Análise da Campanha Cibernética da Rússia Contra a Geórgia, em 2008

Capitão Paulo Shakarian, Exército dos EUA

Em agosto de 2008, o Exército russo invadiu a Geórgia. Diversos ataques cibernéticos coordenados acompanharam a campanha militar. Essa foi a primeira vez que uma operação de ataque contra uma rede de computadores (ARC) de grande escala foi executada em conjunto com importantes operações de combate terrestres. O ataque não teve ligação direta com o governo russo, mas exerceu importante impacto psicológico e de informação na Geórgia: isolou-a do resto do mundo.

Especialistas em segurança identificaram duas fases na campanha cibernética russa. A primeira teve início no anoitecer de 07 de agosto, quando *hackers* atacaram sítios internet do governo da Geórgia e da mídia local[1]. O Coronel Anatoly Tsyganok, chefe do Centro de Previsão Militar da Rússia, disse que essas primeiras ações eram uma reação à invasão de sítios da imprensa da Ossétia do Sul por parte da Geórgia, que haviam ocorrido no início da semana[2]. O fato de esses alegados contra-ataques terem ocorrido apenas um dia antes do desencadeamento da campanha terrestre levou muitos especialistas a sugerirem que os *hackers* sabiam a data da invasão.

O Capitão Paulo Shakarian é professor assistente no Departamento de Engenharia Elétrica e Ciência da Computação da Academia Militar dos EUA (USMA, na sigla em inglês). É bacharel pela USMA e mestre e doutor pela University of Maryland. Serviu duas vezes no Iraque, em funções relacionadas à Inteligência militar.

Durante a primeira fase, a principal ação dos *hackers* russos foi um ataque distribuído de negação de serviço (*Distributed Denial of Service — DDoS*). Um ataque cibernético de negação de serviço é aquele que tenta impedir o uso legítimo de recursos de informática. Quando vários computadores são empregados para atingir esse objetivo, ele se torna um ataque distribuído de negação de serviço. Uma forma de categorizar esses ataques é fazendo a distinção entre os *semânticos* e os que empregam *força bruta*. A negação de serviço semântica tira proveito de uma característica ou de um defeito de *software* do sistema visado. Um ataque de força bruta (ou de "inundação") acontece quando o sistema visado recebe um volume de dados maior do que pode suportar, via internet, o que esgota os recursos de comando e controle do servidor, tornando-o indisponível[3].

Durante essa fase, os ataques distribuídos de negação de serviço foram particularmente levados a cabo por *botnets*[4]. Uma *botnet* é uma rede de computadores conectados à internet [chamados de "zumbis" ou "*bots*" (diminutivo de *robot* ou robô — N. do T.)] e infectados por um aplicativo conhecido como *malware*. O *malware* permite que o servidor de "comando e controle" envie comandos a esses *bots*. *Botnets* são comumente utilizadas para lançar mensagens eletrônicas de campanhas publicitárias (*spam*), mas também podem ser usadas para iniciar ataques de negação de serviço em larga escala. Tipicamente, o "sequestro" dos computadores

zumbis ocorre da mesma maneira que as infecções com outros tipos de vírus (por exemplo, mensagens eletrônicas e páginas falsas, falsos endereços eletrônicos, documentos infectados). Para que não seja detectada, a comunicação do computador de comando e controle com os computadores zumbis pode ser conduzida por meio de canais aparentemente inocentes (como um canal normalmente utilizado para bate-papos *on-line*)[5]. Organizações criminosas, como a Russian Business Network (RBN), usam e alugam *botnets* para uma variedade de propósitos[6]. As *botnets* usadas no violento ataque contra os sítios internet na Geórgia eram afiliadas a organizações criminosas russas, incluindo a RBN[7].

Nessa fase inicial, os ataques foram dirigidos principalmente contra sítios internet do governo georgiano e da mídia local. As *botnets* russas empregaram negação de serviço por força bruta[8]. As redes georgianas, devido à sua natureza débil, estavam mais suscetíveis a inundações do que as redes estonianas, que haviam sido atacadas pelos *hackers* russos no ano anterior[9].

Na segunda fase, os sítios internet da mídia e do governo georgianos continuaram a receber os ataques, mas a operação cibernética russa foi ampliada de modo a infligir danos a mais alvos, incluindo instituições financeiras, empresas, instituições de ensino, mídia ocidental (BBC e CNN) e um sítio internet de *hackers* da Geórgia[10]. Os ataques contra esses servidores não apenas incluíram negação de serviço, mas também a desfiguração dos sítios (um exemplo foi a "grafitagem" pró-Rússia nas páginas do governo, como o emprego de uma imagem comparando o Presidente georgiano Mikheil Saakashvili a Adolf Hitler). Além disso, vários *hackers* russos utilizaram endereços de correio eletrônico de políticos georgianos, disponíveis ao público, para iniciar uma campanha de proliferação de mensagens eletrônicas (*spam*)[11].

Para executar as desfigurações de sítios da internet, os *hackers* russos recorreram ao tipo de ataque conhecido como injeção de SQL (sigla em inglês para *Structured Query Language*, ou Linguagem de Consulta

Militares russos em uma viatura blindada, em algum ponto da Província separatista da Ossétia do Sul, na Geórgia, 09 Ago 08. (AP/Musa Sadulayev)

Estruturada), que se aproveita de um campo de texto em uma página da rede mundial para se comunicar diretamente com o banco de dados *back-end* (normalmente, um banco de dados de SQL comum — daí o seu nome). Em resumo, um sistema suscetível a esse tipo de vulnerabilidade confere ao *hacker* acesso total ao banco de dados em questão — que pode incluir todo tipo de informação, desde listas com as identificações de acesso dos usuários, até registros de transações financeiras, ou até mesmo o conteúdo integral de sítios da internet[12].

> …a atividade cibernética foi concentrada no recrutamento de russos "patrióticos" e seus computadores — frequentemente chamados de "hacktivistas".

Durante essa fase da operação, muito da atividade cibernética foi concentrada no recrutamento de russos "patrióticos" e seus computadores — frequentemente chamados de "*hacktivistas*"[13]. Segundo alguns comentários "postados" por *hackers* russos, imagina-se que muitos desses *hacktivistas* eram membros de movimentos de jovens[14]. O esforço principal do recrutamento foi feito por meio de vários sítios da internet, sendo o mais infame deles o "StopGeorgia.ru", colocado "no ar" em 09 Ago 08[15]. Um desses *hacktivistas* observou que as instruções fornecidas por esses "recrutadores" eram muito fáceis, mesmo para principiantes[16]. O StopGeorgia.ru, por exemplo, fornecia ferramentas e instruções de fácil utilização para o lançamento de ataques de negação de serviço a partir de computadores particulares. Ele chegou a adotar um formato amigável bastante conhecido, um "botão" na tela onde se lia "INUNDAR". Este, quando "clicado", desencadeava vários ataques de negação de serviço contra alvos georgianos. Embora muitos desses ataques de *hacktivistas* dependessem de uma vulnerabilidade diferente com relação às ações de *botnet*, seu objetivo era igualmente sobrecarregar os servidores georgianos, empregando força bruta[17]. As ferramentas fornecidas também eram muito versáteis. Por exemplo, alguns podiam atacar até 17 servidores georgianos ao mesmo tempo. Esses sítios *hacktivistas* também deram destaque a listas de alvos com sistemas da Geórgia — incluindo a indicação sobre se podiam ser acessados a partir da Rússia ou da Lituânia e suas vulnerabilidades conhecidas[18], como a suscetibilidade à injeção de SQL[19]. Também é importante citar que alguns especialistas em segurança conseguiram encontrar vínculos entre o StopGeorgia.ru e o crime organizado russo[20].

Outro aspecto interessante dos sítios de *hackers* russos é o profissionalismo de seus administradores. Eles não só proporcionavam conselhos oportunos aos *hacktivistas* principiantes, como também monitoravam seus sítios com muita eficiência. Durante o conflito, administradores do sítio *hacker* "XAKEP.ru" reagiram rapidamente às varreduras para verificação de "portas" abertas no *host* remoto (*portscans*), lançadas pelo "Projeto *Grey Goose*" — um projeto de segurança (de fonte aberta) baseado nos EUA —, bloqueando temporariamente todos os endereços de IP estadunidenses. Há evidências de que eles tenham conseguido limpar o servidor rapidamente, em uma ocasião, removendo, em questão de horas, uma postagem que continha a palavra-código "ARMY"[21]. As precauções desses administradores tinham fundamento. Uma organização de segurança identificou uma falsa ferramenta carregada em um sítio *hacker* russo, cuja finalidade anunciada seria lançar ataques contra alvos georgianos. Entretanto, esse aplicativo visava tão somente sistemas russos. Especialistas concluíram que *hackers* georgianos carregaram o *software* na página como uma tentativa de iniciar um contra-ataque cibernético, embora não haja evidências de que essa ferramenta tenha causado danos significativos[22].

A reação georgiana aos ataques russos consistiu, primeiramente, na filtragem de endereços IP russos. Contudo, os *hackers* russos se adaptaram rapidamente e usaram servidores não russos ou endereços IP falsificados. Os georgianos, então, transferiram muitos de seus sítios para servidores localizados fora do país (principalmente nos Estados Unidos). Não obstante, mesmo esses servidores no exterior permaneceram suscetíveis à exploração por inundação, devido ao grande volume de força bruta empregado no ataque russo[23].

Análise

A análise a seguir examina os objetivos do ataque. Kenneth Corbin descreveu os objetivos dos ataques cibernéticos russos como sendo "isolar e silenciar" os georgianos[24]. Os ataques tiveram o efeito de silenciar a mídia georgiana e isolar o país da comunidade internacional. Os relatórios sobre o evento e as listas de alvos dos sítios de *hackers* russos conferem credibilidade à hipótese de Corbin. Além disso, a população georgiana experimentou uma derrota significativa nos aspectos psicológico e da informação, porque ficaram incapacitados de transmitir ao mundo exterior o que estava ocorrendo em seu território.

Embora tenha sido cauteloso o bastante para não relacionar os ataques cibernéticos ao governo russo, o Coronel Tsyganok descreveu a campanha cibernética como parte de operações mais amplas, uma batalha de informações com as mídias georgiana e ocidental[25]. O jornalista russo Maksim Zharov descreve as operações cibernéticas como apenas uma pequena parte da campanha de Informações que também incluía "blogueiros" e meios de comunicação[26]. Em determinado momento, simpatizantes russos chegaram a "inundar" uma pesquisa de opinião da CNN/Gallup, com mais de 300 mil respostas que afirmavam que a causa russa era justificada[27]. Vários analistas acreditam que o objetivo principal da primeira fase era prevenir que a mídia georgiana contasse seu lado da história[28], o que parece estar alinhado com a ênfase que os russos deram à campanha de Informações[29].

Isolar a Geórgia do mundo externo talvez explique os ataques contra bancos do país, que ocorreram durante a segunda fase das operações cibernéticas. Naquele momento, vários bancos foram "inundados" com transações fraudulentas. Tentando mitigar o prejuízo, bancos internacionais suspenderam suas operações bancárias com a Geórgia, durante o conflito[30]. Como resultado, o sistema bancário da Geórgia ficou paralisado por dez dias[31]. Isso levou à interrupção de serviços de telefonia celular no país — isolando-o do resto do mundo ainda mais[32]. A intenção de alguns *hackers* russos, que optaram por atacar sítios internet de empresas georgianas, também durante a segunda fase, talvez tenha sido a de causar danos econômicos de forma similar.

Os objetivos de "isolar e silenciar" foram limitados em seu escopo. Evitaram causar danos permanentes às redes georgianas e ao Controle de Supervisão e Aquisição de Dados (*Supervisory Control and Data Acquisition — SCADA*)[33]. Sistemas SCADA são aqueles que coletam dados, controlam e monitoram, em tempo real, estações que fazem parte da infraestrutura crítica, incluindo usinas, oleodutos, refinarias e sistemas de tratamento e distribuição de água[34]. Uma interrupção desses sistemas teria levado a graves implicações para a infraestrutura georgiana, sem dúvida. Considerando que os *hackers* russos provavelmente tinham capacidade para atacar alvos dessa natureza, é razoável presumir que eles tenham sido propositalmente comedidos em suas ações, de modo a não prejudicar esses sistemas. Além disso, é preciso lembrar que a conexão física da Geórgia à internet permaneceu sem ser afetada, em grande parte. Quando ocorreram os ataques, a Geórgia estava conectada à rede mundial por um sistema de linhas físicas que a ligavam à Turquia, à Armênia, ao Azerbaijão e à Rússia. Não existem evidências de que tenham ocorrido tentativas de cortar essas conexões, tanto física quanto virtualmente — nem mesmo as conexões que passam pela Rússia[35]. Isso pode nos sugerir que os agressores russos não tencionavam causar danos permanentes à infraestrutura de internet georgiana, tendo preferido utilizar os servidores particulares do país para alcançar os objetivos de "isolar e silenciar".

Coordenação com Forças Convencionais

A coordenação desse ARC com as Forças convencionais foi muito limitada. Embora muitos peritos afirmem que, no mínimo, os *hackers* russos sabiam o momento em que as operações terrestres iriam começar, não há qualquer outra evidência de coordenação além dessa. Existem duas possíveis razões para isso. Primeira: o governo russo queria preservar sua capacidade de manter-se totalmente desassociado dos ARC (e, de fato, até este momento, não há provas concretas de seu envolvimento). Segunda: as Forças militares da Rússia não haviam adotado qualquer ideia relacionada a operações "conjuntas" na época do conflito — o que levou à compartimentação das operações cibernéticas, com relação às demais[36]. No entanto, alguns dos especialistas puderam identificar certo grau de coordenação entre as Forças terrestres e cibernéticas. Por exemplo, instalações de órgãos da mídia e de comunicações não foram atacadas por meios cinéticos — possivelmente em função do sucesso obtido pelos ARC russos. Além disso, *hackers* russos atacaram um sítio

Militares russos guarnecem um posto de controle nos arredores de Gori, a noroeste da capital Tbilisi, na Geórgia, 15 Ago 08. (AP/Darko Bandic)

internet de aluguel de geradores elétricos a diesel da Geórgia, provavelmente em apoio aos ataques convencionais contra a infraestrutura elétrica do país[37].

Reconhecimento e Preparação

Há muitos especialistas que acreditam que os *hackers* russos prepararam sua operação muito antes da data em que aconteceram os primeiros ataques cibernéticos, em 07 Ago 08[38]. A velocidade com que agiram as *botnets*, na primeira fase, e a disponibilidade de listas de alvos e de diversas ferramentas para ampliar os ataques — que incluíam as conhecidas vulnerabilidades à injeção de SQL — levariam a essa conclusão. Em suma, a eficácia dos ataques contra redes de computadores pelos *hackers* russos nos permite inferir que tenha ocorrido um reconhecimento com bastante antecedência.

Há outros indícios de que houve preparação. Em julho de 2008, servidores da Geórgia (e até a página da Presidência, na internet) foram "inundados" com a mensagem "win+love+in+Russia"[39]. Esses ataques foram originados a partir de uma *botnet* chamada *Machbot Network*, conhecida por ser utilizada por várias organizações criminosas russas[40]. Alguns analistas suspeitam que esse primeiro ataque, ocorrido pouco antes dos ataques de agosto, tenha sido uma espécie de "ensaio geral"[41]. Análises das imagens de grafite usadas para desfigurar os sítios internet da Geórgia levaram os especialistas a concluir que algumas delas haviam sido criadas em 2006, o que pode significar que os ataques cibernéticos talvez tenham funcionado como operações de contingência bem antes de 2008[42].

Atribuição

Muitos "blogueiros" e jornalistas têm tentado descobrir qual teria sido o grau de envolvimento do governo russo nos ataques. A seguir, abordarei algumas dessas teorias, confrontando-as com as evidências.

- *As operações cibernéticas russas foram originadas de forma espontânea, principalmente por "hacktivistas" patrióticos que reagiram aos ataques contra sítios internet da Ossétia do Sul.* Embora talvez pareça razoável, essa teoria apresenta alguns problemas. Primeiro: aparentemente houve uma preparação, com um planejamento e a execução de amplo reconhecimento. É bem provável que ele tenha ocorrido muito antes dos ataques contra os sítios internet da mídia da Ossétia do Sul, em 05 de agosto. Segundo: a maioria dos ARC, na primeira fase das operações, foi lançada de *botnets*. Esses ataques foram bastante severos e ocorreram vários dias antes do surgimento dos

diversos sítios que recrutavam e prestavam apoio aos *hacktivistas*. O emprego de *botnets* sugere o envolvimento do crime organizado russo — seja de forma direta, pelo lançamento de ataques de negação de serviço contra a Geórgia, seja de forma indireta, pelo "aluguel" de suas *botnets* para que outros o fizessem.

> Independentemente de o Kremlin estar ou não envolvido nos ataques cibernéticos, eles foram claramente benéficos às operações russas.

- *A única origem dos ataques cibernéticos foi o crime organizado russo.* O uso de *botnets* e o fato de muitos sítios *hacktivistas* (como o StopGeorgia.ru) estarem vinculados ao crime organizado russo tornam essa hipótese mais confiável que a anterior. Contudo, a pergunta óbvia é: o que ganharam as organizações criminosas com essas operações? Uma teoria sugere que, se não tiver sido o governo russo quem os financiou ou os apoiou, então esses *hackers* podem ter utilizado os ataques cibernéticos para se infiltrarem em certos sistemas da Geórgia para uso futuro (como no caso das instituições financeiras, atacadas na segunda fase).
- *Os ataques cibernéticos foram originados pelo crime organizado russo, a pedido do Kremlin.* Essa teoria foi apresentada por vários autores, que afirmam que muitas organizações como a RBN têm conexões com Vladimir Putin e com o Kremlin[43]. A mencionada coordenação com operações militares convencionais e o vínculo entre StopGeorgia.ru e a Diretoria de Inteligência Militar do Estado-Maior das Forças Armadas Russas reforçam essa teoria[44]. Contudo, essas evidências também são circunstanciais (até o momento da redação deste artigo, não havia provas concretas do envolvimento do Kremlin).

Preparando-se para Enfrentar um Adversário Capacitado na Área Cibernética

Independentemente de o Kremlin estar ou não envolvido nos ataques cibernéticos, eles foram claramente benéficos às operações russas, como um todo. Dessa forma, talvez devamos passar a considerar as capacidades cibernéticas como um sistema operacional do campo de batalha, assim como o são a manobra, a artilharia, a defesa antiaérea, etc. Conhecer adequadamente as capacidades cibernéticas do inimigo é parte importante de qualquer análise. Vimos que o *hacker* inimigo pode assumir várias formas: indivíduos em laboratórios patrocinados pelo governo, militares integrantes de Unidades cibernéticas, membros de organizações criminosas e *hacktivistas*. Distinguir os diferentes participantes que estão no espaço cibernético é algo frequentemente difícil ou mesmo impossível. No entanto, entender quais desses soldados cibernéticos fazem parte da ordem de batalha do inimigo pode trazer esclarecimentos sobre suas ações. Com a ordem de batalha estabelecida, podemos então aplicar "padrões doutrinários" cibernéticos. No exemplo do conflito na Geórgia, incluiríamos as organizações criminosas russas na ordem de batalha, embora não soubéssemos precisamente quais eram suas relações com as Forças convencionais. A partir de sua inclusão na ordem de batalha, poderíamos considerar o padrão doutrinário associado à atuação dos criminosos. Isso poderia indicar a possibilidade de emprego de *botnets* e *hacktivistas*, com a missão de isolar e silenciar o inimigo, mas não para afetar a infraestrutura ou o SCADA permanentemente.

O Aspecto Cibernético da Área de Interesse

Outra lição, que talvez possamos extrair do caso georgiano, é que os comandantes não devem apenas considerar a segurança de redes militares, mas também das redes civis. Ainda que não estivessem direcionados a alvos militares, de modo geral, os ataques cibernéticos russos na Geórgia produziram efeitos psicológicos e de informação significativos. Uma consideração adicional: alguns ataques cibernéticos, como os que foram desencadeados em julho, contra sítios internet do governo georgiano, podem ser indicativos não apenas de ataques cibernéticos em grande escala, mas também da proximidade do início de operações terrestres. Assim, um comandante

talvez queira levantar elementos essenciais de informações que sejam cibernéticos, por natureza. Para ajudar na proteção da população local, talvez seja imperativo garantir a sobrevivência das redes de computadores civis.

Reconhecimento e Vigilância Cibernéticos

Como acabamos de mencionar, ataques cibernéticos secundários podem ser indícios tanto de ARC em maior escala como de operações cinéticas. Além disso, há uma série de outros indícios da iminência de ataques contra redes de computadores, cujos dados podem ser percebidos por uma variedade de indivíduos. Por exemplo, a 6ª seção pode detectar tráfego suspeito em uma rede de computadores, ou um oficial de ligação junto ao governo da nação anfitriã pode reportar tráfego suspeito em uma rede civil. "Blogueiros" e *posts* específicos nos sítios de *hackers* podem fornecer indícios de uma ofensiva cibernética iminente. Os analistas de Inteligência de fonte aberta poderiam monitorá-los. Também deveríamos instruir pessoal de Inteligência de sinais e de Inteligência humana para identificar indícios de ataques cibernéticos que sejam específicos às suas áreas.

A campanha cibernética russa contra a Geórgia, em agosto de 2008, tornou-se a primeira oportunidade em que um ataque contra redes de computadores de grande escala foi desencadeado simultaneamente com importantes operações militares convencionais. Essas operações de ARC produziram significativo impacto psicológico e de informação na Geórgia, pois reduziram a capacidade de comunicar-se com o mundo externo não apenas da mídia e do governo, mas também da população local . Embora não possamos estabelecer vínculos diretos entre os ataques e o governo russo, este último obteve suficientes benefícios de seus efeitos para que consideremos essa possibilidade em conflitos futuros. Processos como o desenvolvimento de elementos essenciais de informações e o planejamento de reconhecimento e de vigilância cibernéticos devem ser ajustados, levando em conta inimigos que sejam capacitados na área cibernética. ■

Referências

1. BUMGARNER, John; BORG, Scott. *Overview by the USCCU of the Cyber Campaign Against Georgia in August of 2008*. U.S. Cyber Consequence Unit Special Report, Aug. 2009, p. 2.

2. TSYGANOK , Anatoly. "Informational Warfare—A Geopolitical Reality", *Strategic Culture Foundation* online magazine, 5 Nov. 2008. Disponível em: http://rbth.ru/articles/2008/11/05/051108_strategic.html. Acesso em: 16 out. 2010. Observe que esta é uma versão em inglês do artigo fornecido pelo sítio internet. "South Ossetian News Sites Hacked", *Civil.ge Daily News Online*, 5 Aug. 2008. Disponível em: http://www.civil.ge/eng/article.php?id=18896. Acesso em: 16 out. 2010.

3. MIRKOVIC, Jelena; REIHER, Peter. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms", *ACM SIGCOMM Computer Communication Review* 34, no. 2, April 2004, p. 39-53.

4. NAZARIO, Jose. "Georgia DDoS Attacks—A Quick Summary of Observations", Arbor SERT (Security engineering and response team), 12 Aug. 2008. Disponível em: http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/. Acesso em: 16 out. 2010.

5. Também observamos que as *botnets* mais recentes usam sistemas de comunicação mais avançados — descrevê-las fugiria ao escopo deste artigo. Consulte COOKE, Evan; JAHANIAN, Farnam; MCPHERSON, Danny. "The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets", *SRUTI* (Steps to Reducing Unwanted Traffic on the Internet Workshop, ou Workshop sobre os passos para reduzir o tráfego indesejado na internet, em tradução livre), 2005, p. 39-44.

6. CARR, Jeffrey. *Inside Cyber Warfare* (Sebastopol, CA, O'Reilly Media, Inc., 2010), p. 121-30.

7. CORBIN, Kenneth. "Lessons from the Russia-Georgia Cyberwar", internet*news.com: Real time IT News*, 12 Mar. 2009. Disponível em: http://www.internetnews.com/government/article.php/3810011/Lessons-From-the-Russia-Georgia-Cyberwar.htm. Acesso em: 16 out. 2010.

8. Nessa fase, as *botnets* russas concentraram-se, particularmente, na vulnerabilidade do protocolo conhecido como exploração TCP SYN. Consulte Nazario para mais detalhes.

9. BUMGARNER; BORG, p. 4.

10. Ibid., p. 5.

11. DANCHEV, Dancho. "Coordinated Russia vs. Georgia Cyber Attack in Progress", *ZDNet*, 11 Aug. 2008. Disponível em: http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670. Acesso em: 16 out. 2010.

12. ULLRICHA, Johannes B.; LAMB, Jason. "Defacing websites via SQL injection", *Network Security*, vol. 2008, issue 1, January 2008, p. 910.

13. DANCHEV.

14. CARR, p. 84.

15. Ibid., p. 15.

16. MOROZOV, Evgeny. "Army of Ones and Zeros: How I became a soldier in the Georgia-Russia Cyberwar", *Slate*, p. 14 August 2008. Disponível em: http://www.slate.com/id/2197514. Acesso em: 16 out. 2010.

17. O ataque de negação de serviço que foi desencadeado utilizando tais ferramentas foi diferente, de certa forma, dos ataques de negação com o emprego de *botnets*. Sempre que as *botnets* empregaram ataques TCP SYN, que exploram o protocolo básico de rede, muitas das ferramentas empregadas pelos "*hacktivistas*" eram destinadas a "inundar" os servidores com pedidos de HTTP. O formato desse ataque era enviar inúmeros pedidos a um dado sítio internet, esgotando a capacidade do servidor. Consulte BUMGARNER e BORG, p. 4 para mais detalhes.

18. MOROZOV.

19. DANCHEV.

20. CARR, p. 105-15.

21. Ibid., p. 16.

22. BUMGARNER; BORG, p. 7.

23. Ibid.

24. CORBIN.

25. TSYGANOK.

26. Uma sinopse dos artigos de Maksim Zharov, produzidos à época do conflito, consta de THOMAS, Timothy. "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia", *Journal of Slavic Military Studies* 22, 2009, p. 31-67.

27. Consulte http://www.theaustralian.com.au/news/attacks-on-cyberspace-preceded-russian-tanks/storye6frg-6to1111117197354. Disponível em: 16 out. 2010).

28. CORBIN.

29. THOMAS, Timothy. "Russian Information-Psychological Actions: Implications for U.S. PSYOP", *Special Warfare* 10, no. 1, Winter 1997, p. 12-19.

30. CORBIN.

31. BUMGARNER; BORG, p. 6.

32. CORBIN.

33. BUMGARNER; BORG, p. 5.

34. FERNANDEZ, John D.; FERNANDEZ, Andres E. "SCADA systems: vulnerabilities and remediation", *Journal of Computing Sciences in Colleges* 20, no. 4 (April 2005): p. 160-68.

35. ZMIJEWSKI, Earl. "Georgia Clings to the Net", *Reneysys: The* Internet *Intelligence Authority*, 10 Aug. 2008. Disponível em: http://www.renesys.com/blog/2008/08/georgia_clings_to_the_net.shtml. Acesso em: 16 out. 2010.

36. BIKKVOL, Tor. "Russia's Military Performance in Georgia", *Military Review* (November-December 2009): p. 57-62.

37. BUMGARNER; BORG, p. 6.

38. Consulte CARR, p. 183 e BUMGARNER; BORG, p. 6.

39. THOMAS, Timothy. "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia", *Journal of Slavic Military Studies* 22, (2009): p. 56.

40. KORNS, Stephen; EASTENBERG, Joshua. "Georgia's Cyber Left Hook", *Parameters* (Winter 2008-2009): p. 60-76.

41. THOMAS, "The Bear Went Through the Mountain", p. 56.

42. BUMGARNER; BORG, p. 5.

43. CORBIN.

44. Essa vinculação circunstancial foi feita com base no registro WHOIS de servidores associados com StopGeorgia.ru. Um dos endereços de registro está localizado perto da sede da Diretoria de Inteligência Militar, em Moscou. Especialistas em segurança e o Projeto *Grey Goose* foram os responsáveis por essa análise. Consulte CARR, p. 105-15.