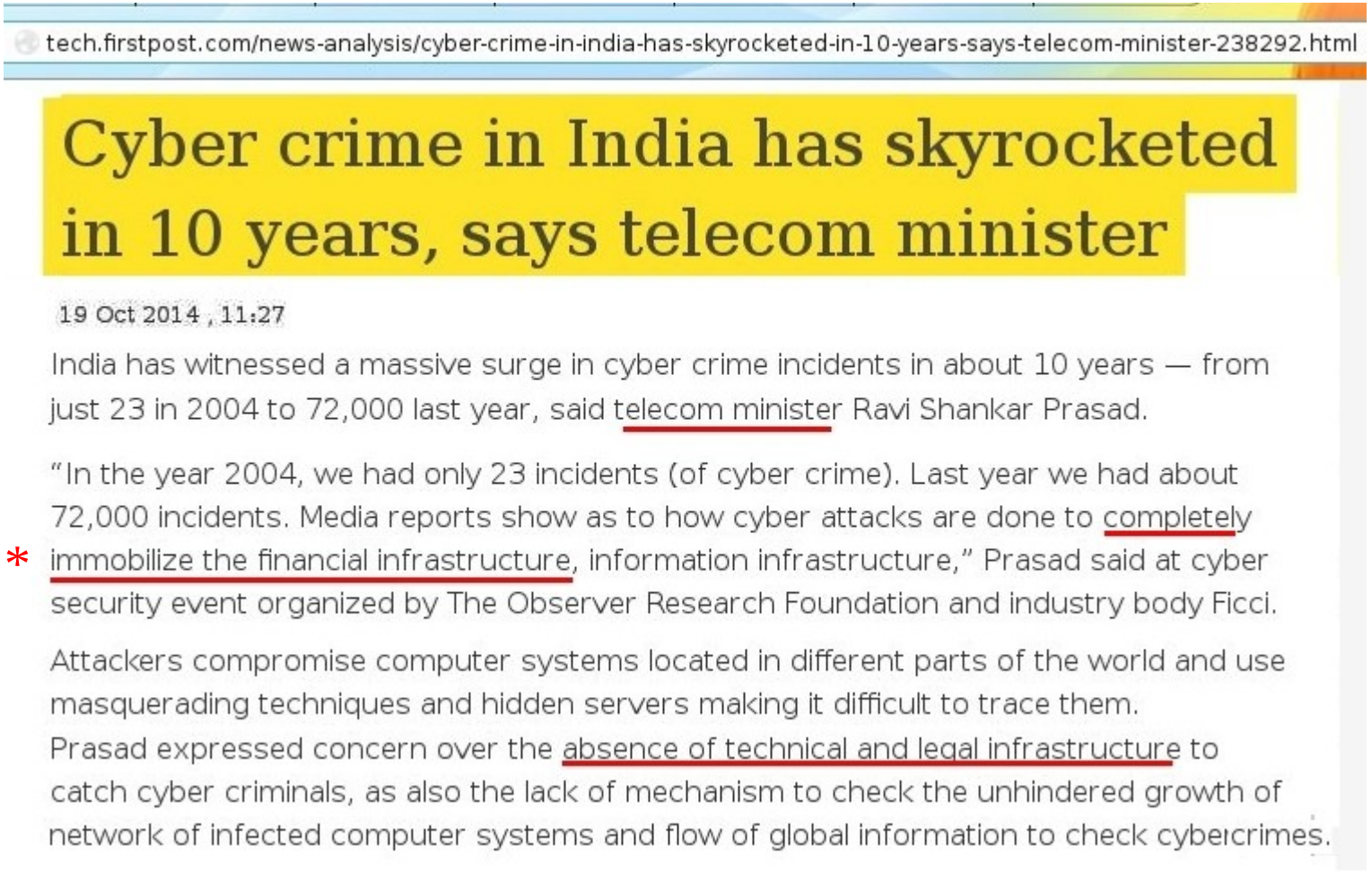
The barriers to launching cybercrime have decreased. Toolkits are becoming more available and cheaper; some are even offered free of charge. Prices are lower and features are richer. Underground forums are thriving worldwide, particularly in Russia, China, and Brazil. These have become popular means to sell products and services

* O segmento mais sofisticado desse mercado, *0-day exploits*, é inflacionado pela demanda de agências de três letras que operam ações de vigilantismo global, mas é aí ignorado.

Seguro *para quem*? contra o que?

No destaque desse relatório da '*Trend*' (tendência), do grupo de países BRIC faltou citar a Índia ...

Índia (sobre cibercrime)



tech.firstpost.com/news-analysis/cyber-crime-in-india-has-skyrocketed-in-10-years-says-telecom-minister-238292.html

Cyber crime in India has skyrocketed in 10 years, says telecom minister

19 Oct 2014 , 11:27

India has witnessed a massive surge in cyber crime incidents in about 10 years — from just 23 in 2004 to 72,000 last year, said telecom minister Ravi Shankar Prasad.

"In the year 2004, we had only 23 incidents (of cyber crime). Last year we had about 72,000 incidents. Media reports show as to how cyber attacks are done to completely
* immobilize the financial infrastructure, information infrastructure," Prasad said at cyber security event organized by The Observer Research Foundation and industry body Ficci.

Attackers compromise computer systems located in different parts of the world and use masquerading techniques and hidden servers making it difficult to trace them.
Prasad expressed concern over the absence of technical and legal infrastructure to catch cyber criminals, as also the lack of mechanism to check the unhindered growth of network of infected computer systems and flow of global information to check cybercrimes.

* Imobilização completa da infraestrutura financeira? Desconhecida. Isto então pode ser aviso (de *psyop*), ameaça (de agente duplo) ou...

Quanto à China ...

China PLA officers call Internet key battleground

Recomendar 65 recomendações. Cadastre-se para ver o que seus amigos recomendam.

By Chris Buckley

BEIJING, Jun | Fri Jun 3, 2011 12:36am EDT

(Reuters) - China must make mastering cyber-warfare a military priority as the Internet becomes the crucial battleground for opinion and intelligence, two military officers said on Friday, two days after

vinha sendo acusada, na mídia corporativa e em relatórios de empresas de segurança digital (parceiras voluntárias ou não de agências de três letras), de ser 'Estado-vilão', que promove ou é conivente com cibercrime organizado.

[Até que, após junho 2013, ações de Edward Snowden puseram em marcha uma *psyop* que nivela 'por baixo' essa percepção coletiva]

www.reuters.com/article/2011/06/03/us-china-internet-google-idUSTRE7520OV20110603

Quanto à China ...

3 Jun 2011 - ELP: "...Assim como a guerra nuclear era a guerra estratégica da era industrial, a ciberguerra é a guerra estratégica da era da informação; e esta se tornou uma forma de batalha massivamente destrutiva, que diz respeito à vida e morte de nações... Uma forma inteiramente nova, invisível e silenciosa, e que está ativa não apenas em conflitos e guerras convencionais, mas também se deflagra em atividades diárias de natureza política, econômica, militar, cultural e científica... Os alvos da guerra psicológica na Internet se expandiram da esfera militar para a esfera pública... Nenhuma nação ou força armada pode ficar passiva e se prepara para lutar a guerra da Internet."

www.reuters.com/article/2011/06/03/us-china-internet-google-idUSTRE7520OV20110603

… e a Rússia …

www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html

The New York Times

SUBSCRIBE NOW

Russian Hackers Amass Over a Billion Internet Passwords

By NICOLE PERLROTH and DAVID GELLES AUG. 5, 2014

A Russian crime ring has amassed the largest known collection of stolen Internet credentials, including 1.2 billion user name and password combinations and more than 500 million email addresses, security researchers say.

473 COMMENTS

The records, discovered by Hold Security, a firm in Milwaukee, include confidential material gathered from 420,000 websites, including household names, and small Internet sites. Hold Security has a history of uncovering significant hacks, including the theft last year of tens of millions of records from Adobe Systems.

Hold Security would not name the victims, citing nondisclosure agreements and a reluctance to name companies whose sites remained vulnerable.

Á única fonte de identificação da autoria – de que os 'hackers' são da Rússia – era um ucraniano que fala russo e está nos EUA ganhando dólares (Hold), cobrando para dizer se a senha de quem lhe paga está entre as "roubadas"

2. Guerra Cibernética

Já começou? O que seria? Como é travada?
O que tem a ver com cibercrime?

Já estamos em Ciberguerra?

- A ciberguerra é (pode ser entendida como)
uma forma de **Contrarrevolução Digital**.

cujo paradigma é:

"Como pode ser a virtualização destrutível"

Pela ideologia neoliberal, como em J. Schumpeter, uma forma – histórica – de “destruição criativa”

(em “*Capitalismo, Socialismo e Democracia*”, 1942)

Como surge a Ciberguerra?

Evolução da Cibernética

Ciclo Década	Inovação principal	Paradigma: Como pode ser...
1940	Arquiteturas	a máquina programável?
1950	Transistores	a programação viável?
1960	Linguagens	a viabilidade útil?
1970	Algoritmos	a utilidade eficiente?
1980	Redes	a eficiência produtiva?
1990	Internet	a produtividade confiável?
2000	Cibercultura	a confiança virtualizável?
2010	Ciberguerra	a virtualização destrutível?

Como é travada a ciberguerra?

Conflito Virtual: por controle econômico, técnico e psicológico

axiomamuse.wordpress.com/2011/12/27/the-fbi-is-aggressively-building-biometric-database-international-in-scope

AxXiom for Liberty How free do you want to be?

HOME ABOUT AXXIOM ON RADIO-LISTENING INFO AXXIOM'S 10 RULES FOR ACTIVISTS TO LIVE BY

The FBI is Aggressively Building Biometric Database, International in Scope

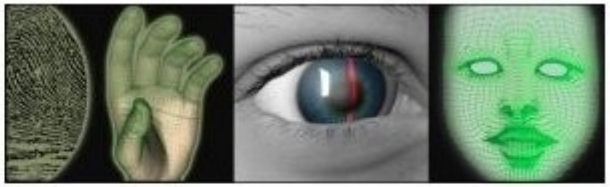
Posted on December 27, 2011 by AxXiom | 1 Comment

Kaye Beach

Dec. 26, 2011

FBI's Next Generation Identification (NGI)

According to the FBI it is official FBI policy to collect ***"as much biometric data as possible within information technology systems"*** and to ***"work aggressively to build biometric databases that are comprehensive and international in scope."*** ***link***



"We need to recognize the change that is occurring in society, Society is taking away the privilege of anonymity."
– Morris Hymes, Head of the ID Assurance Directorate at the Defense Department.

Revoluções "coloridas", seguidas de caos e colapso

Corrida armamentista pela infraestrutura de vigilantismo global – ferramenta para manipular mercados, insuflar "*regime change*" ou controle social em revoltas contra austeridade, escassez, genocídio, etc.

Com cerco normativo

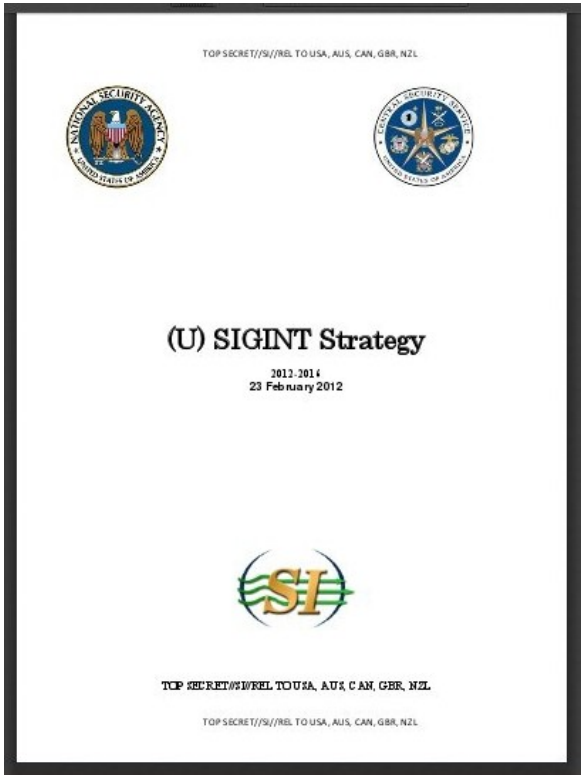
No Conflito Virtual, o vigilantismo global é estratégico para conquista do controle (*ciber*, no grego = controle) social

Precisa, portanto, ser socialmente legitimado (ex.: facebook, etc.)

Teste? http://www.gigapixel.com/image/gigapan-canucks-g7.html

Com cerco tecnológico

SIGINT (Signals Intelligence) - Planejamento 2012-2016 (5 Olhos):


TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) SIGINT Strategy

2012-2016
23 February 2012

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

https://s3.amazonaws.com/s3.documentcloud.org/documents/838324/2012-2016-sigint-strategy-23-feb-12.pdf

Vazado para o Wikileaks - Destaque para:

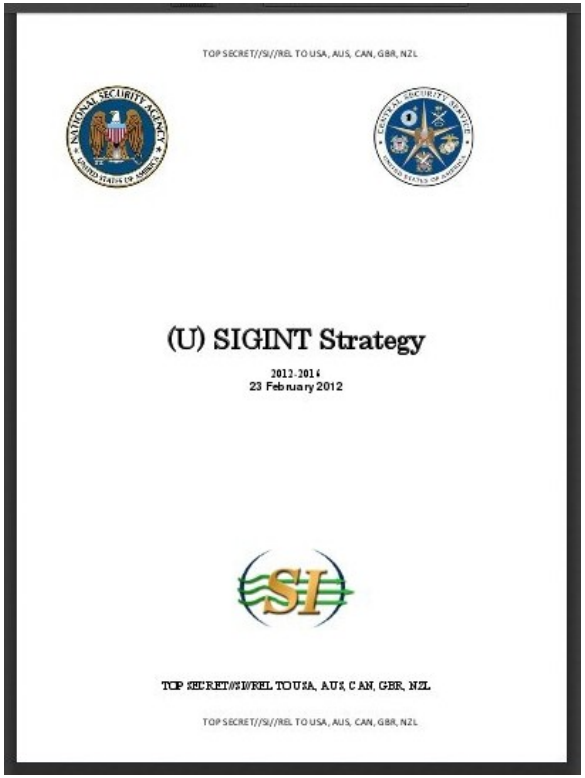
"2.1.3. (TS//SI//REL) *Counter indigenous cryptographic programs by targeting their industrial bases with all available SIGINT + HUMINT (Human Intelligence) capabilities*"

"2.1.4. (TS//SI//REL) *Influence the global commercial encryption market through commercial relationships, HUMINT, and second and third party partners* "

"2.2. (TS//SI//REL) *Defeat adversary cybersecurity practices in order to acquire the SIGINT data we need from anyone, anytime, anywhere*"

Com cerco tecnológico

SIGINT (Signals Intelligence) - Planejamento 2012-2016 (5 Olhos):


TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

(U) SIGINT Strategy

2012-2016
23 February 2012

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

TOP SECRET//SI//REL TO USA, AUS, CAN, GBR, NZL

https://s3.amazonaws.com/s3.documentcloud.org/documents/838324/2012-2016-sigint-strategy-23-feb-12.pdf

Vazado para o Wikileaks - Destaque para:

"2.1.3. (TS//SI//REL) *Enfrentar softwares de criptografia domésticos ou alheios atingindo suas bases industriais com nossas capacidades em inteligência de sinais (SIGINT) e humanas*"

"2.1.4. (TS//SI//REL) *Influenciar o mercado global de criptografia comercial por meio de relações comerciais e pessoais de inteligência, e por meio de parceiros diretos e indireto"*

"2.2. (TS//SI//REL) *Derrotar as práticas de segurança cibernética adversárias para obtermos os dados que precisamos, de qualquer um, a qualquer momento, em qualquer lugar.*"

Com cerco psicológico

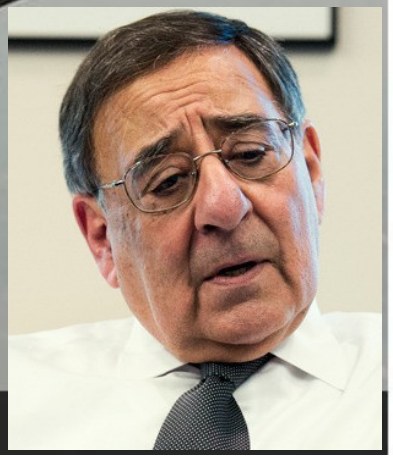
NGI + Radicalização normativa + terror bilateral = Guerra Virtual

rt.com/usa/white-house-lethal-force-878

Department of Justice says White House can use 'lethal force' on American citizens on US soil ← Em breve, também lá

Published time: March 05, 2013 22:23
Edited time: March 06, 2013 07:27

Diretor da CIA **Leon Panetta** à AFP**:**
"Os EUA estão engajados numa guerra global 'ao terror' e *drones* são uma ferramenta eficaz contra militantes que planejam ataques"



rt.com/usa/drone-war-continue-panetta-290

Reuters / U.S. Navy / Erik Hildebrandt / Northrop Grumman / Handout

3. Algumas Reflexões

Mega-cibercrime – em larga escala e acima da lei – como peça do xadrez geopolítico no contexto atual

Sobrevida do dólar e *reset* financeiro

www.bbc.com/news/business-29520685

BBC NEWS BUSINESS

News | Sport | Weather | Earth | Future | Shop | TV | Radio | More...

Home | UK | Africa | Asia | Australia | Europe | Latin America | Mid-East | US &

Market Data | Economy | Entrepreneurship | Business of Sport | Companies

7 October 2014 Last updated at 13:46 GMT

Banker admits Libor fraud conspiracy

Financial institutions in London and New York have settled regulatory allegations of rigging Libor

A senior banker from a UK bank has admitted conspiring to defraud over manipulating the Libor lending rate.

The banker, who can not be named for legal reasons, is the first person in the UK to plead guilty to the offence.

Two men have already pleaded guilty in the US to fraud offences linked to the rigging of Libor, for years the benchmark by which trillions of pounds of financial contracts are based.

The case arose from the **Serious Fraud Office**'s (SFO) investigations

Fraudes que produzem efeitos em mercados de câmbio, financeiros, petróleo, metais, etc.

Quando há punição, só em multas: bem menores que o lucro com fraudes.

Manipulação de mercados pelo FED, BCs e bancos *too-big-to-(j)fail* provocará ruptura monetária quando a oferta de ouro à vista esgotar

Sobrevida do dólar e *reset* financeiro

Evento indistinguível de ataque *false-flag* que justificaria as leis marciais, numa tentativa de controlar o *reset* financeiro, em transição a uma nova moeda de reserva global, rumo à nova ordem mundial

TICs!

Quando esgotar a oferta à vista, a hiperinflação atingirá o dólar e o ouro estocado pode lastrar nova moeda. Que irá requerer <u>infra para transações</u>

Reset financeiro e mega-cibercrime

https://hat4uk.wordpress.com/2014/11/29/explosive-debt-analysis-why-at-least-35-of-global-debt-is-a-fraud-should-be-written-off

THE SLOG. DECONSTRUCT LIES, RECONSTRUCT DECENCY

HOME ABOUT AIMS ANECDOTAGE BORISCONI THE BARBARIAN CO-OP CALUMNY CRASH 2 GLOBAL LOOTING

EXPLOSIVE DEBT ANALYSIS: WHY AT LEAST 35% OF GLOBAL DEBT IS A FRAUD & SHOULD BE WRITTEN OFF

BY JOHN WARD NOVEMBER 29, 2014 | **Huge percentage of debt could be written off with no forgiveness at all**

IRELAND PAYING FOUR TIMES TOO MUCH, GREECE & ITALY THREE TIMES TOO MUCH, EUROZONE 2.5 TIMES TOO MUCH.

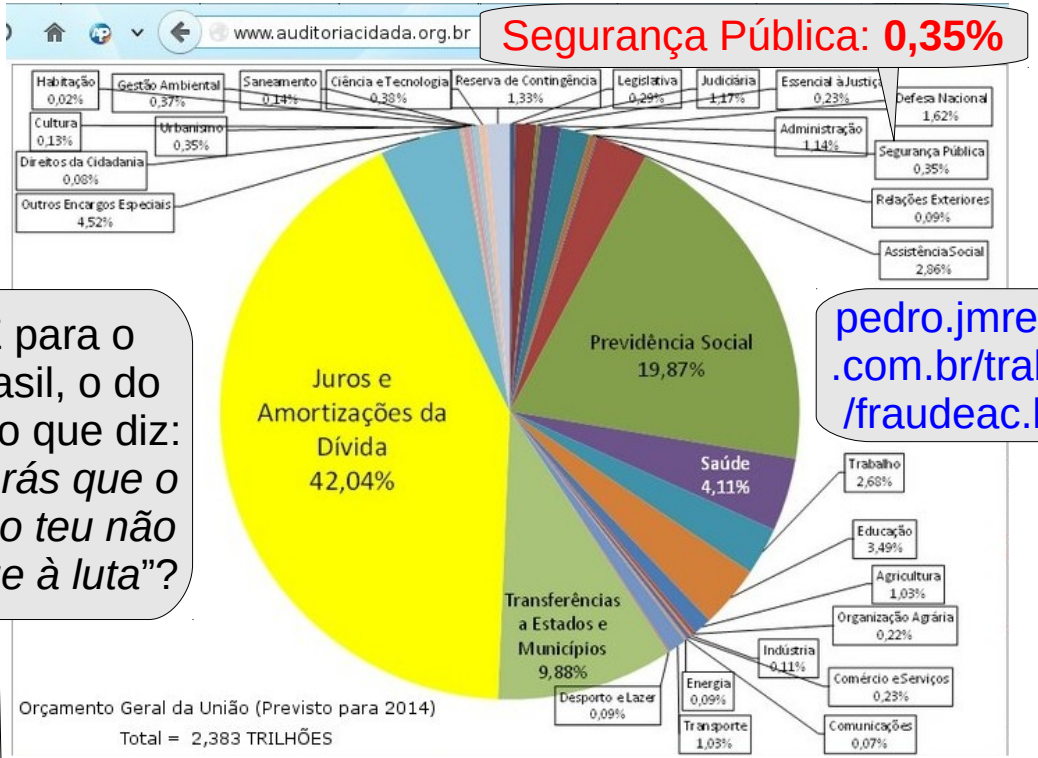
REVEALED: HOW ECONOMIES ARE BEING CRUSHED IN THE NAME OF LEGALISED BANKING FRAUD.

Introduction

Veteran Sloggers will know that I've been banging on about debt forgiveness since mid 2010. That's because the debts can't be repaid without widespread State collapses. Nation States supporting citizens who work for money within those States are far more important (to my mind) than some Hedgie Vulture who bought sovereign debt for 15c on the Dollar… .and now wants to make a 400% profit at the expense of the citizenry.

Para adiar hiperinflação do dólar, 'estímulos' seletivos de crédito-como-moeda geram bolhas e fraudes que tornam a crise e colapso inevitáveis. Evitada por enquanto com chantagem, ameaça militar e *regime change*.

Mega-cibercrime e *regime change*



E para o Brasil, o do hino que diz: "*verás que o filho teu não foge à luta*"?

pedro.jmrezende.com.br/trabs/fraudeac.html

A priorização do serviço de dívidas fraudulentas em países periféricos – no Brasil, até com <u>fraude à Constituição</u> – suprime recursos, até para combate ao cibercrime autônomo (não promovido por Estados). [vide slide "Índia"] Isso serve de pretexto ao *regime change*, onde governos vassalos são então instalados, para a nova ordem mundial.

"*Se, para muitos países, soberania e dignidade nacional são conceitos esquecidos ou relíquias, então, para a Rússia, a verdadeira soberania é condição absolutamente necessária para nossa existência.*" V. Putin
Estado da Federação, 4/12/2014 http://rt.com/news/211411-putin-state-address-top10