SEGURANÇA CIBERNÉTICA

Marco Cepik (26/02/2018)

Neste texto discuto o ponto 13 do conteúdo de Política e Segurança, sobre segurança cibernética. O comentário sobre este tópico também pode ser relevante para assuntos correlatos, referentes aos pontos 8 (Terrorismo), 11 (Sabotagem) e 12 (Interferência Externa) do conteúdo específico de Política e Segurança, bem como do item 9 (Conflitos Geopolíticos Recentes), do conteúdo específico de Geografia Mundial. O texto foi dividido em quatro seções. Na primeira menciono o aumento da percepção de ameaça sobre riscos cibernéticos. Na segunda seção procuro retomar a caracterização do ciberespaço e sua relação com a segurança internacional em termos mais conceituais e estruturais. Na terceira seção apresento alguns elementos institucionais e doutrinários da visão brasileira sobre defesa cibernética e sua conexão com as questões mais amplas de segurança. Finalmente, uma breve conclusão destaca o vínculo entre segurança cibernética e inteligência.

Elementos de Conjuntura

Há um evidente aumento da percepção de ameaça relativa ao ciberespaço nos últimos anos. Três relatórios publicados em janeiro e fevereiro de 2018 destacam a dimensão econômica relativa a crimes cibernéticos.

No último Relatório de Riscos Globais apresentando no Fórum Econômico de Davos, por exemplo, os ataques cibernéticos foram considerados como o terceiro tipo de risco mais provável e como o quinto tipo de risco com maior impacto sobre a economia mundial em 2018 (https://goo.gl/26CsUw). O número crescente de ataques, a quantidade e sofisticação de códigos maliciosos (*malware*) e os custos econômicos foram destacados como os principais problemas. Segundo o relatório, o custo do crime cibernético para as empresas nos próximos cinco anos foi estimado em US$ 8 trilhões. Em 2016, foram identificadas 357 milhões variações de *malware* circulando na internet. Em 2017, um tipo específico de código malicioso, chamado *ransomware* (que impede os proprietários de acessar dados até que um “resgate” seja pago), representou 64% dos e-mails contendo *malware* enviados. Exemplos notáveis

incluíram o ataque WannaCry, que afetou 300 mil computadores em 150 países, e as variantes Petya e NotPetya. Grandes empresas como Merck, FedEx e Maersk registraram perdas coletivas de US$ 300 milhões como resultado do NotPetya.

Na mesma direção apontou o relatório Estimando o Custo Global do Risco Cibernético, elaborado por uma equipe de pesquisadores da RAND Corporation com financiamento da empresa Symantec. Como a ênfase do relatório é na discussão de metodologias, revisão de fontes e formulação de parâmetros de modelagem para estimativas de custos diretos e sistêmicos, por país e ramo da atividade econômica, os valores resultantes são altamente sensíveis aos dados de entrada e suposições adotadas. Para demonstrar isso, custo global do crime cibernético foi estimado com três diferentes modelos, variando de US$ 275 bilhões em custos diretos e US$ 799 bilhões de custos totais no modelo 1 (chamado Dutch Peril and Exposure Estimates), US$ 3,2 trilhões em custos diretos e US$ 10,1 trilhões no modelo 2 (Dutch Peril and SEC Estimates), e US$ 6,6 trilhões em custos diretos e 22,5 trilhões em custos totais no modelo 3 (VaR Direct Estimates). No caso do estudo de caso feito sobre a Holanda usando o modelo 1 (mais conservador), os autores encontraram perdas anuais decorrentes de crimes cibernéticos equivalentes a 1,27% do PIB daquele país (https://goo.gl/H67QYH).

O terceiro exemplo vem do relatório conjunto da empresa McAfee e do Center for Strategic and International Studies (CSIS), preparado por James Lewis, intitulado justamente Impacto Econômico do Crime Cibernético. Segundo este relatório, em 2014 o custo anual agregado dos crimes cibernéticos teria sido de US$ 500 bilhões (0,7% do PIB mundial), aumentando para US$ 600 bilhões em 2017, ou 0,8% do PIB mundial. As razões para o aumento seriam a crescente sofisticação tecnológica dos perpetradores, o aumento do número de pessoas utilizando a internet no mundo todo, uma taxa favorável de risco em relação à expectativa de lucros oriundos do crime, e a facilidade de monetização dos resultados do crime cibernético em paraísos fiscais e no próprio sistema financeiro global, dentre outros fatores (https://goo.gl/phCtF8).

Embora estes três relatórios tenham como foco os crimes cibernéticos, há também um aumento nas trocas de acusações entre Estados e um aumento global da securitização de questões ligadas ao ciberespaço e à internet tais como, por exemplo, governança da Internet, neutralidade da rede, privacidade, algoritmos de redes

sociais e notícias falsas. Também há desenvolvimentos doutrinários, institucionais e operacionais na área de guerra cibernética em diferentes países. Para mencionar apenas um exemplo, no dia 15 de fevereiro de 2018 a Casa Branca acusou publicamente o governo da Rússia de estar por trás do ataque NotPetya em 2017, acompanhando a posição já manifestada pelos governos do Reino Unido, Austrália, Canadá e Nova Zelândia. Moscou negou qualquer envolvimento e também rechaçou as acusações de que estaria tentando influenciar resultados eleitorais em diferentes países.

Também no caso do Brasil aumentou a percepção de ameaça cibernética. Segundo o Relatório de Segurança Digital no Brasil, divulgado pelo DFNDR Lab da empresa Psafe, em 2017 teria havido 205 milhões de ciberataques no Brasil. Entre o terceiro e o quarto trimestre o relatório indica um salto de 107% nos ciberataques de *phishing* (tentativas de obtenção de informações bancárias e pessoais) via aplicativos de mensagens, por exemplo. Apenas no quarto trimestre do ano, teria chegado a 66,1 milhões o total de acesso a links maliciosos, enquanto os ataques via *malware* teriam chegado a 3,1 milhões de ataques. (https://goo.gl/83fqA5).

Por sua vez, os dados disponibilizados pelo Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil (CERT.br) do Comitê Gestor da Internet (CGI.br) são de incidentes notificados. Em 2016 foram notificados ao CERT.br exatos 647.112 incidentes, dentre os quais mais de 50 mil ataques a servidores Web, 60 mil ataques de negação de serviço (DoS), mais de 100 mil tentativas de fraude, e mais de 380 mil varreduras e propagações de *malware* (https://goo.gl/Sc6ubL).

No caso da Administração Pública Federal (APF), o Centro de Tratamento de Incidentes de Redes do Governo (CTIR) do Departamento de Segurança de Informação e Comunicações (DSIC), subordinado ao Gabinete de Segurança Institucional da Presidência da República (GSI), divulgou relatório indicando que em 2017 recebeu 28.219 notificações de incidentes, das quais 11.207 revelaram ser de fato eventos adversos. Abusos e indisponibilidades de sítio governamental web responderam por 52,25% dos incidentes (https://goo.gl/Q4yZM1).

Ao chamar de eventos adversos e não de ataques, os dois centros brasileiros de respostas a incidentes contribuem para diminuir a confusão causada por empresas e governos internacionalmente, afinal o uso de uma linguagem bélica (ataque e defesa)

tende a provocar no público a percepção de que estamos em meio a uma guerra cibernética global, uma noção precariamente lastreada em premissas polêmicas e evidências demonstráveis (Cepik; Canabarro; Borne, 2015).

Ciberespaço e Segurança Internacional

Conforme destacam Canabarro, Borne e Leal (2014), o ciberespaço é formado pelas diversas estruturas, equipamentos, códigos, agentes e interações que utilizam o espectro eletromagnético com a finalidade de criação, armazenamento, modificação e/ou troca de informações através de redes interconectadas. Nesse sentido, redes de telégrafo, de rádio amador, de telefonia fixa e móvel, de televisão via satélite, ou os sistemas de controle de tráfego aéreo e de navegação marítima, por exemplo, configuram o ciberespaço desde muito antes da invenção da Internet.

O crescimento atual da Internet como dimensão crucial do ciberespaço é marcado por duas tendências: ubiquidade e convergência digital. A ubiquidade diz respeito à qualidade de onipresença da rede, com dispositivos de todo o tipo sendo desenvolvidos para conectarem-se uns aos outros, utilizando os protocolos de comunicação da Internet. Segundo o Gartner Group, em 2017 havia 8,4 bilhões de dispositivos conectados para uma população mundial de 7,8 bilhões de humanos. A previsão deles é que em 2020 este número de dispositivos conectados suba para 20,4 bilhões, sendo que o mercado de equipamentos e serviços associados ao que se chama hoje de “Internet das Coisas” (IoT) já movimentou dois trilhões de dólares no ano passado (https://goo.gl/X9bUr9).

A convergência digital é, portanto, um fenômeno social complexo de fusão de tecnologias, a qual vem revolucionando as instituições e o modo de produção neste século. Um aparelho móvel de uso pessoal, por exemplo, já é ao mesmo tempo uma televisão, um rádio, um telefone, uma central de comunicações, um roteador, um terminal bancário, uma máquina fotográfica, uma plataforma de acesso à web para múltiplos serviços, um mapa interativo, uma biblioteca e uma série de outras funções que se modificam rapidamente.

As ameaças e vulnerabilidades no ciberespaço acompanharam o crescimento da internet e a crescente convergência digital, mas como em várias áreas da segurança internacional o desencadeamento da Guerra Global ao Terrorismo por parte dos

Estados Unidos depois dos atentados de 11 de setembro de 2001 marca um ponto de virada na segurança cibernética (Cepik; Canabarro; Borne, 2014). Desde o caso do vírus Stuxnet de sabotagem contra sistemas de controle industrial, lançado pelos Estados Unidos em 2010 como ferramentas de guerra informacional contra o Irã, a noção de guerra cibernética (*cyberwarfare*) adquiriu proeminência como ponte entre os domínios operacionais físicos (terra, mar, ar e espaço sideral) e as camadas lógicas do ciberespaço. No quadro abaixo está sintetizada uma tentativa feita há poucos anos para classificar o espectro do conflito no ciberespaço.

Tipologia de conflitos cibernéticos:

Tipo de conflito	Caracterização
Hacktivismo	Mistura de ações *hacker* com ativismo político. Geralmente tem como objetivo a inviabilização de sítios eletrônicos e servidores.
Crime cibernético	Desenvolvimento de ações ilícitas com o emprego de computadores e da Internet.
Espionagem cibernética	Acesso não autorizado a computadores e servidores com a finalidade de se testar a configuração e os sistemas de defesa de um determinado computador, ou ganhar acesso a informações sigilosas.
Sabotagem cibernética	Criação de empecilhos ao desenvolvimento de processos e rotinas de trabalho nos setores público e privado a partir de meios eletrônicos.
Terrorismo cibernético	Ataques ilícitos *contra* computadores – e a informação neles armazenada – e redes computacionais com o objetivo de intimidar ou coagir governos e/ou suas populações para o alcance de objetivos políticos. Dos ataques, *deve* decorrer a violência contra bens e pessoas, tanto quanto for necessária para se gerar o nível de medo adequado ao rótulo de 'terrorismo cibernético' (grifos nossos). Nas palavras de Möckly (2012, p. 116, tradução nossa): "O termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".
Guerra cibernética	Emprego de meios eletrônicos para atrapalhar as atividades de um inimigo, bem como atacar sistemas de comunicação. Nas palavras de Möckly (2012, p. 116, tradução nossa): "[o] termo é também usado de forma imprecisa e vaga para incidentes cibernéticos de natureza política variada".

Fonte: Cepik; Canabarro; Borne, 2014, p. 169.

Existem outras classificações, mas todas elas (incluindo a nossa obviamente) estão sujeitas ao crivo da crítica e da própria evolução da realidade. Cabe destacar, entretanto, que a principal dificuldade prática e teórica para o desenvolvimento de políticas públicas, doutrinas, instituições e pessoas voltadas para a segurança cibernética ainda tem a ver com a necessidade de separar a mera presença na e o uso da internet por parte de criminosos, terroristas, serviços de inteligência, empresas ou forças armadas de diferentes países, daquilo que seriam atos terroristas ou de

guerra realizados através do, ou contra o ciberespaço, principalmente aqueles que tenham implicações cinéticas e simbólicas fora dele (Cepik; Canabarro; Borne, 2014, p. 178).

Segurança e Defesa cibernética no Brasil

Conforme o Manual de Campanha para a Guerra Cibernética, adotado pelo Exército em 2017, as ações governamentais brasileiras de segurança e defesa no espaço cibernético deverão ter as seguintes denominações, de acordo com o nível de decisão: a) nível político: Segurança da Informação e Comunicações (SIC) e Segurança Cibernética, conformando políticas coordenadas pela Presidência da República e abrangendo a administração pública federal (APF) direta e indireta, bem como as infraestruturas críticas da informação inerentes às infraestruturas críticas nacionais; b) nível estratégico: Defesa Cibernética, a cargo do Ministério da Defesa, do Estado-Maior Conjunto das Forças Armadas (EMCFA) e dos comandos das forças armadas (Marinha, Exército e Força Aérea); c) níveis operacional e tático: Guerra Cibernética, denominação restrita ao âmbito interno das forças armadas (https://goo.gl/nLnjUR).

A fase mais recente do desenvolvimento da segurança, defesa e guerra cibernética no Brasil iniciou com o chamado “caso Snowden”, em 2013, quando, dentre outras denúncias baseadas em documentos vazados, tornou-se público que o governo dos Estados Unidos de fato espionava sistematicamente a Petrobrás e as comunicações da presidente Dilma Rousseff. A partir dali houve ações brasileiras importantes no âmbito das Nações Unidas e dos fóruns internacionais de governança da internet, como o Encontro Multissetorial NETmundial (https://goo.gl/udTgoy). No plano nacional, diversas vulnerabilidades foram identificadas pela Comissão Parlamentar de Inquérito (CPI) da Espionagem naquele mesmo ano (https://goo.gl/Fxp2aa). No ano seguinte, o Marco Civil da Internet (Lei 12.965/2014) consagrou legalmente os princípios fundamentais da governança da rede no país e o modelo multissetorial e participativo do Comitê Gestor da Internet (CGI.br). A continuidade de tais ações, nos últimos anos, foi severamente enfraquecida com risco para o Brasil.

Na área de segurança e defesa mais especificamente, também em 2013 uma série de decretos e regulamentos administrativos iniciou a formatação institucional atual do

setor. Por exemplo, em novembro o Decreto 8.135/2013 regulamentou o interesse de segurança nas comunicações de dados da administração pública federal direta, autárquica e fundacional. Anteriormente, em julho daquele ano, o Decreto Legislativo 3.703/2013 havia atualizado a Estratégia Nacional de Defesa (END) e aprovado o Livro Branco de Defesa Nacional (LBDN), especificando assim que a proteção do espaço cibernético abrangia áreas como capacitação, Inteligência, pesquisa científica, doutrina, preparo e emprego operacional, além de gestão de pessoal.

Atualmente, em termos institucionais, portanto, o Gabinete de Segurança Institucional (GSI) é responsável pela coordenação da segurança cibernética brasileira, contando com órgãos como o Departamento de Segurança de Informação e Comunicações (DSIC), apoiado pelo Centro de Tratamento de Incidentes de Redes do Governo (CTIR), e pelo Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações (CEPESC), que faz parte da estrutura da ABIN (https://goo.gl/ALTHLm). Criado em 2014, o Comando Conjunto de Defesa Cibernética (ComDCiber), juntamente com outros órgãos relacionados, tais como o Centro de Comunicações e Guerra Eletrônica (CCOMGEx) do Exército, a Escola de Defesa Cibernética e o Centro de Defesa Cibernética (CDCiber), têm sido os principais focos da implementação de políticas, estratégias, doutrina e prática de defesa cibernética no Brasil. Vale dizer que a segurança e a defesa cibernética no Brasil diferem pelo nível de abrangência, estruturas de comando e interações com a sociedade civil e as empresas do setor privado (Kreibich, 2016; Batista, 2016; Leal, 2015; Oliveira et al, 2017).

Desafíos de Inteligência

Como conclusão, reitero o senso comum de que a internet e o ciberespaço são cada vez mais importantes para o funcionamento das sociedades contemporâneas. Seu desenvolvimento depende de segurança e defesa, mas também de liberdade e equidade. Do ponto de vista das atividades de inteligência, acompanhar os desenvolvimentos tecnológicos, as interações estratégicas entre os atores relevantes e demandas legais e institucionais variadas em termos de governança para o futuro do ciberespaço certamente constituem em si mesmo um desafio relevante. Além disso, as capacidades para conduzir operações de guerra informacional, bem como

dissuadir ou reprimir atividades criminais, aproximam crescentemente inteligência e cibersegurança. Evitar a securitização excessiva, ao mesmo tempo em que se desenvolvem capacidades estatais adequadas, é crucial na medida em que cresce a dependência digital sistêmica da sociedade brasileira nos próximos anos.

Sugestão de Leitura:

ALCANTARA, Bruna T. Internet, Terror e Ciberterrorismo: uma análise comparativa. Dissertação de Mestrado. Programa de Pós-Graduação em Estudos Estratégicos Internacionais. Porto Alegre-RS, Universidade Federal do Rio Grande do Sul, 2018.

BATISTA, Ana L. F. H. Segurança cibernética: uma abordagem comparativa das estruturas de defesa cibernética norte-americana e brasileira. Dissertação de Mestrado. Programa de Pós-Graduação em Ciências Militares. Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2016.

BRASIL. Doutrina Militar de Defesa Cibernética. MD31-M-07. Brasília: EMCFA, 2014. Disponível em: https://goo.gl/kZaxoi. Último acesso em 24/02/2018.

BRASIL. Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018. Brasília: GSI, 2015. Disponível em: https://goo.gl/mS7eXX. Último acesso em 24/02/2018.

BRASIL. Manual de Campanha Guerra Cibernética. EB70-MC-10.232. Brasília, COTER, 2017. Disponível em: https://goo.gl/jRLYEf. Último acesso em 24/02/2018.

BRASIL. Política Cibernética de Defesa. Brasília: Ministério da Defesa, 2012. Disponível em: https://goo.gl/RdUzSb. Último acesso em 24/02/2018.

CANABARRO, Diego; BORNE, Thiago; LEAL, Marcelo. A Era Digital e os Estudos de Segurança: conceitos e práticas. In: PIMENTA, Marcelo; CANABARRO, Diego [organizadores]. Governança Digital. Porto Alegre-RS, Editora UFRGS, 2014. Páginas 130-150.

CARNEIRO, Aristides S. L. A Defesa Cibernética como Extensão do Papel Constitucional das Forças Armadas na Defesa Nacional. In: PINTO, José C. R. [org.]. Ciberdefesa e Cibersegurança: novas ameaças à segurança nacional. Rio de Janeiro, ESG, 2016.

CEPIK, Marco; CANABARRO, Diego Rafael; BORNE, Thiago. A Securitização do Ciberespaço e o Terrorismo: uma abordagem crítica. Do 11 de Setembro à Guerra ao Terror - reflexões sobre o terrorismo no século XXI, IPEA, 2014.

CEPIK, Marco; CANABARRO, Diego; BORNE, Thiago. Cyberwar: Clausewitzian Encounters. Space & Defense, v. 08, p. 19-33, 2015.

KREIBICH, Eduardo. Ciberespaço brasileiro: caracterização, organização e políticas. Trabalho de Conclusão de Curso em Relações Internacionais. Porto Alegre, Universidade Federal do Rio Grande do Sul, 2016.

LEAL, Marcelo. Guerra e Ciberespaço: uma análise a partir do meio físico. Dissertação de Mestrado. Programa de Pós-Graduação em Ciência Política. Porto Alegre-RS, Universidade Federal do Rio Grande do Sul, 2015.

LOPES, Gills V. Relações Internacionais Cibernéticas (CIBERRI): uma defesa acadêmica a partir dos estudos de segurança internacional. Tese de Doutorado em Ciência Política. Universidade Federal de Pernambuco. Recife, 2016.

MACHADO, Jussara. Inteligência e Ciberespaço: Desafios do Século XXI. In: CEPIK, Marco [organizador]. Inteligência Governamental: contextos nacionais e desafios contemporâneos. Niterói-RJ, Editora Impetus, 2011. Páginas 271-317.

MANDARINO, Raphael Jr. Segurança e defesa do espaço cibernético brasileiro. Recife-PE, Cubzac, 2010.

OLIVEIRA, Marcos; PAGLIARI, Graciela; MARQUES, Adriana; PORTELA, Lucas; FERREIRA NETO, Walfredo. Guia de Defesa Cibernética na América do Sul. Recife-PE, Editora UFPE, 2017.

SANCHO, Carolina H. Ciberseguridad: presentación del dossier. URVIO, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 8-15.