

Ciberguerra ou Contrarrevolução digital?

ENSOL 2011 – João Pessoa, PB

Pedro A. D. Rezende
Ciência da Computação
Universidade de Brasília

www.pedro.jmrezende.com.br/sd.php

Ciberguerra ou Contrarrevolução digital?

1- Contexto

Processo, Conjuntura, Panorama, Estratégias

2- Ciberguerra declarada

Retórica, Rumores, Posturas

3- Quem, contra que(m), como, por que?

Como as peças vão se encaixando...

“This is for real”

1. Contexto

(como chegamos a isso)

1. Processo

- *As transições sociotécnicas* produzidas pela revolução digital alteram relações de poder, em favor dos que controlam novos fluxos informacionais (que abastecem o saber, que distribuem a produção, etc), através de comunicação e agregação mais ágeis.
- Esse controle se sustenta não só com domínio das tecnologias, mas principalmente, com domínio do **processo normativo** que regula os usos das TIC (e por meio destas, de outras tecnologias também). Poderes (políticos e econômicos) já consolidados reagem a isso.

1. Processo

- Essa **conjuntura** transforma o *processo político*, onde os papéis e as ações estratégicas dos principais agentes – Estados centrais e grandes corporações – sofrem profundas transformações.
- Essas transformações são induzidas por mudanças nas fronteiras de maior eficiência entre cooperação e competição.
- Essa mudança de fronteiras se reflete na viabilidade do Software Livre, mas não só ...

REFLETE-SE **TAMBÉM** NAS FRONTEIRAS:

- ENTRE ESTADO E CORPORAÇÕES;
- ENTRE OS 3 PODERES DO ESTADO DEMOCRÁTICO.

1. Conjuntura

- Uma percepção limitada desta *conjuntura histórica*, e do que nela está em jogo, produz distopias, como por exemplo:

A crença de que a inovação tecnológica é um bem comum e cumulativo + a crença de que a atual crise econômica sinaliza esgotamento do neoliberalismo (ou desta versão de capitalismo).

- Nesta análise, tal crise representa um **panorama de oportunidades** para ofensivas unilateralistas, nas quais interesses hegemônico-monopolistas convergem para controlar regimes de uso de tecnologias "em nome do interesse público" (ver Naomi Klein: "*The Shock Doctrine*")

1. Panorama

- Iniciativas recentes para negociação de tratados (globais ou não), supostamente justificados por “vazios normativos” causados pela disseminação de TICs, seguem uma **linha estratégica** de crescente radicalização e severidade, do *Broadcast treaty*, à Convenção de Budapeste, ao ACTA (*Anti-Counterfeiting Trade Agreement*).
- O Brasil não participou, nem participa, da negociação dos dois últimos, mas sofre pressões crescentes para aderir ao Tratado de Budapeste (Azeredo), contra seu princípio diplomático de não aderir a tratados de cuja negociação não tenha participado. Já o panorama do ACTA é mais insidioso e abrangente.

1. Estratégias

- Essa linha estratégica busca criar instrumentos cada vez mais poderosos para combater certas práticas de uso de Tecnologias, muitas já tipificadas como crime, enquanto *ofuscam* a lógica que molda a definição de novos tipos criminais e de novos ritos processuais, seus efeitos colaterais e as possíveis interações entre esses, e a lógica de convergência com interesses político-militares
- O que esta análise revela, em perspectiva, é uma escalada de progressivo **cercamento normativo** que leva à *catraquização* do ciberespaço. Cabe então investigar quais interesses estão sendo contemplados e quais cerceados nesse processo **neocolonialista**.

1. Estratégias: cerco normativo



1. Estratégias: neocolonialismo

Forum shifting: TRIPS(+), *Broadcast*, Budapeste, rumo ao...

ACTA: Tratativas secretas, depois herméticas, depois hipócritas.

“Pontes de PI”: As pontes estão sendo lançadas e cruzadas

Caso MS vs. TomTom (2010): ataque frontal ao Linux (FAT);

Googlizon (2010), MS+Skype (2011): Começo do fim (FCC?)

da neutralidade da Rede e do isolamento intercamadas do TCP/IP

Cavalos de Tróia da PI e Erosão do Direito:

Patentes esotéricas, DRM, UPOV e outras sandices a reboque do direito autoral e do direito de marcas. (ACTA, etc)

Ciberguerra: “*Code is law*” ... *and weapon* (Hydraq, Stuxnet, etc.)

1. Estratégias: *Forum shifting*

- Interesses monopolistas encastelados ou convergentes na estratégia da proprietarização do conhecimento promovem iniciativas de radicalização normativa em várias instâncias e fóruns transnacionais: OMC (TRIPS), OMPI, UE, ALCA, etc.
- Quanto uma iniciativa é neutralizada, por ações organizadas na periferia do capitalismo, eles migram e se reagrupam, capturando ou fundando outras instâncias ou fóruns, mais extremistas:
- Entre 2007-09: OMPI → TRIPS+ (Patentes)
OMPI → UE (Broadcast); OMPI → ACTA (secreto, a convite);
- 2010-11: ACTA → TPP, Bilaterais; UE, US (para aprovação)

1. Estratégias: *Forum shifting*

- Em 14/02/2011, 18 Deputados dos EUA enviaram uma carta ao presidente Obama exigindo um capítulo sobre PI “de alto padrão” no TPP (*Trans Pacific Partnership*). Na carta, os signatários afirmam: “o TPP apresenta uma oportunidade para estabelecer 'proteção à PI para o século XXI' que pode **servir de molde para futuros Tratados Internacionais de Comércio**” (FTAs). Eles também pedem que a ambição de concluir o tratado até novembro de 2011 “não seja perseguido às custas de um 'forte acordo com um capítulo moderno sobre PI' – um que **abra novos mercados** para empresas americanas na economia atual baseada em conhecimento.”

www.ip-watch.org/weblog/2011/03/16/

1. Estratégias: Cavalos de Tróia da PI

Vazado em Mar 2011: A escalada na proposta do TPP inclui tudo que o USTR não conseguiu forçar no ACTA, e mais:

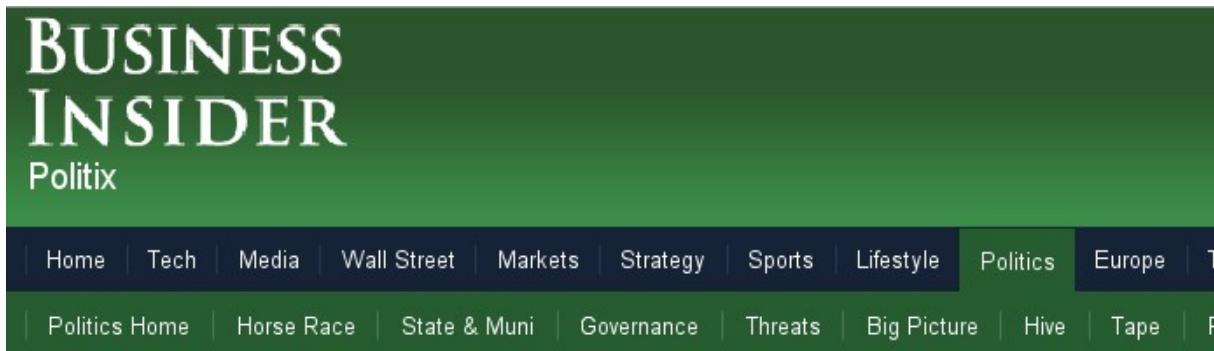
- Dispositivos gerais incluem uma lista de outros tratados que os países signatários do TPP teriam que antes também aderir.
- Critérios de patenteabilidade: países signatários perdem autonomia sobre exclusões e exceções (só com “razoabilidade”)
- “Alta proteção” para software e outros materiais protegidos por copyright, incluindo regras para “aquisição e gerência de software e outros materiais para uso governamental.”

ip-watch.org/weblog/2011/03/16/michaelgeist.ca/content/view/5686/99999

2. Ciberguerra declarada

(como vem sendo)

2. Retórica



Pentagon Says It Will Respond To Cyber Attacks With Military Force

Grace Wyler | May 31, 2011, 6:13 PM | 🔥 830 | 💬 3

 Tweet 112  Email A A A

The Pentagon is in the final stages of drafting its first cyber warfare strategy, which considers cyber attacks an act of war and allows the U.S. to respond with traditional military force, according to the Wall Street Journal.



2. Retórica

guardian government computing

Information management in public services

Government plans cyber weapons programme

Cabinet Office and GCHQ lead on developing offensive cyber capability

Guardian Government Computing
Guardian Professional, Tuesday 31 May 2011 10.38 BST
[Article history](#)

Whitehall officials have revealed to the Guardian that work has begun on a range of offensive cyber weapons to add to its defensive capability.

It is understood that the Cabinet Office and the Cyber Security Operations Centre at GCHQ have taken the lead on the issue, and that in time there will be some input from the Ministry of Defence.

The MoD recently appointed General Jonathan Shaw from the Parachute Regiment to head a defence cyber-operations group. He told the Guardian cyberspace represented "conflict without borders".

The armed forces minister, Nick Harvey, told the Guardian that "action in cyberspace will form part of the future battlefield", and that he now

 Tweet 67

 Share

 reddit this



A larger | smaller

Guardian Government Computing

National security · Central government · Information security

More news

[UK to exchange intra-EU air passenger data](#)
Immigration minister says coalition has signed up to European directive on sharing

2. Retórica

31 Mai 11 - MoD: "...Do Ministro da Defesa da Grã Bretanha, Nick Harvey, ao Guardian: "ações no ciberespaço farão parte do teatro de guerras futuras". Hoje as armas cibernéticas devem ser "parte integral do armamento de um país". "Precisamos de um ferramental dessa capacidade, e a estamos desenvolvendo" disse. "As circunstâncias e maneiras em que usaremos essas armas são geralmente análogas ao que faríamos com qualquer armamento convencional", e acrescentou: "As regras e a lógica [de combate] se traduzem para o ciberespaço".

"Com as nucleares ou biológicas, a habilidade técnica necessária [para operar as armas] é alta. Com as cibernéticas, o dedo sobre o botão pode ser qualquer um, de um Estado a um *estudante*".

2. Retórica

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

Tweet

Share this

Email

Print

Related News

Washington weighs security after "serious" Google allegation

Thu, Jun 2 2011

Cyber attacks run risk of wider instability

Thu, Jun 2 2011

Cybersecurity becoming U.S. diplomatic priority

Thu, Jun 2 2011

Google reveals Gmail

2. Retórica

3 Jun 11 - 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..."

“Recentemente, um furacão varreu a Internet pelo mundo ... Os alvos da guerra psicológica na Internet se expandiram da esfera militar para a esfera pública... Confrontadas com [isso], nenhuma nação ou força armada pode ficar passiva e está se preparando para lutar a guerra da Internet.".

2. Rumores

BBC Mobile News | Sport | Weather | Travel | TV

NEWS US & CANADA

Home | UK | Africa | Asia-Pac | Europe | Latin America | Mid-East | South Asia | **US & Canada** | Business | Health

30 May 2011 Last updated at 11:07 GMT

[digg](#) [f](#) [stumbleupon](#) [t](#) [email](#) [print](#)

US defence firm Lockheed Martin hit by cyber-attack

US defence firm Lockheed Martin says it has come under a significant cyber-attack, which took place last week.

Few details were available, but Lockheed said its security team had detected the threat quickly and ensured that none of its programmes had been compromised.

The Pentagon said it is working to establish the extent of the breach.

Lockheed makes fighter jets, warships and multi-billion dollar weapons systems sold worldwide.

Lt Col April Cunningham, speaking for the US defence department, said the impact on the Pentagon was "minimal and we don't expect any adverse effect".



Lockheed Martin makes F-16 fighter

bbc.co.uk/news/world-us-canada-13587785

2. Rumores



Search Threatpost



Friday, July 22nd, 2011

The Kaspersky Lab Security News Service

Home

Topics

Blogs

Multimedia

Reso

Home › Data Breaches ›

April 1, 2011, 9:25PM

RSA: SecurID Attack Was Phishing Via an Excel Spreadsheet

by Dennis Fisher

Share



21 Comments

Excel flash RSA confirmed on Friday that the attack that compromised the company's high-value SecurID product was essentially a small, targeted phishing campaign that included a payload of a malicious Flash object embedded in an Excel file.

The much-discussed [attack on RSA](#), which the company revealed last month, resulted in the company warning customers that the security of their SecurID authentication tokens may be reduced. Speculation about the exact nature of the attack has been rampant in the security community ever since the disclosure, and RSA has been quite tight-lipped about the details of the incident.

But on Friday the company briefed analysts about the details of the attack and then published a series of explanatory blog posts that spilled some, but not all, of the specifics about the incident.

threatpost.com/en_us/blogs/rsa-securid-attack-was-phishing-excel-spreadsheet-040111

2. Posturas



Matéria de capa do jornal Valor Econômico de 14 de junho de 2011

2. Posturas

Moacir Drska e Gustavo Brigatto

De São Paulo

O governo brasileiro começou a colocar em prática medidas para proteger o país no ciberespaço. As ações, que já vinham sendo planejadas há mais de um ano, ganharam corpo em meio à recente escalada dos ataques de hackers a redes públicas, empresas privadas e organismos internacionais, como o FMI.

Na prática, o tema assume contornos de segurança nacional. As medidas de proteção serão coordenadas pelo Centro de Defesa Cibernética (CDCiber), uma unidade subordinada ao Exército cuja função é integrar as ações defensivas e de contra-ataque das Forças Armadas. Concebido em 2010, o CDCiber tem previsão de entrar em funcionamento efetivo no próximo semestre.

visam o roubo de informações estratégicas são o principal ponto de atenção, apesar de representar apenas 1% das ameaças. “Registramos 2,1 mil tentativas de invasão por hora. Quanto mais se destaca no cenário internacional, mais o Brasil desperta o interesse dos hackers”, afirma Mandarino.

É a ascensão de um novo tipo de hacker — diferente das gangues em busca de lucro com fraudes — que está preocupando os governos. Trata-se do chamado hacker ativista, que tem supostas aspirações ideológicas. Cresce também o risco de invasões patrocinadas por outros Estados e grupos terroristas. Há duas semanas, o governo dos Estados Unidos equiparou as ameaças digitais aos ataques com armas convencionais, abrindo a possibilidade de uma resposta militar. **Página B3**

Interesse dos “hackers”? Não seria das grandes potências?

[Textos selecionados da matéria de capa, primeira página](#)

2. Posturas

No início de junho, a Organização do Tratado do Atlântico Norte (Otan) divulgou um relatório sobre a possível extensão desses ataques a novas fronteiras. Para a Otan, “o surgimento de ativistas hackers pode levar a uma nova classe de conflitos internacionais entre esses grupos e nações, ou mesmo a conflitos entre entidades exclusivamente virtuais”.

A Otan observa que pelo que se sabe, grupos terroristas como a Al Qaeda ainda não têm a capacidade de executar ataques cibernéticos, mas que no futuro, o crime organizado e grupos de hackers podem vir a vender seus serviços a essas organizações terroristas.

Contexto

Formados por indivíduos com amplos conhecimentos sobre computadores e segurança da informação, os grupos de ativistas hackers declaram-se defensores de causas como a liberdade de expressão na internet. A militância ocorre por meio das redes sociais. Usando blogs e sites como Facebook e Twitter, eles divulgam suas ideias e recrutam colaboradores. Para se manifestar contra quem os desagrada, atacam sites e redes de computadores. Um dos

casos de maior repercussão é o do ataque aos serviços on-line da Sony. A ação foi uma resposta à decisão da companhia de processar um hacker que driblara o sistema de segurança do console PlayStation 3, permitindo o uso de jogos piratas. Em dezembro, o grupo Anonymous ficou conhecido por promover uma série de ataques que tiraram do ar os sites da Visa e da Mastercard. O motivo foi a decisão das companhias de não fornecer mais seus sistemas de pagamento ao WikiLeaks.

Somos nós?

2. Posturas

GEOPOLITICS - GEOECONOMICS

F WILLIAM ENGDahl



F W ENGDahl

GEOPOLITICS / EURASIA

CHINA GAUNTLET

PUTIN'S GAS

PRICING THE RISK

IRAN OIL BOURSE

NIGHTMARE

OUFLANKED

COLOR REVOLUTIONS

RUSSIAN GIANT

PUTIN

OIL IN AFRICA

PEAK OIL & RUSSIA

MYANMAR

KOSOVO

SINCE KENNAN

MEDVEDEV

CAUCASUS WAR

SAAKASHVILI

CORRECTION

AFRI.COM

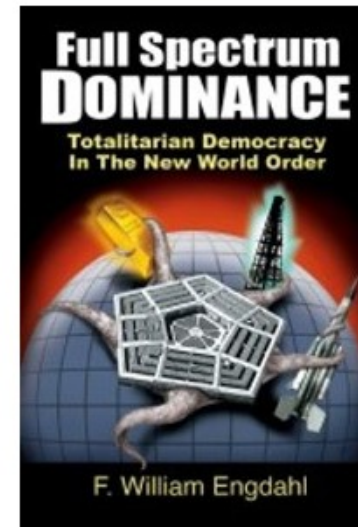
NATO ENTRY

Wikileaks -- a Big Dangerous US Government Con Job

By F. William Engdahl, 7 December 2010

The story on the surface makes for a script for a new Oliver Stone Hollywood thriller. A 39-year old Australian hacker holds the President of the United States and his State Department hostage to a gigantic cyber "leak," unless the President leaves Julian Assange and his Wikileaks free to release hundreds of thousands of pages of sensitive US Government memos. A closer look at the details, so far carefully leaked by the most ultra-establishment of international media such as the New York Times, reveals a clear agenda. That agenda coincidentally serves to buttress the agenda of US geopolitics around the world from Iran to Russia to North Korea. The Wikileaks is a big and dangerous US intelligence Con Job which will likely be used to police the Internet.

It is almost too perfectly-scripted to be true. A discontented 22-year old US Army soldier on duty in Baghdad, Bradley Manning, a low-grade US Army intelligence analyst, described as a loner, a gay in the military, a disgruntled "computer geek," sifts through classified information at Forward Operating Base Hammer. He decides to secretly download US

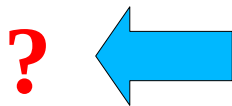


3.

**Quem, contra que(m),
como, por que?**

(as peças vão se encaixando ...)

3. Porque ...



... deve haver um Governo Global, acima da soberania do Estado-Nação

3. Como

Out 2010 – Análise (KEI) revela: discussões entre autoridades dos EUA sugerem que o USTR acredita que poderá ignorar dispositivos explícitos do ACTA com base no Artigo 1.2:

*"Each Party shall be free to determine the **appropriate** method of implementing the provisions of this Agreement within its own legal system and practice.* keionline.org/node/990

15 Nov 2010 – Texto da proposta é divulgado (pendendo ajustes finais, na 12ª rodada). Dez dias depois o Parlamento Europeu aprova, por 331 a 294, resolução de “suporte geral” à proposta.

- **06 Dez 2010** – Texto final da proposta é divulgado (após 12ª rodada) www.dfat.gov.au/trade/acta.

3. Como

Fev 2011 – Wikileaks: Telegramas sobre o ACTA: **Objetivos**
laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history

“Padrão ouro” para “PI global”...[Um oficial dos EUA abordou os japoneses]... Um dos principais objetivos é dar a volta por cima dos organismos internacionais em cargo da propriedade imaterial (WIPO, WTO, OECD, etc), onde países “maximalistas” (extremistas) como EUA e UE têm enfrentado crescente oposição de países em desenvolvimento. De início os Japoneses propuseram pedir ajuda à OECD, mas os agentes dos EUA insistiram num processo diferente, alegando terem *expertise* suficiente e exigindo que fosse evitada qualquer colaboração de organização internacional. **Prioridade máxima:** Adoção rápida de um acordo extremista porém exportável.

3. Como

Fev 2011 – Wikileaks: Telegramas sobre o ACTA: **México**
laquadrature.net/en/wikileaks-cables-shine-light-on-acta-history

Uma preocupação central é a de que o ACTA parecesse ser o que de fato é – um acordo costurado por países ricos, para ser imposto a países em desenvolvimento. Autoridades mexicanas estavam especialmente interessadas em ajudar nesse *front*. Num encontro com oficiais dos EUA, os mexicanos destacaram sua disposição em “aderir às tratativas (do ACTA) para contrabalançar os esforços do Brasil em 'minar direitos de PI' em organizações internacionais” Os mexicanos denunciaram o esforço do Brasil em favor de posições progressistas em fóruns internacionais, e se ofereceram para posar de 'bom mocinho' agindo em conjunto com os EUA em prol de padrões maximalistas globais na área de patentes e direito autoral.

3. Como

5 Mar 2011 – USTR Divulga: **Relatório “Special 301”**

ipbrief.net/2011/05/07/ustr-publishes-the-2011-special-301-report/

Depois de examinar 77 países, 12 foram incluídos na lista *Priority Watch List*, e 22 na *Watch List*. A maioria dos países que aparecem no “Special 301” deste ano tem sido frequentadores regulares em versões anteriores. Pela primeira vez, o USTR **convida esses países para “negociar um plano de ação mutuamente acordado”** que poderia eventualmente retirá-los de relatórios futuros. Para isso o USTR incluiu uma breve seção sobre “melhores práticas” na qual destaca:

- 1) “Cooperação melhorada e engajamento de interessados (*stakeholders*) em mudanças legislativas e regulatórias”;
- 2) “Esforços para atacar novos desafios na proteção da PI e na execução de sanções”;
- 3) “Ativa construção de capacidades.”

3. Como assim?

(Vazado em mar 2011) - Ago 2008, DHS para USTR: “ACTA é ameaça à Segurança Nacional dos EUA” keionline.org/print/1117

A seção “*Border Measures*” do ACTA pode ser interpretada como retirando autoridade da *Customs and Border Protection* (CBP) e protegendo titulares de direitos contra ressarcimentos de custas incorridas em seu benefício. O ACTA consumiria boa vontade internacional ao requerer de outros governos que mudem seus sistemas e práticas legais. Isso pode encorajar autoridades alfandegárias a bloquear importações e exportações se eles decidirem por conta própria que certo bem viola algum copyright ou confunde alguma marca. Isso lhes dá poder excessivo para agir contra suspeitos de violação de PI, e esse poder pode ser facilmente abusado. Esses abusos podem até prejudicar exportadores nos EUA, que competem com fornecedores

3. Contra quem?

Nov 2010 – ICE para visitantes web: “**Este site foi apreendido**”
torrentfreak.com/u-s-government-seizes-bittorrent-search-engine-domain-and-more

O braço investigativo do *Department of Homeland Security* parece estar fechando websites que “facilitam” violações de direito autoral. O *Immigration and Customs Enforcement* (ICE) apreendeu dezenas de nomes de domínio nos últimos dias, de acordo com o TorrentFreak. Os sites são substituídos por uma nota dizendo: "*This domain named has been seized by ICE, Homeland Security Investigations.*" O dono de um dos sites 'apreendidos' disse à TorrentFreak que seu site (nome de domínio) foi bloqueado sem nenhum aviso ou advertência prévia.

Entre os sites 'apreendidos', há também um site de esportes na Espanha considerado legal lá. allheadlinenews.com/briefs/articles/90032944

3. Contra quem?

Abr 2011 – Lawyer to bittorrent user: **“Stop uploading Debian”**
lists.debian.org/debian-legal/2011/04/msg00054.html

A lawyer from Augsburg, Germany sent a "Abmahnung" (cease & desist letter) to a person which downloaded Debian using Bittorrent. The company "Media Art Holland b.v" claimed to have the "Nutzungs und Verwertungsrechte" (something like distribution rights). The lawyer wants the poster to pay 700 Euro and stop uploading of Debian.

– “This behavior is not good for Debian's reputation and the project should take legal action against the lawyer and this company”

3. Contra quem?

Abr 2011 – Lawyer to bittorrent user: “**Stop uploading Debian**”
lists.debian.org/debian-legal/2011/04/msg00054.html

A lawyer from Augsburg, Germany sent a "Abmahnung" (cease & desist letter) to a person which downloaded Debian using Bittorrent. The company "Media Art Holland b.v" claimed to have the "Nutzungs und Verwertungsrechte" (something like distribution rights). The lawyer wants the poster to pay 700 Euro and stop uploading of Debian.

– “This behavior is not good for Debian's reputation and the project should take legal action against the lawyer and this company”

– “Please be aware that this turned out to be a bad joke. As far as I've read the thread, it was an ex-boyfriend who justed wanted to scare the user. He later called her, after finding this thread together with the information that she filed a charge against him, and apologized.”.

3. Contra quem:



2 x 1 = 2	3 x 1 = 3	4 x 1 = 4	5 x 1 = 5	6 x 1 = 6	7 x 1 = 7	8 x 1 = 8	9 x 1 = 9
2 x 2 = 4	3 x 2 = 6	4 x 2 = 8	5 x 2 = 10	6 x 2 = 12	7 x 2 = 14	8 x 2 = 16	9 x 2 = 18
2 x 3 = 6	3 x 3 = 9	4 x 3 = 12	5 x 3 = 15	6 x 3 = 18	7 x 3 = 21	8 x 3 = 24	9 x 3 = 27
2 x 4 = 8	3 x 4 = 12	4 x 4 = 16	5 x 4 = 20	6 x 4 = 24	7 x 4 = 28	8 x 4 = 32	9 x 4 = 36
2 x 5 = 10	3 x 5 = 15	4 x 5 = 20	5 x 5 = 25	6 x 5 = 30	7 x 5 = 35	8 x 5 = 40	9 x 5 = 45
2 x 6 = 12	3 x 6 = 18	4 x 6 = 24	5 x 6 = 30	6 x 6 = 36	7 x 6 = 42	8 x 6 = 48	9 x 6 = 54
2 x 7 = 14	3 x 7 = 21	4 x 7 = 28	5 x 7 = 35	6 x 7 = 42	7 x 7 = 49	8 x 7 = 56	9 x 7 = 63
2 x 8 = 16	3 x 8 = 24	4 x 8 = 32	5 x 8 = 40	6 x 8 = 48	7 x 8 = 56	8 x 8 = 64	9 x 8 = 72
2 x 9 = 18	3 x 9 = 27	4 x 9 = 36	5 x 9 = 45	6 x 9 = 54	7 x 9 = 63	8 x 9 = 72	9 x 9 = 81

ATENÇÃO: Sistema protegido com restrição de acesso

Informamos que V.Sa. é um criminoso, na medida em que V.Sa. acaba de violar o artigo 285-B no PL 84/99, que proíbe a "obtenção, transferência ou fornecimento não autorizado de dado ou informação". Especificamente, revelamos que V.Sa. não recebeu autorização para obter qualquer informação contida acima nesta página, nem para transferir qualquer delas para vosso computador ou vossa memória, nem para fornecê-las a qualquer parte de vosso cérebro em qualquer operação mental.

Nem tampouco recebeu V. Sa. autorização para obter qualquer dado codificado por sequência de letras ou símbolos anteriores ao fim desta sentença, nem para transferi-los a vossas retinas, nem para fornecê-los à vossa consciência.

A autorização tácita ou implícita no acesso a esta página web restringe-se apenas à obtenção, transferência para outras máquinas ou mentes e fornecimento a terceiros, do seu título e link, deste parágrafo e seguintes. Aconselhamos a V.Sa., respeitosamente, que contrate um advogado enquanto aguarda as consequências deste vosso crime. A pena será de 1 a 3 anos de reclusão e multa por cada violação, se o [PL 84/99 virar Lei](#). (Ora, por que achais que seu número é 1984?)

21-07-2011: ATUALIZAÇÃO: 2 a 6 anos se for o [PL 427/11](#).

3. Contra quem:

The Telegraph

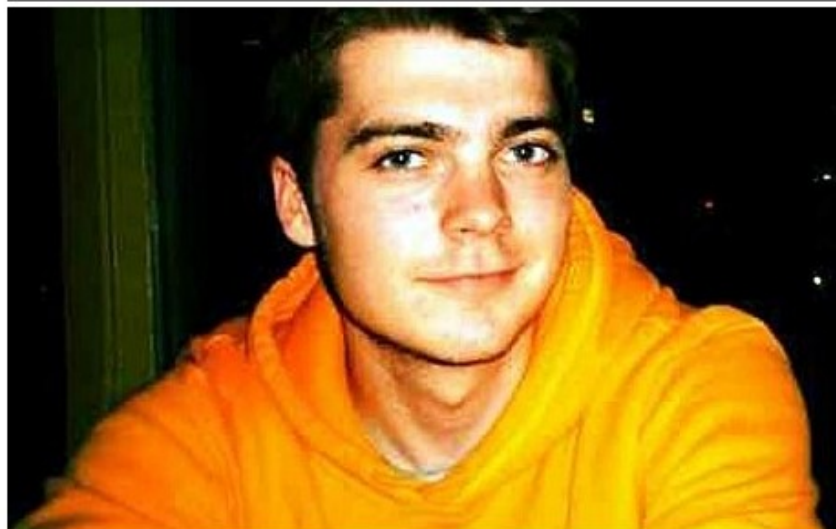
HOME NEWS SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFESTYLE

Technology News Technology Companies Technology Reviews Video Games Technology

Technology News

Student faces extradition to US over TV website

A British student is facing extradition to the United States and up to five years in jail for running a website that offered links to pirated films and television shows.



Richard O'Dwyer is facing extradition to the United States Photo: CENTRAL

By Christopher Williams, and Andy Bloxham

7:30AM BST 17 Jun 2011



Technology News

News » USA »
UK News »
Technology »
Andy Bloxham »

IN TECHNOLOGY



3. Contra quem:

› Law & Disorder

› Tech law and policy in the digital age



Former Reddit co-owner arrested for excessive JSTOR downloads

By Timothy B. Lee | Published July 19, 2011 3:03 PM



LATEST TOP STORIES

- ✎ Judge blasts Google/Oracle over damages estimates in patent dispute
- ✎ Samsung-funded study finds 3D video causes extra eye strain, fatigue
- # Linux kernel version bumped up to 3.0 as 20th birthday approaches
- 🔬 Physicists find hints of a light Higgs boson in LHC data
- * Still need a Spotify invite? Ars has some for you
- 🔬 If you care about your sperm, watch out for secondhand smoke
- 🍏 Rumored Apple bid for Hulu doesn't make a whole lot of sense
- 👤 Judge calls \$1.5M file-sharing judgment "appalling," slashes to

3. Contra quem:

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

AARON SWARTZ,

Defendant

Crim. No.

VIOLATIONS:

18 U.S.C. § 1343 (Wire Fraud)

18 U.S.C. § 1030(a)(4) (Computer Fraud)

18 U.S.C. § 1030(a)(2), (c)(2)(B)(iii)
(Unlawfully Obtaining Information from a
Protected Computer)

18 U.S.C. § 1030(a)(5)(B), (c)(4)(A)(i)(I),(VI)
(Recklessly Damaging a Protected Computer)

18 U.S.C. § 2 (Aiding and Abetting)

18 U.S.C. § 981(a)(1)(C), 28 U.S.C. § 2461(c),
and 18 U.S.C. §982(a)(2)(B) (Criminal
Forfeiture)

INDICTMENT

The Grand Jury charges that at all relevant times:



3. Contra o quê?



[Content](#) > [Volume 61](#) > [Issue 3](#) > [Punitive Damages, Remunerated Research, and 1...](#)

Volume 61, Issue 3 - December 2008

NOTE

[Punitive Damages, Remunerated Research, and the Legal Profession](#)

Shireen A. Barday 61 STAN. L. REV. 711

PDF 

A sociology professor is sitting in his office one day when he receives an unsolicited call from a representative of a large corporation facing a devastating punitive damages award. The caller says that the corporation is "exploring . . . whether it's feasible to get something published in a respectable academic journal, talking about what punitive damage awards do to society, or how they're not really a very good approach." The caller explains, "[t]hen, in [the corporation's] appeal, we can cite the article, and note that professor so-and-so has said in this academic journal, preferably a quite prestigious one, that punitive awards don't make much sense."¹ The professor was William Freudenburg and the corporation was Exxon, which contacted Freudenburg and a host of other scholars in the wake of its appeal of a \$5 billion punitive damages verdict arising from the Exxon Valdez oil spill off the coast of

Aaron Swartz ^{Alaska} colaborou com este artigo minerando dados em 441 mil trabalhos científicos da área jurídica publicamente acessíveis

stanfordlawreview.org/content/article/punitive-damages-remunerated-research-and-legal-profession

3. Quem?

Abr 08 - **Craig Mundie**
na **RSA Conference '08**



*“The **foundation** has been laid for good security practices. The **challenge** now is related to **management practices** ... The overall management systems today are not **integrated** enough, they're too complicated. That has been a **major focus** for Microsoft.”*

MS Trusted Computing Group Manager:

*“With everything we do, there's always skepticism and conspiracy theories. The answer is no; **this is for real.**”*

news.com/8301-10784_3-9914240-7.html?tag=yt

O teatro da Ciberguerra

Liberdade ao conhecimento
versus Liberdade ao capital



Poder escolher em quem confiar

Liberdade ao conhecimento
vs. Liberdade ao capital

Mundo dos Símbolos

Mundo dos
Átomos



Mundo da
Vida