ISSN: 2525-457X
Análise Estratégica
Vol 8 (2) Mar/Maio 2018

Hacktivismo e a Defesa Cibernética do Brasil

Victor Hugo Lima*

RESUMO

Desde a publicação das primeiras medidas de defesa cibernética do Brasil, observam-se grandes dificuldades em sua implementação. Com a chegada de grupos *hacktivistas* ao país, tais dificuldades se tornaram cada vez mais evidentes, colocando em questão a capacidade estatal de gestão e elaboração de políticas de defesa cibernética para proteção e segurança do país neste campo. Apesar da crescente preocupação com o tema e de sua priorização no marco da política de defesa sinalizarem importante evolução no pensar estratégico do Brasil, persistem desafios no tocante aos investimentos, treinamento de pessoal e melhoria da capacidade estrutural de defesa cibernética.

Palavras-chave: *hacktivismo*; defesa cibernética; política de defesa; Brasil.

ABSTRACT

Since the enactment of the first cyber defense measures in Brazil, several difficulties in their implementation have been observed. With the surge of first hacktivist groups in the country, such difficulties became even more evident, as well as those related to the state capabilities in policy making and management to provide adequate levels of security and protection in this area. Despite the growing concern with and the priority assigned to cyber defense, signaling an important departure in Brazil´s strategic thinking, important challenges remain as to investments, training and the enhancement of structural cyber defense capabilities.

Keywords: *hacktivism*; cyber defense; defense policy; Brazil.

*Graduado em Relações Internacionais pela Universidade de Brasília possui experiência na área de Defesa, com ênfase em Defesa Cibernética. Realizou pesquisa junto ao CNPq no tema de Defesa Cibernética e Cibersegurança brasileiros, assim como é membro do Grupo de Estudos e Pesquisa em Segurança Internacional do IREL-UnB.

1. Introdução

Com o decorrer dos anos, a internet deixou de ser um meio apenas de comunicação e se tornou também um modo de manifestação social organizada e massiva, o que se deve ao surgimento e desenvolvimento dos *hackers* e, em seguida, do *hacktivismo*. Este segundo ganha o papel principal dentro da lógica relacional da internet e movimentos sociais.

O *hacktivismo*[1] ganha os holofotes no século XXI e protagoniza revoluções e dá estopim a movimentos sociais ao redor do mundo. No Brasil o movimento mostrou sua força a partir de 2010 e se tornou um catalisador para a produção de políticas de defesa e segurança nacional na órbita estatal e para estratégias de segurança também na esfera privada.

O *hacktivismo*, em busca de cumprir o seu papel social de proteger a sociedade de quaisquer ameaças evidentes à liberdade (papel criado e tomado como dever pelos próprios *hacktivistas*), não difere organismos estatais de empresas privadas, quando se dispõem a cumprir o seu papel. E apesar de tais grupos se verem como defensores sociais, são grandes protagonistas no espaço cibernético brasileiro e representam ameaça real para a segurança e defesa do Brasil.

Frente a isso, a defesa cibernética do Brasil não cumpre seu papel, e deixa a desejar nos mais diversos ataques ao país, não apenas no plano estatal, mas também da cidadania e das corporações. A política, gestão, elaboração, e aplicação da defesa no campo cibernético são débeis e possuem um longo caminho adiante para melhorar.

[1] *Hacktivismo* surgiu a partir da junção entre *hackear*, atividade de utilizar a internet para invasões ou ataques a outros, e ativismo, utilização do espaço público para a reivindicação de algo. O *hacktivismo* é a utilização do meio cibernético, de uma maneira mais técnica, para a reivindicação ou defesa de causas, muitas vezes, públicas.

2. *Hacktivismo*: surgimento no Brasil e sua importância

Com o advento da internet, e de suas enormes possibilidades de organização, coordenação e comunicação entre pessoas, grupos, empresas etc, novas formas de protesto e demonstração de indignação surgiram. O ambiente cibernético teve como um de seus frutos mais inquietantes e nocivos o *hacktivismo*.

Primeiramente é necessário entender o que são os *hackers* e como agem. Para isso, vê-se datada no tempo, exatamente em 26 de julho de 1981, publicação do New York Times apontando uma definição para *hackers*, a qual continua sendo válida até os dias de hoje:

> *Hackers* são experts técnicos; habilidosos, muitas vezes jovens, programadores de computadores, que colocam em perigo as defesas de outros sistemas computacionais, procurando sempre os limites e possibilidades do computador. Apesar de seu papel aparentemente subversivo, *hacker* são ativos reconhecidos na indústria de computadores, e muitas vezes são altamente premiados. (NYT; 1981; tradução livre).

Porém os primeiros *hackers* surgiram entre os anos 1960 e 1970, nos laboratórios do *Massachussets Institute of Technology* (MIT), onde as capacidades destes foram desenvolvidas enormemente. *Hackers* trabalham nas mais diversas formas, e cada tipo de *hacker* tem um modo diferente de agir na internet. Tratamos aqui especificamente dos *hacktivistas* que geralmente agem através de: sit-ins virtuais; bloqueios virtuais; bombas de e-mails; invasão de websites, e-mails; invasão de computadores, celulares, sistemas em geral; vírus para sistemas operacionais e worms.

O *hacktivismo* em si é uma nova forma de desobediência civil, que uma vez era sedentária e concreta, e agora se tornou um corpo indefinido eletrônico, muito difícil de

ser controlado (ENSEMBLE, p.1, 1996). De fato, o *hacktivismo* surge como uma maneira de proteção à sociedade civil, e protesto por parte da mesma, uma vez que os *hacktivistas* se colocam como protetores dos civis, e os civis também participam do movimento, fazendo dele sua voz frente a diversos problemas.

O fenômeno teve início nos Estados Unidos, Europa e Rússia, que foram os primeiros países a disporem de tecnologias da informação disseminadas e acessíveis às massas. Porém, à medida em que se popularizaram e se tornaram acessíveis ao resto do mundo, viu-se o fenômeno do *hacktivismo* surgindo em outras partes do globo. Em países considerados de terceiro mundo, onde a população possui grande indignação e anseio por representação, o fenômeno foi acolhido pelas massas e assumiu grandes proporções.

O maior exemplo da proporção e poder do *hacktivismo* e da internet foi o estopim da Primavera Árabe. Com início na Tunísia e Egito, os *hacktivistas* presentes nos eventos da Primavera Árabe utilizaram mídias sociais e técnicas de invasão para ajudar a depor governos ditatoriais e corruptos de seus países. Tais revoluções apenas foram possíveis graças ao poder de organização proporcionado pela internet, e pela audácia dos *hacktivistas*.

No Brasil o movimento não teve essa mesma força e proporção, mas, ainda assim, merece atenção e análise cuidadosa. No país, o principal expoente tem sido o grupo *hacktivista Anonymous*, insurgente de um fórum na internet no ano de 2008 e que tem como símbolo a máscara de Guy Fawkes[2] (MACHADO, p.21, 2013). O Brasil entrou no mapa do hacktivismo em 2010-2011, com o início de nichos locais de aderentes às ideias da *Anonymous*.

De 2011 ao presente, o grupo *Anonymous* tem se mantido ativo no cenário político brasileiro. É comum encontrar sites de líderes religiosos, políticos, governantes, estados, governo federal, e agências como a ANATEL, invadidos e modificados pelo grupo. Na grande maioria das vezes os ataques não sofrem críticas do público brasileiro, pois os *hacktivistas* sempre buscam representar eletronicamente as pessoas que se sentem indignadas pelas mesmas razões que eles.

Não apenas de invasões sobrevive o movimento *hacktivista* no Brasil. O movimento também organiza manifestações por meio da internet e de redes sociais, tendo como exemplo àquelas do ano de 2013. O poder de organização proporcionado pelo ativismo é grande e representativo, consegue movimentar massas que apenas necessitam confirmar presença em um evento marcado através das redes sociais.

Ainda no âmbito de movimentos sociais catalisados pelos *hacktivistas* no Brasil, é importante notar que os mesmos agiram de maneira contrária a um anseio popular, no ano de 2015 e recentemente em 2016, quando invadiram diversos sites de movimentos populares que defendiam a saída da então presidente, Dilma Rousseff, defendendo a ideia de que tal movimento era antidemocrático.

3. O *hacktivismo* e a defesa cibernética brasileira

O número de ataques cibernéticos tem crescido no Brasil desde 2001, tendo como alvos bancos, agências governamentais, organismos internacionais, e partidos políticos. Devido à fragilidade na defesa deste espaço nacional, o país também tem sido alvo

[2] Guy Fawkes ficou conhecido na história por ser um dos responsáveis pela Conspiração da Pólvora em 1605, que almejava explodir o parlamento inglês no dia 05 de novembro. O plano falhou, mas Guy Fawkes ficou marcado na história como o único homem a entrar no parlamento com boas intenções. Seu rosto virou uma máscara, e símbolo de luta para a organização *Anonymous*.

de espionagem de modo recorrente, como a promovida pelos Estados Unidos em 2013.

Sete anos após o primeiro ataque cibernético e sua propagação no decorrer do tempo, o Brasil adicionou em sua Estratégia Nacional de Defesa (END) de 2008 o quadro de Política de Defesa Cibernética, além de publicar o Livro Verde de Segurança Cibernética (JUNIOR, CANONGIA. 2010), onde o setor se tornava estratégico para a defesa e a segurança nacional. Entretanto, poucos avanços foram alcançados desde então.

Com a publicação dos referidos documentos, adveio o estabelecimento do objetivo de criar um Sistema Militar para Defesa Cibernética , a introdução de defesa cibernética em exercícios das juntas militares e simulações de combate (LOBATO, KENKEL, p.34, 2015). Tal objetivo levou à criação do primeiro simulador de ataque cibernético no Brasil e à inserção de exercícios de defesa cibernética nas academias militares em todo o território nacional.

Essas iniciativas, por mais que possuam um caráter evolutivo e promissor, ainda continuam sendo insuficientes, mesmo decorridos oito anos da publicação da seção de defesa cibernética na Estratégia Nacional de Defesa (END, Art.1). A inteligência de defesa na área ainda continua muito obsoleta se comparada à capacidade de ataque dos criminosos cibernéticos. O Brasil ainda continua muito debilitado e atardado em questões técnicas e operacionais, e com a chegada do movimento *hacktivista*, essa vulnerabilidade na defesa nacional se tornou ainda mais evidente.

O que nos concerne apresentar e analisar é a grande influência *hacktivista* na defesa nacional cibernética. A partir de 2011, com o primeiro ataque cibernético protagonizado no Brasil pelo Grupo *Anonymous*, os investimentos tiveram aumento significativo e diversas de escolas foram criadas para o desenvolvimento da área.

Em 2013 o Simulador Nacional de Operações Cibernéticas entrou em funcionamento, no Centro de Instrução de Guerra Eletrônica em Brasília, e começou a ser utilizado pelo Exército Brasileiro para treinamento de profissionais, com o objetivo de melhor capacitá-los a defender o Brasil nesse campo. No ano seguinte o Centro de Defesa Cibernética foi criado junto ao Estado Maior do Exército. Este, por sua vez, organizou e dividiu as funções para desenvolvimento desta área em dez órgãos, estes são:

1. Organização do Centro de Defesa Cibernética: CDCiber - Brasília

2. Planejamento e Execução da Segurança Cibernética: CITEx - Brasília

3. Estrutura de Apoio Tecnológico e Desenvolvimento de Sistemas: CDS - Brasília

4. Estrutura de Pesquisa Científica na Área Cibernética: IME - Rio de Janeiro

5. Estrutura de Capacitação e de Preparo e Emprego Operacional (Força Cibernética): CCOMGEX - Brasília

6. Arcabouço Documental: CDCiber - Brasília

7. Estrutura para Produção do Conhecimento Oriundo da Fonte Cibernética: CIE - Brasília

8. Gestão Pessoal: CDCiber - Brasília

9. Rede Nacional de Segurança da Informação e Criptografia: RENASIC - Brasília

10. Rádio Definido por Software: CTEx - Rio de Janeiro

E mesmo com todas essas subdivisões e organização o país ainda continua distante de uma capacidade consistente em matéria de defesa cibernética, tanto técnica quanto estrutural. Diversos ataques cibernéticos protagonizados por grupos *hacktivistas*, internos e externos, ainda ocorrem em grandes números. Graças aos investimentos e treinamentos, muitos destes ataques puderam ser contidos; em muitos casos, a recuperação dos mesmos é rápida. Como exemplo, citam-se os ataques feitos aos sites da Câmara dos Deputados e Senado Federal no ano de 2016, devido aos trâmites do impeachment, onde os grupos derrubaram os serviços dos sites, que foram recuperados rapidamente.

Houve evolução no quesito de defesa nacional e recuperação de ataques cibernéticos, mas ainda persiste grande deficiência no quesito identificação dos infratores e retaliação aos ataques. Com efeito, a grande falha do Brasil neste campo tão importante para a defesa nacional não apenas se manifesta na pobreza técnica e estrutural. A tabela abaixo ilustra a situação acima demonstrada.

Tabela - Documentos e agências governamentais responsáveis por regular a defesa cibernética

DOCUMENTOS	AGÊNCIAS
- BRASIL, 2008: Estratégia de Defesa Nacional (Lei n° 6.703, 18/12/2008). - BRASIL, 2012: Política de Defesa Cibernética (Ordem n° 3.389/MD, 21/12/2013).	ABIN - Agência Brasileira de Inteligência MD - Ministério da Defesa EB - Exército Brasileiro CDCiber - Centro de Defesa Cibernética Presidência da República CDN - Conselho de Defesa Nacional DSIC - Departamento de Segurança da Informação e Comunicações Gabinete de Segurança Institucional da Presidência (GSI-PR) CREDEN - Comissão de Relações Exteriores e Defesa Nacional

Como é possível notar na tabela, existem diversos órgãos e agências que possuem jurisprudência administrativa sobre a defesa cibernética do país, e dessa maneira, o andamento das políticas nesta área se torna lento.

Considerações Finais

A primeira seção deste artigo buscou demonstrar como surgiu o movimento *hacktivista* no mundo e como ele se espalhou até chegar ao Brasil. A importância do histórico do movimento revela, por sua vez, as crescentes vulnerabilidades do país e os problemas que, apesar dos avanços em seu reconhecimento e na articulação de políticas para seu enfrentamento, persistem no âmbito da defesa cibernética.

O discurso social difundido por ativistas *hackers* lhes dá grande penetração social, mas mesmo assim não legitima sua ação na internet, que é maléfica tanto para o país quanto para própria sociedade. Porém, a responsabilidade pelas falhas na segurança

cibernética não pode ser creditada aos movimentos *hacktivistas*, já que, em grande parte, a falha em defender o Brasil no meio cibernético se deve tanto às carências materiais, tecnológicas e de recursos humanos e à má gestão e aplicação de leis na área como também aos descuidos e despreparo também por parte das corporações privadas e da própria cidadania.

O Brasil precisa evoluir muito em matéria de defesa cibernética, nas políticas da mesma, e na gestão do setor, caso queira neutralizar grupos *hacktivistas* no país. Entretanto, o fato de já existir uma preocupação com este campo da defesa representa uma grande evolução no pensar estratégico do Brasil. Ainda existe um grande caminho a percorrer para que o campo cibernético se torne seguro para os cidadãos, para o Estado para as empresas brasileiras, o que pressupõe grandes investimentos em treinamento de pessoal, aumento da capacidade estrutural de defesa cibernética e maior importância no âmbito da própria Defesa nacional.

Referências

CORTEZ, Igor Siqueira; KUBOTA, Luis Claudio. Contramedidas em segurança da informação e vulnerabilidade cibernética: evidência empírica de empresas brasileiras. Rev. Adm. (São Paulo), São Paulo , v. 48, n. 4, p. 757-769, Dec. 2013 . Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0080-21072013000400010&lng=en&nrm=iso>. Acesso em: 05/10/2016. http://dx.doi.org/10.5700/rausp1119.

ENSEMBLE, Crítical Art. Electronic Civil Desobedience in Electronic Civil Desobedience and other unpopular ideas. Mídia Autônoma: Estados Unidos da América. (1996).

Estratégia Nacional de Defesa. Disponível em www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm> Acesso em: 24/10/2016.

LOBATO, Luísa Cruz; KENKEL, Michael Kai. Discourses of cyberspace securitization in Brazil and the United States. Revista Brasileira de Política Internacional. 58 (2): 23-43. 2015.

MACHADO, Murilo B. Por Dentro dos *Anonymous* Brasil: poder e resistência na sociedade de controle. Dissertação (Mestre em Ciências Humanas e Sociais) - Universidade Federal do ABC, 2013.

Ministério da Defesa. CDCiber: perspectivas em face da espionagem eletrônica. Disponível em:m <http://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf> Acesso em: 02/10/2016.

New York Times. Case of the purloined password. Disponível em: <http://www.nytimes.com/1981/07/26/business/case-of-the-purloined-password.html?pagewanted=all> Acesso em: 29/09/2016.

Saint Petersburg Times. A history of hacking. Disponível em: <http://www.sptimes.com/Hackers/history.hacking.html> Acesso em: 29/09/2016.

SYMANTEC. (2012) 2012 Norton cybercrime report. [http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf] Acessado em 02/10/2016.