

A GUERRA CIBERNÉTICA:

cyberwarfare e a securitização da Internet

MARCELO CARREIRO*

RESUMO

A popularização computação – e especialmente da Internet – vem sendo apontada por uma série de analistas de segurança internacional como um espaço cuja insegurança sistêmica colocaria em risco ativos estratégicos dos Estados nacionais. Nesse sentido, o espaço virtual das redes de computadores vem sendo gradativamente militarizado, com o discurso de que a virtualidade seria a nova faceta da guerra, na qual a preocupação de formulação de ataques a infraestruturas inimigas coexistiria com a necessidade de proteção dos ativos nacionais virtuais de valor estratégico. Essa doutrina, definida pelo nome *cyberwarfare* ou “guerra cibernética”, contudo, é desprovida de uma base técnica sólida – e sugere uma insegurança artificial cuidadosamente fabricada e difundida para a securitização da Internet.

Palavras-chave: Segurança internacional - *Cyberwarfare* - Internet

ABSTRACT

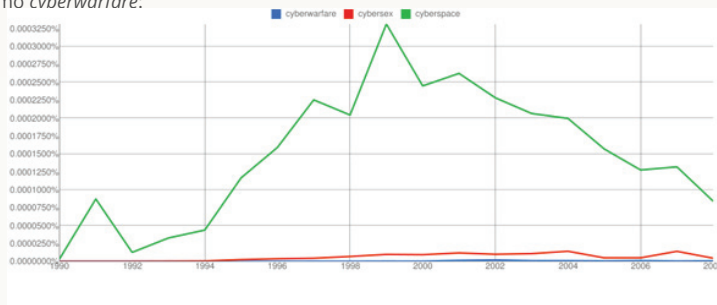
The popularization of computing – and specially the Internet – has been pointed by a number of international security analysts as a space which systemic insecurity could put in risk strategic assets from national states. In this sense, the virtual space of computer networks has been gradually militarized, with the discourse that the virtual would be the new face of war, in which the concern of formulating attacks on enemy infrastructure would coexist with the need to protect virtual national assets of strategic value. This doctrine, defined by the name of *cyberwarfare*, nevertheless, devoided of a sound technical basis – and suggests a carefully constructed artificial insecurity, fabricated and disseminated for the securitization of the Internet.

Keywords: International security - *Cyberwarfare* - Internet

* Tecnólogo em Processamento de Dados (PUC-Rio), administrador de redes especializado em segurança; bacharel em História (UFRJ), mestre em Relações Internacionais, Segurança e Defesa Nacional (Pró-Defesa/PPGHC/UFRJ), doutorando em História Comparada (PPGHC/UFRJ) e membro do grupo de pesquisa UFFDefesa.

Desde que usada por William Gibson em sua novela de ficção científica distópica “*Neuromancer*” em 1984,¹ a palavra *cyber* (eventualmente aportuguesada como “cibernética”) ganhou vida na cultura popular global, sendo usada de forma explosiva na “bolha ponto-com” dos anos 1995-2000. Nesse período, o marketing passou a usar *cyber* como um prefixo mágico, que concedia a qualquer produto ares futuristas ousados e virtuais, sendo empregada das mais diversas formas, de cybercafés à cyberterrorismo, de cyberspaço à cybersegurança.

Hoje, num mundo pós-bolha das empresas “ponto-com” e muito mais interconectado, o uso do prefixo *cyber* arrefeceu consideravelmente na cultura popular – prova disso é a incidência decrescente de termos que usam seu radical, como *cyberspaço*, *cybersexo* – e mesmo *cyberwarfare*:



Fonte: Books Ngram Viewer, Google Labs².

Figura 1-Uso de palavras com o prefixo “cyber” em livros em inglês (1990-2010)

Entretanto, na contramão da superação do modismo do uso do prefixo *cyber*, o Pentágono acaba de revitalizar o conceito de *cyberwarfare* na exposição de sua doutrina de segurança informacional, na qual um ataque virtual à sua infraestrutura torna-se passível de ser respondido com ações militares reais - bits respondidos com bombas. Uma invasão digital como *casus belli*, sem a definição de “ataque” e “infraestrutura”, é o mais novo produto do pensamento de defesa estadunidense sobre a *cyberwar*.³

O uso específico – e insistente – da palavra *cyber* pelo Pentágono aponta mais do que desconhecimento do desuso do conceito, indicando mesmo uma sincronia imaginativa com o período onde o prefixo foi criado, na criativa década de 1980/1990, no qual o “maravilhoso mundo dos computadores conectados” era apresentado sempre com uma preocupação apocalíptica, seguindo a linha clássica dos maléficos “cérebros eletrônicos” da ficção científica da década de 1950/60.

Exemplos do delineamento dessa paranoia são abundantes na produção cinematográfica estadunidense: *Wargames* (John Bradham, 1983)⁴, *Sneakers* (Phil Robinson, 1992), *The Net* (Irwin

1 GIBSON, William. *Neuromancer*. Nova Iorque: Ace Books, 1984.

2 Disponível na Internet no endereço http://ngrams.googlelabs.com/graph?content=cyberwarfare%2Ccyberspace&year_start=1990&year_end=2010&corpus=0&smoothing=0. Acessado em 20 de novembro de 2012.

3 GORMAN, Siobhan. BARNES, Julian. *Cyber Combat: Act of War - Pentagon Sets Stage for U. S. to Respond to Computer Sabotage with Military Force*. In Wall Street Journal, 31 de maio de 2011. Disponível na Internet no endereço <http://online.wsj.com/article/SB10001424052702304563104576355623135782718.html>, acessado em 30 de junho de 2011.

4 Não por acaso, *Wargames* será refilmado, indicando o retorno ao clássico tema dos anos oitenta do “perigo dos computadores”. FLEMING, Mike. *King of Kong* Director Seth Gordon Ready to Play “War Games” in MGM Reboot. In Deadline Breaking News, 23 de junho de 2011. Disponível na Internet no endereço <http://www.deadli>

Winkler, 1995), e, o carro-chefe da consolidação desse temor, *Hackers* (Iain Softley, 1995), que teve considerável impacto cultural em sua época ao apresentar a subcultura digital ainda em construção ao imaginário popular⁵. Misturando o tema da temível interconexão digital com a apocalíptica previsão de traços claramente milenaristas de colapso absoluto nos sistemas de informação na virada do século (o “bug do milênio”), ainda temos *Y2K* (Richard Pepin, 1999).

Ainda que fortemente datadas, tais produções nunca foram mais do que entretenimento – mesmo quando de seus lançamentos, suas visões técnicas eram brutalmente distorcidas em prol da dramatização. Nunca o mundo digital foi retratado de forma sequer próxima da realidade nas fantasias luditas paranoicas e conspiratórias de Hollywood.

Nesse sentido, é espantoso o tema ser retomado em uma superprodução cinematográfica mesmo após a popularização em massa da Internet e uma percepção direta da realidade operacional de um planeta de informações conectadas: em 2007 é lançado o filme *Live Free or Die Hard* (Len Wiseman, 2007), no qual é apresentada uma realidade na qual os EUA encontram-se submetidos em toda a sua infraestrutura a um ataque de *hackers*. O filme, como era de se esperar ao falar de um ataque terrorista em larga escala na realidade pós-9/11, tocou fundo no imaginário norte-americano – mesmo sendo a quarta instância de sua franquia, foi a mais lucrativa, tendo arrecadado cerca de US\$135 milhões nas exibições estadunidenses⁶, enquanto seus predecessores chegaram a apenas US\$83 milhões (*Die Hard*, 1983)⁷, US\$117 milhões (*Die Hard 2: Die Harder*, 1990)⁸ e US\$100 milhões (*Die Hard: With a Vengeance*, 1995)⁹.

É clara, então, que a desconfiança americana com computadores, e em especial os conectados em rede, não é exatamente uma novidade – muito pelo contrário, chega a acompanhar toda a Revolução Digital, embora sempre expressada através do exagero ridículo do entretenimento, longe de se preocupar com as tecnicidades e operacionalidades reais envolvidas na questão. O que, na verdade, pode ser identificado como uma tendência da cultura estadunidense – já nos anos 1970, Stanley Cohen aponta a tendência estadunidense de produzir “medo moral” com espantalhos cada vez menos plausíveis, propagados por uma imprensa sensacionalista que vive para uma sociedade do espetáculo aos moldes da teorizada por Guy Debord¹⁰.

Do Imaginário ao Noticiário

Contudo, mesmo tendo a paranoia como elemento recorrente na cultura estadunidense, especificamente no campo da tecnologia da informação (TI) ela extrapola toda a razoabilidade. Exemplo disso foi a piada veiculada pelo jornal cômico *Weekly World News* em 2000 – portanto, ridicularizando o fracasso apocalíptico do Y2K, o “bug do milênio” – onde deixava claro:

ne.com/2011/06/king-of-kong-director-seth-gordon-ready-to-play-war-games-in-mgm-reboot/, acessado em 24 de junho de 2011.

5 GLEIBERMAN, Owen. *Hackers*. In Entertainment Weekly, n° 294, 29 de setembro de 1995. Disponível na Internet no endereço <http://www.ew.com/ew/article/0,,298899,00.html>, acessado em 20 de novembro de 2012.

6 Box Office Mojo. *Live Free or Die Hard*. Disponível na Internet no link <http://www.boxofficemojo.com/movies/?id=diehard4.htm>, acessado em 20 de novembro de 2012.

7 Box Office Mojo. *Die Hard*. Disponível na Internet no link <http://www.boxofficemojo.com/movies/?id=diehard.htm>, acessado em 20 de novembro de 2012.

8 Box Office Mojo. *Die Hard 2*. Disponível na Internet no link <http://www.boxofficemojo.com/movies/?id=diehard2.htm>, acessado em 20 de novembro de 2012.

9 Box Office Mojo. *Die Hard: With a Vengeance*. Disponível na Internet no link <http://www.boxofficemojo.com/movies/?id=diehardwithvengeance.htm>, acessado em 20 de novembro de 2012.

10 COHEN, Stanley. *Folk Devils and Moral Panics*. Londres: MacGibbon & Kee, 1973.

"Hackers podem transformar seu PC numa BOMBA... e explodir sua família em pedacinhos!".¹¹

A boataria subsequente ao artigo foi logo respondida pela imprensa especializada¹² – mas o estrago no imaginário coletivo foi grande. Prova disso foi a retomada da associação entre hackers e explosões em 2007, agora não mais por um jornal cômico – mas pelo canal televisivo KTTV, de Los Angeles, afiliado da rede Fox News. Em sua reportagem, para ilustrar o perigo de "hackers" (na realidade, apenas usuários anônimos) como "terroristas domésticos", o canal apresenta a chocante imagem de uma van amarela indo pelos ares – algo completamente sem ligação à matéria, atestando um sensacionalismo inacreditável.¹³

Do Imaginário à Realidade

No entanto, a segurança online frequentemente é tema de preocupação das forças de defesa – a novidade da nova doutrina do Pentágono resume-se apenas à inversão lógica de insegurança virtual resultar não resultar em novas medidas de segurança virtual, mas em bombas.

Sistemas de informação seguros apresentam minimizadas suas chances de interrupção, corrupção e furto de dados. Como todo segmento da sociedade hoje depende em grande medida de tais sistemas, seu bom funcionamento operacional (*reliability*) é essencial para todo Estado. Portanto, é uma justa preocupação da segurança nacional a segurança digital – não apenas de forma normativa no estabelecimento de parâmetros de segurança, mas também no combate à quebra de tais proteções, quando temos um ato ilícito que deve ser tratado em legislação própria.

Historicamente, o estabelecimento da normatização de protocolos de segurança eletrônica surgiu mesmo antes dos crimes eletrônicos: já em 1978 o Departamento de Defesa norte-americano publicou o rascunho da primeira obra do gênero, o *Department of Defense Trusted Computer System Evaluation Criteria*¹⁴, apelidado de *Orange Book*, devido à peculiar escolha da cor de sua capa¹⁵. O livro seria publicado em sua versão final apenas em 1983, já sob a coordenação específica do Centro Nacional de Segurança Computacional (NCSC), criado em 1983 no contexto da Agência Nacional de Segurança (NSA) estadunidense.

Logo o *Orange* foi seguido *Green, Light Yellow, Yellow, Red, Teal Green...* Compoem um festival cromático que se estendeu até 1993 totalizando cerca de trinta livros identificados por cores diferentes – o que motivou a série a ser conhecida em TI como *Rainbow Series*.¹⁶

Sob o aspecto da repressão policial a crimes digitais, ela se inicia nos EUA apenas em 1986, quando é aprovado o *Computer Fraud and Abuse Act*, que tipifica pela primeira vez uma gama

11 JEFFRIES, Randy. Hackers Can Turn Your Home Computer Into a BOMB... & Blow Your Family to Smithereens". In *Weekly World News*. Lantana, Vol. 21, nº 28, 4 de Abril de 2000, pág. 45. Disponível na Internet no endereço <http://weeklyworldnews.com/archive/>, acessado em 20 de novembro de 2012.

12 HACKERS Can Make your PC Explode. In *The Register*. Londres, 4 de julho de 2000. Disponível na Internet no endereço http://www.theregister.co.uk/2000/07/04/hackers_can_make_your_pc/, acessado em 20 de novembro de 2012.

13 EXPLODING Van. In *Know Your Meme*. Disponível na Internet no endereço <http://knowyourmeme.com/memes/exploding-van>, acessado em 20 de novembro de 2012.

14 ESTADOS UNIDOS DA AMÉRICA – DEPARTAMENTO DE DEFESA. *Department Of Defense Trusted Computer System Evaluation Criteria* (CSC-STD-001-83). 15 de Agosto de 1983. Disponível na Internet no endereço <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt>, acessado em 20 de novembro de 2012.

15 SCHNEIER, Bruce. *Applied Cryptography*. Nova Iorque: John Wiley and Sons, 1996. 2ª Edição. Cap. 25.2.

16 *NSA/NCSC Rainbow Series*. Federation of American Scientists – Intelligence Resource Program. Disponível na Internet no endereço <http://www.fas.org/irp/nsa/rainbow.htm>, acessado em 20 de novembro de 2012.

de crimes digitais como crimes federais, tais como: dano a computadores, fraude, invasão, conspiração para invasões, etc.¹⁷

Contudo, o código só resulta em condenações em 1990, quando é sentenciado o estudante da Universidade de Cornell Robert Morris – inventor do primeiro *worm* (aplicativo que se replica sem autorização até resultar na parada do sistema), em 1988. Logo após, em 1995, surge o caso mais midiático: Kevin Mitnick é o primeiro hacker condenado da História – e, com isso, assume ares míticos na cultura *underground* de TI em rápida expansão através da popularização de *Bulletin Board Systems* (BBS), espécies de clubes virtuais locais que antecederam a Internet comercial.¹⁸

Apesar da imensa cobertura da imprensa e de considerável comoção pública, apenas 47 condenações à prisão tendo como base crimes digitais ocorreram nos EUA de 1998 a 2006.¹⁹

Enquanto é possível sustentar um debate sobre a aplicabilidade de uma pena criminal a um crime digital – como no famoso caso do hacker Albert Gonzalez, condenado a inacreditáveis vinte anos de prisão pelo acesso não autorizado a informações²⁰, enquanto a pena média por estupro nos EUA é de apenas cerca de nove anos²¹ – a associação entre crimes digitais e segurança nacional é mais recente, começando a se consolidar a partir do ano 2000.

É conhecida a estratégia política de se classificar um tema relevante qualquer como associado à segurança nacional, na tentativa evitar a crítica e o escrutínio público na implantação de medidas polêmicas. Essa *securitização* de temas funciona não apenas como dispositivo facilitador na implantação de políticas, mas também oferece garantias da ampliação constante das ameaças ao Estado, consequentemente fabricando ameaças capazes de sustentar o orçamento militar e mesmo o prestígio da defesa no debate político nacional, ainda que em tempos de paz. Assim sendo, a securitização é um instrumento anti-democrático de controle social, que deve ser combatida pelas sociedades democráticas.²²

A securitização dos crimes digitais, que até então era apenas caso policial, inicia-se nos EUA a partir de junho de 2009, com o estabelecimento do *United States Cyber Command*, ou USCYBERCOM, subordinado diretamente ao *United States Strategic Command* – um comando misto que amalgama unidades militares de todas as outras forças que já se dedicavam ao tema. Pela primeira vez, a segurança das redes estadunidenses é reconhecida como tema especificamente militar, relacionada diretamente à segurança nacional – em sua missão, o USCYBERCOM declara se dedicar a

(...) dirigir as operações e defesa de redes específicas do Departamento de Defesa; preparar e, quando ordenado, conduzir operações militares completas no ciberespaço, para prover ações em todos os campos e garantir aos EUA e seus aliados a liberdade de ação no ciberespaço, negando o mesmo

17 ESTADOS UNIDOS DA AMÉRICA. United States Code, Title 18, Part I, Chapter 47, §130, 1986. Fraud And Related Activity In Connection With Computers. Disponível na Internet no endereço <http://www.law.cornell.edu/uscode/18/1030.html>, acessado em 20 de novembro de 2012.

18 SCHELL, Bernadette. MARTIN, Clemens. *Cybercrime: A Reference Book*. Santa Barbara, 2004. Pág. 118.

19 DEPARTAMENTO DE JUSTIÇA ESTADOS UNIDOS DA AMÉRICA. *Computer Crime Cases*. Disponível na Internet no endereço <http://www.justice.gov/criminal/cybercrime/cccases.html>, acessado em 20 de novembro de 2012.

20 ZETTER, Kim. *TJZ Hacker Gets 20 Years in Prison*. In *Wired*, 25 de março de 2010. Disponível na Internet no endereço <http://www.wired.com/threatlevel/2010/03/tjz-sentencing/>, acessado em 20 de novembro de 2012.

21 DEPARTAMENTO DE JUSTIÇA ESTADOS UNIDOS DA AMÉRICA. *Prison Sentences and Time Served for Violence*. Abril de 1995. Disponível na Internet no endereço <http://bjs.ojp.usdoj.gov/content/pub/pdf/PSATSFV.PDF>, acessado em 20 de novembro de 2012.

22 BUZAN, Barry. *People, States & Fear – The National Security Problem in International Relations*. Brighton: The Harvester Press, 1983. Pág. 279.

aos nossos adversários.²³

A missão, portanto, vai além da segurança digital entendida como defensiva, sugerindo a possibilidade da tomada de ações de ataque. Além disso, especifica seu raio de ação como também incluindo os aliados dos EUA. É a consolidação do conceito de *cyberwarfare*, já presente nos debates de segurança da OTAN desde 2006 – TI como arma, disparada através da Internet.

O conceito de *cyberwarfare* é confuso desde sua criação – a “guerra digital” seria a resposta a atos de *cyberterrorism*. É notável que, mesmo em uma das primeiras tentativas de explanação do tema na OTAN, admita-se que “os comentários não são feitos sob o ponto de vista técnico”²⁴. Ora, não sendo uma questão técnica na qual os administradores de redes e especialistas em segurança digital participam, o “debate” torna-se mera especulação e fabricação política da insegurança. Não é de se estranhar que o responsável por “não-definição” seja precisamente o executivo de uma empresa de segurança israelense – portanto, com interesse comercial direto no tema.

Segurança é um conceito político derivado de um contexto relacional. Portanto, ela jamais é absoluta: cabe ao poder político uma análise econômica ao empregar seus recursos limitados na tentativa de fazer frente à ameaças ilimitadas – uma escolha que, idealmente deve ser ditada pela realidade da ameaça, seus danos possíveis e sua probabilidade de efetivamente ocorrer.²⁵

Ignorar isso é sancionar o absurdo como tema de preocupação da defesa nacional – absurdos que sequer resultam no aumento da segurança real do Estado e seus cidadãos. Pior ainda, o estabelecimento desses “espantalhos” na defesa nacional apenas garante a manutenção de verbas e o inchaço do complexo militar-industrial – são as forças de defesa nacional, no lugar de exercerem seu papel de provedoras de segurança, passando a serem elementos parasíticos do Estado, ao consumir recursos em volumes superiores ao devido, desviando verbas públicas de outros setores do Estado responsáveis pelo bem-estar social.

Nesse sentido, a securitização de TI foi imediatamente denunciada como tecnicamente absurda – mais que isso, como fabricada e incompatível com a realidade técnica da Internet. Logo após o estabelecimento do USCYBERCOM, James Lewis, do *think-tank Center of Strategic International Studies* esclarece que “Cybercrime does not rise to the level of an act of war, even when there is state complicity, nor does espionage – and crime and espionage are the activities that currently dominate cyber conflict.”²⁶

Mesmo Howard Schmidt, o coordenador de cybersegurança apontado pela Casa Branca em 2009, responsável por apresentar propostas que aumentem a segurança digital estadunidense, teve que se distanciar da crescente militarização do cyberspaço e admitir que “não há nenhuma cyberwar(...). Eu acho que essa é uma metáfora horrível e acho o conceito horrível”²⁷.

23 UNITED STATES CYBER COMMAND. *Factsheet*. 2009. Disponível na Internet no endereço http://www.stratcom.mil/factsheets/Cyber_Command/, acessado em 20 de novembro de 2012. Tradução livre.

24 EREZ, Amichai. *Cyber-Terrorism – How Much of a Threat is It?*. In CARVALHO, Fernando. DA SILVA, Eduardo. *Cyberwar-Netwar*. Amsterdã: IOS Press, 2006. Pág. 51-52.

25 KOLODZIEJ, Edward. *Security and International Relations*. Nova York: Cambridge University Press, 2005. Pág. 23.

26 LEWIS, James. *The “Korean” Cyber Attacks and Their Implications for Cyber Conflict*. Washington: Center for Strategic and International Studies, Outubro de 2009. Pág. 3. Disponível na Internet no endereço http://csis.org/files/publication/091023_Korean_Cyber_Attacks_and_Their_Implications_for_Cyber_Conflict.pdf, acessado em 20 de novembro de 2012.

27 SINGEL, Ryan. *White House Cyber Czar: There is No Cyberwar*. In Wired. 4 de março de 2010. Disponível na Internet no endereço <http://www.wired.com/threatlevel/2010/03/schmid-cyberwar/>, acessado em 20 de novembro de 2012. Tradução livre.

Essa voz civil dissidente, contudo, não impediu a progressão militar do tema – em maio de 2010, o Pentágono designa seu primeiro general encarregado exclusivamente de *cyberwarfare*: o quatro-estrelas Keith Alexander, que assume o comando do USCYBERCOM. Pela primeira vez é veiculada publicamente a ideia de que um ataque virtual pode ser respondido com uma ofensiva militar tradicional.²⁸

A comunidade de TI responde à crescente militarização da Internet em diversos artigos, apontando o absurdo técnico do conceito de *cyberwar* – Robert Graham, conhecido especialista em segurança de redes, é explícito:

O que me intriga é que ninguém parece se dar conta de que 'cyberwarfare' é uma história de ficção, e que 'armas' não existem no cyberspace.(...) colocar 'cyber' na frente de algo é apenas uma maneira de pessoas lidarem com conceitos técnicos (...) infelizmente, são essas pessoas ignorantes, que acreditam nessas analogias, que estão conduzindo a política nacional. (...) Militares nunca entenderão o cyberspace..²⁹

Da mesma forma, a imprensa especializada tem o mesmo tom de resposta – Mike Masnick, do *TechDirt* escreve um artigo inteiro sobre o tema, cujo título revelador é “*Dear Journalists: There is no Cyberwar*”.³⁰ Mais ainda, especialistas em segurança de redes apontam com preocupação a militarização da liberdade informacional da Internet, com os militares estadunidenses intencionalmente confundindo eventos díspares como ataques virtuais, espionagem, política de Estado e ato de guerra: Bruce Schneier³¹, Jeffrey Carr^{32 33}, Richard Stiennon e Marc Rotenberg³⁴ publicam artigos nesse sentido, concordando no absurdo técnico da militarização do *cyberspace*, apontando mesmo os ganhos corporativos por trás dessa nova doutrina³⁵.

O debate também tem sua base acadêmica – Jerry Brito e Tate Watkins publicam artigo sobre o problema da dimensão errônea da segurança digital na atual política de defesa estadunidense³⁶. Logo os acadêmicos Ian Brown e Peter Sommer publicam, a pedido da

28 BEAUMONT, Peter. *US Appoints First Cyber Warfare General*. In *The Observer*, Londres, pág. 10, 23 de maio de 2010. Disponível na Internet no endereço <http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general>, acessado em 20 de novembro de 2012.

29 GRAHAM, Robert. *Cyberwar is Fiction*. In *Errata Security*, 07 de junho de 2010. Disponível na Internet no endereço <http://erratasec.blogspot.com/2010/06/cyberwar-is-fiction.html>, acessado em 20 de novembro de 2012. Tradução livre.

30 MASNICK, Mike. *Dear Journalists: There is no Cyberwar*. In *TechDirt*, 9 de abril de 2010. Disponível na Internet no endereço <http://www.techdirt.com/articles/20100407/1640278917.shtml>, acessado em 10 de junho de 2010.

31 SCHNEIER, Bruce. *The Threat of Cyberwar Has Been Grossly Exaggerated*. In *Schneier on Security*, 7 de julho de 2010. Disponível na Internet no endereço http://www.schneier.com/blog/archives/2010/07/the_threat_of_c.html, acessado em 20 de novembro de 2012.

32 CARR, Jeffrey. *Inside Cyber Warfare – Mapping the Cyber Underworld*. Nova Iorque: O'Reilly, 2009.

33 WHATIS Cyber War Anyway? A Conversation with Jeff Carr, Author of 'Inside Cyber Warfare'. In *The New New Internet*, 2 de março de 2010. Disponível na Internet no endereço <http://www.thenewnewinternet.com/2010/03/02/what-is-cyberwar-anyway-a-conversation-with-jeff-carr-author-of-inside-cyber-warfare/>, acessado em 20 de novembro de 2012.

34 THE Cyber War Threat Has Been Grossly Exaggerated. In *Intelligence 2*, 28 de junho de 2010. Disponível na Internet no endereço <http://www.intelligencesquared.com/events/the-cyber-war-threat-has-been-grossly-exaggerated>, acessado em 20 de novembro de 2012.

35 ELLIOTT, Steven. *Cyberwarfare – Fact or Fiction?*. In *InfoSec Island*, 27 de agosto de 2010. Disponível na Internet no endereço <https://www.infosecisland.com/blogview/6845-Cyberwarfare-Fact-or-Fiction.html>, acessado em 20 de novembro de 2012.

36 BRITO, Jerry. WATKINS, Tate. *Loving The Cyber Bomb? The Dangers Of Threat Inflation In Cybersecurity Policy*.

Organização para a Cooperação e Desenvolvimento Econômico (OCDE), um relatório sobre o tema³⁷, no qual repetem que a *cyberwar* é um modismo exagerado e reincide na afirmação de que “*descrever coisas como fraudes online e hacktivism como cyberwar é algo profundamente enganoso*”.³⁸

Apesar das resistências, a securitização da Internet prossegue – em 19 de junho de 2010, três senadores americanos apresentaram uma proposta de lei, intitulada “*Protecting Cyberspace as a National Asset Act of 2010*”, que concede ao presidente estadunidense o poder de “desligar partes ou mesmo o todo da Internet”³⁹ – o absurdo técnico do conceito faz a proposta ser conhecida como “o botão desligar da Internet”.⁴⁰ Mesmo enfrentando forte oposição de grupos como o *American Civil Liberties Union*, o *American Library Association* e a *Electronic Frontier Foundation*, a proposta de lei voltou a ser debatida em janeiro 2011. Sua aprovação futura não parece impossível, dada a similitude do texto com legislações anteriores (em especial o texto do *USA Patriot Act*, de 2001).⁴¹

É nesse contexto de rápida progressão da securitização da internet, da militarização do *cyberspace*, que se insere a nova doutrina do Pentágono de interpretar ataques virtuais capazes de deixar inoperante a infraestrutura estadunidense como *casus belli*. São oferecidos comumente três incidentes internacionais como exemplos precursores de ataques virtuais como armas militares: o ataque à Estônia (2007), à Geórgia (2008) e ao Irã (2010). É preciso, portanto, desmistificar cada um desses eventos.

Análise de Caso: Estônia (2007)

No caso da Estônia, a partir de abril de 2007, uma série de sites governamentais e de empresas locais foi tirada do ar ou alterada para exibir conteúdos diferentes dos originais (um tipo de vandalismo digital conhecido como *defacement*). O método de ataque que indisponibilizava os sites era simples – a geração de gigantescas quantidades artificiais de pedidos de acesso, até os sistemas não conseguirem mais processá-las e saírem do ar. Essa técnica de ataque, conhecida como *Distributed Denial of Service* (DDoS) exige participação em massa de computadores dedicados ao processo – com ou sem o conhecimento de seus proprietários.⁴²

Apesar disso, o governo da Estônia prontamente acusou a Rússia de coordenar o ataque

In *Working Paper*. Washington, Mercatus Center – George Mason University, N° 11-24, abril de 2011. Disponível na Internet no endereço http://mercatus.org/sites/default/files/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy_0.pdf, acessado em 20 de novembro de 2012.

37 SOMMER, Peter. BROWN, Ian. *Reducing Systemic Cybersecurity Risk*. OECD, 14 de janeiro de 2011. Disponível na Internet no endereço <http://www.oecd.org/dataoecd/57/44/46889922.pdf>, acessado em 20 de novembro de 2012.

38 KOBIE, Nicole. Q&A: *Threat of Cyberwar is “Over-Hyped”*. In PC Pro. Londres: 3 de junho de 2011. Disponível na Internet no endereço <http://www.pcpro.co.uk/news/interviews/364435/q-a-threat-of-cyberwar-is-over-hyped>, acessado em 20 de novembro de 2012. Tradução livre.

39 ESTADOS UNIDOS DA AMÉRICA. *Protecting Cyberspace as a National Asset Act of 2010*. 19 de junho de 2010. Disponível na Internet no endereço http://hsgac.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=4ee63497-ca5b-4a4b-9bba-04b7f4cb0123, acessado em 20 de novembro de 2012.

40 GROSS, Grant. *Obama “Internet Kill Switch” Plan Approved by US Senate Panel*. In TechWorld, 25 de junho de 2010. Disponível na Internet no endereço <http://news.techworld.com/security/3228198/obama-internet-kill-switch-plan-approved-by-us-senate-panel/>, acessado em 20 de novembro de 2012.

41 KRAVETS, David. *Internet ‘Kill Switch’ Legislation Back in Play*. In Wired, 28 de janeiro de 2011. Disponível na Internet no endereço <http://www.wired.com/threatlevel/2011/01/kill-switch-legislation/>, acessado em 20 de novembro de 2012.

42 THE Cyber Raiders Hitting Estonia. BBC News, 17 de maio de 2007. Disponível na Internet no endereço <http://news.bbc.co.uk/2/hi/europe/6665195.stm>, acessado em 20 de novembro de 2012.

– algo que confronta o *modus operandi* do ataque pulverizado em questão. Embora o governo Russo tenha negado diplomaticamente o ataque, a Estônia tratou o caso como uma violação real a seu território, invocando o suporte militar da OTAN, que despachou um time de especialistas em TI para observar o cenário e auxiliar a retomada dos serviços. Pela primeira vez, a OTAN admitiu em público a relação entre ataques virtuais e uma guerra real: “Se o centro de comunicação de um estado-membro é atacado com um míssil, você chama isso de um ato de guerra. Então, do que você chama se a mesma instalação é desabilitada por um cyber-ataque?”.⁴³

A perversidade do raciocínio é gritante – ataques virtuais, diferente de mísseis, não destroem instalações e seus equipamentos. Muito pelo contrário, ataques virtuais obtêm sucesso apenas quando as redes atacadas possuem brechas através da má configuração e gestão de suas informações – falando de outra forma, parte da culpa de uma invasão é a fragilidade de um mal administrador de redes em estabelecer servidores inseguros. Algo muito diferente, sem dúvida, da inevitabilidade e do poder de destruição de um míssil.

Posteriormente, em 2008, um dos especialistas em segurança envolvidos na defesa dos sistemas estonianos, Gadi Evron, publicou um artigo detalhando tecnicamente os ataques e suas contramedidas. No *paper*, Evron sustenta que a fonte exata dos ataques ainda permanece desconhecida (como seria de se esperar em um ataque pulverizado como um DDoS) – e aponta que o “*cyber-riot*” começou quase que simultaneamente à manifestações reais, indicando que muito mais provável de que um ataque estatal, foram massas de usuários que pessoalmente conduziram o ataque, através de blogs e fóruns de discussão.⁴⁴

É de se notar que mesmo em setembro de 2007 o ministro da defesa estoniano admitia não ter qualquer evidência da coordenação russa do ataque, que na realidade teria tido como origem centenas de computadores espalhados pelo planeta. Mais importante ainda, nem os especialistas da OTAN nem da Comissão Europeia designados para investigar o caso conseguiram apresentar qualquer evidência do envolvimento do governo russo, que sempre negou ter realizado os ataques.⁴⁵

Ainda que o ataque tenha atingido alguns serviços do governo e páginas de bancos, os tipos de ação (DDoS e *defacement*) não acarretam a perda de dados ou a destruição de equipamentos. Nem mesmo serviços vitais da infraestrutura da Letônia foram afetados – como a rede elétrica e de telefonia, por exemplo. Um quadro bem diferente do que a OTAN e os teóricos de defesa criaram à posteriori.

Análise de Caso: Geórgia (2008)

Na Geórgia, os ataques foram diferentes, ocorrendo no contexto do conflito militar russo-georgiano na Ossétia do Sul, em agosto de 2008. Contudo, apesar de se situar no meio de um conflito militar real, os ataques foram similares aos da Estônia em 2007 – *defacement* de sites, como do Parlamento da Geórgia, acompanhados de DDoS que tiraram do ar sites oficiais como o da página oficial do presidente e do Ministério do Exterior. Sites russos também foram

43 A Cyber-riot. The Economist, Londres, 12 de maio de 2007, pág. 76-77.

44 EVRON, Gadi. *Battling Botnets And Online Mobs: Estonia's Defense Efforts During The Internet War*. In Georgetown Journal of International Affairs. Georgetown, inverno/primavera 2008, Vol. IX, nº 1.

45 ESTONIA Has No Evidence of Kremlin Involvement in Cyber Attacks. RIA Novosti, 6 de setembro de 2007. Disponível na Internet no endereço <http://en.rian.ru/world/20070906/76959190.html>, acessado em 20 de novembro de 2012.

atingidos, assim como páginas da Ossétia do Sul.⁴⁶

Difícilmente sites oficiais podem ser encarados como infraestrutura essencial de um Estado – ainda mais como ativos relevantes em uma guerra. Mas a reação propagandística seguiu chamando os ataques de “*cyber-cerco ao cyberspace georgiano*”, culpando imediatamente o governo russo ou hackers sob comando deste.⁴⁷ Imediatamente os ataques foram interpretados como um dos fronts do conflito em curso – embora não tenham sido apresentadas vítimas nem perdas financeiras resultantes da indisponibilização de sites oficiais, não tendo influência alguma no conflito militar real em curso.⁴⁸ O governo russo, mais uma vez, negou qualquer envolvimento – apesar de declarações como a do presidente polonês de que o bloqueio a sites georgianos caracterizavam uma “agressão militar”.⁴⁹

Apenas em outubro de 2008 ficou delineado que os ataques partiram da iniciativa pessoal de jovens russos – em especial, a partir do depoimento de Leonid Stroikov à revista russa *Xakep*, onde o hacker detalhava suas ações e motivações, ficou clara a origem pessoal dos ataques. Mais uma vez, a pulverização dos DDoS e outros métodos primitivos de ataque permitem criar um cenário consideravelmente diferente da fantasia do Pentágono de *cyberwarriors* treinados e com *cyberweapons* capazes de danificar a infra-estrutura nacional de um Estado.⁵⁰

Análise de Caso: Irã (2010)

Finalmente, no caso do Irã temos não um ataque do tipo DDos e *defacements* – mas o aparente uso de uma ferramenta específica, o *worm* Stuxnet, que teria sido capaz de atingir e danificar centrífugas nucleares iranianas.

Fruto de uma engenharia sofisticada, o Stuxnet é um programa desenhado para afetar um hardware específico – o controlador-programador lógico (PLC) Siemens S7-300, com drives de frequência variável fabricados por apenas dois vendedores: a empresa Vacon, finlandesa, e a Fararo, iraniana. Mais ainda, ele ataca apenas os motores que funcionam entre a frequência de 807 e 1210Hz – incluindo aí as centrífugas à gás de enriquecimento de urânio. Ao encontrar tão específicos parâmetros de funcionamento, o Stuxnet altera o funcionamento dos motores, ocultando essa diferença em sua operação e inviabilizando seu funcionamento.⁵¹

Além dessa capacidade específica de ataque, o Stuxnet foi construído tendo salvaguardas operacionais como dispositivos de auto-destruição para impedir sua análise forense

46 WATTS, Mark. *Cyberattacks Became Part of Russia-Georgia War*. In Computer Weekly, 13 de agosto de 2008. Disponível na Internet no endereço <http://www.computerweekly.com/Articles/2008/08/13/231812/Cyberattacks-became-part-of-Russia-Georgia-war.htm>, acessado em 20 de novembro de 2012.

47 MOSES, Asher. *Georgian Websites Forced Offline in 'Cyber War'*. In The Sidney Morning Herald, Sidney, 12 de agosto de 2008. Disponível na Internet no endereço <http://www.smh.com.au/news/technology/georgian-websites-forced-offline/2008/08/12/1218306848654.html>, acessado em 20 de novembro de 2012.

48 GRAY, Andrew. *Georgia Hacking Stirs Fears Of Cyber Militias*. In Reuters, 1º de setembro de 2008. Disponível na Internet no endereço <http://www.reuters.com/article/2008/09/01/us-georgia-osssetia-cyberattacks-idUSN2945446120080901>, acessado em 20 de novembro de 2012.

49 ESPINER, Tom. *Georgia Accuses Russia of Coordinated Cyberattack*. In CNet News, 11 de agosto de 2008. Disponível na Internet no endereço http://news.cnet.com/8301-1009_3-10014150-83.html, acessado em 20 de novembro de 2012.

50 SHACHTMAN, Noah. *Russian Coder: I Hacked Georgia's Sites in Cyberwar*. In Wired, 23 de outubro de 2008. Disponível online no endereço <http://www.wired.com/dangerroom/2008/10/government-and/>, acessado em 20 de novembro de 2012.

51 CHIEN, Eric. *Stuxnet: A Breakthrough*. In Symantec Official Blog, 12 de novembro de 2010. Disponível na Internet no endereço <http://www.symantec.com/connect/blogs/stuxnet-breakthrough>, acessado em 20 de novembro de 2012.

aprofundada, caracterizando uma sofisticadíssima programação em sua produção⁵² – na verdade, tão elaborada que indica o envolvimento de recursos (tempo e mãos) disponíveis apenas através de sua produção estatal.⁵³

Como resultado de suas detalhadas especificações de funcionamento, cerca de 60% das infecções do Stuxnet ocorreram no Irã⁵⁴, indicando que seu uso foi direcionado como uma sabotagem ao programa de enriquecimento de urânio do país.

No entanto, o que seria o primeiro caso de dano relevante de uma infraestrutura nacional através da Internet tem um detalhe importantíssimo – o Stuxnet não foi disseminado através da Internet, mas de pendrives contaminados.⁵⁵ Essa diferença é crucial e identifica o Stuxnet como uma sofisticada ferramenta de sabotagem, empregada localmente, tornando sua ação compatível com um ato de espionagem tradicional – ou seja, para sua inoculação ele dependeu da mão humana em uma ação direta e local. Nesse sentido a apropriação da ação do Stuxnet como um “míssil cibernético teleguiado”, como apontado pela imprensa⁵⁶, é de um erro conceitual medonho - diferente de um míssil real, o Stuxnet: a) não “trafegou” por lugar algum, já que não usou a Internet; b) não provocou dano material, apenas o mal funcionamento das centrífugas; c) não indisponibilizou uma infraestrutura nacional, já que apenas retardou o programa de enriquecimento nuclear iraniano, incapacitando o uso correto de apenas um décimo das centrífugas em uso⁵⁷; d) não teve uma origem clara de seu “disparo” – não há “vetores de origem” na Internet.

O Stuxnet como uma sabotagem ativada localmente, em uma típica ação de espionagem, mostra uma realidade dos sistemas de informação dificilmente lembrada pelos teóricos do *cyberwarfare* – sistemas de alta prioridade **não** são conectados à Internet, pelo simples fato de sua demanda de uso ser local. Isso é essencial para entendermos a segurança digital: sítios da Internet tem sua operação em modelos absolutamente diferentes de sistemas vitais, como sistemas de transações bancárias, sistemas de faturamento, sistemas de controle elétrico e mesmo sistemas militares. Dessa forma, apesar do imaginário, “invadir” o Pentágono não tem relação alguma com a segurança dos mísseis termonucleares estadunidenses, tratando-se na verdade, na ampla maioria das vezes, apenas da adulteração ou indisponibilização de seu sítio.

Essa diferenciação é essencial para a compreensão da atual condição de segurança na Internet – sítios são *front-ends* de informações. Metaforicamente, atuam como publicações impressas: é possível destruir um jornal impresso, ou mesmo recortá-lo para qualquer outro fim – mas sua redação e parque de impressão continuam intactos. Em outras palavras, a cópia

52 GROSS, Michael J. *A Declaration of Cyber-War*. In Vanity Fair, Nova Iorque, abril de 2011. Disponível na Internet no endereço <http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104>, acessado em 20 de novembro de 2012.

53 KEIZER, Gregg. *Is Stuxnet the 'Best' Malware Ever?* In InfoWorld, 16 de agosto de 2010. Disponível na Internet no endereço <http://www.infoworld.com/print/137598>, acessado em 20 de novembro de 2012.

54 MCMILAN, Robert. *Iran Was Prime Target of SCADA Worm*. In ComputerWorld, 23 de julho de 2010. Disponível na Internet no endereço http://www.computerworld.com/s/article/9179618/iran_was_prime_target_of_SCADA_worm, acessado em 20 de novembro de 2012.

55 CLAYTON, Mark. *Stuxnet Spyware Targets Industrial Facilities, Via USB Memory Stick*. In Christian Science Monitor, 23 de junho de 2010. Disponível na Internet no endereço <http://www.csmonitor.com/USA/2010/0723/Stuxnet-spyware-targets-industrial-facilities-via-USB-memory-stick>, acessado em 23 de junho de 2011.

56 SCOFIELD, Gilberto. *Guerra Cibernética: Medo de Infiltração do Supervírus Stuxnet*. In O Globo, Digital & Mídia, 30 de abril de 2011. Disponível na Internet no endereço <http://oglobo.globo.com/tecnologia/mat/2011/04/30/epidemia-do-supervirus-stuxnet-se-infiltra-em-industrias-empresas-de-energia-tele-924355583.asp>, acessado em 23 de junho de 2011.

57 CLAYTON, Mark. *Stuxnet Attack on Iran Nuclear Program Came About a Year Ago, Report Says*. In Christian Science Monitor, 3 de janeiro de 2011. Disponível na Internet no endereço <http://www.csmonitor.com/USA/2011/0103/Stuxnet-attack-on-iran-nuclear-program-came-about-a-year-ago-report-says>, acessado em 23 de junho de 2011.

da informação é passível de mudança – mas dificilmente sua origem é posta em perigo.

Isso explica porque não vemos aviões caindo com hackers, usinas nucleares explodindo ou, numa imagem amplamente difundida graças aos filmes-catástrofes desse tema, semáforos fora do controle – sistemas desse tipo têm como pressuposto de seu funcionamento o desligamento da rede: seus usuários autorizados devem trabalhar localmente em terminais desconectados da Internet. *Desconectar é assegurar.*

É exatamente o que vemos no caso do Stuxnet – as centrífugas iranianas não tinham justificativa operacional alguma para estarem conectadas à Internet. O contágio pelo Stuxnet deu-se através da ação humana direta não-autorizada ao equipamento. Em outras palavras, o contágio exigiu o contato direto com o equipamento – o que traz a questão de que, como esse contato direto já foi conseguido, qualquer outro tipo de sabotagem era possível. A falha de segurança foi no controle de acesso humano – não na insegurança da Internet.

Estudo de Caso: Brasil (2005/2007)

Um excelente exemplo dessa fantasia estadunidense de imaginar todos os sistemas digitais como englobados pela Internet – e com o mesmo nível de segurança que sítios – foi a acusação, feita em novembro de 2009 pelo programa *60 Minutes* da rede CBS, de que os apagões no Brasil de 2005 e 2007 foram causados por hackers. Na reportagem, Richard Clarke, que havia sido Conselheiro Especial do Presidente sobre cyberssegurança, finalmente fornece um exemplo para as antigas afirmações da CIA de que hackers já haviam causado interrupções no fornecimento de eletricidade de “alguns países” – Clarke cita o Brasil, acompanhado de “meia dúzia” de fontes, “militares, membros das comunidades de inteligência e segurança”.⁵⁸

Imediatamente a imprensa especializada considera o caso uma peça alarmista – pior ainda, foi apontado o repetido sensacionalismo do programa ao tratar do tema da segurança digital, muitas vezes se utilizando diretamente de peças hollywoodianas no lugar de técnicos da área.⁵⁹ Imediatamente o ministro das Minas e Energia do Brasil à época, Edison Lobão, negou os supostos ataques⁶⁰, com o caso sendo definitivamente encerrado apenas no final de 2010, quando da divulgação pelo Wikileaks de telegramas secretos entre a embaixada estadunidense e o Operador Nacional do Sistema Elétrico (ONS) do Brasil, que atesta que o sistema de controle elétrico brasileiro funciona com uma rede separada da Internet, pela qual um acesso não autorizado implicaria no acesso de terminais específicos e, portanto, seria rastreável.⁶¹

A acusação da CBS torna-se mais grave ao colocar em contexto um trecho do discurso do presidente estadunidense, que fala que “ataques [pela internet] deixaram outros países no

58 *CYBERWAR: Sabotaging the System*. In CBS News, 8 de novembro de 2009. Disponível na Internet no endereço <http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml>, acessado em 23 de junho de 2011.

59 POULSEN, Kevin. *Report: Cyber Attacks Caused Power Outages in Brazil*. In Wired, 7 de novembro de 2009, disponível no endereço <http://www.wired.com/threatlevel/2009/11/brazil/2009>, acessado em 23 de junho de 2011.

60 MINISTRO Nega que Ataque Hacker possa ter Causado Apagão. In Folha de São Paulo, 11 de novembro de 2009. Disponível na Internet no endereço <http://www1.folha.uol.com.br/folha/cotidiano/ult95u650656.shtml>, acessado em 23 de julho de 2011.

61 ROHR, Altieres. *Documento do Wikileaks Descarta Ataque Hacker em Apagão Brasileiro*. In G1 – Tecnologia e Games, 2 de dezembro de 2010. Disponível na Internet no endereço <http://g1.globo.com/tecnologia/noticia/2010/12/documento-do-wikileaks-descarta-ataque-hacker-em-apagao-brasileiro.html>, acessado em 23 de junho de 2011.

escuro” – dando a entender que o Brasil seria um exemplo desses ataques. Claro, sem revelar evidências, fontes ou quaisquer detalhes técnicos.⁶²

A propensão estadunidense às mais absurdas paranoias foi delineada pelo historiador Richard Hofstadter ainda em 1964 como um resultado do conservadorismo puritano aliado ao descrédito por especialistas, alimentado por uma mídia de massa que impulsiona o medo como estratégia sensacionalista de vendas⁶³. Nesse sentido, a paranoia da insegurança digital apresenta-se como uma nova versão recorrente de temores xenofóbicos e reacionários norte-americanos – dessa forma, temos a permanência histórica de um vilão fabricado culturalmente, que seria capaz de colocar sob ameaça o *american way of life*. Isso ocorre através das sucessivas fabricações de personagens como os iluministas, os maçons, os jesuítas, os comunistas, os nazistas, os mafiosos, os traficantes, os terroristas... e os hackers.

Crimes Digitais e Defesa Nacional

É preciso a desmistificação imediata dessa ficção absurda do hacker como uma figura poderosa e ainda capaz de “explodir seu computador”. Para isso, é preciso entender os crimes digitais como eles realmente são – não como são propagandeados por grupos de lobby e pela imprensa não-especializada.

Inicialmente, é preciso se colocar o óbvio – sim, nenhum sistema digital é absolutamente seguro. Como já exposto, até mesmo a conceituação da categoria *segurança* atesta sua relatividade. Especialmente na segurança de rede, ela sempre será um processo contínuo entre o valor da informação e os custos justificáveis para sua proteção. Mais ainda, independente do custo da proteção, uma rede e os sistemas nela contidos terão sempre o componente humano como elemento de preocupação fundamental – erros e displicências humanas são a maior fonte de insegurança digital, tomando uma miríade de formas, como o insistente uso de senhas fracas, falta de atualização de softwares, equipamentos fisicamente desprotegidos, compartilhamento de senhas e equipamentos entre diversos usuários, má configuração de sistemas...⁶⁴

Uma perfeita ilustração da segurança como responsabilidade do segurador foi o acesso não autorizado à Playstation Network (PSN) da Sony em abril de 2011 – não apenas todos os dados de seus usuários estavam disponíveis em um único bando de dados, como ainda seus números de cartões de crédito não se encontravam encriptados (codificados)⁶⁵. Pior ainda, essa considerável falha estrutural na defesa da rede da Sony foi explorada por ferramentas conhecidas, executadas através de métodos já estabelecidos de ataque a sites mal configurados – o que foi imediatamente apontado pela imprensa especializada como evidência de que, de fato, o fator segurança não era sequer considerado na administração da PSN⁶⁶, o que fica

62 APAGÃO: Para CBS e Até Obama, Brasil Já Foi Alvo de Hackers. In O Globo, 11 de novembro de 2009. Disponível na Internet no endereço <http://oglobo.globo.com/tecnologia/mat/2009/11/11/apagao-para-cbs-ate-obama-brasil-ja-foi-alvo-de-hackers-914699484.asp>, acessado em 23 de junho de 2011.

63 HOFSTADTER, Richard. *The Paranoid Style in American Politics*. In Harper's Magazine, novembro de 1964, pp. 77-86. Disponível na Internet no endereço http://karws.gso.uri.edu/jfk/conspiracy_theory/the_paranoid_mentality/the_paranoid_style.html, acessado em 23 de junho de 2011.

64 WADLOW, Thomas. *Segurança de Redes – Projetos e Gerenciamento de Redes Seguras*. Rio de Janeiro: Campos, 200. Pág. 4-9; 39-48.

65 SCHREIER, Jason. *PlayStation Network Hack Leaves Credit Card Info At Risk*. In Wired, 26 de abril de 2011. Disponível na Internet no endereço <http://www.wired.com/gamelifelife/2011/04/playstation-network-hacked/>, acessado em 23 de junho de 2011.

66 SATTER, Raphael. *Sony Security Slammed by Experts Over Hacking Vulnerabilities*. In Huffington Post, 3 de junho de 2011. Disponível na Internet no endereço <http://www.huffingtonpost.com/2011/06/04/sony-security->

evidenciado pela demissão de funcionários especializados na segurança dos usuários poucos dias antes do incidente, com evidências de que os esforços da empresa se concentravam na proteção de seus dados corporativos, não o de seus usuários⁶⁷. Essa insegurança sistêmica começou a ser combatida pela empresa apenas após o acesso aos dados de seus usuários, quando foi criado o cargo de *Chief Security Officer* (CISO) – um responsável central pela sua segurança digital. A inexistência desse cargo comum em TI aponta claramente que a segurança não possuía importância suficiente para ter uma gestão própria na PSN.⁶⁸

Nesse quadro, a segurança digital (das redes e seus sistemas) apresenta-se mais do que um processo sem absolutos – mas, essencialmente, como um componente gerencial entre custo e operacionalidade do produto final. Em outras palavras, há uma relação direta entre o investimento em segurança e a confiabilidade final do sistema – em 2010 apenas cerca de 18% das empresas investiram acima de 10% de seu orçamento de TI especificamente em segurança, evidenciando a prioridade baixa do tema na gestão empresarial.⁶⁹

Com isso, fica claro nos dados mais recentes o caráter absolutamente inócuo dos “ataques” digitais⁷⁰:

a) A maioria dos ataques resulta na indisponibilização de sítios (33%), especialmente através de táticas DDoS (32%). Apenas 4% dos ataques representam perda monetária. Nunca na história da humanidade um banco teve seu balanço anual afetado por ações de crimes digitais – muito pelo contrário, a crise financeira iniciada em 2008, a maior da História, foi integralmente gestada pelos próprios bancos, não por hackers.

b) A totalidade estatística do sucesso dos ataques é a má configuração e gestão de sistemas – 95% dos casos, divididos em: poucas defesas automatizadas (36%); entrada de dados tratada de forma indevida (23%); saída de dados tratada de forma indevida (12%); pouca autenticação (5%); aplicativos sem configuração apropriada (5%); validação insuficiente de processos (4%); erros de configuração (4%); senhas fracas (3%); vazamento de informações pessoais, como senhas (3%).

c) Da miríade de alvos, sites governamentais correspondem por apenas 17% dos ataques – dos quais a maior incidência (26%) resultou apenas na alteração indevida da página (*defacement*).

d) Apesar das fantasias hollywoodianas, nunca na história da humanidade um crime digital – que, em sua essência, é dano à propriedade digital⁷¹ – resultou

-hacks_n_871310.html, acessado em 23 de junho de 2011.

67 LEVINE, Dan. *Sony Laid Off Employees Before Data Breach-Lawsuit*. In Reuters, 23 de junho de 2011. Disponível na Internet no endereço <http://www.reuters.com/article/2011/06/24/sony-breach-lawsuit-idUSN1E75M1Y320110624>, acessado em 24 de junho de 2011.

68 MESSMER, Ellen. *Sony Creates CISO Position to Clean Up Mess After PSN Hack*. In Computer World UK, 11 de Maio de 2011. Disponível na Internet no endereço <http://www.computerworlduk.com/in-depth/careers/3277005/sony-creates-ciso-position-to-clean-up-mess-after-psn-hack/>, acessado em 23 de junho de 2011.

69 COMPUTER Security Institute (CSI). *15th Annual – 2010/2011 Computer Crime And Security Survey*. Nova Iorque: Computer Security Institute, 2011. Pág. 27. Disponível na Internet no endereço <http://analytics.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html>, acessado em 23 de junho de 2011.

70 TRUSTWARE SpiderLabs. *The Web Hacking Incident Database – Semiannual Report, July to December 2010*. Disponível na Internet no endereço <https://files.pbworks.com/download/XR2dVxBTeg/webappsec/37719371/Web%20Hacking%20Incidents%20Database%20Report%20July-December%202010%20FINAL.PDF>, acessado em 30 de junho de 2011.

71 A diferença entre a propriedade digital e real sempre é ignorada pela mídia e definidores de políticas: diferente da propriedade real, a digital possui uma elasticidade única, que permite sua cópia e restauração imediatas sem dano ao original. Copiar uma informação, nesse sentido, se distancia do roubo de propriedade

em uma morte. Da mesma forma, nunca uma “infraestrutura essencial”, pública ou privada, foi destruída pela ação de hackers agindo como terroristas digitais – a distribuição elétrica nunca foi interrompida, usinas geradoras de energia nunca foram desligadas, mísseis nunca foram lançados, semáforos nunca foram desligados, sistemas de controle de voo nunca foram adulterados.

É possível argumentar que tudo isso possa eventualmente acontecer, mas (apesar de toda a impossibilidade técnica) é preciso apontar a gigantesca diferença entre possibilidade e probabilidade – algo essencial na definição da segurança, especialmente a nacional.

Conclusão

Com essa delineação da segurança digital – e os efeitos técnicos dos crimes digitais – sua relação com a segurança nacional torna-se difícil de justificar. Nesse sentido, a crescente campanha estadunidense pela consideração dos crimes digitais como ameaças militares surge como absolutamente desconectada da realidade cotidiana da segurança de redes – o que levanta questionamentos sobre seus verdadeiros objetivos.

Nesse sentido, é revelador que pesquisadores chineses tenham respondido à nova doutrina do Pentágono como uma tentativa de reafirmação de sua hegemonia bélica, oferecendo uma útil justificativa de definições amplas para o emprego de sua força militar. Se antes uma operação militar deveria ser considerada uma resposta a um ataque, à morte e destruição, agora ela poderia ser apenas a resposta apropriada a um “ataque” virtual – indisponibilizar o sítio da Casa Branca pode ser tomado como uma declaração de guerra. Sem vítimas americanas sacrificadas, sem propriedades destruídas – mas também dificilmente com uma origem geográfica definida e com um ator estatal responsável.⁷²

Dessa forma, uma fantasia hollywoodiana com bases na cultura conservadora estadunidense de desconfiança à inovações foi gradualmente alimentada como uma ameaça militar considerável, numa ficção que permite a continuidade da ampla ação das forças de defesa estadunidenses, em total dissonância com a realidade da segurança digital. A fabricação do termo *cyberwar*, a securitização da Internet, encontra-se longe de prover garantias técnicas para a segurança digital – muito pelo contrário, seu pior inimigo continua sem ser afetado: sistemas mal-configurados e orçamentos de TI pouco dedicados à segurança. Enquanto isso, felizmente alheios ao debate, sistemas vitais das infraestruturas nacionais seguem em segurança, devidamente desconectados da Internet.

real, já que o conceito original pressupõe a destruição da propriedade com o roubo – digitalmente, mantém-se o original ao realizar-se uma cópia, autorizada ou não.

72 WANT China Times. *China Warns of Pentagon's Dangerous Cyber Strategy*. 3 de junho de 2011. Disponível na Internet no endereço <http://www.wantchinatimes.com/news-subclass-cnt.aspx?cid=1101&MainCatID=&id=20110603000109>, acessado em 30 de junho de 2011.