



Seminário SEGSI

SERPRO, Brasília, novembro 2016

## Redes Sociais Uma visão geopolítica

Pedro A. D. Rezende

Ciência da Computação - Universidade de Brasília

[pedro.jmrezende.com.br/sd.php](http://pedro.jmrezende.com.br/sd.php)

# Paradoxo de uma nova era

- *“We may think we are all passengers on the ‘Magic History Bus’, but in reality we all have a steering wheel, a gas pedal, and a brake, and the actions and decisions we make every day drive and steer history.”*

Richard Quirck

# O paradoxo do humanismo teológico

- *“We may think we are all passengers on the ‘Magic History Bus’, but in reality we all have a steering wheel, a gas pedal, and a brake, and the actions and decisions we make every day drive and steer history.”*

Richard Quirck

- “Podemos pensar que somos todos passageiros no “Ônibus Mágico da História”, mas na realidade **todos nós** temos um volante de direção e pedais de acelerador e freio, e as decisões e ações que praticamos todos os dias conduzem e dirigem a História”



# O paradoxo do humanismo teológico

- *“We may think we are all passengers on the ‘Magic History Bus’, but in reality we all have a steering wheel, a gas pedal, and a brake, and the actions and decisions we make every day drive and steer history.”*

Richard Quirck,

Diretor da Divisão de Inteligência de Sinais – SIGINT (Espionagem) da NSA, em **“Generally Speaking:...”**, *SIDToday Newsletter*, 2/2/2005



Vazado por Edward Snowden e publicado em <https://theintercept.com/snowden-sidtoday/3008523-generally-speaking-iraq-worth-all-the-effort/> (16/08/2016).

Mais detalhes em

<http://www.activistpost.com/2016/08/10-orwellian-moments-found-in-the-newly-leaked-private-nsa-newsletters.html>

# O paradoxo do humanismo teológico

- *“We may think we are all passengers on the ‘Magic History Bus’, but in reality we all have a steering wheel, a gas pedal, and a brake, and the actions and decisions we make every day drive and steer history.”*

De  
Ou

a’?



[Propaganda de recrutamento no aeroporto da capital da Austrália]

# Ciberespaço com teatro de guerra

China PLA officers call Internet key battleground



By Chris Buckley

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

Recomendar

65 recomendações

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

Começa no *front* psicológico: Até 2011, a mídia corporativa e relatórios de empresas de segurança digital (parceiras de agências de três letras) vinham pintando a China como nação-vilã, que estaria provocando a **ciberguerra** e/ou sendo conivente com o cibercrime organizado.

Em 2013, começa outra fase: ações de Edward Snowden puseram em marcha uma **psy-op** para nos condicionar a um regime dominante de vigilantismo global.

[www.reuters.com/article/2011/06/03/us-china-internet-google-idUSTRE7520OV20110603](http://www.reuters.com/article/2011/06/03/us-china-internet-google-idUSTRE7520OV20110603)

# Ciberespaço como teatro de guerra

China PLA officers call Internet key battleground



**3 Jun 2011 – Exército de Libertação Popular da China:** "...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 só 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**."

# Cerco tecnológico

## O que os vazamentos de Snowden revelam:

Parte essencial de uma estratégia ofensiva de **guerra híbrida**, posto em marcha para implantar um regime dominante de vigilantismo global (para nova ordem mundial), a pretexto do inevitável jogo de espionagem das nações, nele camuflado como combate ao terrorismo, cibercrime, etc

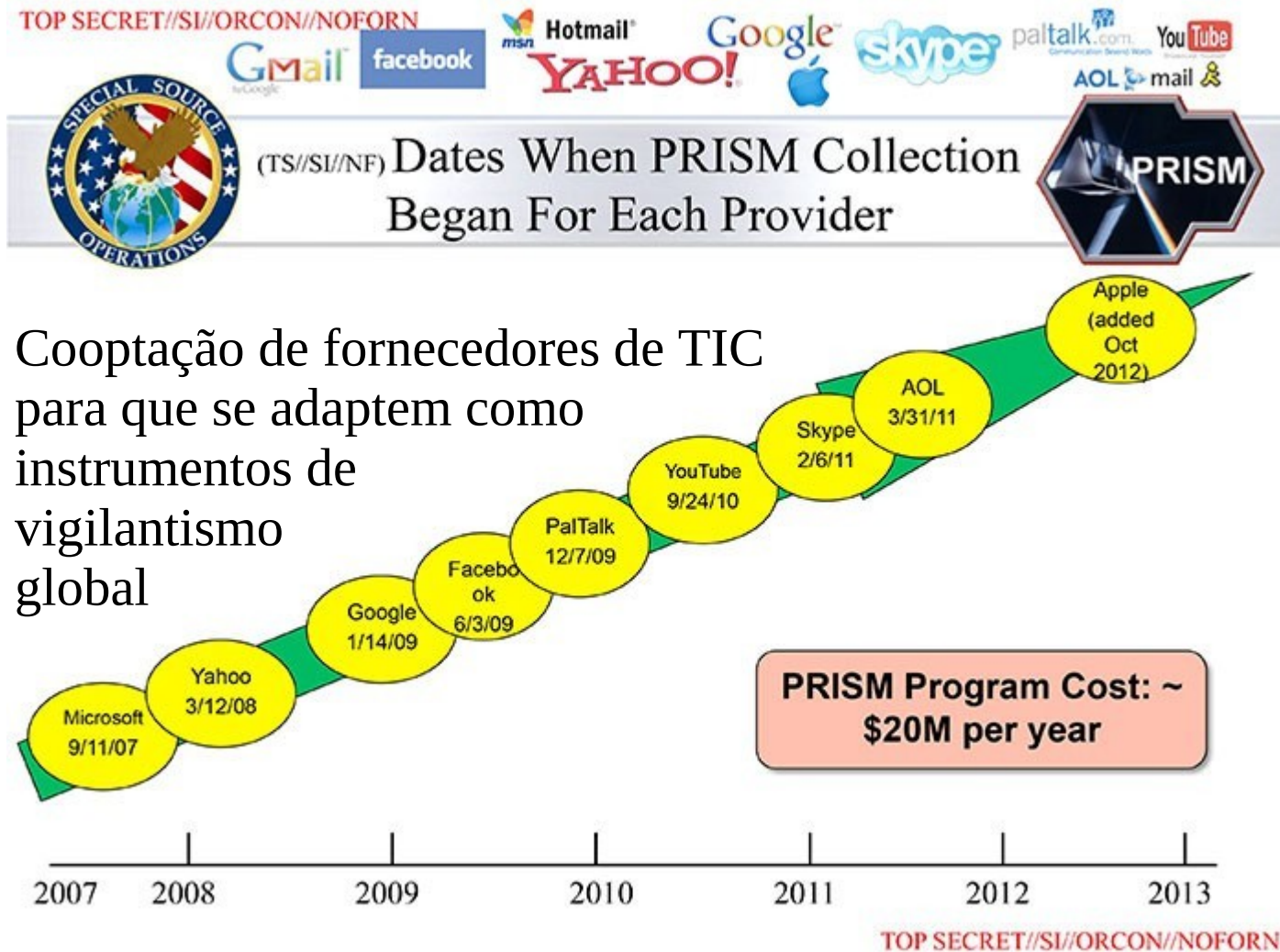
## Vendo o “episódio Snowden” como *psyop* de bandeira falsa:

Transição da fase de cooptação clandestina no ciberespaço (projeto **PRISM**, sabotagem de padrões criptográficos e produtos essenciais como o **Heartbleed** no OpenSSL e o **Equation Group** em firmware de HDs)

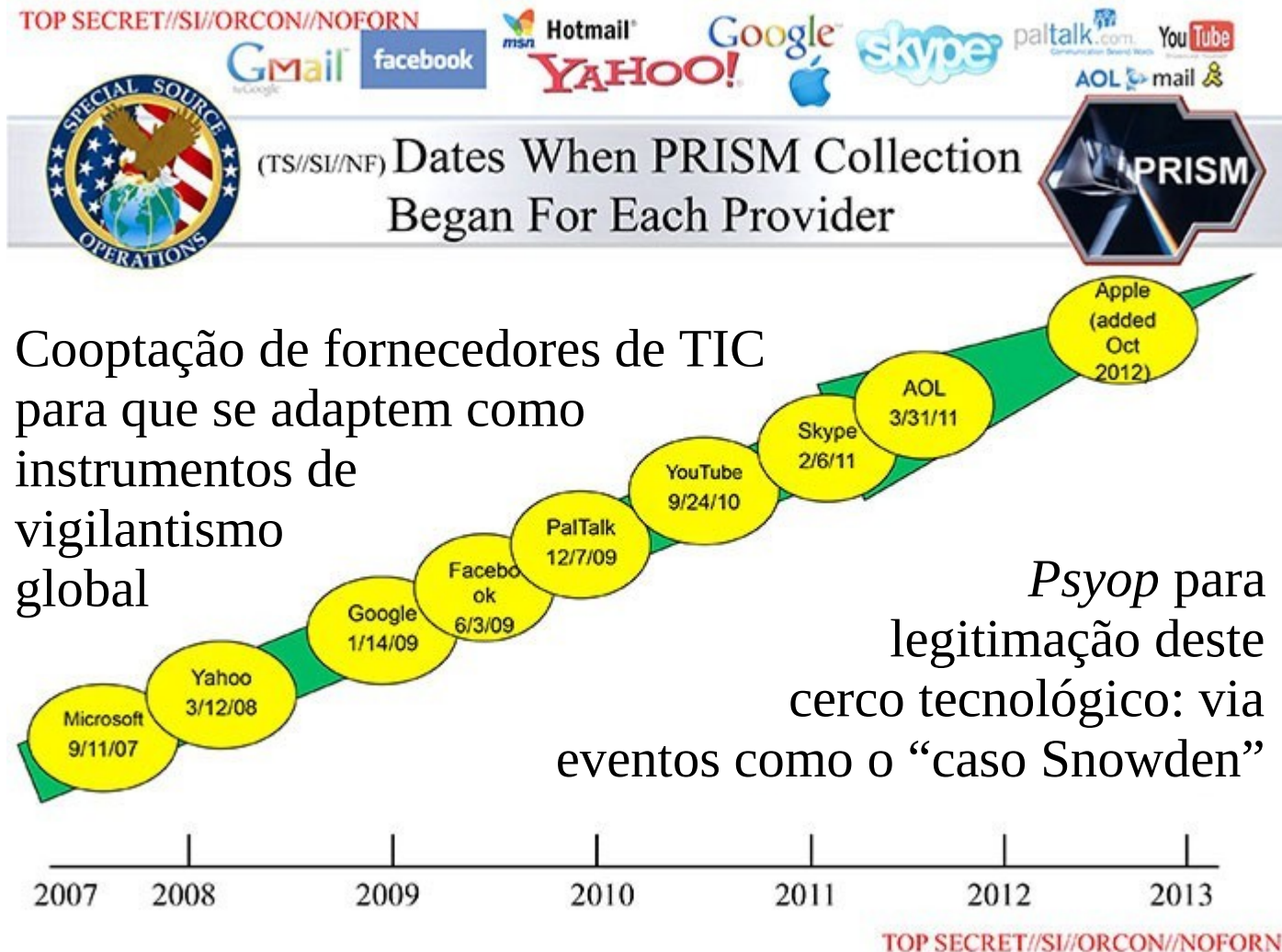
...



# Cerco tecnológico



# Cerco tecnológico



# Cerco tecnológico – exemplo emblemático

[www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage](http://www.kaspersky.com/about/news/virus/2015/equation-group-the-crown-creator-of-cyber-espionage)

home → About Us → Corporate News → Malware → 2015 → Equation Group: The Crown Creator of Cyber-Espionage

**KASPERSKY** LAB

## Equation Group: The Crown Creator of Cyber-Espionage

16 Feb 2015  
Virus News

For several years, Kaspersky Lab's Global Research and Analysis Team (GREAT) has been closely monitoring more than 60 advanced threat actors responsible for cyber-attacks worldwide. The team has seen nearly everything, with attacks becoming increasingly complex as more nation-states got involved and tried to arm themselves with the most advanced tools. However, only now Kaspersky Lab's experts can confirm they **have discovered** a threat actor that surpasses anything known in terms of complexity and sophistication of techniques, and that has been active for almost two decades – The Equation Group.

### Equation group's malware timeline

The chart displays the following malware families and their active periods:

Malware Family	Approximate Active Period
EquationLaser	2001 - 2003
EquationDrug	2003 - 2011
DoubleFantasy	2004 - 2011
Fanny	2008 - 2010
GrayFish 1.0	2008 - 2011
DFH	2009 - 2010
GROK keylogger	2010 - 2011
GrayFish 2.0	2011 - 2014
TripleFantasy	2011 - 2014

**Feb 2015:**  
Grupo extremo em quase todos aspectos:  
complexidade dos *malwares*, técnicas de infecção, *stealth*, extração sobre *air gap*, etc.

Kaspersky lab recuperou módulos que permitem reprogramar o *firmware* de HDs e *pendrives* dos doze maiores fabricantes, talvez

a mais poderosa arma para vigilantismo global no arsenal desse grupo (talvez o mesmo grupo que desenvolveu o Stuxnet e seus derivados)

# Cerco tecnológico – evolução

## O que os vazamentos de Snowden revelam:

Parte essencial de uma estratégia ofensiva de **guerra híbrida**, posto em marcha para implantar um regime dominante de vigilantismo global (para nova ordem mundial), a pretexto do inevitável jogo de espionagem das nações, nele camuflado como combate ao terrorismo, cibercrime, etc

## Vendo o “episódio Snowden” como *psyop* de bandeira falsa:

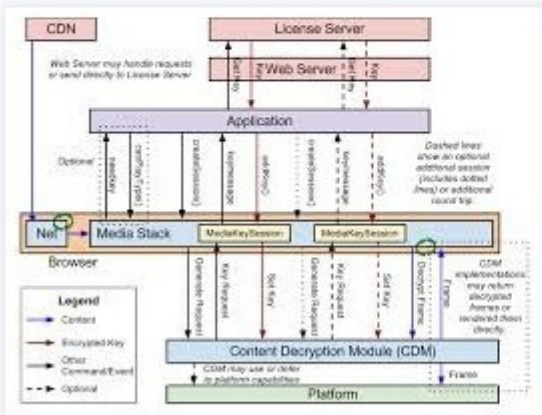
Transição da fase de cooptação clandestina no ciberespaço (projeto **PRISM**, sabotagem de padrões criptográficos e produtos essenciais como o **Heartbleed** no OpenSSL e o **Equation Group** em firmware de HDs) ... Para uma fase de coerção explícita em conflitos de interesses virtuais (**EME** no W3C, **Unlockable bootloader** no UEFI, **ETP** no HTTP 2.0, **CISPA**, **EO-1/4/15**, etc.) que subvertem a integridade de projetos colaborativos autônomos em TI, tais como os de software livre importantes.

# Cerco tecnológico – W3C

bookseller-association.blogspot.com.br/2013\_05\_01\_archive.html

Brave New World

Thursday, May 30, 2013  
HTML5 To Be Put Under DRM?

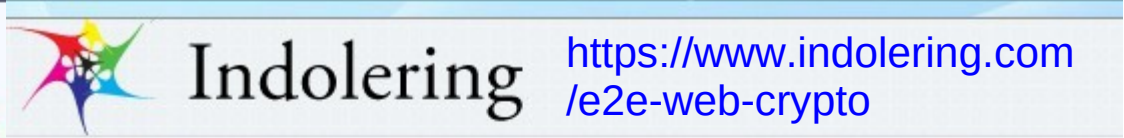


## Encrypted Media Extensions

Proposta de padrão  
**EME** pelo W3C :

Funções criptográficas instaladas à revelia do usuário  
em navegadores web com html 5

https://www.indolering.com/e2e-web-crypto

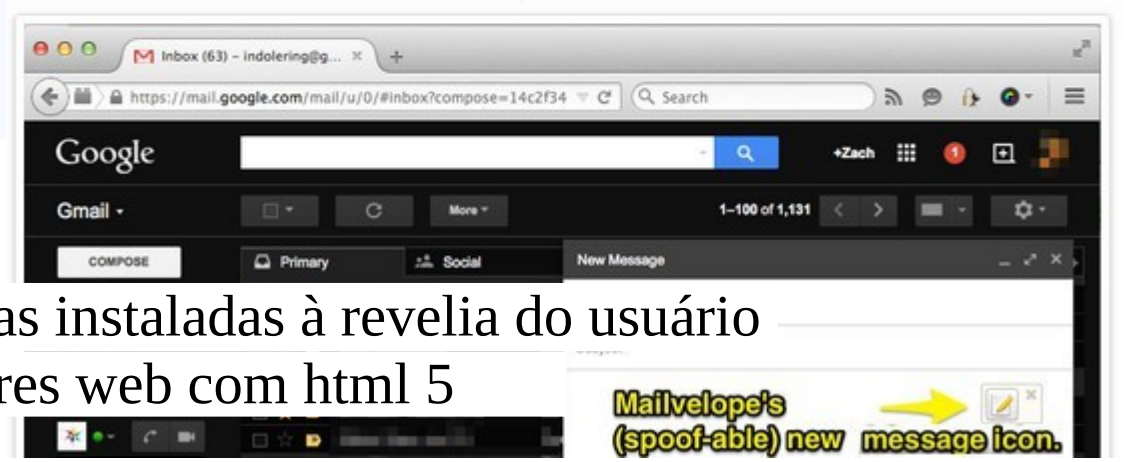


in Research, Security

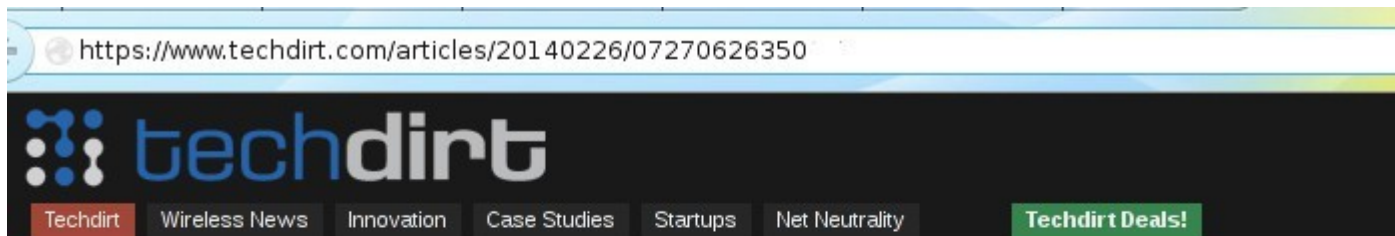
## End-To-End Web Crypto: A Broken Security Model

End-to-end encryption of web services is increasingly popular: [Mailvelope](#) aims to bolt a PGP client onto webmail and both [Yahoo](#) and [Google](#) are working to add support directly. However, the fundamental nature of the web and the limits of human cognition make web-based E2E encryption susceptible to MITM attacks. While still potentially useful, **such systems should not be used by high-risk populations** such as journalists and human rights workers.

The dynamic nature of the web gives service providers the ability to target individual users with a backdoored version of their web client *every time the site is loaded*, an attack [validated](#) in 2007



# Cerco tecnológico – IETF



**(Mis)Uses of Technology**  
by Glyn Moody  
Thu, Feb 27th 2014  
3:10am

## IETF Draft Wants To Formalize 'Man-In-The-Middle' Decryption Of Data As It Passes Through 'Trusted Proxies'

from the *you-jest* dept

One of the (many) shocking revelations from the Snowden leaks is that the NSA and GCHQ use "man-in-the-middle" (MITM) attacks to impersonate Internet services like Google, to spy on encrypted communications. So you might think that nobody would want to touch this tainted technology with a barge-pole. But as Lauren Weinstein points out in an interesting post, the authors of an IETF (Internet Engineering Task Force) Internet Draft, "Explicit Trusted Proxy in HTTP/2.0," are **proposing not just to use MITMs, but also to formalize their use**. Here's his explanation of the rationale:

<https://www.techdirt.com/articles/20140226/07270626350>

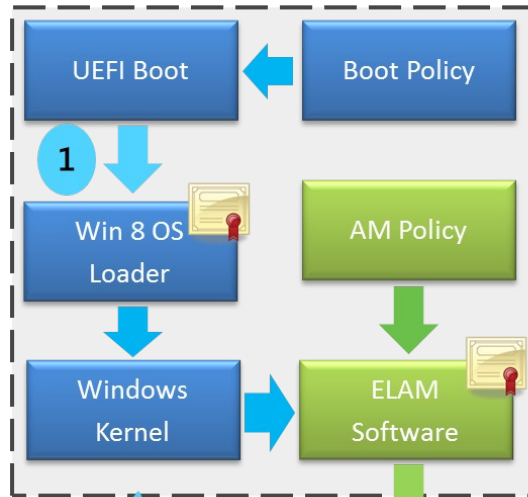
Proposta de padrão

**ETP** pelo IETF :

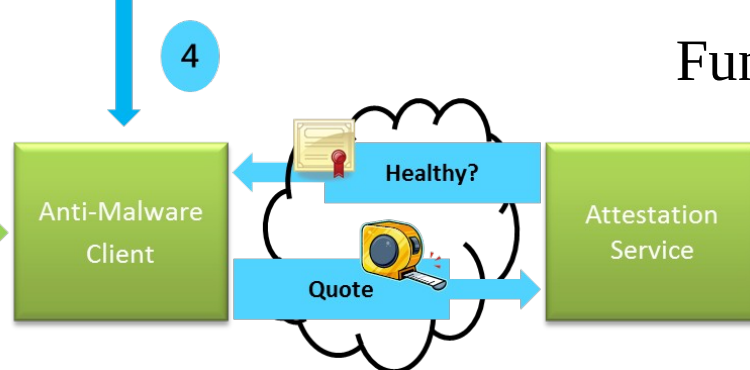
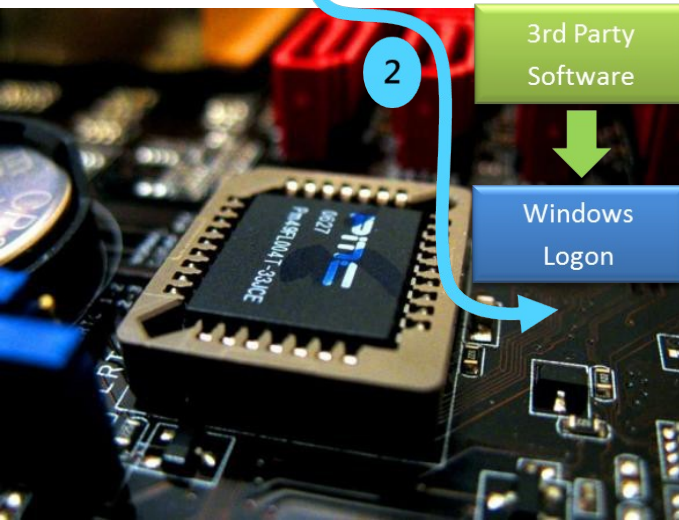
Funções criptográficas instaladas à revelia do usuário em proxies de provedores de conexão http 2.0

# Cerco tecnológico – Fabricantes

## Windows 8 Platform Integrity Architecture



- 1 Secure boot (UEFI) prevents running a unknown OS loader
- 2 The kernel launches Early Launch Anti-Malware (ELAM) they enforce 3rd party drivers and apps
- 3 Measurements of the system start state were recorded in the TPM during boot
- 4 To prove a client is healthy, the anti-malware software can quote TPM measurements to a remote verifier



Funções ocultas  
por baixo:  
Boot **UEFI**  
Controla  
instalação  
e acesso de *qualquer* software ao hardware

# Arranjos evolutivos na arte da guerra

- **Guerra híbrida** = **Revolução colorida + Guerra não-convencional** (ou, de 4ª geração) - Andrew Koribko: *Hybrid wars: an adaptive approach to regime change\**, 2015

- **Ciberguerra**: pode ser vista como uma forma de contra-revolução digital, fundamental para as 2 componentes da guerra híbrida. Ocorre na interface entre guerras convencional e híbrida, com o paradigma:

*Como pode ser a virtualização destrutível?*

Pela óptica neoliberal, estamos fechando mais um ciclo do capitalismo, com “destruição criativa” (J. Schumpeter: *Capitalismo, Socialismo e Democracia*, 1942): colapso da ordem econômica e de Estados.

- **Regime change**: desmonte dos Estados-nação para formação de um governo totalitário global, sustentado com massivos dispositivos de des/controle social (aqui batizados como **tecnologia política**).

\*- <http://orientalreview.org/wp-content/uploads/2015/08/AK-Hybrid-Wars-updated.pdf>



# Arranjos evolutivos na arte da guerra

Este ciclo do capitalismo que está por encerrar, se caracteriza pelo surgimento das TIC eletrônicas – baseadas em arquiteturas de dispositivos digitais programáveis –, que evoluíram assim:

<b>Ciclo Década</b>	<b>Inovação principal</b>	<b>Paradigma: Como pode ser...</b>
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?

# Arranjos evolutivos na arte da guerra

- **Guerra de 4ª geração:** Cel. William Lind et. al.: “*The Changing Face of War: Into the Fourth Generation\**”, Marine Corps Gazette, 1989



## Guerras não-convencionais

*"Operações psicológicas (psyops) se tornam a arma estratégica dominante, na forma de intervenção midiática/informacional*

*...Um importante alvo será o apoio da população inimiga ao seu governo e à guerra. **Noticiários** de televisão podem se tornar uma arma operacional mais poderosa do que divisões blindadas."*

*"Distinção civil/militar pode se desfazer"*

- **Estratégia 5 anéis :** Cel. John Warden: “*The enemy as a system\*\**”, Airpower Journal, 1995 (USAF) – Destruição psicológica de efeito centrípeto, destruição física de efeito centrífugo.

\* [globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html](http://globalguerrillas.typepad.com/lind/the-changing-face-of-war-into-the-fourth-generation.html)

\*\* [www.emory.edu/BUSINESS/mil/EnemyAsSystem.pdf](http://www.emory.edu/BUSINESS/mil/EnemyAsSystem.pdf)

# Tecnologia política

- **Teoria do caos aplicada ao controle comportamental:** Steven Mann: *“Chaos theory and strategic thought \*”*, Parameters, 1992 (US Army)



*“Para mudar a energia de conflito entre pessoas – suprimi-la ou direcioná-la de maneiras favoráveis aos nossos interesses e metas – é preciso mudar o software.*

*Como mostram os hackers, o modo mais agressivo para mudar software é com um vírus; e o que é ideologia, senão outro nome para vírus de software humano?”*

- **Dominação de amplo espectro:** *“J. Vision 2020\*\*”*, 2000 (Pentágono)  
*“Capacidade de conduzir pronta, sustentada e sincronizadamente, operações com forças adaptadas a situações específicas, com acesso e liberdade para operar em todos domínios – terra, mar, ar, espaço e **informação**”.*

\* [strategicstudiesinstitute.army.mil/pubs/parameters/Articles/1992/1992%20mann.pdf](http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/1992/1992%20mann.pdf)

\*\* [en.wikipedia.org/wiki/Full-spectrum\\_dominance](http://en.wikipedia.org/wiki/Full-spectrum_dominance)

# Tecnologia política

- **Guerra neocortical:** Richard Szafranski: “*Neocortical warfare? The acme of skill* \*”, 1994 (Rand Corporation)



*"Busca controlar ou moldar o comportamento dos organismos inimigos, mas sem destruí-los, influenciando a consciência, percepções e vontade dos agentes. Tenta delimitar o **espaço cognitivo** de suas lideranças a uma estreita ou desorientadora gama de avaliações e cálculos comportamentais. Influenciar líderes para não lutar (ou para lutarem entre si) é fundamental."*

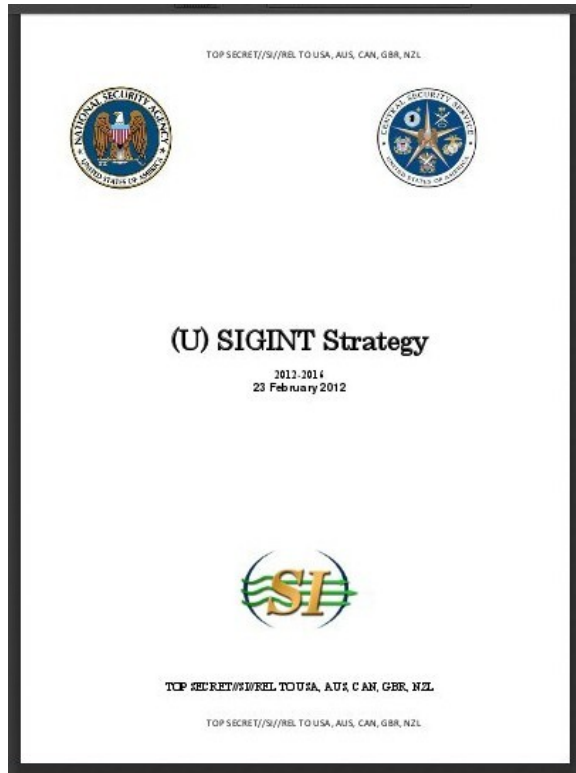
- **Guerras não-convencionais**  
**Netwar:** Arquilla & Ronfeldt “*The advent of netwar*\*\*”, 1996 (Rand C)  
Gerenciamento de percepção coletiva e engenharia do consentimento “internetizados”, escaláveis de cadeias de comando para *hubs* e malhas. Operações focadas em “efeitos enxame” com fins desestabilizadores.

\* [www.rand.org/content/dam/rand/pubs/monograph\\_reports/MR880/MR880.ch17.pdf](http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR880/MR880.ch17.pdf)

\*\* [www.rand.org/pubs/monograph\\_reports/MR789.html](http://www.rand.org/pubs/monograph_reports/MR789.html)

# Netwar na agenda unipolar

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



<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 indiretos.*"

"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.*"

# para controle da infraestrutura digital

## The Digital Infrastructure

- ◆ IT and Payment Systems Run by Private Corporations
- ◆ Non-Transparent Contracting Budgets
- ◆ Destruction and Suppression of Place Based Financial Systems
- ◆ Centralized Clearance, Payments and Wire Systems
- ◆ Integration of NSA into the Telecommunications Backbone
- ◆ Globalized Satellite Systems
- ◆ The Patriot Act
- ◆ Smart Phones, Cell Towers and the “Internet of Things”



*“quem controlar as vias digitais, os cabos submarinos e canais satelitais, controlará a moeda global. O que tem requerido cada vez mais violência.”*

– **Catherine Austin-Fitts:** (junho 2014) O cerne da “guerra na internet” é pela centralização do controle de sistemas e fluxos de pagamentos: O colapso controlado do dólar, e a ascensão de outra moeda para reserva de valor e no comércio global (SDR?, yuan?) dependem desse controle:

*“quem controlar as vias digitais, os cabos submarinos e canais satelitais, controlará a moeda global. O que tem requerido cada vez mais violência.”*

# A eficiência combina com segurança?

Maior centro de operações financeiras do mundo



**2008**

UBS *trading floor* nos EUA

**2016**

Em menos de dez anos, quase todas as mesas de câmbio operadas por corretores foram substituídas por software (*algorithm trading, HFT*)

[www.zerohedge.com/news/2016-09-01/transformation-wall-street-just-two-photos-ubs-trading-floor-2008-and-2016](http://www.zerohedge.com/news/2016-09-01/transformation-wall-street-just-two-photos-ubs-trading-floor-2008-and-2016)

# Eficiência + segurança? Depende...

Maior centro financeiro do mundo admite avalanche de fraudes



SegInfo - Portal, Podcast e Evento sobre Segurança da Informação

SETEMBRO 26, 2016

Reino Unido sofreu “uma fraude financeira a cada 15 segundos” no 1º semestre de 2016



Mais de 1 milhão de incidentes de fraude financeira foram registrados no Reino Unido no primeiro semestre de 2016 segundo o FFA - UK (*Financial Fraud Action*), órgão dos bancos e empresas de pagamento

<https://seginfo.com.br/2016/09/26/reino-unido-sofreu-uma-fraude-financeira-a-cada-15-segundos-no-primeiro-semester-de-2016>



# Eficiência + segurança? Depende...



O programador Sergey Aleynikov foi acusado de “roubar” código de software da Goldman Sachs quando deixou a empresa em julho de 2009. Preso em 48 horas, o FBI e promotores guardaram o código confiscado como se fosse em *Fort Knox*.

Goldman alega que o software poderia ser usado para "**manipular** o mercado de forma desleal."

Mas o que exatamente a Goldman faz com o sw? E por que o governo dos EUA está protegendo esse software em vez de analisá-lo para determinar como pode ser usado para manipular mercados?

O software é para HFT (*High Frequency Trading*), técnica com a qual a *Virtu Financing* só teve 1 dia com perdas em 6 anos de operação. Durante o 1º julgamento (em que o réu foi condenado, cumprindo pena enquanto aguarda sentença do 2º), os promotores americanos pediram sessão secreta ao juiz quando detalhes sensíveis do software de HFT fossem discutidos.

<http://investmentwatchblog.com/goldman-the-government-and-the-aleynikov-code/>  
[www.zerohedge.com/news/2015-08-13/project-omega-why-hfts-never-lose-money-criminal-fraud-explained](http://www.zerohedge.com/news/2015-08-13/project-omega-why-hfts-never-lose-money-criminal-fraud-explained)

# Eficiência + segurança? Depende...



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 “desleais” 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, BCE, e bancos *too-big-to-(j)fail*, mesmo pela sobrevida do dólar, pode provocar ruptura e crise monetária.

# Eficiência + segurança? Depende...

GS [www.bloomberg.com/news/articles/2015-08-31/currency-probe-by-u-s-said-to-expand-to-russia-brazil-trades](http://www.bloomberg.com/news/articles/2015-08-31/currency-probe-by-u-s-said-to-expand-to-russia-brazil-trades)

BloombergBusiness 1

News

Markets

Insights

Video

## U.S. Currency Probe Expands to Russia, Brazil Trades

by Tom Schoenberg and Silla Brush

U.S. prosecutors have expanded their probe of currency-market manipulation by some of the world's largest banks to include the Russian ruble and Brazilian real, according to two people familiar with the matter.

Prosecutors are relying on information provided by banks that resolved the currency probe in May, according to the people. The banks -- Citigroup Inc., Barclays Plc, UBS Group AG, Royal Bank of Scotland Group Plc and JPMorgan Chase & Co. -- all have immunity from additional prosecution from the currency probe as long as they cooperate with investigators

Manipulação de mercados de câmbio por bancos que são compradores diretos (*primary dealers*) do BC do Brasil empurram a taxa Selic para níveis extorsivos, inexplicáveis como somente *spread* de risco

# Instrumentalização das tecnopolíticas

Perfilamento psicológico (*profiling*), rastreamento e direcionamento cognitivo em projetos de engenharia social são municiados por, e minerados em, redes sociais centralizadas, e podem operar nas mesmas.

Anonimato e pseudonimato neutralizáveis por agregação massiva de dados pessoais biometrízáveis - NGI (*New Generation Identification*)

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

HOME ABOUT AXIOM ON RADIO-LISTENING INFO AXIOM'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.

# Instrumentalização das tecnopolíticas

Alvos de *drones* selecionados sem identificação pessoal, apenas por padrão de comportamento minerado no vigilantismo (NGI), em situações onde a guerra não-convencional ganha intensidade psicológica

rt.com/usa/cia-drone-strikes-unknown-targets-293

## Classified documents reveal CIA drone strikes often killed unknown people

Published time: June 06, 2013 03:36

Edited time: June 07, 2013 05:47

A review of classified US intelligence records has revealed that the CIA could not confirm the identity of about a quarter of the people killed by drone strikes in Pakistan from 2010 to 2011.

One key term in analyzing drone strike records are what are known as "*signature*" strikes, when drones kill suspects based on behavior patterns but without positive identification, versus "*personality*" strike. One former senior intelligence official said that at the height of the drone program in Pakistan in 2009 and 2010, as many as half of the strikes were classified as signature strikes.



Northrop Grumman / Chad Slattery / Handout via Reuters

# Instrumentalização das tecnopolíticas

NGI do FBI, Pentágono, outras agências de tres letras, mais o Complexo industrial-militar dos EUA, instrumentam a ideologia excepcionalista para consolidação de um regime hegemônico global (NWO).

Projeto globalista dos Bilderbergers, PNAC, Illuminati, etc para NWO.  
(*New World Order*)



## Facebook & Google are CIA Fronts



February 16, 2011

In the case of Google and Facebook, three talented students in their 20's came out of obscurity to establish multi-billion dollar enterprises. Do you suppose they had some help?

**BY SANDEEP PARWAGA**  
(FOR HENRYMAKOW.COM)

nzance.blogspot.com.br/2011/04/fbi-launches-1-billion-biometrics.

MONDAY, 4 APRIL 2011

## FBI Launches 1 Billion \$ Biometrics Project With Lockheed Martin

The FBI launched this week a massive program aimed to record all citizen's biometrics data. This will eventually enable instant surveillance and recognition of any individual walking on the street or entering a building. The 1 Billion \$ deal was awarded to Lockheed Martin - world's largest defence company, who is part of elite groups such as the CFR (Council of Foreign Relations) and the Trilateral Commission. In short, Lockheed Martin is the official defence company of the world's shadow government.

LOCKHEED MARTIN



[rt.com/usa/169848-pentagon-facebook-study-minerva](http://rt.com/usa/169848-pentagon-facebook-study-minerva)

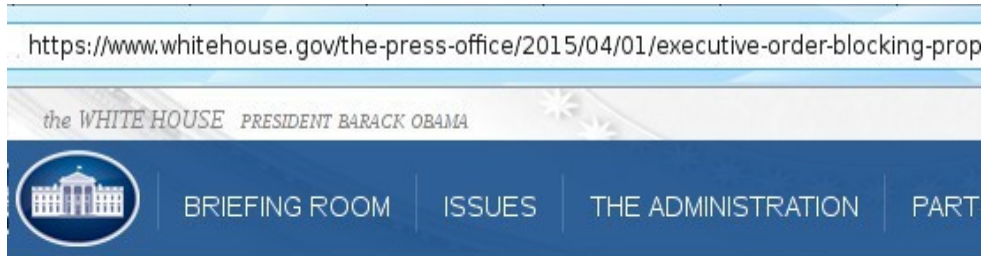
[henrymakow.com/social\\_networking\\_dupes\\_the\\_ma.html](http://henrymakow.com/social_networking_dupes_the_ma.html)

[vigilantcitizen.com/latestnews/fbi-launches-1-billion-biometrics-project-with-lockheed-martin](http://vigilantcitizen.com/latestnews/fbi-launches-1-billion-biometrics-project-with-lockheed-martin)

# **Algumas reflexões**

Sobre o momento histórico que estamos vivendo

# Há um verniz normativo para a NWO



The White House  
Office of the Press Secretary

For Immediate Release

April 01, 2015

## Executive Order -- "Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"

EXECUTIVE ORDER

externa e economia dos EUA, e para lidar com esta ameaça declara:

### *Emergência Nacional*

*Seção 1. (a) Todos os bens e interesses próprios de tais pessoas que estão ou que vierem para os EUA, ou que vierem a estar sob controle de terceiros nos EUA, estão bloqueados e não podem ser transferidos, pagos, exportados, retirados, ou de qualquer modo trocados ...*

**EO 1/4/2015:** O Presidente dos EUA acha que o aumento das atividades cibernéticas maliciosas provenientes ou dirigidas por pessoas localizadas fora dos EUA constituem ameaça incomum para a segurança nacional, política



# Há também uma convergência ideológica



Congressman Grayson tweets:

Ex-NSA chief Keith Alexander wants to form a joint WH-bank war council. So now Wall Street gets to declare war?

## BIG BANKS WANT POWER TO DECLARE CYBER WAR

Published: July 9, 2014

Bloomberg reports:

### MERGER OF BIG BANKS AND NATIONAL SECURITY POWER ... WHAT COULD POSSIBLY GO WRONG?

Wall Street's biggest trade group has proposed a government-industry cyber war council to stave off terrorist attacks that could trigger financial panic by temporarily wiping out account balances, according to an internal document.

The proposal by the Securities Industry and Financial Markets Association, known Sifma, calls for a committee of executives and deputy-level representatives from at least eight U.S. agencies including the Treasury Department, the National Security Agency and the Department of Homeland Security, all led by a senior White House official.



Um conselho de guerra híbrida formado pela Casa Branca e os maiores bancos do mundo – como quer ex-diretor da NSA – consolidaria o fascismo (na definição de Mussolini) como forma do regime hegemônico global

# Verniz normativo que cola por medo difuso



ONU, 15/9/2015: “Agenda 21”  
foi estendida para Agenda 2030.

Sob a meta de “desenvolvimento  
sustentável”, o item 16.9 projeta  
para 2030 “**identificação univer-  
sal biométrica**” para todos os ha-  
bitantes da Terra. Com base de

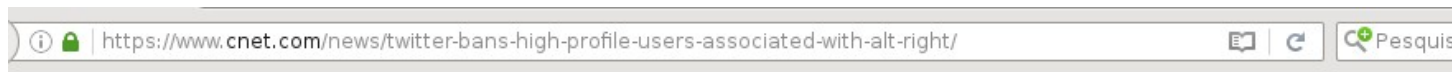
dados, o procedimento  
de identificação será iniciado  
pelos atuais refugiados de guerra.

[www.thenewamerican.com/tech/  
computers/item/21914-globalists-  
and-un-push-mandatory-biometric  
-id-for-all](http://www.thenewamerican.com/tech/computers/item/21914-globalists-and-un-push-mandatory-biometric-id-for-all)

[www.youtube.com/watch?  
v=1r7\\_wlzlauA](http://www.youtube.com/watch?v=1r7_wlzlauA)



# Twitter bane ativistas que têm ligações com a direita alternativa



CNET > Digital Media > Twitter bans high-profile users with alt-right ties

## Twitter bans high-profile users with alt-right ties

The social media network recently said it would crack down on online abuse, and white nationalists who spread hatred are on its list.



<https://www.cnet.com/news/twitter-bans-high-profile-users-associated-with-alt-right/>

# Facebook revela plano de sete pontos para erradicar “notícias falsificadas”



**19/11/2016:**

- 1- *Improve our ability to classify misinformation;*
- 2- *Make it much easier for people to report stories as fake;*
- 3- *Third party verification;*
- 4- *Label stories flagged as false;*
- 5- *Raise the bar for stories linked in News Feed;*
- 6- *Disrupt fake news economics with advertising policies;*
- 7- *Continue to work with journalists and others in the news industry to get their input, in particular to understand their fact checking systems.*

<http://www.zerohedge.com/news/2016-11-19/facebooks-zuckerberg-reveals-7-point-plan-eradicate-misinformation>

# Concluindo:

A Tecnologia Política aqui exposta faz uso de um arsenal semio-lógico que é essencial para o atual estado de guerra (híbrida), cujo objetivo é a instalação de um governo totalitário global, e cujos adversários são toda forma de resistência em favor do multilateralismo.

- *“Um Estado totalitário realmente eficiente seria um no qual os todo-poderosos mandantes da política e seus exércitos de executivos controlam uma população de escravizados que não precisam ser coagidos, porque eles adoram a sua servidão.”*  
Aldous Huxley, em “Admirável Mundo Novo”
- *“Excelência suprema consiste em quebrar a resistência do inimigo sem lutar.”* Sun Tsu, em “A Arte da Guerra”

## Concluindo:

A Tecnologia Política aqui exposta faz uso de um arsenal semio-lógico que é essencial para o atual estado de guerra (híbrida), cujo objetivo é a instalação de um governo totalitário global, e cujos adversários são toda forma de resistência em favor do multilateralismo.

- *“Um Estado totalitário realmente eficiente seria um no qual os todo-poderosos mandantes da política e seus exércitos de executivos controlam uma população de escravizados que não precisam ser coagidos, porque eles adoram a sua servidão.”*

Aldous Huxley, em “Admirável Mundo Novo”

- *“Excelência suprema consiste em quebrar a resistência do inimigo sem lutar.”* Sun Tsu, em “A Arte da Guerra”

---

*“E então será revelado o iníquo, a quem o Senhor Jesus matará como o sopro de sua boca, e destruirá com a manifesta-ção da sua vinda; ... por isso Deus lhes envia a operação do erro, para que creiam na mentira,”* Apóstolo Paulo, em **2Ts 2:8,11**