Securitização da Cibersegurança no Brasil[1]

ROBERT MUGGAH
MISHA GLENN
GUSTAVO DINIZ

RESUMO

■ O Brasil vem incrementando sua arquitetura de cibersegurança e ao mesmo tempo consolidando sua posição de potência emergente. Embora o crime organizado seja uma das principais ameaças ao ciberespaço brasileiro, são dirigidos recursos às soluções militares que melhor serviriam à excepcional hipótese de guerra. Há menos ênfase na ampliação da capacidade de segurança pública, de modo a identificar e reagir ao crime cibernético bem como aos delitos digitais correlatos. Em razão da ausência de uma posição uniforme do governo sobre a questão, ou de dados confiáveis, o Brasil possui uma abordagem pouco coerente sobre a cibersegurança. Caso o Brasil volte a organizar sua abordagem, o governo deverá incentivar um amplo debate com uma estratégia clara de comunicações sobre as exigências da cibersegurança e quais as suas formas. Há necessidade de maior pensamento crítico sobre forma e conteúdo das estratégias ponderadas e eficientes para fazer face às ameaças cibernéticas. Torna-se essencial aperfeiçoar a coordenação entre as polícias estaduais de modo a melhor se antecipar e lidar com os crimes cibernéticos.

1 O presente estudo possui como base a Nota Estratégica elaborada pelo Instituto Igarapé, que se encontra no portal http://igarape.org.br/desconstruindo-a-seguranca-cibernetica-no-brasil-ameacas-e-respostas/.

APRESENTAÇÃO

■ O Brasil sofre ameaças de uma ampla variedade das chamadas *ameaças cibernéticas*, inclusive as fraudes virtuais, os crimes cibernéticos e a vigilância digital. Nem todas estas ameaças são por natureza iguais. Indiscutivelmente, o risco mais sério e difundido é o crime virtual de motivação econômica – aquele que visa os bancos privados, firmas e pessoas físicas em busca de proveito. Outro importante conjunto de ameaças cibernéticas emana de grupos de hackers nacionais e estrangeiros, os quais procuram sabotar serviços governamentais, portais e alvos empresariais. Por exemplo, os maciços protestos populares de junho a agosto de 2013 coincidiram com uma alta no ativismo dos hackers. Por final, as divulgações por Edward Snowden de que as redes oficiais de comunicações do Brasil se sujeitavam à espionagem rotineira pela Agência de Segurança Nacional (NSA) norte-americana, criou o espectro de uma nova ameaça cibernética no país: A ciberespionagem e segundo alguns a ciberguerra.

E ao passo que aumenta em todo o Brasil e América Latina a inquietude com as ameaças cibernéticas, conhece-se de fato relativamente pouco sobre as mesmas. Quase não há debates sobre os protagonistas dos quais emanam estas ameaças, seus interesses e motivações, seu *modus operandi* ou quais suas relações com as mais tradicionais organizações criminosas ou políticas. Há poucos especialistas se ocupando de uma avaliação pormenorizada destas variadas – e até bastante diferenciadas – ameaças cibernéticas, e muito menos ponderando as reações públicas e privadas. Em que pese a profunda falta de conhecimento, mesmo assim o governo brasileiro organizou com rapidez uma abrangente infraestrutura de cibersegurança e defesa. Curiosamente, a resposta possui foco limitado em apenas algumas dimensões destas ameaças – em especial as estrangeiras. Entre as muitas instituições deste meio, o *Centro de Defesa Cibernética* do Exército Brasileiro (o CDCiber) é peça chave na postura de defesa do país.

Até determinado ponto, a aparelhagem de cibersegurança em célere avanço no Brasil, mostra-se *em desalinho com as ameaças reais emergentes no ciberespaço. No lugar de mirar com mais precisão o cibercrime internacional e interno, o estado procura uma resposta no aperfeiçoamento da luta contra a ciberguerra e de sua capacidade antiterrorismo. Não significa afirmar que não há perigos nítidos e presentes relativos ao ciberterrorismo e à ciberguerra. Pelo contrário, o presente Estudo Estratégico opina que o governo brasileiro procura uma abordagem de securitização contra* as ameaças cibernéticas, no lugar de se contrapor aos desafios mais urgentes em face aos cidadãos, em especial o cibercrime. De forma sucinta, o estado (o agente)

securitiza o ciberespaço (o referente) em nome do povo (a plateia). Securitizado o objeto, é possível legitimar os meios extraordinários de solução do problema percebido, inclusive com legislação de emergência, ao mobilizar as forças armadas ou outros.[2] Não há consequências apenas na política pública e nos gastos; a resposta militar exagerada poderá arriscar colocar em jogo os direitos básicos dos cidadãos devido à vigilância e censura onipresente, entre outros. Por exemplo, o CDCiber em conjunto com a ABIN criaram plataformas para monitorar as mídias sociais após os protestos de 2013.

A abordagem securitizada de tratar a insegurança cibernética no Brasil acha-se de acordo com o esforço mais amplo de redefinir o papel das forças armadas do país para o século vinte e um. Na medida da consolidação da democracia, estabilidade e economia do Brasil, as forças armadas redefinem seu papel e postura relativos às ameaças não tradicionais. Por um lado, as mesmas visam mais o controle de fronteiras e as atividades antidrogas.[3] E pelo outro lado, as forças armadas procuram ampliar seu alcance e influência no domínio dinâmico e em constante evolução do ciberespaço. Ao mesmo tempo as demais importantes instituições públicas que lidam com ameaças cibernéticas, a exemplo da Polícia Federal, dispõem de menos recursos e organização. Logo, o desenvolvimento de capacidade militarizada para a resposta cibernética possui inspiração em parte no esforço e desejo do Brasil de ampliar seu alcance e relevância geopolíticas. Na condição de potência em ascensão, o governo brasileiro se vale não apenas da incipiente arquitetura de cibersegurança do país, mas também com maior amplitude de seus conhecimentos em governança cibernética, de modo a projetar o soft power nas relações bilaterais e nos fóruns multilaterais.

O presente *Estudo Estratégico* considera a evolução e as implicações desta visão securitizada na administração dos bens da cibernética do Brasil A primeira seção apresenta um panorama da paisagem cibernética do Brasil. A segunda seção avalia as ameaças reais e implícitas ao ciberespaço brasileiro, com ênfase nas prioridades nacionais bem como as deficiências na resposta do estado. A terceira seção se concentra nas respostas jurídicas e programáticas a tais ameaças, com especial atenção ao papel das instituições de segurança. A seção quatro discorre sobre os dilemas surgidos da abordagem por demais militarizada à cibersegurança. Aqui há também pormenores de como os esforços do país de afirmação internacional acabam moldando o processo interno de tomada de decisões com relação a ciber-

2 Veja a obra de Waever (1995) sobre a securitização.
3 Veja Diniz e Muggah (2012).

segurança e defesa. A conclusão oferece um resumo de conclusões assim como um conjunto de recomendações para fazer face aos desafios no Brasil de governança cibernética e segurança.

DEFINIÇÃO DO CIBERESPAÇO BRASILEIRO

■ O Brasil acha-se sob uma revolução digital com poucos paralelos no mundo em desenvolvimento. O índice de penetração digital e adoção das mídias sociais elevou-se de forma exponencial na última década. Durante este prazo o Brasil assistiu a um aumento de dez vezes em acessos à Internet e assinaturas de telefones celulares, constando no presente mais da metade de sua população de 200 milhões conectadas.[4] A quantidade de fatores relativos às melhoras no Brasil do desenvolvimento social e econômico impulsionam estas tendências. O clima macroeconômico bastante estável bem como as políticas sociais de redistribuição levaram à ampliação da classe média no país. Ao mesmo tempo, a marcha dos novos consumidores motivou a procura por tecnologias de informação e de comunicações (TICs), transformando a escala de suprimento a níveis em conformidade com o vasto mercado interno do Brasil.

A aparição de uma classe média ampliada e conectada dá forma ao ambiente cibernético no Brasil. O acesso mais ágil às novas tecnologias de informações deu causa a uma ampla gama de formas de capacitação social, política e econômica no país. Sem surpresa alguma, a capacitação digital vem acompanhada de maiores desafios a exemplo dos protestos em massa e do crime organizado. Como país de renda mediana, o Brasil se vê obrigado a tratar de suas arraigadas desigualdades dentro e fora dos meios digitais. As contradições aparecem à medida em que seus legisladores procuram integrar mais plenamente os cidadãos recém capacitados na democracia e economia formal do país. Como potência emergente, o país se encontra também frente a dilemas com seu maior comprometimento com políticas globais. Logo, fatores internos e internacionais possuem um papel crítico no rumo da governança cibernética do Brasil.

Poucos países foram tão drasticamente afetados pela capacitação digital como o Brasil. A escala e dinamismo do ciberespaço brasileiro atingiu novas alturas nos últimos anos. A começar com as manifestações em massa de inspiração digital, atingindo as ruas do país entre junho e agosto de 2013, até a presença rotineira

4 Veja o portal Internet World Stats (http://www.Internetworldstats.com), em dezembro de 2013.

do mesmo no topo de *rankings* relativos ao cibercrime.[5] O Brasil é conhecido de modo geral como autor e vítima da criminalidade digital. Ademais, o Brasil ainda se ressente das divulgações de espionagem realizadas por alguns países, em especial os Estados Unidos, Canadá e Reino Unido, tendo iniciado processos de reforma na ONU e internamente. A natureza complexa da "ameaça cibernética" – bem como sua interpretação no Brasil [6] – exerceu um expressivo papel na moldagem da governança cibernética e arquitetura de cibersegurança do país.[7]

Há necessidade de uma avaliação equilibrada ao se considerar as respostas contra as ameaças cibernéticas e a cibersegurança. Torna-se importante levar em conta os poderosos interesses bem como as lutas simbólicas que dão forma à definição do que constitui ameaça digital em determinada sociedade. Uma cuidadosa análise da narrativa e dos fatores por trás da mesma, seria capaz de revelar como se determinam as prioridades e recursos selecionados. É possível partir para além do curto prazo em direção à visão de prazo mais amplo que formula as decisões dos grandes protagonistas. Apenas com a adoção da visão bruta será possível compreender por completo o conceito, construção e aplicação da cibersegurança. Tais escolhas possuem peso, pois exercem influência fundamental em questões de segurança pública e de direitos pessoais à privacidade, dentro e fora dos meios digitais.

---

5 A International Telecommunications Union (ITU) define o cibercrime como atividade que emprega computadores ou redes como ferramentas, alvos ou locais para fins criminais. Foram definidas cinco categorias: 1) infrações contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computação; 2) infrações relativas a conteúdo; 3) infrações relativas a computadores; 4) infrações relativas a direitos autorais e marcas registradas; e 5) infrações complexas e combinadas (a exemplo de lavagem de dinheiro, ciberterrorismo e guerra, espionagem e ação de hackers, em determinado medida). Veja ITU (2009).

6 Nossa escolha do termo "ameaça cibernética" no lugar do "cibercrime" revela a visão mais expansiva das reais dimensões das atividades digitais nocivas. Muitos países do mundo em desenvolvimento, inclusive na América Latina, acham-se expostas a determinadas "ameaças cibernéticas" que não se enquadram por completo na rigorosa definição da ITU. Ademais, a expressão "ameaça cibernética" abarca percepções que não necessariamente implicam em risco real objetivo. É importante avaliar o que a sociedade percebe como ameaças digitais primárias e como as mesmas são conduzidas através do tempo.

7 De acordo com especialistas brasileiros, a segurança cibernética inclui ações preventivas e repressivas, que normalmente embutem um estado de alerta persistente assim como o preparo dos sistemas e das pessoas engajadas. Utiliza-se também a mesma no trato de práticas privadas de proteção do ciberespaço, por pessoas e empresas." Por outro lado, a defesa cibernética inclui "atividades operacionais instaladas para combates ofensivos ou contraofensivos no ciberespaço, de forma normal ligadas aos serviços militares e de inteligência dos países." Veja Canongia e Mandarino (2009). Também nos referimos à governança cibernética em vista de suas ligações com a segurança cibernética.

ADVENTO DAS NOVAS TECNOLOGIAS

A demografia da Internet no Brasil se assemelha a diversos outros países grandes de renda mediana, embora com expressivas diferenças em virtude da grande extensão territorial do mesmo. De modo especifico, o Brasil está bem posicionado em comparação a outras pujantes economias emergentes, em especial no meio do grupo Brasil, Rússia, Índia, China e África do Sul (os BRICS). O Brasil situa-se entre Rússia e China no tocante ao percentual de usuários da Internet (entre a população total do país).[8] Em comparação com seus vizinhos e demais potências emergentes, o Brasil lidera o grupo. O Brasil está bem na frente de seus pares da América Latina e do Caribe (ALC) no que tange ao emprego de TICs. Aqui se encontra a maior população latino-americana dentro e fora dos meios digitais: há cerca de 110 milhões de usuários da Internet no país, ou algo como 54,2 por cento da população.[9] O mesmo representa quase o dobro do total de usuários do segundo país da América Latina mais conectado digitalmente, o México.[10]

Diversas facetas relativas ao emprego da Internet no Brasil merecem especial atenção. Primeiro, os brasileiros em especial são produtores ávidos e usuários da mídia social. A ALC é a maior região mundial consumidora de mídia social,[11] o que se deve em grande parte à imensa predileção no Brasil pelas redes digitais. Os brasileiros passam em média 2,2 horas por semana em plataformas de mídia social, a exemplo do Facebook.[12] Quase 60 por cento dos usuários da Internet no Brasil possuem conta no Facebook, atrás apenas dos Estados Unidos na quantidade de perfis.[13] O mesmo se confirma em se tratando do Twitter: Os brasileiros possuem 33 milhões de contas e os registros continuam em ascensão.[14] Os brasileiros lideram assim como seguem tendências; 20,5 por cento dos usuários

8 Rússia possui 87 milhões de usuários de Internet (61,4%), Índia 195 milhões (15,2%), China 621 milhões (45,8%) e África do Sul 24 milhões (49%). Veja o portal Internet World Stats (2013).

9 Veja o portal Internet World Stats em dezembro de 2013.

10 México possui 52 milhões de usuários da Internet, ou 43,5% de penetração. Veja o portal Internet World Stats (2013).

11 Os latino-americanos ocupam 56% mais tempo em plataformas de redes sociais do que a média global. Veja http://thenextweb.com/twitter/2013/01/16 twitter-to-open-office-in-brazil-its- second-biggest- market-after-the-us-in-accounts/.

12 Veja http://online.wsj.com/news/articles/SB10001424127887323301104578257950857891898.

13 Veja o portal Internet World Stats (resultados para dezembro de 2013).

14 Veja http://semiocast.com/en/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_ superseds_Japan.

de Internet no país visitam a plataforma constantemente. Em termos globais, o Brasil é o quinto lugar no uso do Twitter.[15]

Segundo, nos últimos anos o Brasil experimentou um maciço incremento digital de atividades eletrônicas, econômicas e financeiras. O Brasil ostenta elevados níveis de comprometimento com serviços financeiros, que se assemelham aos meios de alta renda da América do Norte e Europa Ocidental. A economia digital tem evoluído *pari passu* com a economia nacional como um todo. No tocante ao *e-commerce*, o valor total das operações em 2012 atingiu US$ 11,3 bilhões, ou seja, aumento anual de 25 por cento em comparação com 2011.[16] Porém, está no setor de *e-banking* a verdadeiro vigor da economia digital no Brasil. Quase todas as contas bancárias hoje no Brasil possuem acesso via Internet. No total, a base de correntistas dos bancos aumentou em oito por cento em 2012 e abrigam 54 milhões de pessoas, o que representa 42 milhões de contas correntes na Internet além de 3,4 milhões de contas através dos celulares, incremento de 11 por cento e de 49 por cento respectivamente comparado a 2011.[17] Tais estatísticas são de dimensões fora do comum e ilustram a natureza inusitada do ciberespaço brasileiro. Sem dúvidas, o cibercrime no Brasil não deixou de organizar seus alvos e práticas em torno dos sistemas e usuários do *e-banking*.

Uma terceira característica da utilização da Internet no Brasil tem a ver com o acesso e emprego com celular, cujo crescimento foi vertiginoso nos últimos três anos. Há nos dias de hoje uma média de mais de duas assinaturas por pessoa.[18] A vasta maioria dos telefones celulares servem ainda para chamadas pessoais ou o envio de mensagens de texto. No entanto, há em curso um movimento vigoroso em direção aos *smartphones* e *tablets*. A quantidade de *smartphones* dobrou durante a primeira metade de 2012 e atingiu 60,1 milhões de aparelhos.[19] Os celulares com conexão Internet em banda larga já perfazem cerca de 36 por cento do mercado de telefonia móvel no Brasil.[20] A predileção pelos *smartphones* indica uma aceleração para o futuro próximo. As autoridades do país investem de modo maciço na difusão nas conexões em banda larga bem como a transição das redes

15 Veja http://www.billhartzer.com/pages/comscore-twitter-latin-america-usage/.
16 Veja http://wyse.com.br/portugues/2012/03/o-comercio-eletronico-no-brasil/.
17 Veja http://www1.folha.uol.com.br/fsp/mercado/69329-bancos-perdem-r-15-bi-com-fraudes.shtml.
18 Veja Dados e Estatísticas dos TICs ITU em http://www.itu.int/ITU-D/ict/statistics/explorer/index.html.
19 Veja http://tecnologia.ig.com.br/2013-01-18/entre-os-celulares-usados-no-brasil-36-sao-smartphones-diz-nielsen.html.
20 Ibid.

de 3G para as de 4G. Tais movimentos encontram explicação em parte nos mega-eventos esportivos recentes e futuros, inclusive a Copa do Mundo da FIFA (2014) e as Olimpíadas (2016), que insuflam a procura por conectividade mais rápida e confiável. O governo resolveu isentar de impostos os fabricantes locais dos *smartphones*, em garantia da redução dos preços no varejo.[21] A ampliação de acesso aos *smartphones* (assim como os preços mais baixos) recebeu assistência também da tomada do mercado brasileiro pelos produtos chineses de preços mais em conta.[22]

Em quarto lugar, houve uma sensível mudança de quem e como se adquire acesso à Internet. Mais de 66 por cento dos usuários da Internet no Brasil ingressam na rede todos os dias, enquanto 25 por cento o fazem no mínimo uma vez por semana. Embora os mais jovens (entre 16 e 34 anos de idade) formam a maioria dos usuários, não há expressiva diferença no tempo de uso entre as faixas etárias. Como também não há diferenças marcantes entre os gêneros, ao menos no tocante à utilização: há igual quantidade entre os dois gêneros nas redes sociais, pessoas que permanecem ligadas por prazos mais ou menos iguais.[23] As políticas públicas de promoção da inclusão digital, as maiores rendas e produtos mais acessíveis também mudaram a forma de acesso à rede pelos brasileiros. Em 2011, a Internet era acessada 59 por cento das vezes em casa, 14 por cento a partir das LAN houses (Local Area Networks), 12 por cento no trabalho, 8 por cento da casa dos outros, 3 por cento na escola, 2 por cento a partir de aparelhos móveis e 1 por cento a partir de espaços públicos com wi-fi grátis.[24] Estudos recentes realizados pelo CTS-FGV indicam uma queda acentuada na quantidade das LAN houses nos anos recentes, à medida que o custo dos laptops, tablets e aparelhos celulares vem declinando, inclusive em áreas mais pobres e densamente habitadas, a exemplo das favelas.[25] Até as residências nos mais modestos dos setores sociais são capazes atualmente de adquirir novas tecnologias para uso pessoal, do sorte que o acesso a partir de casa através de aparelhos móveis está se tornando a regra com celeridade.

---

21 Vejahttp://www.redebrasilatual.com.br/tecnologia/2013/04/programa-de-inclusao-digital-deve-reduzir-preco-de-smartphones-nacionais.

22 Veja a apresentação do CTS-FGV durante o evento Open Development (IDRC – Montevidéu, Uruguai, abril de 2013).

23 Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm Percentage using internet on a daily basis regarding age: 10-15 (57%); 16-24 (66%); 25-34 (70%); 35-44 (68%); 45-59 (68%); e maior de 60 (68%).

24 Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-04a.htm.

25 Veja CTS-FGV (2012) em http://direitorio.fgv.br/node/2507.

Finalmente, mesmo assim a escala de atividades brasileiras no ciberespaço reflete ainda as desigualdades estruturais do país. As diferenças de renda, educação e região geográfica influenciam como e se as pessoas acessam a internet. Por exemplo, 50 por cento das residências nos estados de São Paulo, Rio de Janeiro, Minas Gerais e do Espírito Santo possuem acesso à Internet, porém este percentual decai para 22 por cento na região Norte.[26] Ademais, as classes mais abastadas permanecem muito mais tempo conectados na Internet do que os pobres. A proporção dos que acessam o serviço pelo menos uma vez por semana é de cerca de 80 por cento dos usuários de categoria mais elevada, de 65 por cento nas classes médias e inferior a 50 por cento nas classes de baixa renda. A diferença fica nítida também entre os níveis de escolaridade. Embora 55 por cento da população analfabeta do país acesse a Internet em bases semanais, o tempo de permanência aumenta do forma expressiva em se tratando de pessoas de ensino superior, com diploma universitário. A frequência de acessos semanais é de 87 por cento.[27]

A conectividade em alta bem como a capacitação digital no Brasil está intimamente ligada às desigualdades estruturais do país.[28] Este fato se torna mais nítido ao analisarmos o espectro completo de usuários e as atividades correlatas no Brasil. Grupos organizados e desorganizados começam a se aproveitar do ciberespaço, seja para forçar a mudança política e social, seja para realizar seus próprios interesses econômicos particulares, inclusive os criminosos. Há exemplos edificantes de movimentos sociais que se atrelaram ao poder das novas redes e infraestrutura de comunicações, de modo a promover a transformação política positiva e progressiva. Aumenta a tendência de exploração da Internet para fins de ganhos pessoais e criminais, em grande parte devido aos formidáveis desafios estruturais do Brasil.

AVALIAÇÃO DAS AMEAÇAS CIBERNÉTICAS

■ O tratamento das ameaças cibernéticas de amplo espectro é crítico para superar equívocos e lidar com políticas mal formuladas. Em razão da novidade e

26 Veja www.cetic.br/usuarios/tic/2011-total-brasil/index.htm.

27 54% das pessoas com escolaridade fundamental acessam a Internet pelo menos uma vez por semana; esta taxa sobe para 63% das pessoas com escolaridade de nível médio. Veja http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm.

28 Os indicadores da inclusão digital no Brasil refletem também disparidades quando confrontados em termos nacionais e internacionais. Veja FGV-CPS (2012a e 2012b) e http://tecnologia.terra.com.br/internet/inclusao-digital-no-brasil-esta-acima-da-media-mundial,c91cfe32cdbda310VgnCLD200000bbcceb0aRCRD.html.

da natureza técnica da questão, governos e cidadãos possuem parcas informações sobre a forma de reagir. Os cidadãos, os negócios e as instituições com frequência sentem que a compreensão das questões acha-se além da sua capacidade, ou que ameaças não lhes sejam relevantes. Com frequência a ignorância ou a falsa percepção acaba em ausência de ação no tratamento direto das ameaças de cibersegurança. As estratégias, quando implementadas, tendem a unir retalhos pinçados mediante premissas espúrias e sem comprovação. Raramente há dados robustos para fundamentar a tomada de decisões. Urge uma abordagem com maior peso na evidência, de forma a avaliar as ameaças cibernéticas – com apoio na ciência dos inúmeros riscos digitais interligados. Infelizmente, tempo e recursos já escassos são com frequência dirigidos às áreas de menor importância no lugar das verdadeiras ameaças principais. A seção a seguir leva em conta o cibercrime convencional, as ciberinfrações complexas assim como as ameaças emergentes, no esforço para a formação de uma agenda mais sofisticada no Brasil.

QUADRO 1. Os três principais conjuntos de ameaças cibernética no Brasil

Categoria	Definição	Exemplos	Reações normais do governo	Realidade brasileira
Cibercrime convencional	Trata-se das formas mais difundidas no mundo de infrações cibernéticas, cuja tipologia é a proposta pela ITU (2009) [veja nota de rodapé 4].	Acesso ilícito (cracking), interceptação de dados, pornografia infantil, spam, discurso de ódio, fraude bancária, furto de identidade, infração contra direitos autorais.	Exclusivamente a segurança pública, visto que normalmente compreende crimes tradicionais, já categorizados nos códigos criminais.	Há dois grandes subconjuntos de crimes cibernéticos convencionais: 1) os de motivação econômica (em especial a fraude bancária) e 2) relativos ao conteúdo (por ex: racismo e pornografia infantil nas redes de mídia social).
Cibercrime complexo	Leva em conta e amplia a definição da ITU de infrações cibernéticas complexas ou combinadas, as que se enquadram em mais de uma categoria do cibercrime convencional.	Ciberterrorismo, ciberguerra, ataques contra a infraestrutura crítica, ciberespionagem e ação dos hackers.	Combinação de inteligência, ação militar e segurança pública, visto que há distintas fontes múltiplas e potenciais de ataques (sejam internas ou externas) assim como alvos.	Espionagem comercial e ação dos hackers são duas porém distintas ameaças. Há escassa comprovação de que o Brasil sofra de outros tipos de ameaças nesta categoria.
Ameaças emergentes	Ameaças relativas à expansão do ciberespaço que não se enquadram bem nas categorias da ITU, ou por serem emergentes ou por sua relação com o mundo em desenvolvimento.	TICs empregados pelos mais tradicionais grupos criminais, quadrilhas do crime organizado (drogas e tráfico de armas, extorsão digital, difusão da cultura de violência), ciberlavagem de dinheiro e sonegação fiscal, etc.	Deveria estar mais ligado à segurança pública, porém este campo acaba de emergir e há falta de reação do estado.	O Brasil sofre com os altos níveis de violência interpessoal e organizada, em especial com relação às quadrilhas e o crime organizado que lucra com o tráfico de drogas. Estes já assimilaram o poder das TICs para expandir e fortalecer seus negócios.

Cibercrime convencional

A exemplo das demais atividades ilícitas do mundo real, o cibercrime é extremamente difícil de mensurar com precisão. O ciberespaço é simplesmente enorme e descentralizado demais para aquilatar, acompanhar e relatar com certeza toda a sua atividade dolosa. Com efeito, torna-se bastante difícil até estimar uma ordem de grandeza da cibercriminalidade. Deve-se isto à relutância dos governos e empresas em divulgar este tipo de informação por temor de danos a suas reputações e perda de confiança e investimento. No entanto, algumas agências de estado assim como firmas privadas de cibersegurança emitem relatórios regulares sobre as dimensões estimadas dos mercados da cibercriminalidade. Valores e dados que na melhor hipótese são aproximações brutas, levando a amplas discrepâncias no impacto projetado destes mercados. Não obstante, os mesmos proporcionam alguma visão das grandes tendências capazes de deflagrar a determinação de prioridades assim como as questões sobre a alocação de recursos.

Os relatórios disponíveis apontam para expressivo aumento da cibercriminalidade no Brasil no decorrer da década. Tal expansão coincide com o acesso ampliado aos TICs em todo o país a partir do ano 2000. A quantidade total de incidentes cibernéticos recebidos pelo CERT.br (a central do Grupo de Resposta a Incidentes de Segurança em Computadores, ou CSIRT, no Brasil), saltou de 6000 em 2000 para mais de 466.000 em 2012.[29] Pelo menos 75 por cento dos usuários da Internet no Brasil dizem ter sido vítimas de uma ou outra forma de cibercrime. A média global é de 67 por cento, com as maiores taxas localizadas na Rússia (92 por cento), China (84 por cento) e África do Sul (80 por cento). No tocante aos hackers dos perfis das redes sociais, o Brasil encabeça a classe em conjunto com a China, com 23 por cento dos usuários que acusaram a tomada de suas contas por outros usuários. No mínimo 12 por cento dos brasileiros relatam que seus PCs foram infectados por *malware* através de manobras de *phishing* por falsos portais transmitidos pela mídia social.[30]

As empresas de cibersegurança também oferecem indicações sobre as dimensões das atividades digitais dolosas no Brasil. De fato, o Brasil consta em primeiro

29 Incidentes Totais em Computadores Relatados ao CERT.BR todo ano (1999-2012). Veja http://www.cert.br/stats/incidentes/ (CERT.br possui estatísticas sobre avisos dos incidentes ocorridos. Estes são espontâneos e se referem a incidentes ocorridos nas redes que avisaram a CERT.br espontaneamente).

30 Veja http://oglobo.globo.com/tecnologia/brasil-perde-16-bilhoes-por-ano-com-ciberataques-6280831#ixzz2BZTx7kkV.

lugar na região da ALC, como fonte e alvo dos ataques digitais. O mesmo vale para toda sorte de infrações cibernéticas cometidas através da informática, a exemplo de códigos maléficos, *spam zombies, phishing hosts* e *botnets*, entre outros. Estas tendências grassam a taxas alarmantes. A cibercriminalidade no Brasil evoluiu a passos largos na última década, sendo que as firmas de segurança dos Estados Unidos e Europa identificaram o Brasil como um dos países mais problemáticos desde 2006 por suas atividades com o cibercrime.[31] Os principais cibercrimes cometidos no Brasil na atualidade incluem a difusão de vírus ou *malware* (68 por cento), *hacking* de perfis na mídia social (19 por cento) assim como o *phishing* (11 por cento).[32] Embora o Brasil confirme sua grande atividade com *spam* (3,4 por cento dos fluxos globais em 2012, colocação modesta em comparação com a liderança, EUA com 42,2 por cento), os fluxos vêm decrescendo visivelmente e já não são problema grave entre os usuários.[33]

A fraude bancária é quase que uma especialidade no Brasil, em parte por motivo do tamanho do setor de serviços bancários no país.

A Federação Brasileira de Bancos – FEBRABAN relata que as perdas totais das instituições financeiras em 2011 atingiu R$ 750 milhões. A mesma observou também que 60 por cento do incremento anual nas fraudes bancárias ocorreram através da Internet, telefonia móvel, operações das centrais de atendimento e cartões de crédito. Um relatório da Kapersky Labs em 2011 colocou o Brasil na frente da China e da Rússia no emprego do *trojan horse* para penetrar nas contas bancárias através da rede: 16,9 por cento do total em ataques anuais partiram contra usuários no Brasil, contra 15,8 por cento na Rússia e 10,8 por cento na China.[34] Não obstante, grande parte destas fraudes foram perpetradas fora dos meios digitais, através de fraudes com telefones e cartões de crédito (US$ 450 bilhões). Diz-se que foram perdidos US$ 150 milhões através da Internet e do

31 Veja http://www1.folha.uol.com.br/tec/1143535-cibercriminoso-brasileiro-promove-ataque-sofisticado-a-banco-on-line.shtml.

32 Ibid. Em 2012 o Brasil constava em quarta colocação nos ataques de *phishing* (4%), atrás apenas dos EUA (29%), do Reino Unido (10%) e Austrália (5%). As perdas totais daquele ano por esta classe de fraude foram de US$ 10,5 bilhões. Fonte: Veja http://www1.folha.uol.com.br/mercado/1181392-ataques-ciberneticos-causam-perdas-de-us-21-bilhoes-a-empresas.shtml (RCA/EMC data).

33 As estatísticas de spam são criadas através de informações adquiridas por via de reclamações ao SpamCop e remetidas ao CERT.br. Veja http://cetic.br/seguranca/index.htm e http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33298&sid=4#.UXpdF6LU_Io.

34 Vejahttp://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (dados Kapersky).

e-banking móvel. Outros US$ 150 milhões foram furtados mediante pagamentos digitais de faturas de cartões de crédito.[35] Em algumas regiões o Brasil supera a América do Norte e a Europa Ocidental em segurança digital do setor bancário: por exemplo, a alteração dos sistemas de senhas, verificação em dois estágios e a biométrica se tornaram padrão.

O Brasil se tornou um porto seguro de outras espécies de cibercrimes identificados pela International Telecommunications Union (ITU). Entre estes, os principais são aqueles perpetrados contra empresas e negócios,[36] relativos a conteúdo[37] assim como infrações contra direitos autorais e marcas registradas.[38] Os custos globais do crime via Internet no Brasil, inclusive fraude e furto de informações bancárias, atinge cerca de US$ 8 bilhões anualmente (ou 7 por cento do total de perdas globais geradas pela cibercriminalidade).[39] Tais estimativas sugerem que o país seja o terceiro mais afetado em todo o mundo pelas atividades digitais ilícitas. O Brasil é de longe o alvo número um na América Latina: O México fica atrás do Brasil com perdas anuais de cerca de US$ 2 bilhões por conta da cibercriminalidade.

35 Vejahttp://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl.

36 PricewaterhouseCoopers (PwC) definiu que 32% das empresas brasileiras são vítimas de alguma forma de cibercrime a cada ano. Valor mais elevado do que a média global (223%). A PwC calculou que 39% (a maioria dos negócios atingidos) sofreu perdas entre US$ 100,000 e US$ 5 milhão. Cerca de 5% sofreram perdas de até US$ 1 bilhão. A demais, apenas 24% das empresas brasileiras afirmaram poder detectar e conter o vazamento de dados sensíveis sobre seus clientes e fornecedores. Veja http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (dados da PricewaterhouseCoopers) e http://www1.folha.uol.com.br/fsp/tec/90924-empresas-falham-na-protecao-de-dados-admitem-executivos.shtml.

37 Veja dados no portal da Safernet (http://indicadores.safernet.org.br/). A Safernet é uma ONG brasileira que centraliza relatórios sobre infrações digitais no Brasil relativos a conteúdo.

38 Pouco se sabe sobre o âmbito e a escala deste mercado cinzento no Brasil, porém podemos colher informações da International Intellectual Property Alliance (IIPA), a qual concluiu em um relatório recente que a Internet é o principal vetor da pirataria no Brasil, com crescimento exponencial. A mesma acrescentou que esta atividade ilícita dá origem a "perdas globais na economia que totalizam US$ 4,16 bilhões." Cerca de um bilhão de canções são baixadas de modo ilícito todo ano no Brasil, sem mencionar outras formas de propriedade intelectual e artística. Veja IIPA "2012 Special 301 Report on Copyright Protection and Enforcement".

39 Veja Norton/Symantec "*Norton Cybercrime Report 2012*" http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml.

Cibercrime complexo

■ Outra categoria da cibercriminalidade acha-se nas chamadas *infrações cibernéticas complexas* – em especial as ameaças às instituições governamentais.[40] Suas dimensões e natureza no Brasil ainda não se acham muito claras. Há uma falta de pesquisas quantitativas e qualitativas que ilumine a escala destas "ameaças", embora os especialistas demonstrem preocupação. Em seu lugar, há evidência empírica de infrações complexas passíveis de servirem como indicação de fenômenos mais amplos. Tais infrações são as que mais preocupam os governos federal, estaduais ou municipais, além das forças armadas e da segurança pública, até certo ponto. As mesmas também informam e orientam as escolhas dos governos no tocante à formação de infraestrutura da cibersegurança. Os maiores preocupados com as infrações cibernéticas complexas reproduzem estatísticas e empirismos repetidas vezes, porém sem apresentar evidências ou dados de corroboração. Há três infrações cibernéticas merecedoras de atenção especial.

Primeiro, ao contrário das formas benignas do ativismo digital, As autoridades no Brasil visam a ação dos hackers com grande suspeita. Não estão claras as dimensões dos danos físicos e econômicos ocasionados pelos hackers, sejam oriundos de alterações na aparência dos portais governamentais ou do setor privado, ou ataques contra a infraestrutura (DDoS). A maior preocupação das autoridades reside sem dúvida no furto e divulgação de informações oficiais sensíveis. Na forma dos casos Assange e Snowden, as informações obtidas por estes meios poderão ser divulgados e espalhados com rapidez e eficiência. Em outras ocasiões as informações poderão servir para negociações, extorsões e chantagens. No Brasil, governo (a Presidência e diversos ministérios, inclusive o Itamaraty), as forças de segurança (inclusive exército e forças policiais),[41] assim como empresas públicas e privadas (Petrobras e bancos, a exemplo do Banco do Brasil, Itaú e Bradesco), alvos frequentes dos hackers.[42]

---

40 São definidas pela ITU as infrações complexas ou combinadas, como tipos de cibercrimes passíveis de serem enquadradas em mais de uma categoria entre as que seguem: *Infrações contra a confidencialidade, integridade e disponibilidade de dados de computação e sistemas; infrações relativas a conteúdo; infrações relativas à computação; e infrações relativas a direitos autorais e marcas registradas.* Veja ITU (2009), pags. 51-59.

41 Veja http://www1.folha.uol.com.br/cotidiano/1211459-hackers-invadem-perfil-de-gcm-e-divulgam-dados-pessoais-em-rede-social.shtml.

42 Veja alguns outros casos e exemplos em http://www.bloggingsbyboz.com/search/label/cyber-security.

Os grupos de hackers mais em evidência no Brasil são os Anonymous e LulzSec, embora o segundo tenha supostamente suspendido suas atividades.[43] Devido ao desejo de preservar o anonimato assim como a estrutura descentralizada e não hierarquizada, os integrantes dos grupos são de difícil aproximação. Quando se manifestam, justificam seus atos com base em ideais tênues,[44] a exemplo de sua contrariedade às "desigualdades difundidas na América Latina" (em se tratando de grandes empresas e instituições financeiras) e "contra a manipulação generalizada de informações pelas autoridades."[45] Em outras ocasiões, os hacktivistas objetivam mais a realização de trotes e promoção de traquinagens. Os ataques do gênero eram mais frequentes em 2011 e no início de 2012 (Mais de 1250 casos).[46] No decorrer de 2012 e início de 2013 a incidência se reduziu rapidamente. A ação dos hackers tende a ocorrer em situações específicas, como a votação de um projeto controverso no Congresso. Não causa surpresa que durante os protestos de rua em meados de 2013 houve um surto expressivo este ativismo, visando a mídia preponderante do país, inclusive Globo e Veja.[47] A Copa das Confederações de 2013 e a Copa do Mundo de 2014, promovidas pela FIFA, se tornaram alvos.

Segundo, o governo brasileiro detectou ataques crescentes contra os sistemas e redes do estado. Tais ameaças alarmam as autoridades, em especial a administração pública federal bem como as forças armadas. O Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI-PR) é o responsável pela primeira e garante "a disponibilidade, integridade, confidencialidade e autenticidade" das informações e comunicações nesta esfera. Desde 2009, o Diretor do DSIC e chefe da cibersegurança no Brasil, Raphael Mandarino,[48] aludiu diversas vezes a algo como 2000 ataques lançados por hora contra as 320 redes públicas federais. Embora raramente se mencione a origem dos ataques, Mandarino argumenta

43 Veja http://idgnow.uol.com.br/seguranca/2011/06/27/lulzsec-encerra-atividades-depois-de-50-dias-de-caos/.

44 Com efeito, durante os protestos de 2013, a ação do grupo Anonymous no local adotou uma postura de pouca relevância, sem muitos objetivos nítidos. Veja http://www.diariodocentrodomundo.com.br/o-ultrarreacionarismo-do-anonymous-do-brasil/.

45 Veja http://www.google.com/hostednews/afp/article/ALeqM5jyNoFn4ZXfibMLdscIqXDnIXVDjw e http://itdecs.com/2011/06/brazil-suffers-its-biggest-cyber-attack-yet/.

46 Veja Wyss (2011) e Kishetri (2013), p. 145.

47 Veja http://www.anonymousbrasil.com/brasil/twitter-da-veja-e-hackeado/ e http://www.tecmundo.com.br/Ataque-hacker/42249-Perfil-do-G1-no-Twitter-e-hackeado-por-ativistas.htm.

48 Veja http://www.gsi.gov.br/sobre/quem_e_quem/quem_e_quem_secretaria_executiva.

que 70 por cento constituem esforços para se obter informações financeiras dos bancos públicos.

Outros 10 por cento visam a INFOSEG no Ministério da Justiça, rede fechada que abriga quantidades de dados sobre investigações e processos criminais. Mais 15 por cento destinam-se a desvendar dados pessoais de funcionários públicos.[49] O General José Carlos dos Santos, antigo comandante do CDCiber, com frequência chamou a atenção às dimensões dos ataques contra as redes militares, de cerca de 30.000 diárias.[50] Surpreende o fato de que parte preponderante (30 por cento) destas redes estão sob a administração de provedoras privadas e das redes civis,[51] revelação inquietante à luz da sensibilidade das informações militares. Em que pese tamanha escala dos ataques diários perpetrados contra estas redes – muitos com motivação criminosa ou econômica – apenas dois casos lograram o vazamento de informações para o domínio público.[52]

A terceira ameaça cibernética complexa é o ciberterrorismo e a ciberguerra. Invoca-se regularmente a ameaça terrorista pelos governos e forças armadas em todo o mundo, para justificar a securitização do ciberespaço de um país. Por exemplo, os militares dos Estados Unidos elegeram a cibernética com a quinta mais importante prioridade do campo de batalha. No Brasil, um par de fatores são frequentes para justificar a postura rígida das autoridades com a cibersegurança. O primeiro e a proteção das *infraestruturas nacionais críticas*. As revelações sobre o *worm* Stuxnet infiltrado em 2010 nas instalações de enriquecimento de urânio em Natanz, no Irã, deu causa a expressiva apreensão no Brasil. De fato, circulou em Brasília uma leva de boatos infundados de que o apagão nacional há alguns anos teve origem em um ataque semelhante.[53] Com as autoridades do ramo no país incapazes de explicar os motivos dos apagões, os especialistas em cibersegurança lembraram os alegados ataques cibernéticos às redes de trans-

49 Veja http://info.abril.com.br/noticias/seguranca/redes-do-governo-tem-48-mil-ataques-por-dia-23082009-4.shl.

50 Vejahttp://www.defesanet.com.br/cyberwar/noticia/1632/CDCiber---Na-guerra-cibernetica--Brasil-adota-estrategia-do-contra-ataque.

51 Veja Canal Livre (programa de TV da Rede Bandeirantes, 29 de julho de 2011. Disponível em http://www.youtube.com/watch?v=lD8N7y86Aow.

52 O primeiro vazamento foi de informações não restritas e não sensíveis. Incluiu dados pessoais dos soldados ocupados em projetos sociais no Nordeste brasileiro. O segundo caso tratou da divulgação de detalhes pessoais de nomes e endereços de policiais com base no Rio de Janeiro, durante os protestos de 2013. Veja http://www1.folha.uol.com.br/cotidiano/2013/09/1342381--hackers-invadem-site-e-divulgam-dados-de-50-mil-policiais-militares-no-rio.shtml

53 O noticiário dos Estados Unidos jamais sustentou tais afirmações com evidências factíveis.

missão de 2005 e 2007.[54] A proteção da CNIS contra as "ameaças externas" de certa forma se assemelha à teoria convencional de dissuasão. Caso as autoridades acreditem que o "inimigo" seja capaz de danos reais – mesmo sendo mínimas a ocorrência de um ataque – as mesmas investirão nas defesas nacionais contra as possíveis ameaças.

Para as autoridades brasileiras, a grande preocupação é visibilidade de suas *redes de megaeventos*. O Brasil tem acolhido um número crescente de grandes iniciativas, inclusive eventos esportivos, conferências internacionais e festivais de arte.[55] Com isto, as principais cidades como Brasília, Rio de Janeiro e São Paulo figurarão no palco global. O CDCiber se encarrega da proteção destas redes. Como exemplo, há o papel do CDCiber em segurança na Conferência da ONU Rio+20 em 2012. A unidade se juntou à Polícia Federal para proteger as redes de ataques recorrentes durante o evento.[56] Embora a maioria das incursões partiram de criminosos comuns, houve também ataques mobilizados por grupos de hackers (por ex: o Anonymous) e outros que visavam dados sensíveis.[57] O CDCiber também atuou na coordenação da cibersegurança durante a visita ao Brasil do Papa Francisco, bem como na Copa das Confederações (2013) e a Copa do Mundo (2014) da FIFA. Persiste a questão se a ameaça do terrorismo ou um ataque solitário faz jus a uma resposta complexa.

O quarto risco em uso atualmente no aumento da securitização do ciberespaço é a *ciberespionagem*. Antes de 2013, o Brasil não registrava casos de ciberespionagem por um governo estrangeiro. De certo, não havia relatos públicos mesmo de espionagem industrial antes da figura de Edward Snowden, perto da época dos protestos digitais e de rua em meados de 2013. O que mudou por completo com as revelações da vigilância em massa pela NSA – Agência de Segurança

54 Impressiona a falta de informações precisas sobre o caso. Um documento atribui a alegação a um discurso do Presidente Obama, o qual se referiu ao caso sem dar nome ao país: "Sabemos que os intrusos acessaram nossa rede de transmissão de energia, e que em outros países tais ataques mergulharam cidades inteiras na escuridão. Agora ficou claro que esta ameaça cibernética figura como um dos mais graves desafios econômicos e de segurança nacional que a nação já enfrentou." Veja http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf.

55 Os eventos incluem por exemplo a Copa das Confederações (2013) e a Copa do Mundo (2014) da FIFA, além dos Jogos Olímpicos no Rio de Janeiro (2016).

56 Vejahttp://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

57 O grupo Anonymous lançou a operação #OPHackInRio durante a Rio+20. Veja http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.Vejahttp://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

Nacional dos Estados Unidos. De acordo com uma série de artigos do *Guardian* e demais agências de notícias, milhões de telefonemas e emails de brasileiros foram interceptados pela NSA.[58] Em se tratando da intensidade da vigilância cibernética patrocinada pela NSA, o Brasil se coloca em segundo lugar atrás dos Estados Unidos.[59] Diz-se que as autoridades de inteligência dos Estados Unidos justificaram esta vigilância devido à ocupação pelo Brasil de posição estratégica na administração de uma estrutura global de telecomunicações (i.e. linhas de transmissão e cabos de fibra óptica). Não se tratava de inimigos, retrucaram, mas apenas a "proteção" destes ativos críticos. Ao mesmo tempo houve alegações de interceptação de telefonemas e emails da Presidente Dilma Rousseff, de autoridades do Ministério de Minas e Energia e de altos executivos da Petrobras,[60] as quais conduziram ao cancelamento da visita de estado da Presidente aos Estados Unidos e acusações na ONU.[61]

Naturalmente, o governo brasileiro não é totalmente inocente no tocante à ciberespionagem. Ao passo que as autoridades do país expressaram sua indignação contra a vigilância pela NSA, foram autorizados ABIN e CDCiber – os responsáveis pela proteção do país precisamente contra este tipo de interferência – a monitorar as atividades das mídias sociais no Brasil relativas aos protestos em massa de junho a agosto de 2013.[62] A ABIN recebeu críticas por não antecipar os eventos que deram origem aos protestos de 2013. Mesmo assim, a ABIN introduziu a plataforma Mosaico, de monitoramento da mídia social, para rastrear usuários e se adiantar aos novos acontecimentos. O sistema de monitoramento é controverso aos olhos de alguns ativistas da Internet, pois poderá levar à autocensura bem como a pressões sobre os movimentos sociais legítimos.[63] O mesmo se

58 Vejahttp://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934.

59 Veja http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/.

60 Veja http://noticias.uol.com.br/internacional/ultimas-noticias/2013/10/06/ministerio-de-minas-e-energia-foi-espionado-por-canadenses.htm.

61 A Presidente Dilma Rousseff instou a ONU a se adiantar e regular a conduta dos estados no tocante aos TICs e declarou que o Brasil "apresentaria propostas para a definição de uma estrutura civil multilateral de governança e emprego da Internet, em garantia da proteção efetiva de dados que transitam através da rede" (veja maiores detalhes na seção quatro). Veja o discurso completo em http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

62 Veja http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915.

63 Veja http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm.

diz do programa Guardião elaborado pelos militares no CDCiber.[64] No entanto, o Brasil avança na consolidação de seu controle sobre seu ciberespaço. O governo brasileiro possui parceria com Portugal de um c abo de fibra óptica de US$ 185 milhões, em garantia de maior autonomia sobre o tráfego de Internet a partir de e para o país.[65]

Formas emergentes da cibercriminalidade e lacunas de conhecimento. Antecipar e rastrear as ameaças cibernéticas se tornou um desafio de peso para governos e empresas. As ameaças tratam das probabilidades, se existem e quando e onde poderão ocorrer. A abordagem crítica destas duas dimensões poderá contribuir para esclarecer o que as instituições deixam de enxergar e o que não desejam enxergar em razão de interesses mesquinhos. Há uma série de áreas carentes de maior debate, apenas para alargar o diálogo no Brasil sobre os delitos digitais. É importante levá-los em conta, de forma a contestar as reações mal concebidas.

Em primeiro lugar, há a questão de quem são os infratores. O especialista em cibersegurança Mikko Hypponen, da F-Secure, afirma que os governos perdem a batalha contra os infratores porque não investem o suficiente para determinar quem são eles. Os estados tampouco possuem indícios de sua motivação, natureza organizacional ou mesmo seu tipo de atividade. Este conhecimento é essencial na elaboração de estratégias eficazes de restrição, administração, prevenção e redução da cibercriminalidade. Em seu lugar, há a tendência de combinar as categorias de infratores, o que levaria a uma reação genérica ao cibercrime e não ao reconhecimento da natureza heterogênea da prática de crimes. Seus integrantes adaptam com frequência suas ferramentas e métodos, para contornar os novos mecanismos de defesa cibernética.

A Polícia Federal no Brasil criou uma base de dados de pessoas sujeitas a processos em razão de cibercrimes. Com a promulgação da nova legislação contra a cibercriminalidade, este conjunto de dados irá aumentar e cobrir uma gama ampliada de infrações cibernéticas. Organizar e colocar em prática estes dados é fundamental. Ao invés de recorrer a uma rede de arrasto, o conjunto auxiliará informar e moldar as estratégias de cibersegurança de modo a aliviar determinadas ameaças. Já temos ciência de alguns fatos através dos dados existentes:Tipicamente, os meliantes brasileiros são homens de boa formação, de classe média alta entre 25 e 35 anos de idade. No entanto, estas informações têm

64 Vejahttps://protestos.org/2014/06/18/exercito-usou-software-guardiao-para-monitorar-redes-sociais/.

65 Veja http://www.bloomberg.com/news/2014-10-30/brazil-to-portugal-cable-shapes-up-as-anti-nsa-case-study.html.

como base uma pequena amostragem de 177 pessoas presas e acusadas de fraudes cibernéticas entre 2010 e 2012.[66]

De acordo com a Polícia Federal, não há registros públicos de ataques por pessoas ou por grupos estrangeiros,[67] porém, estas incursões poderão tomar vulto. Devido em parte à realização no país de diversos megaeventos, à sua classe média em ascensão e à digitização dos serviços financeiros, os brasileiros com certeza irão enfrentar ataques mais freqüentes da cibercriminalidade estrangeira.[68] Há também evidências de que desde 2004, que a infração cibernética incrementou suas atividades estrangeiras.[69] Portugal e Espanha se tornaram alvos principais, embora a cibercriminalidade do Brasil tenha dado maior atenção a um mais amplo conjunto de comunidades de língua portuguesa e espanhola nos Estados Unidos, no Reino Unido e nas Américas do Sul e Central.[70]

O *modus operandi* dos hackers nacionais passou a ser entendido através de uma série de revelações recentes. Um antigo hacker no Brasil relatou como os grupos do cibercrime tendem a se organizar em grupos de três a cinco pessoas. Estas poderão se encontrar em uma única cidade, estado ou país, ou mesmo em diversos países. Muitos deles também integram fóruns de cibercriminalidade na *Deep Web*, a parte da Internet não acessada pelas ferramentas de buscas padrão. No entanto, estes fóruns começaram a rarear em razão da infiltração pelas autoridades de segurança pública e de inteligência, internacionais e dos Estados Unidos. Em geral há um contato chave de intermediação direta com grupos criminosos organizados, o qual fornece os recursos para criar os códigos maléficos. Há casos de traficantes de drogas, por exemplo, que pagam programadores de software para a criação de portais ilícitos,[71] facilitando a venda de narcóticos. Um excelente exemplo é a SilkRoad[72], embora existam muitos outros.

66 Veja http://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl?2.

67 Entrevista com o antigo chefe da Unidade da Polícia Federal de Repressão à Cibercriminalidade, o Delegado Sobral. O CERT.br relata que apenas 20% dos ataques em sistemas e redes no Brasil têm origem no exterior. Isto não significa que os ataques sejam necessariamente perpetrados por brasileiros, com o emprego dos IPs remotos fora do território nacional.

68 Entrevista com o Delegado Sobral.

69 Veja Glenny (2009).

70 Veja http://goo.gl/orTW9.

71 A *Deep Web* constitui um vasto ecossistema de portais e comunicações normalmente não catalogados pelas ferramentas de buscas convencionais, e com frequência acessíveis apenas remotamente. As estimativas definem a mesma em 500 vezes do tamanho da Rede "visível" ou de superfície. Veja, por exemplo, http://en.wikipedia.org/wiki/Deep_Web.

72 Diz-se que a SilkRoad foi derrubada por um hacker em 2013. Veja http://www.bbc.co.uk/news/technology-22381046.

Há outrossim conhecimento da *migração do crime organizado tradicional para o ciberespaço.* As quadrilhas têm marcado maior presença virtual – em especial nos portais da mídia social. Os traficantes e grupos de milícias publicam periodicamente testemunhos de seus feitos e inimigos no Facebook, Twitter e YouTube.[73] São exibidos clips frequentes dos chamados *funks proibidões,* enaltecendo a violência virtual.[74] Mais nefasto, os grupos do crime organizado já adotaram novas técnicas de expansão não apenas das redes de drogas, prostituição e contrabando, mas também da intimidação, coerção e proteção do território. Houve a migração para os crimes com caixas automáticas – passando pela remoção de máquinas inteiras de suas fixações até a prática delicada de clonagem dos cartões de crédito.[75]

De sua parte, a Polícia Federal e outras começaram a rastrear o movimento do crime organizado e das quadrilhas virtuais, inclusive nas cidades grandes e médias. Embora haja apenas poucos exemplos de grupos de cidadãos que empregam ferramentas de *crowd-mapping* para detector crimes bem como a vitimização (principalmente por temor de retribuição[76]), as agências de segurança têm investido em peso na analítica de previsão e em sistemas de fusão de dados para prever tendências e padrões da criminalidade.

A principal preocupação das autoridades brasileiras é a *lavagem de dinheiro*. Estimativas recentes sugerem que a lavagem abrange entre US$ 2,5 e 4 bilhões por ano no Brasil.[77] O ciberespaço facilita o movimento, segmentando e dispersando os recursos anonimamente. Embora não considerado como um "grande" crime cibernético no Brasil, a questão é levada muito a sério pela Polícia Federal e o Ministério da Justiça. Por exemplo, o governo designou *laboratórios de tecnologia contra a lavagem de dinheiro* (LAB-LDs),[78] os quais empregam ferramentas digitais para análise, interpretação e investigação. Estas novas tecnologias são utilizadas para rastrear os crimes de colarinho branco a exemplo da sonegação fiscal, além de atividades sistêmicas de lavagem de dinheiro.

---

73 Veja http://www.vice.com/read/mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief.

74 Veja por exemplo, http://www.youtube.com/watch?v=u2thkZZvyos e http://www.youtube.com/watch?v=GtAGrAhnfu4.

75 Informações fornecidas pela URCC da Polícia Federal durante entrevista.

76 Veja Muggah e Diniz (2013).

77 Veja Ollinger (2013).

78 Veja http://goo.gl/2u1Uz e a estratégia nacional contra a corrupção e lavagem de dinheiro (ENCCLA) desde 2006.

Um objetivo central das instituições nacionais de segurança é a proteção da integridade da CNIS. Embora os sistemas como a SCADA[79] e outros sejam de fato desligados da Internet, sua vulnerabilidade a ataques não fica inteiramente limitada. Algumas autoridades do país reconhecem que a sua CNIS depende menos de sistemas de controle informatizado em comparação com países mais desenvolvidos,[80] o que paradoxalmente protege sua infraestrutura contra ataques. Embora aqui haja vantagem em termos de cibersegurança (justamente em razão da menor interconectividade com outras redes), o governo não alardeia este fato, passível de transmitir fraqueza na condição de potência emergente. Neste meio tempo, emerge outro plano nacional de proteção da infraestrutura crítica, distinto da atual arquitetura da cibersegurança nacional.[81]

A MÃO PESADA DO ESTADO

■ O Brasil desenvolve uma infraestrutura de cibersegurança que tende em maior grau às prioridades militarizadas e securitizadas. O foco durante o processo visa em especial alguns tipos específicos de ameaças cibernéticas, visivelmente desconhecendo outras. Tais escolhas possuem expressivas consequências para a governança cibernética no Brasil. Com efeito, as decisões tomadas pelas instituições públicas influenciam a escala e o âmbito da vigilância, questões de neutralidade da rede, proteção (ou sua ausência) da privacidade assim como os direitos à informação pelos cidadãos. Logo, torna-se importante saber como o Brasil desenvolve sua arquitetura de cibersegurança. Ademais, torna-se crítico analisar as regras e práticas que regem a governança cibernética no país.

79 SCADA é a sigla de "controle de supervisão e aquisição de dados". Trata-se de um sistema de controle industrial informatizado de monitoramento e controle dos processos mecânicos em situações reais [O que é um "processo mecânico em situação real?" -NT] que ocorre em indústrias e demais instalações como a CNIS.

80 Informações fornecidas por um dos nossos entrevistados. O Brasil não aparece no documento elaborado pela TrendMicro a pedido da OAS CICTE, que avalia o grau de "conectividade" da CNIS nos países da América Latina. Veja TrendMicro (2013).

81 Há em andamento um Plano para a Segurança da Infraestrutura. Por enquanto há apenas uma referência disponível ao público sobre como o governo pretende proteger a infraestrutura de informações críticas, de autoria do DSIC: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf.

A arquitetura institucional de cibersegurança do Brasil

■ Há uma variedade de órgãos públicos que se ocupam da administração da cibersegurança nacional. Muitas destas visam apenas administração os sistemas, o desenvolvimento técnico e o aperfeiçoamento das ferramentas. Temos como exemplos o CSIRT (CERT.br) local, o Centro de Informações de Rede (NIC.br, encarregado de administrar os principais nomes de domínio no país) o Centro Renato Archer para Segurança da Informação, do Ministério de Ciência e Tecnologia, SERPRO e INI, entre outros. Uma pequena parcela trata do campo da cibersegurança como um todo. A depender da agência, a mesmo poderá se ocupar da elaboração de normativos, tomar decisões políticas ou autorizar iniciativas desde o nível nacional ao local.

Há uma hierarquia de instituições de estado que se ocupam da administração da cibersegurança nacional. No topo da pirâmide se encontra o *Gabinete de Segurança Institucional* (GSI). Diretamente ligado à Presidência, o GSI é o órgão governamental chave que trata de todos os aspectos civis de cibersegurança. É responsável também por outras áreas, inclusive assuntos militares e defesa cibernética (integra o *Conselho de Defesa Nacional* – CDN). As ramificações do GSI incluem o *Departamento de Segurança da informação e Comunicações* (DSIC), voltado para garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicações na administração pública federal. Há uma coordenação muito próxima com a *Casa Civil*, também voltada à supervisão da concessão de certificados de segurança digital (para a infraestrutura pública chave). Ademais, encontram-se no GSI a *Secretaria de Assuntos Estratégicos* (SAE) assim como a *Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo* (CREDEN), comissão de assessoria da Presidência. O conjunto DSIC, SAE e CREDEN é o protagonista chave na formulação dos debates sobre a cibersegurança no país.[82]

Outras instituições que influenciam a pauta de cibersegurança no Brasil incluem o *Departamento de Polícia Federal* (DPF), sob a supervisão do *Ministério da Justiça* (MJ). Embora seu papel primordial seja a segurança pública em nível federal, ela também possui unidades voltadas para a cibersegurança. De igual maneira, a *Agência Brasileira de Inteligência* (ABIN) que monitora a mídia social, assumiu competências criptográficas na proteção das instituições públicas.

82 Os mesmos propuseram recentemente a elaboração para o país de uma estratégia nacional de longo prazo para a cibersegurança e defesa cibernética.

Tal atividade é conduzida através da *Centro de Pesquisas e Desenvolvimento para a Segurança das Comunicações* (CEPESC). Por fim, há o *Ministério da Defesa* (MD) que supervisiona as forças armadas e serve de ligação entre civis e militares. O papel do MD na formulação da arquitetura de cibersegurança nacional passa por análise mais pormenorizada nas seções seguintes. O MD abriga também o Estado-Maior Conjunto das Forças Armadas (EMCFA), com um papel também na coordenação da reação cibernética.

Reações normativas às ameaças cibernéticas

■ O Brasil agiu com celeridade na elaboração de leis sobre a Internet bem como a cibercriminalidade. Há no momento mais de 1000 projetos de lei sobre o tema em trâmite no Congresso Nacional. [83] O *Marco Civil da Internet* é de longe o mais importante e de mais amplo conhecimento. O *Marco Civil* é a "Declaração dos Direitos" da Internet nacional e a primeira do gênero em todo o mundo.[84] A iniciativa no Brasil tem grande aprovação popular e recebeu expressivo apoio dos usuários da Internet durante sua elaboração inicial. Sua formulação se deu mediante um processo participativo, com contribuições de todo o país. O *Marco Civil* estabelece os princípios fundamentais para Internet, inclusive a liberdade de expressão, neutralidade da rede e proteção à privacidade. O projeto recebeu aprovação em abril de 2014 e espera-se que o mesmo fortaleça e preserve os direitos dos usuários, que por sua vez será passível de se contrapor a práticas mais nefastas que solapam os direitos dos usuários.

O Congresso Nacional deveria ter aprovado o *Marco Civil* já em 2012, porém as divergências com relação a duas questões chave detiveram o andamento do processo. A primeira destas versava sobre a *neutralidade da rede*. As empresas de telecomunicações procuraram obstruir e debilitar o princípio da neutralidade da rede, tentando limitar as proteções jurídicas.[85] O segunda questão controversa era sobre infrações aos *direitos autorais*. Os setores dependentes da manutenção dos direitos autorais desejavam o poder de exigir a remoção pelas ISPs de conteúdo ilícito sem ordem judicial. E apesar da oposição das telecoms e dos setores de direitos autorais, o Congresso agiu para conservar a neutralidade da rede e impedir

83 Veja http://observatoriodainternet.br/link-estadao-pls-de-internet-no-pais.

84 Veja o portal da MCI em http://edemocracia.camara.gov.br/web/marco-civil-da-internet.

85 O argumento do ramo de telecom era de que no mínimo a "redução das conexões rigorosamente por motivos técnicos" deveria ser permitida de modo explícito. Veja *Le Monde Diplomatique Brasil*, N. 65, dezembro de 2012.

a retirada arbitrária de conteúdo (salvo nos casos de vingança e pornografia). Não admira que atualmente o Brasil talvez seja a liderança mundial em solicitações para a retirada de conteúdo do Google.[86]

Outro elemento chave na formação da segurança cibernética e atualmente sob discussão na estrutura do *Marco Civil*, é o chamado *log register.* O mesmo é mecanismo fundamental das investigações cibernéticas e perícias correlatas. O que se acha em jogo durante as supra referidas deliberações legislativas era durante quanto tempo as ISPs e provedores de conteúdo deveriam manter "registros de conexões" para análise pelas autoridades. Diversos especialistas defendiam que a agência regulatória das telecomunicações no Brasil (ANATEL) deveria servir de órgão controlador, embora outros opinavam que o Congresso deveria ditar as regras.[87] Os primeiros venceram e o Congresso Nacional determinou que as ISPs deveriam conservar seus dados durante um ano, os provedores de conteúdo conservando-os por até seis meses. Surgiram também preocupações com a administração dos cibercafés. De um lado, estes desempenham uma função crítica no sentido de facilitar o acesso à Internet para grupos de baixa renda. Por outro lado, são frequentados de modo rotineiro pela cibercriminalidade. No final, a questão não recebeu tratamento direto no *Marco Civil.*

Embora a intenção primitiva do *Marco Civil* era estabelecer garantias e salvaguardas constitucionais relativas à administração do ciberespaço brasileiro, o mesmo se tornou um incentivo para a legislação agressiva de prevenção da cibercriminalidade.[88] Com efeito, foram promulgadas as primeiras leis contra a cibercriminalidade no país em razão da ira popular sobre um caso amplamente divulgado de ativismo por hackers, relativo ao vazamento de fotografias pessoais da conta de email de uma conhecida atriz de novelas. [89] O clamor da mídia tradicional e social atiçou crescentes ansiedades com relação à questão ainda não definida da privacidade digital. O Congresso convocou uma sessão de emergência e promulgou um projeto de lei redigido em 2011 (além de mais outro que dormi-

86 Veja https://knightcenter.utexas.edu/blog/00-13690-brazil-tops-googles-transparency-report-most-requests-censor-online-content

87 Veja http://www1.folha.uol.com.br/tec/2013/06/1295456-analise-rede-esta-virando-uma-ferramenta-de-vigilancia.shtml?utm_source

88 O Brasil foi um dos últimos países na América Latina a adotar a legislação contra a cibercriminalidade. Veja o portal OAS REMJA em http://www.oas.org/en/sla/dlc/remja/cyber_crime.asp

89 A atriz em questão era Carolina Dieckmann, da TV Globo, em 2012.

tava desde 1999). O primeiro projeto de lei – posteriormente lei no. 12,373/12[90] – possui expressivas implicações para os bens da cibernética no Brasil. Um segundo projeto de lei – atualmente a lei no. 12,735/12 – sofreu tantas emendas que sua validade é questionada.[91] Embora alguns críticos[92] argumentem que a legislação é confusa e incoerente, as leis definem com sucesso e elaboram controles e penalidades relativas às atividades na Internet. Por exemplo, é ilícito atualmente "invadir aparelhos de TI", "obter dados privados", ou "interferir ou prejudicar serviços de TI".[93] Muitos aspectos permanecem pouco claros.

Vale a pena observar que estas estruturas e leis mais recentes foram aprovadas em época na qual as autoridades brasileiras começaram a repensar a legislação criminal, a qual remonta a 1940. O novo código penal será votado no próximo ano e embora o mesmo inclua disposições contra a cibercriminalidade, estas não parecem solucionar as contradições e lacunas nas leis em vigor.[94] Há outros 40 projetos de lei relativos à luta contra a cibercriminalidade, que aguardam aprovação pelo Congresso.[95] O estoque em atraso reflete um problema de amplo conhecimento relativo ao excesso de legalismo do sistema político do Brasil; destaca também como o governo do país continua mal aparelhado para reagir ao panorama dinâmico e em célere mutação do cibercrime.

Reações da segurança pública às ameaças cibernéticas

■ As autoridades policiais e militares do país acham-se em vias de investimentos substanciais com a cibersegurança no território. No entanto, parece haver um descompasso entre os tipos de ameaças ao ciberespaço brasileiro e a natureza das reações pelas autoridades se segurança. O crime organizado é uma das principais

90 Veja a lei integral em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

91 Veja http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.

92 Entrevista com Walter Capanema. Veja http://goo.gl/59zMo.

93 A clonagem ou furto de dados de cartões de crédito já foi abordado por leis que criminalizam a falsificação de documentos.

94 Informações fornecidas por Walter Capanema durante o evento SEGINFO 2012 (setembro). Disponível em: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31777&sid=18.

95 Talvez a questão mais importante para a cibersegurança seja o projeto de lei que visa proteger os dados pessoais do usuário. Há uma expectativa entre ativistas de que a mesma seja uma lei equilibrada, que proteja a privacidade enquanto fortaleça e proteja novos serviços importantes para a sociedade digital, a exemplo da computação nas nuvens e a *big data*. Veja http://goo.gl/PqZOF.

ameaças ao ciberespaço nacional, porém são dirigidos recursos no país em disparidade com as soluções militares que melhor serviriam à (um tanto excepcional) hipótese de guerra convencional. Há menos ênfase na ampliação da capacidade da segurança pública do dia a dia, de modo a identificar e reagir aos grupos do crime organizado. Em razão da ausência de uma posição uniforme do governo sobre a questão, e de dados confiáveis, o Brasil possui uma abordagem pouco coerente sobre a cibersegurança. Em seu lugar, poucos órgãos e pessoas que exercem influência estão à frente dos debates de modo a determinar no fundo o futuro da arquitetura nacional da cibersegurança.[96]

A *Unidade de Repressão à Cibercriminalidade* (URCC) da Polícia Federal é a autoridade máxima de segurança pública encarregada da prevenção e reação aos cibercrimes. Suas competências abrangem desde a investigação de crimes contra instituições públicas federais às infrações com ramificações interestaduais e internacionais. Dado que na cibercriminalidade quase sempre figuram pessoas e tecnologias de diversos estados assim como protagonistas no exterior, a Polícia Federal torna-se um agente operacional crítico de certa forma.A mesma se ocupa de investigar fraudes eletrônicas (*e-banking* e golpes com cartões de crédito) bem como redes virtuais criminosas de maus tratos de crianças. Em decorrência da supra referida lei nº. 12,373/12, a Polícia Federal em breve se responsabilizará pelo acesso não autorizado dos sistemas e redes de TI.

A URCC, com base em Brasília, também administra a aparelhagem de ciberinteligência[97] com equipes localizadas na maioria dos estados. Trata-se de grupos de pequeno porte (a própria URCC possui cerca de 20 policiais) e não necessariamente integrados por especialistas em cibersegurança. No entanto a URCC coordena as redes internacionais de segurança pública de forma a facilitar o intercâmbio de informações e administrar protocolos operacionais. Ademais, a agência está ligada diariamente 24 horas por dia à Cooperação Policial de Emergência da Interpol e à Ameripol, podendo também alavancar acordos bilaterais para a cooperação jurídica. A URCC parece operar bem no intercâmbio de informações sobre assuntos operacionais, com as autoridades de segurança pública do exterior e com os tribunais.[98] Em contrapartida, se um caso exigir a colaboração das empresas privadas de Internet nos Estados Unidos, a exemplo de Google ou

96 Vale mencionar dois exemplos, inclusive Raphael Mandarino Jr. (DSIC) e o General José Carlos dos Santos, antigo comandante do CDCiber. Este foi substituído em 2014 pelo General Paulo Sergio Melo de Carvalho.

97 Centro Integrado de Inteligência Policial e Análise Estratégica da Polícia Federal (Cintepol).

98 Entrevista pelos autores com o Delegado Sobral (URCC-DPF).

Facebook, surgem com frequência grandes demoras e entraves.[99] Estas empresas tendem a evitar colaborar com a segurança pública em razão das obrigações jurídicas e contratuais nos países que abrigam seus serviços chave e servidores.[100]

A URCC já realizou operações contra diversos grupos do cibercrime, inclusive Trojan Horse, Matrix, Ponto.com, Liontech e Azahar.[101] Para aperfeiçoar sua capacidade investigativa, a Polícia Federal implantou dois projetos, o *Tentáculos* (de filtração de dados cruzados visando a redução da quantidade de processos em avaliação) e o *Oráculo*, elaborado em especial para a Copa do Mundo da FIFA. O *Oráculo* constitui um sistema analítico prognóstico de inteligência, para a avaliação de ameaças futuras e informações básicas sobre os prováveis autores.[102] A URCC administra também o Centro de Monitoramento em busca de atividades digitais suspeitas. Durante o evento Rio+20 de 2012, a URCC logrou fundir o Centro de Monitoramento com a ala de cibersegurança das Forças Armadas, obtendo mais uma camada de apoio. [103]

As autoridades de segurança pública dos 26 estados do Brasil e do Distrito Federal, acham-se cada vez mais engajados contra a cibercriminalidade em nível subnacional. O agente Alexandre Wendt, identificou oportunidades assim como desafios que confrontas as forças militares bem como da polícia civil.[104] Do lado positivo Alexandre observou o estabelecimento crescente no decorrer da década, de unidades policiais especializadas para combater o cibercrime. Cidadãos e empresas tomaram maior conhecimento destas unidades especializadas e em diversos

99 A Polícia Federal chegou a prender o presidente da filial da Google no Brasil em 2012, após a mesma se negar a retirar o vídeo do YouTube que comprometia um político do país (observação de Daniel Oppermann). Para maiores informações sobre o episódio, veja: http://economia.ig.com.br/empresas/2012-09-26/presidente-do-google-no-brasil-e-preso-pela-policia-federal.html.

100 As autoridades de segurança pública dos Estados Unidos acessam dados das empresas registradas naquele país quando munidos de um mandado da justiça, o que confere aos mesmos uma vantagem estratégica.

101 Azahar foi uma operação contra a rede de pedofilia, que atuava basicamente através da Internet. A operação foi deflagrada em 2006, em 30 países ao mesmo tempo. Veja http://idgnow.uol.com.br/mercado/2006/02/21/idgnoticia.2006-02-21.5692495488/.

102 Veja http://www.sagapolicial.com/2012/01/saiba-mais-da-pf-projeto-oraculo.html.

103 Observado por Clayton da Silva Bezerra durante o evento SEGINFO 2012 (setembro). Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31793&sid=18#.Ue3JyI21HNw.

104 Observado por Alexandre Wendt durante o evento SEGINFO 2012 (setembro). Disponível em http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31750&sid=18#.Ue3JhY21HN.

casos procuram auxílio com as mesmas.[105] Ao mesmo tempo, Wendt se preocupa de que a polícia exiba capacidade investigativa e de perícia deficientes.[106] Os problemas variam da ausência de infraestrutura técnica e recursos financeiros, até pessoal com treinamento deficiente, cooperação limitada entre os órgãos de segurança pública assim como a resistência das empresas privadas a divulgar as dimensões da cibercriminalidade. As ameaças persistem, em especial a f alta de padronização na coleta de evidências e procedimentos periciais, bem como a capacidade restrita de realizar a ciberinteligência. Por fim, há em aberto questões sobre como administrar a cibercriminalidade em uma estrutura federal complexa, na qual permaneça pouco claro quem é o encarregado de encabeçar as investigações ou administrar os processos jurídicos.

Reações das forças armadas às ameaças cibernéticas

■ A intensidade do preparo dos militares em face da ciberguerra não se coaduna com a possível ameaça de conflito armado. Sem dúvida, o Brasil não se viu engajado em uma guerra em seu território desde 1870 e jamais se tornou alvo do terrorismo internacional.[107] No entanto, o governo brasileiro prepara suas forças armadas para assumir um papel de liderança na proteção do ciberespaço do país, embora seu principal propósito seja civil. Houve expressivos investimentos no aperfeiçoamento da cibercapacitação militar – com certeza maior do que no setor de segurança pública. E embora outros poderes de expressão tenham adotado uma abordagem semelhante,[108] o grau de envolvimento do setor militar do país em matéria de cibernética não é adequado ou inevitável. Na América Latina onde o autoritarismo era a regra desde a década de 60 até a de 80, apenas a Colômbia incentivou o papel das forças armadas neste campo, a um grau igual ao do Brasil.

105 Importante observar que as forças policiais estaduais achavam-se no meio de uma controvérsia durante os protestos de 2013 no país. Por exemplo, a unidade policial do Rio de Janeiro especializada em cibercrimes (DRCI) prendeu preventivamente manifestantes que planejavam protestosnasruas.Vejahttp://oglobo.globo.com/rio/doze-ativistas-deixam-complexo-penitenciario-de-bangu-na-madrugada-desta-quinta-feira-13284027.

106 A polícia no Brasil não depende de operações secretas, visto que as mesmas não são regulamentadas pelo governo (logo, a polícia prefere não se arriscar) [observação do Delegado Sobral]. As operações secretas são fundamentais em outros locais para combater a cibercriminalidade (veja Glenny, 2011).

107 O país sofreu 21 anos de ditadura militar (1964-1985), época caracterizada pelos abusos dos direitos humanos por parte dos agentes do estado.

108 EUA, França, Israel, Reino Unido, Rússia e China, por exemplo.

Há diversas razões para o Brasil adotar a arquitetura de defesa da cibersegurança por meios militares. Primeiro, as forças armadas procuram com afinco ampliar seu papel de protagonista chave ao moldar o rumo das relações do país. Ao passo que o sistema democrático do Brasil continua a se consolidar, os militares também se reestruturam e procuram um novo papel no futuro interno e externo do país.[109] Esta visão implica mudar o foco de atenção para as ameaças extra fronteiras (inclusive a cibercriminalidade) e realizar operações de segurança interna. A crescente influência das forças armadas nos assuntos civis ainda passará por prolongadas análises internas. Com certeza as forças armadas brasileiras desfrutam de inusitado apoio favorável pela população. Em que pese o histórico da ditadura militar no país, as forças armadas são tidas pela maioria do povo como a mais confiável instituição nacional.[110]

Parte pelo menos do motivo sobre a necessidade de debate acerca do papel das forças armadas nacionais na cibersegurança, tem a ver com o segredo que acoberta boa parte de suas atividades. Não há registro público ou informações detalhadas sobre quando o exército iniciou o desenvolvimento de sua capacidade operacional no ciberespaço. Somente a partir de 2008, este campo passou a fazer parte oficialmente da doutrina militar. Naquele ano a cibernética foi designada um dos três grandes pilares da renovação das forças armadas, junto com o setor aeroespacial e a energia nuclear.[111] De lá para cá, o Ministério da Defesa investiu recursos expressivos no setor. Recentemente o mesmo lançou a *Política de Defesa Cibernética* nacional, documento que enumera os princípios, objetivos e diretrizes que nortearão suas atividades com a matéria nos próximos anos.[112] O Ministério da Defesa indicou o Exército para liderar o desenvolvimento da capacidade de defesa cibernética (a Marinha tem a seu cargo o setor nuclear e a Aeronáutica o setor aeroespacial).

Especificamente, o Exército recebeu o controle de uma aparelhagem de supervisão dos assuntos civis: o CDCiber. O mesmo foi constituído em 2010 e se tornou operacional no final de 2011. Criou-se o CDCiber com o fim de coordenar as atividades de defesa cibernética. Conforme o observado, o CDCiber se situa entre os níveis estratégicos e operacionais da arquitetura brasileira da defesa ciber-

109 Consulte http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.

110 Veja http://fgvnoticias.fgv.br/node/2847.

111 Veja a Estratégia Nacional de Defesa (END), a partir de 2008.

112 O conteúdo do documento consta em http://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa.

nética, em coordenação com o MD, o qual por sua vez recebe ordens do GSI-PR. Esta estratégia inclui as atividades cibernéticas de cinco áreas chave: Inteligência, Ciência e Tecnologia, Capacidade Operacional, Doutrina e Recursos Humanos. O objetivo principal do CDCiber é a proteção das redes militar e governamental contra ataques internos assim como externos. Eventualmente, o mesmo tratará de proteger a integridade da infraestrutura nacional de informática. O CDCiber possui um simulador de ciberguerra, um laboratório de análise códigos virtuais maléficos, além de quase cem especialistas com treinamento em cibersegurança.[113] De igual forma, o CDCiber é convocado para garantir a segurança durante megaeventos internacionais e cumpre a legislação nacional que delega às forças armadas a segurança em eventos oficiais e públicos, "em especial os que contarão com a participação de chefes de governos/estados estrangeiros."[114]

Equilíbrio entre ameaças e reações

■ Uma grande indagação trata da reação às ameaças cibernéticas pelo estado brasileiro quanto às dimensões dos riscos correlatos. Há preocupações de que a reação das forças armadas e da segurança pública poderá ser não apenas desproporcional, mas servir para solapar as liberdades civis conquistadas a duras penas. Há uma boa quantidade de motivos para fortalecer a capacidade de lidar com as ameaças cibernéticas, sendo que não todas estas digam respeito a ameaças reais palpáveis. Antes, o Brasil utiliza as ameaças cibernéticas para reforçar suas habilidades internas e ampliar sua influência geopolítica. Há diversos riscos relativos à atual abordagem.

Primeiro, a arquitetura da cibersegurança no país outorga competências nítidas a seus principais agentes em um campo por natureza mal definido. Teoricamente a Polícia Federal está encarregada de combater a criminalidade comum (inclusive as investigações), ao passo que o Exército deveria se preparar para a ciberguerra (inclusive a defesa do ciberespaço nacional contra a ciberguerra e o ciberterrorismo, formulando iniciativas ofensivas caso necessário). No entanto, a questão da atribuição continua extremamente difícil no ciberespaço. Com frequência, continua impossível definir com certeza absoluta quem ou o que esteja por trás de uma grave ação do cibercrime, detectar sua origem ou que motivou

113 Veja http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

114 Veja o Decreto no. 3897 de 2001 em http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm.

seus autores. Com efeito, a cibercriminalidade é com frequência recrutada pelos governos para uma ampla gama de atividades. Tal fato poderá levar o Exército a se ver em situações onde não haverá de se colocar, em termos lícitos ou operacionais. O que também indica a razão crítica da colaboração entre agências – em especial em inteligência.

Segundo, o discurso de segurança das agências que se ocupam da cibersegurança e de ações de defesa é por natureza tendenciosa. A maioria dos órgãos de segurança sustenta que todos os riscos cibernéticos acima referidos são bastante reais, perigosos e iminentes. Grande parte dos militares fazem alusão a "espaços sem governo" e "faroeste" ao se referir ao ciberespaço. Regra geral, tal terminologia vem acompanhada de afirmações sobre a necessidade de conquistar e controlar este espaço.[115] Por exemplo, o General José Carlos Santos, antigo comandante do CDCiber, observou que seria possível empregar a ciberinteligência do Exército para informar outras autoridades sobre "movimentos suspeitos e mobilização em torno de protestos sociais passíveis de subverter a ordem pública…" [116] Conforme observamos, foi este o caso quando o CDCiber e a ABIN deram início ao monitoramento sistemático da mídia social no Brasil através dos programas Guardião e Mosaico. Dada a experiência recente do país com o autoritarismo, este tipo de retórica e prática dá causa a desconforto por parte de muitas pessoas.[117] A matéria se torna ainda mais problemática, visto que no futuro próximo os militares poderão ter acesso a dados civis. Com certeza, recentemente o governo anunciou que as redes da administração pública federal estarão ao alcance do CDCiber, algo que na atualidade é responsabilidade de um órgão civil, o DSIC.[118] Tais acontecimentos surtem maiores preocupações no tocante ao controle democrático das forças armadas e a ampliação dos direitos à privacidade.[119]

Terceiro, há iniciativas em elaboração e implantação despidas de estratégia nítida, uniforme e previsível. Toda a documentação oficial com orientações ou diretrizes relativas à cibersegurança são mais descritivas do que normativas. Observe-se em especial o *Livro Verde: Segurança Cibernética no Brasil* (2010) e

115 Estas reivindicações são observadas na República Federativa do Brasil, Presidência da República, Secretaria de Assuntos Estratégicos (2011). Veja por exemplo páginas 16, 31 e 32.

116 Entrevista em janeiro de 2014.

117 Veja http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

118 Veja http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

119 Veja http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915.

SAE Desafios Estratégicos para a Segurança e Defesa Cibernética (2011).[120] Do seu lado, a *Estratégia Nacional de Defesa* (2008) não deixou claro como integrar a cibersegurança em uma estratégia abrangente, mesmo que o documento eleva a cibernética como esteio do estamento militar nacional no século vinte e um. O *Livro Branco de Defesa Nacional* (2012b)[121] deverá verter luz sobre estas questões, porém aguarda a aprovação da Presidência. A atual *Política Cibernética de Defesa* do Ministério da Defesa apenas estabelece princípios, objetivos e diretrizes elementares para a consolidação cibernética em específico na esfera da defesa.

Por fim, recursos escassos são desviados com regularidade das grandes prioridades e gastos de forma inadequada. Embora as ameaças principais ao ciberespaço nacional estejam provavelmente ligadas ao crime econômico e deverão resultar em iguais aumentos na alocação de recursos para a segurança pública, as forças armadas vem recebendo a maior parcela de apoio.[122] Por exemplo, além dos custos de seu lançamento, o CDCiber recebeu US$ 60 milhões em 2012[123] e receberá mais US$ 200 milhões no decorrer de 2015.[124] Conforme estimativas constantes do *Livro Branco de Defesa Nacional*, o orçamento esperado para a defesa cibernética é de cerca de US$ 420 milhões até 2035, tratando-se na verdade de uma pequena parcela de todo o orçamento militar projetado para este prazo.[125]

120 O Livro Verde da Segurança Cibernética (2010) é fruto de um grupo de trabalho no GSI. O mesmo expõe o que considera os aspectos chave da cibersegurança no Brasil (veja mais na nota de rodapé 161). "Desafios Estratégicos para Segurança e Defesa Cibernética" (2011) é o documento resultante da conferência da alto nível organizada pela Secretaria de Assuntos Estratégicos da Presidência (SAE). O mesmo traz colaborações de especialistas e autoridades brasileiras do campo da cibernética.

121 O Livro Branco de Defesa Nacional é o primeiro do gênero no Brasil. Sua produção foi antecedida de consultas dentro do governo, e também junto à sociedade civil. O mesmo abrange todos os aspectos da política de defesa nacional e articula a visão estratégica de longo prazo das forças armadas.

122 É desconhecido o total de recursos dirigidos à segurança pública. Não obstante, há indícios através de informantes chave de que o valor investido com a polícia acha-se bem abaixo do que se aplica com as forças armadas. Torna-se difícil quantificar o apoio à polícia, em razão da forma de distribuição dos recursos a múltiplas forças policiais.

123 Em 2012, alocou-se R$ 5 milhões com um aplicativo de simulação de software (de autoria de um empresa brasileira). Trata-se de parte da estratégia de integrar a cibersegurança com projetos mais amplos de desenvolvimento no país, conforme proposta constante do Livro Verde de cibersegurança. Veja República Federativa do Brasil, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações (2010). Veja também http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.

124 Veja http://www.tecmundo.com.br/tecnologia-militar/37801-exercito-deve-receber-r-400-milhoes-para-prevencao-de-guerra-cibernetica-.htm.

125 Veja República Federativa do Brasil, Ministério da Defesa (2012b) .

Há também preocupações legítimas de que a forma de aplicação destes recursos é ineficiente e nada eficaz.[126] Divulgações recentes constataram que o orçamento do país para 2012 não foi inteiramente aplicado,[127] tendo sido quase todo empregado na construção das instalações do CDCiber.[128] O valor alocado foi mínimo no desenvolvimento de tecnologias, capacidade de imóveis a treinamento de pessoal. O motivo comunicado pelo Ministério da Defesa foi que "aplicar US$ 50 milhões para a defesa cibernética nos dias de hoje significa que o Brasil terá que adquirir tecnologia de fora."[129]

PROJEÇÃO DO *SOFT POWER* INTERNACIONALMENTE

■ Um fator chave que influencia os investimento brasileiros na cibersegurança é seu desejo de se posicionar como protagonista global em assuntos internacionais de paz e segurança. O *status* mais ou menos recente do Brasil como potência emergente vem criando um real impacto internamente. Em sua procura de afirmação no cenário internacional, o Brasil fortalece seu arsenal de poder duro, ou militar. O Brasil também decididamente começa a alavancar seu poder brando no exterior, com o emprego de sua capacidade civil. Por exemplo, o Brasil procura destacar iniciativas bem sucedidas de política interna em setores chave, para angariar influência geopolítica. Governança e segurança cibernética são novas, desejáveis na linguagem popular, áreas de exploração. Possuem também a vantagem de serem bastante econômicas em comparação, por exemplo, com a ampliação das habilidades militares ou de manutenção da paz. O ciberespaço continua em evolução, o que permite aos novos participantes adotar medidas pioneiras e liderar as agendas multilaterais.

126 Embora os militares recebam mais recursos do que a segurança pública, não significa necessariamente que seja adequado. O Brasil é uma potência séria e deveria ser capaz de custear questões internacionais de cibersegurança (não restritas pela geografia) e fortalecer suas reações a questões legitimamente nacionais. De um orçamento de defesa total de US$ 30 bilhões (2012-2015), o orçamento específico de US$ 250 milhões em cibernética é minúsculo em face das atuais ameaças cibernéticas. Veja http://g1.globo.com/jornal-da-globo/noticia/2013/07/governo-destina-baixo-orcamento-para-seguranca-cibernetica.html.

127 Uma fonte da mídia indicou que houve aplicação de apenas 8,9% do orçamento de 2012. Veja http://noticias.terra.com.br/brasil/brasil-usou-89-do-orcamento-para-defesa-cibernetica,76b782fb0acdf310VgnVCM3000009acceb0aRCRD.html.

128 Veja http://www.bloggingsbyboz.com/2013/07/brazils-cybersecurity-budget-is-mess.html.

129 Veja http://www1.folha.uol.com.br/mundo/2013/07/1312345-gastar-r-100-mi-em-ciberdefesa-significa-comprar-tecnologia-de-fora-diz-amorim.shtml.

Há uma série de reivindicações por parte do Brasil com relação ao incremento de suas habilidades de poder duro e brando no ciberespaço. Por exemplo, o CDCiber é a primeira unidade cibernética militar exclusiva na América Latina. As URCCs da Polícia Federal, embora em formação, oferecem um modelo de segurança pública e colaboração judicial internamente e entre os países e regiões. O Brasil também ostenta o desenvolvimento e aplicação de estratégias de cibersegurança projetados para Megaeventos. Ademais, em breve o Brasil pode ter em breve uma estratégia nacional de segurança e defesa cibernética das mais abrangentes no mundo. E talvez o mais expressivo, o Brasil criou a primeira Declaração dos Direitos digital[130] e lançou a iniciativa da ONU de promover a soberania digital. Todas estas atividades, embora não necessariamente coerentes ou coordenadas internamente, sugerem que o país reivindica seu crédito na formulação das agendas internacional e regional sobre cibersegurança.

Ao mesmo tempo as autoridades nacionais têm criticado ativamente e procuraram reformular o regime atual de cibersegurança. Por exemplo, o governo tem criticado a *Convenção da Cibercriminalidade* (Convenção de Budapeste de 2001) do Conselho da Europa, o qual até a data é o único conjunto de normas internacionais legalmente válidas que regem questões relativas à cibercriminalidade. O Brasil alega que o processo de redação excluiu propositadamente os não integrantes do Conselho, e logo se opõe aos países fora da União Europeia. Entretanto, o Brasil se adiantou juntamente com a UNODC na redação de uma convenção internacional sobre a cibercriminalidade, tendo angariado o apoio de outros países da América Latina e do Caribe. Tomou-se esta decisão durante o 12º Congresso da ONU sobre a Repressão ao Crime e Justiça Criminal, realizado em 2010 em Salvador, Bahia, embora o processo evolua mais lentamente do que se esperava.[131]

Há também inquietação sobre as negociações globais do Brasil acerca da soberania digital bem como o potencial de balcanização da Internet. Vejamos, o Brasil apoiou até certo ponto a China e o Irã durante a Conferência Internacional da ITU em Dubai (2012). O Brasil estava a favor da regulamentação da Internet através de um tratado internacional sob a supervisão da ONU. No entanto, há receio de que esta abordagem daria poderes excessivos aos governos e levaria à regulamentação potencialmente morosa, restritiva e invasiva. Estas preocupações

130 Inclui o reconhecimento especial recente por Tim Berners Lee. Veja http://www1.folha.uol.com.br/poder/2013/05/1280037-criador-da-web-elogia-brasil-por-projeto-que-vai-regular-a--internet.shtml.

131 Veja http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

se tornam intensas pelo fato de que o controle da Internet pelos Estados Unidos e pela Internet Corporation for Assigned Names and Numbers (ICANN), com base nos Estados Unidos, está em fase de se afrouxar de modo a permitir demais governos, ONGs e ISPs o desempenho de um papel mais proeminente. Ademais, a ITU suscitou a possibilidade de permitir a *deep package inspection* (DPI), o primeiro passo para a censura, já em vigor em alguns países.[132] No entanto, são alvissareiros os sinais de que a abordagem do Brasil poderá mudar. Juntamente com a Alemanha e a ICANN, o governo brasileiro patrocinou recentemente um evento de alto nível, o NetMundial, em São Paulo. O Brasil propôs o estabelecimento de um *Marco Civil* global e pediu mais *multistakeholderism* com relação à governança da Internet.[133]

No nível regional, o Brasil colabora estreitamente com esforços de combate ao cibercrime, em coordenação com a Organização dos Estados Americanos (OEA) e sua *Estratégia Interamericana de Combate às Ameaças contra a Cibersegurança* (adotada pela Assembleia Geral da OEA em 2004). *O Brasil não apenas adotou os pilares da cibersegurança esboçadas pela OEA, mas também trabalha com afinco no aperfeiçoamento das medidas propostas. O país organizou conferências com os três departamentos da OEA que administram a implantação da Estratégia e com frequência desloca especialistas em apoio de missões de assistência técnica, participando de eventos em toda a América Latina bem como o Caribe.134 Em sua própria região da América do Sul, o Brasil promove a agenda dentro da UNASUR – União das Nações Sul-Americanas.* Reuniões entre os Ministros da Defesa, Justiça e Interior dos 12 estados-membro visaram a criação de mecanismos de promoção da cooperação contra o crime organizado transnacional, em especial a cibercriminalidade.[135]

O Brasil também lidera no desenvolvimento da cooperação bilateral de administração da cibersegurança e defesa cibernética. O país celebrou com a Rússia em 2010 o Tratado de Não Agressão com Armas de Informática, o primeiro tratado bilateral do gênero. Além de resultar no tratado de não agressão, o mesmo dispõe do intercâmbio aperfeiçoado de informações, fortalecimento de capacidade e exercícios conjuntos de ciberguerra. Embora o tratado soe estranho, há sinais

132 Veja http://www1.folha.uol.com.br/colunas/ronaldolemos/1210826-brasil-se-alinha-a-china-e-ira-em-leis-da-internet.shtml A posição do Brasil sobre a DPI continua pouco clara.

133 Para maiores informações sobre os resultados do evento, veja http://netmundial.br/.

134 Veja Diniz e Muggah (2012).

135 Veja http://www.unasursg.org/index.php?option=com_content&view=article&id=516:ultima-unasur-debate-cooperacion-regional-en-crimen-trasnacional-organizado-y-nuevas-amenazas&catid=66:noticias-unasur.

de cooperação em alta com a cibersegurança, entre os integrantes dos BRIC.[136] Ao mesmo tempo os Ministros de Defesa de Argentina e Brasil assinaram em 2011 uma Declaração Conjunta de revisão da cooperação bilateral no setor de defesa, inclusive com relação à informática e cibersegurança. De igual forma, os Ministros de Defesa de Brasil, Chile e Colômbia realizaram sessões restritas no Pentágono dos EUA, destinadas a revisar as ameaças cibernéticas, e solicitaram apoio para o fortalecimento da resiliência das redes de hardware e software contra violações.

CONCLUSÕES

■ O Brasil vem incrementando sua arquitetura de cibersegurança e ao mesmo tempo consolidando sua posição de potência emergente. As autoridades públicas visam não apenas a cibercriminalidade interna e o ciberativismo, mas também a expansão da habilidade do estado para a redução das ameaças cibernéticas, em nível internacional. Na reação estratégica do Brasil a ambos os riscos, acha-se o CDCiber na condição de pilar básico. No entanto, a ênfase na reação militar poderá ser fora de propósito com as ameaças reais (e não existenciais) que assombram o país e a sociedade como um todo. O fato permanece de que o Brasil enfrenta relativamente poucas ameaças cibernéticas por governos estrangeiros ou grupos terroristas. No entanto, o aumento dos protestos digitais e de cibercriminalidade está mais do que evidente, porém recebem relativamente menor atenção e investimentos. Urge a necessidade de uma leitura mais informada e com base em evidências das ameaças contra o país, e sua abordagem através da cuidadosa apreciação do equilíbrio entre a segurança pública e os direitos individuais.

A arquitetura de cibersegurança do Brasil acha-se ainda em evolução. Há ainda linhas conflitantes de responsabilização entre as instituições, prioridades distorcidas de custeio, debate público confuso, medidas legislativas opostas e a importação sem critério de soluções estrangeiras para os desafios internos. Há críticos que argumentam que a "reação" do estado às ameaças cibernéticas é mal concebida e não se coadunam com os reais desafios que o país enfrenta. Em seu lugar, os militares "capturaram" recursos para a defesa cibernética, que implicam em perigos, de modo geral, para as liberdades civis. Outro importante desafio se encontra na ausência de coordenação entre as instituições do governo e a frag-

136 Veja http://www.scmp.com/news/china/article/1276995/brics-emerging-economies-expand-co-operation-internet-security.

mentação das reações. E ainda, o engajamento limitado no Brasil da sociedade civil nos debates sobre a cibersegurança significa que as forças armadas estão desimpedidas para a ampliação de seus interesses corporativos.[137] Em seu lugar, estas tendem a adotar também abordagens estanques, com algumas tendências com foco em questões de defesa, outras em policiamento, e ainda outras em soberania digital, liberdades civis, etc. O essencial é a estratégia equilibrada da cibersegurança que avalie com precisão as ameaças em curso, ao mesmo tempo elaborando reações proporcionais e prospectivas.

O primeiro passo seria a concentração nas lacunas de conhecimento. Há um debate vivo no Brasil sobre as múltiplas realizações positivas com relação à *e-governance*, cidades inteligentes, soberania digital e demais TICs novas.[138] Há, por estranho que pareça, silêncio sobre questões relativas a cibersegurança e defesa cibernética. Quando há debates, estes tendem a permanecer confinados aos mais altos níveis de governo, forças armadas, órgãos de segurança pública e meios acadêmicos de banda estreita. Caso o Brasil desenvolva uma reação mais equilibrada e proporcional contra as ameaças emergentes, a cibersegurança deverá ser aceita como característica integral da governança cibernética e determinante chave dos direitos civis, sociais e políticos. No mínimo, os estudiosos brasileiros necessitam de um melhor entendimento da dinâmica dos hackers e dos grupos da cibercriminalidade, das formas do crime tradicional migrar para a rede, das maneiras de adaptação pelas forças de segurança de novas tecnologias de vigilância e demais questões. Significa também que o governo deverá incentivar um mais amplo debate com uma estratégia clara de comunicações sobre as exigências da cibersegurança e quais as suas formas.

O segundo passo é iniciar o debate sobre o conteúdo das estratégias ponderadas e eficientes para fazer face às ameaças cibernéticas. Visto que os orçamentos alocados às questões relativas à cibernética são flexíveis e de difícil previsão, há bastante concorrência burocrática por verbas. Os órgãos militares, de segurança pública e civis são passíveis de exagerar os riscos de modo a aumentar seu acesso às verbas. As negociações mais informadas contribuiriam para um carteira mais equilibrada de cibersegurança. As principais prioridades no Brasil incluem a melhora na capacidade investigativa das polícias federais e estaduais, inclusive no

137 Veja em Diniz e Muggah (2012) a visão geral da maneira da sociedade civil lidar com a cibersegurança na América Latina.

138 Veja por exemplo as obras dos grupos de pesquisa, como ITS-Rio, CTS-FGV, UFABC (Grupo de pesquisa "Cultura Digital e Redes de Compartilhamento") e UNICAMP (Grupo de pesquisa "Políticas Públicas de Acesso à Informação").

tocante às perícias cibernéticas. De igual modo, torna-se essencial aperfeiçoar a coordenação entre as polícias estaduais de modo a melhor se antecipar e lidar com os crimes cibernéticos. Talvez mais radical, porém estratégia adotada em outros países, será identificar e recrutar hackers brasileiros que colaborem no aperfeiçoamento das habilidades do estado. O Ministro de Ciência e Tecnologia no Brasil já seu sinais nesta direção, e convidou hackers a avaliar os riscos de segurança na rede do governo federal. O CDCiber também realizou movimentos neste sentido.[139] No entanto, o czar da cibersegurança no Brasil determinou que todo hacker é criminoso (e que o hacker nacional não possui a habilidade do estrangeiro).[140]

Em terceiro lugar, o Brasil deverá dar início a um debate sofisticado sobre o que constitui uma ameaça cibernética bem como os tipos de reação necessárias. Há uma tendência de simplificar o debate sobre ameaças cibernéticas e cibercriminalidade. Em algumas hipóteses, diversas atividades se combinam. Em outras, a tendência é exagerar o foco em determinada categoria de ameaça. Caso o Brasil adote uma abordagem mais progressiva, será necessária maior ênfase na melhora de qualidade de educação e debate. O fato é que a consciência sobre cibersegurança no Brasil é bastante baixa.[141] Há necessidade de um esforço organizado para elevar a compreensão e comprometimento, como ocorre na América do Norte e Europa, entre outros. Os debates do gênero deverão ser acessíveis a uma gama de interesses e possuir base em dados empíricos comprovados. Caso o Brasil deseje uma arquitetura de cibersegurança adequada a seus fins, torna-se imperativo o debate de qualidade.

Robert Muggah é diretor de pesquisas do Instituto Igarapé, encarregado de pesquisas na SecDev Foundation e principal cientista social do SecDev Group.

Misha Glenny é autor internacional sobre assuntos que variam dos Balcãs e do Brasil ao crime organizado e aos crimes cibernéticos.

Gustavo Diniz foi investigador adjunto no Instituto Igarapé.

139 Veja http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

140 Veja http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27324&sid=21 e http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27454&sid=15#.UaKzStLU-Io.

141 Diz-se que cerca de 42% dos brasileiros desconhecem que os vírus de computadores passam despercebidos (a média global é de 40%). Veja Norton/Symantec "*Norton Cybercrime Report 2012*".

REFERÊNCIAS

CANONGIA, C. e MANDARINO, R. Segurança cibernética: o desafio da nova Sociedade da Informação. *Parceria Estratégica*. Brasília-DF, vol. 14, n. 29, p. 21-46, jul-dez, 2009.

DINIZ, G. e MUGGAH, R. *A Fine Balance: Mapping Cyber-(In)security in Latin America*. Strategic Paper 2. Igarapé Institute: Rio de Janeiro, junho, 2012. Disponível em http://igarape.org.br/a-fine-balance-mapping-cyber-insecurity-in-latin-america/

FGV-CPS . *Mapa da Inclusão Digital*. Marcelo Neri (Coord). Rio de Janeiro, 2012a. Disponível em: http://www.cps.fgv.br/cps/telefonica/

FGV-CPS. *O Início, o Fim e o Meio Digital: Cobertura, Capacidades e Conectividade*. Marcelo Neri (Coord). Rio de Janeiro, 2012b. Disponível em: http://www.cps.fgv.br/cps/vivo/

GLENNY, M. *Dark Market:* Cyberthieves, Cybercops and You, 2011.

GLENNY, M. *McMafia:* A Journey Through the Global Criminal Underworld. Nova York: Random House, 2009.

INTERNATIONAL INTELLECTUAL PROPERTY ALLIANCE – IIPA. *Special 301 Report on Copyright Protection and Enforcement: Brazil,* fevereiro, 2012. Disponível em http://www.iipa.com/rbc/2012/2012SPEC301BRAZIL.PDF

INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: A Guide for Developing Countries*. Genebra: ITU-D ICT Applications and Cybersecurity Division, 2009.

KISHETRI, N. *Cybercrime and Cybersecurity in the Global South*. Palgrave MacMillan: Reino Unido, 2013.

MUGGAH, R. e GLENNY, M. Brazil´s Cybersecurity Conundrum, Council on Foreign Relations, janeiro 2015, http://blogs.cfr.org/cyber/2015/01/12/guest-post-brazils-cybersecurity-conundrum/.

MUGGAH, R., DINIZ, G. e M. GLENNY. Brasil aposta na militarização da segurança cibernética, Le Monde Diplomatique, novembro, 2014.http://www.diplomatique.org.br/acervo.php?id=3082.

MUGGAH, R. e DINIZ, G. Using Information and Communication Technologies for Violence Prevention in Latin America. In: MANCINI, F. (ed.) *New Technology and the Prevention of Violence and Conflict.* Nova York: International Peace Institute, abril, 2013. Disponível em: http://www.undp.org/content/dam/undp/library/crisis%20prevention/20130410NewTechnologyandPreventionofViolenceandConflictv2.pdf

OLLINGER, M. La Propagación del Crimen Organizado en Brasil: Una mirada a partir de lo ocurrido en la última década". In: GARZÓN. G. e

OLSON, E. (eds). *La Diáspora Criminal:* La difusión transnacional del Crimen Organizado y cómo contener su expansión. Woodrow Wilson International Center for Scholars – Latin America Program. Washington D.C, 2013. http://www.wilsoncenter.org/publication/Criminal Diaspora

REPÚBLICA FEDERATIVA DO BRASIL, Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações. *Livro Verde da Segurança Cibernética no Brasil*. Mandarino, R. e Canongia, C. (Eds). Brasília, 2010. Disponível em: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. *Estratégia Nacional de Defesa*, 2008. Disponível em http://www.mar.mil.br/diversos/estrategia_defesa_nacional_portugues.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. "Política Cibernética de Defesa". Portaria Normativa No 3389 (dezembro 21), Gabinete do Ministro. DOU Seção 1 – No. 249 (dezembro 27), 2012a.

REPÚBLICA FEDERATIVA DO BRASIL, Ministério da Defesa. *Livro Branco de Defesa Nacional*. Brasília, 2012b. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf

REPÚBLICA FEDERATIVA DO BRASIL, Presidência da República, Secretaria de Assuntos Estratégicos. Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília, 1ª edição, 2011. Disponível em http://www.sae.gov.br/site/?p=6151

TREND MICRO. *Latin American and Caribbean Cybersecurity Trends and Government Responses*. Maio, 2013. Disponível em http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends--and-government-responses.pdf

WÆVER, O. Securitization and Desecuritization. In: LIPSCHUTZ, R. ed. *On Security*. Nova York: Columbia University Press, 1995.