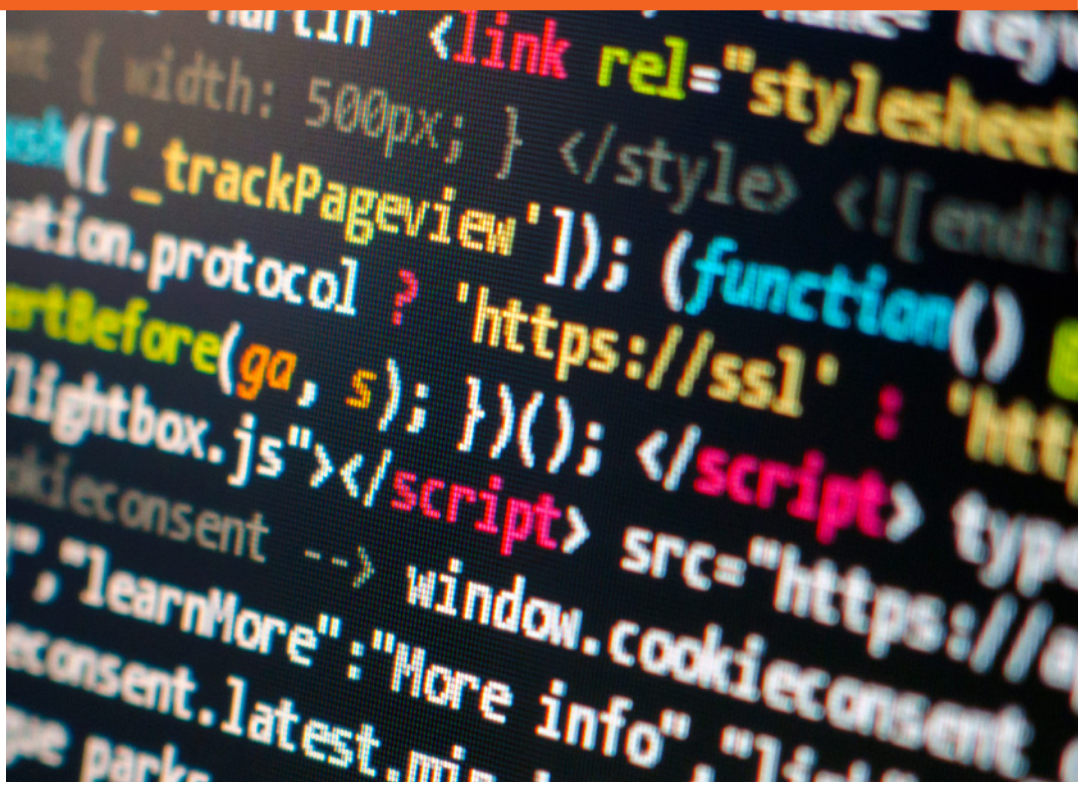
INSTITUTO IGARAPÉ
a think and do tank

NOTA
ESTRATÉGICA
30
SETEMBRO 2018

Uma Estratégia para a Governança da Segurança Cibernética no Brasil

Louise Marie Hurel e Luisa Cruz Lobato



Sumário

Uma Estratégia para a Governança da Segurança Cibernética no Brasil

Série:
Segurança Cibernética e Liberdades Digitais

Louise Marie Hurel e Luisa Cruz Lobato

Resumo

O presente estudo explora a institucionalização da agenda de segurança cibernética no Brasil e busca identificar oportunidades para cooperação multissetorial. Para esse fim, analisa-se os principais momentos e processos que marcaram o desenvolvimento da atual arquitetura de segurança cibernética no país, destacando-se as tensões que surgiram com a introdução da agenda como prioridade associada à segurança nacional. A descrição do ecossistema de governança da segurança cibernética permitiu a identificação de oportunidades sólidas de cooperação entre os diferentes setores envolvidos com a agenda, tanto no campo técnico (criptografia e resposta a incidentes), quanto na elaboração de legislações, políticas e campanhas de conscientização.

Siglas

ABIN – Agência Brasileira de Inteligência

APF – Administração Pública Federal

CCSDCiber – Centro de Coordenação de Segurança e Defesa Cibernética

CDCiber – Centro de Defesa Cibernética

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CGI.br - Comitê Gestor da Internet no Brasil

ComDCiber – Comando de Defesa Cibernética

CPI – Comissão Parlamentar de Inquérito

CSIRT – Grupos de Respostas a Incidentes de Segurança Cibernética

CTIR.gov – Centro de Tratamento de Incidentes de Redes do Governo

DNS – Sistema de Nomes de Domínio (do inglês *Domain Names System*)

DSIC-GSI – Departamento de Segurança da Informação e Comunicações

END – Estratégia Nacional de Defesa

GSI-PR – Gabinete de Segurança Institucional da Presidência da República

IoT - Internet das Coisas, em inglês Internet of Things

MD – Ministério da Defesa

NIC.br – Núcleo de Coordenação do Ponto BR

PF – Polícia Federal

1. Introdução

Na última década, observou-se a institucionalização progressiva da segurança cibernética no Brasil. Grande parte desse processo concentrou-se na atuação de diferentes setores dentro da Administração Pública Federal (APF), tendo como epicentro as áreas de defesa e segurança nacional. A Estratégia Nacional de Defesa (END), de 2008, foi o primeiro documento oficial a reconhecer a importância do espaço cibernético, marcando a inserção da segurança cibernética na agenda nacional.

O presente estudo identifica os principais desafios e oportunidades de cooperação para a governança da segurança cibernética no Brasil. Argumenta-se que a elaboração de políticas e diretrizes nessa área não se trata, somente, de uma questão de segurança ou de defesa nacional. Faz parte de um processo amplo de governança, que compreende arranjos formais e informais de cooperação entre os diferentes atores que compõem a estrutura de segurança cibernética brasileira. Esta abordagem, fundamentada nos processos de governança da segurança cibernética, lança luz sobre outras possibilidades de colaboração entre setores que dificilmente são vislumbradas a partir de uma estrutura mais rígida pautada em agrupamentos de competências (segurança cibernética, segurança da informação e defesa cibernética).

Os principais resultados encontrados foram:

- O processo de institucionalização da segurança cibernética no Brasil foi catalisado por dois eventos principais. O primeiro foi a aprovação do Marco Civil da Internet, em 2013, motivado pelo impacto político das revelações a respeito da estrutura de vigilância virtual dos Estados Unidos. O segundo foi consequência direta dos megaeventos sediados no país entre 2012 e 2016, que incluem esforços como (i) a criação do Centro de Defesa Cibernética (CDCiber); (ii) a construção de capacidades de instituições públicas nos âmbitos federal e municipal; (iii) o incremento da colaboração entre governos e setor privado; e (iv) o estabelecimento de doutrinas, políticas e diretrizes relacionadas à segurança cibernética.

- O processo de institucionalização acelerada e os megaeventos tiveram quatro impactos principais: (i) a excessiva securitização e uma acentuada militarização da segurança cibernética; (ii) a exclusão de atores não-estatais da definição de termas relevantes para a agenda política; (iii) a preferência, cada vez maior, por soluções que buscam o bloqueio de aplicações, remoção de conteúdo; e (iv) a dificuldade de coordenação no âmbito da Administração Pública Federal.

- Estes impactos estão refletidos nos desafios enfrentados na formulação de políticas para a segurança cibernética, com destaque para: (i) tensões entre abordagens de cunho proibicionista e criminalizante e aquelas focadas na garantia de direitos digitais; (ii) pouca colaboração entre atores no governo, setor privado, sociedade civil e academia envolvidos na formulação de políticas para a área; e (iii) ausência de mecanismos eficazes de colaboração e governança para a segurança cibernética no país.

- O maior desafio para uma governança multissetorial da segurança cibernética consiste na definição dos papéis e responsabilidades para cada setor. Observou-se que a falta de consenso e de coordenação dificulta a sustentabilidade das políticas.

Os achados acima indicam que, para superar esses desafios, é fundamental identificar áreas de interesse comum e espaços de construção de confiança entre os setores envolvidos. Assim, a consolidação de uma estrutura coerente de governança de segurança cibernética facilitará a identificação e o compartilhamento de boas práticas, bem como estimulará uma crescente coordenação entre setores, tão necessária para responder aos crescentes desafios para a segurança, estabilidade e resiliência das redes.

Este artigo estratégico se divide em três partes. A primeira aborda o processo de desenvolvimento da atual arquitetura de governança da segurança cibernética no Brasil e oferece um panorama das principais instituições engajadas nesse processo. A segunda retrata os desafios operacionais e práticos para a cooperação nesta área durante o ciclo de megaeventos sediados no país entre 2012 e 2016, bem como seus efeitos no desenvolvimento acelerado de estruturas da Administração Pública Federal. A parte final traz recomendações para o avanço da cooperação entre setores. Os métodos adotados no estudo incluíram o mapeamento das instituições pertencentes à estrutura de governança cibernética no país e a organização de um grupo focal composto por especialistas técnicos e representantes de setores do governo, academia, sociedade civil e setor privado.

2. Estrutura de governança e instituições

A política de segurança cibernética brasileira se desenvolveu a partir de uma preocupação cada vez maior com o aumento do número de ataques cibernéticos e com a (in)capacidade do país em combatê-los. Contudo, a crescente diversificação dos meios e das ameaças cibernéticas não explicam, em sua totalidade, o crescimento exponencial de incidentes no Brasil desde 2011.[1]A potencial projeção do Brasil junto às principais potências mundiais que atuam no combate às ameaças cibernéticas e a exposição do país a estas contribuíram para o desenvolvimento de políticas e diretrizes nacionais para segurança cibernética.

Neste contexto, identificou-se dois processos que culminaram na a diversificação e no amadurecimento da atual arquitetura da governança da segurança cibernética no país: (i) a criação de novas instituições[2], dedicadas a questões de natureza técnica, estratégica e/ou operacional específicas dessa área; e (ii) a reorientação de instituições já existentes,[3] que passaram a incluir aspectos da segurança cibernética[4] e vigilância das redes[5] em seu rol de responsabilidades.

O primeiro impulso à consolidação desta estrutura de governança cibernética e de suas respectivas instituições no país ocorreu no período de reestruturação e fortalecimento das capacidades nacionais de defesa, do final da década de 1990, com a criação do Ministério da Defesa (MD).[6] Neste período, o Ministério criou uma política de segurançada informação, estruturando políticas e órgãos especializados na esfera da APF.[7]

Em um segundo momento, já no ciclo de megaeventos sediados pelo país entre 2012 e 2016, foram criados espaços de cooperação e coordenação entre os setores técnico e de defesa. Além disso, questões relacionadas a ameaças à segurança e defesa nacionais, como ciberterrorismo e infraestruturas críticas, foram priorizadas, incentivando políticas e estratégias nesta área.

1 CERT.br (2018).

2 A exemplo do CERT.br, CIRT.gov, CDCiber, ComDCiber, entre outros.

3 A exemplo da Polícia Federal e da ABIN.

4 EXÉRCITO (2016).

5 MUGGAH ; THOMPSON (2016).

6 ABDENUR (2014).

7 BRASIL (2000).

2.1. Reestruturação do setor de defesa e estabelecimento da política de segurança da informação

Com o início da Internet comercial em 1993 (World Wide Web), a interconectividade deixou de ser restrita às redes acadêmicas, ganhando escala e propulsão em todo o mundo, inclusive no Brasil.[8] Neste contexto, a criação do Comitê Gestor da Internet (CGI.br), em 1995, ofereceu um espaço favorável não só para o desenvolvimento de políticas e de um diálogo multissetorial referente aos desdobramentos da Internet no país, mas também para a elaboração de novas estruturas pertencentes a essa governança

As preocupações com os riscos de segurança que emergiram com a rápida expansão da internet comercial e com a necessidade de manter uma infraestrutura resiliente e operacional levaram à criação de dois órgãos dedicados ao assunto: o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br)[9] e o Núcleo de Coordenação do Ponto BR (NIC.Br). O CERT.br foi criado em 1997 a partir de um estudo encomendado pelo CGI.br para o estabelecimento de uma "coordenadoria de segurança de redes".[10] Já o NIC.br foi criado, em 2003, para implementar as decisões do CGI.br e, em 2005, passou a administrar o registro de nomes sob o domínio ".br".

O CERT.br é o ponto focal para notificação e resposta a incidentes no país, além de promover treinamentos e produzir e disseminar recursos educacionais para conscientização sobre riscos e ameaças na rede (exemplo, botnets, malware, phishing, spam).

O final dos anos 90 e o início dos anos 2000 marcaram o começo da consolidação de conceitos e competências relacionadas à segurança da informação. Tais processos ocorreram simultaneamente à consolidação de órgãos e políticas para a governança da internet no país, bem como do entendimento de segurança das redes. No ano 2000, sob os auspícios do Conselho de Defesa Nacional, criou-se a Política de Segurança da Informação e o Comitê Gestor da Segurança da Informação. Ambos tinham mandato para estabelecer diretrizes, princípios e objetivos para o desenvolvimento de normas, tecnologias nacionais e capacitação de entidades e órgãos da APF no campo da segurança da informação.[11]

Na ocasião, foi estabelecido um sistema hierárquico de tomada de decisões federais, partindo da Presidência da República, no nível estratégico, e se ramificando até o nível operacional, a exemplo de forças-tarefa dentro da Polícia Federal e do Centro de Defesa

8 Ver: RNP (s.d).

9 O CERT.br se estrutura a partir de preocupações com os riscos de segurança da abertura e expansão da internet comercial. Ver: NIC (1996).

10 GOMIDE et al. (1996).

11 Idem, Ibidem

Institucional da Presidência da República (GSI-PR) prestar assistência à presidência em temas de defesa e segurança, além de coordenar as atividades de inteligência federal e segurança da informação, por meio da Agência Brasileira de Inteligência (ABIN).

Subordinado ao GSI-PR, o Departamento de Segurança da Informação e Comunicações (DSIC-GSI) é diretamente responsável pela coordenação de ações de segurança cibernética, inclusive com a operação e manutenção de um Centro de Tratamento de Incidentes de Redes do Governo (CTIR.gov).[12] Contudo, é importante destacar que a manutenção da segurança das redes não compete somente ao GSI-PR, mas também a atores do sistema de inteligência, à Polícia Federal, a empresas privadas, operadores de redes e a Grupos de Resposta a Incidentes de Segurança (CSIRTs).

Paralelamente, o Núcleo de Coordenação do Ponto BR - criado em 2005 - se tornou uma das principais estruturas para a coordenação de diferentes aspectos técnicos da governança da internet, abarcando, inclusive o CERT.br e o Registro.br, responsável pelo registro e manutenção de nomes de domínios que utilizam o .br e pela definição de padrões de segurança que visam garantir a integridade e funcionalidade do sistema DNS (ver Anexo 1). Assim, além de implementar decisões do CGI.br, o NIC.br desempenha uma importante função de garantir a segurança, resiliência e estabilidade da rede. Conforme veremos na próxima seção, as instituições voltadas para a governança da internet e da segurança cibernética se sobrepõem operacionalmente no que diz respeito à resposta a incidentes e ataques. Historicamente, são processos que ocorreram em setores específicos da APF (Ministério da Ciência, Tecnologia e Comunicações e Ministério da Defesa), mas que acarretaram em novos canais de cooperação.

Para garantir a segurança das redes no âmbito da APF, o Decreto nº 5.772, de 2006, criou, como mencionado, o Centro de Tratamento de Incidentes de Redes do Governo (CTIR.gov).

A partir desse momento, o tratamento e a resposta a incidentes cibernéticos dentro da APF passam a ser coordenados pelo CTIR.gov, entidade integrante do DSIC-GSI. Além disso, o Centro serve como ponte de cooperação técnica entre outras entidades dentro da AFP e a rede nacional de CSIRTs (ver Anexo 2). Paralelamente a esses processos na Presidência, em 2012, o Ministério da Justiça (MJ), por meio da Polícia Federal (PF), estabeleceu o Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos, voltado para a prevenção e a investigação de ataques contra sistemas e infraestruturas críticas do governo federal. Embora não seja um órgão voltado para a segurança e defesa cibernéticas, compete à PF o combate a determinados tipos de crimes virtuais, dado o seu caráter transnacional.[13]

12 CTIR.gov (2011).

13 É competência constitucional da Polícia Federal a investigação de crimes de natureza transnacional em que o Brasil se comprometeu por meio de tratados internacionais e por crimes contra a APF direta ou indireta (Art. 144, Constituição Federal). A Lei n. 13.124/2015 amplia a competência da PF para investigação de crimes contra bancos e caixas eletrônicos.

No âmbito do Ministério da Defesa (MD), a Estratégia Nacional de Defesa (END), lançada em 2008 e atualizada em 2012, reconhece o espaço cibernético, ao lado dos setores nuclear e espacial, como um dos três principais setores estratégicos para a defesa e segurança nacionais.[14]

A END se destaca como parte de um processo político-estratégico de estruturação e desenvolvimento tecnológico no setor militar com o intuito de promover maior cooperação entre as Forças Armadas, e responsabiliza o Exército pela coordenação e integração de programas relativos ao setor cibernético.[15]

Em 2016, estabeleceu-se o Comando de Defesa Cibernética (ComDCiber), composto por representantes do Exército, da Marinha e da Aeronáutica. O órgão é encarregado de "planejar, orientar, coordenar e controlar as atividades operativas, doutrinárias, de desenvolvimento e de capacitação no âmbito do Sistema Militar de Defesa Cibernética".[16]

Trata-se de um comando operacional conjunto que se insere na estrutura regimental do Exército Brasileiro, junto ao Estado-Maior Conjunto, chefiado pela Marinha, e o Departamento de Gestão e Estratégia, chefiado pela Aeronáutica. Nesse sentido, a criação do ComDCiber marca uma maior integração entre as Forças Armadas, além de colocar em evidência um processo de fortalecimento das capacidades do Centro de Defesa Cibernética (CDCiber), conforme previsto na revisão da END, em 2012.[17]

14 BRASIL (2008).

15 A END de 2008 identifica três setores estratégicos para o país e atribui a cada força um setor correspondente; deste modo, o Exército fica encarregado pelo setor cibernético, a Marinha, pelo setor nuclear e a Aeronáutica, pelo setor espacial. Em sua atualização, em 2012, a END estabelece como uma de suas prioridades o fortalecimento do então Centro de Defesa Cibernética, de modo que este viesse a evoluir para o atual Comando de Defesa Cibernética.

16 MD (2017).

17 BRASIL (2015).

Figura 1. Estrutura da Governança da Segurança Cibernética no Brasil

Conforme detalhado, a institucionalização da segurança cibernética no país engloba órgãos técnicos, de natureza governamental, que contribuem para o desenvolvimento de políticas, normas e práticas diferentes, porém intrinsecamente relacionadas. A figura 1 retrata o panorama mais geral da estrutura da governança da segurança cibernética no Brasil, tendo em vista a participação desses diferentes setores. Ela nos permite identificar os principais grupos e temas pertencentes a essa estrutura, mostrando também que a segurança cibernética é preocupação compartilhada por uma vasta gama de atores, e que sua governança deve incluir a ampliação da colaboração entre eles no que tange à formulação de políticas integradas.

No universo da estrutura da governança da segurança cibernética no país, vislumbra-se um conjunto de competências em relação a diferentes setores na sociedade, que operam partir da ou na interseção entre essas. A distinção entre segurança cibernética, defesa cibernética e segurança da informação apresentada na figura 1 é tanto operacional quanto temática. No entanto, é importante ressaltar que se trata de uma divisão didática e que, na prática, os três temas se sobrepõem. A segurança da informação é a mais ampla das três, dizendo respeito a riscos inerentes a sistemas de informação e todos os tipos de controle (físicos, técnicos, processuais e de pessoal). Frequentemente, enseja medidas defensivas,

capazes de assegurar que eventuais vulnerabilidades sejam mitigadas e tratadas. Segurança cibernética, por sua vez, diz respeito ao conjunto de riscos apresentados no e a partir do ciberespaço, compreendendo em si aspectos da segurança da informação. Finalmente, a defesa cibernética engloba as ameaças que porventura afetem diretamente a segurança nacional do Estado brasileiro, assim como ameaças oriundas de atores estatais. Trata-se da competência mais específica entre as três.

Finalmente, nota-se que a compreensão dos diferentes termos (por exemplo, segurança cibernética, defesa cibernética, e segurança da informação)[18] e o mapeamento da interação entre as diferentes partes nesse campo, são desafios que permanecem no horizonte de potenciais desdobramentos na elaboração de políticas.

A próxima seção aprofunda a discussão sobre a acelerada institucionalização da segurança cibernética no âmbito do Ministério da Defesa e identifica espaços que surgiram para cooperação, com destaque para o ciclo de megaeventos.

2.2. Ciclo de megaeventos e consolidação do regime de segurança e defesa cibernéticas no âmbito nacional

Em 2013, foi revelado por Edward Snowden, ex-membro da CIA, que o Brasil também era alvo de espionagem por parte dos EUA. Diante desse contexto e do ciclo de megaeventos sediados no Brasil entre 2012 e 2016, identificou-se uma crescente demanda por parte da Presidência da República e do Ministério da Defesa por mecanismos, instituições e políticas para a segurança cibernética no país.[19] Novas práticas de segurança cibernética, implementadas a partir destes episódios, caracterizaram uma nova fase no desenvolvimento e institucionalização do setor no país. Essa fase foi marcada pela ênfase em ameaças à segurança nacional e pela estruturação de um Sistema Militar de Defesa Cibernética no âmbito da Administração Pública Federal. No entanto, observa-se que, iniciativas de coordenação entre esses órgãos e instituições técnicas também tiveram espaço no mesmo período.

Eventos como a Conferência das Nações Unidas sobre o Desenvolvimento Natural (Rio+20) (2012), a Jornada Mundial da Juventude (2013), a Copa das Confederações (2013), a Copa do Mundo (2014) e as Olimpíadas e Paralimpíadas (2016) envolveram uma série de esforços coordenados entre o Centros de Estudo, Resposta e Tratamento de Incidentes (CERT.Br),

18 Cepik, Canabarro e Borne argumentam que "diferentes tipos de incidentes cibernéticos carecem de uma clara delimitação conceitual. A confusão semântica que se estabeleceu em torno desses conceitos não apenas prejudica a pesquisa, mas impõe desafios à adoção de políticas públicas relativas ao ciberespaço e à Internet" (2014), p.178. O desafio, constatado ainda em 2014, permanece um obstáculo para o avanço e abertura do processo de participação na elaboração de políticas. Enquanto existe uma percepção mais clara de cada ator sobre suas respectivas competênciaso que não ocorre quando se trata da relação entre diferentes entidades.

19 MINISTÉRIO DA DEFESA (2014)

Grupos de Respostas a Incidentes de Segurança Cibernética (CSIRTs, sigla em inglês) e outros órgãos com competência para tratar de assuntos de segurança cibernética. Além disso, esses eventos também trouxeram uma série de estruturas de caráter excepcional designadas para a ocasião.

Ainda em 2011, criou-se a Secretaria Extraordinária de Grandes Eventos para promover maior integração entre órgãos federais, estaduais e municipais no campo da segurança. Em 2012, a Portaria nº 2.221, por exemplo, estabeleceu orientações para a participação do MD em atividades de planejamento de emprego temporário das Forças Armadas na segurança e defesa cibernética em cidades-sede de grandes eventos. Criou-se, ainda, o "Rio 2016 CSIRT", uma equipe de respostas a incidentes voltada especificamente para atender à segurança das Olimpíadas e que operou de maneira conjunta com o CDCiber, o Centro de Coordenação de Segurança e Defesa Cibernética (CCSDCIBER), o CTIR.gov e o CERT.br.

O intenso envolvimento de órgãos e instituições militares no campo da segurança cibernética, nesse período, marca um processo de "securitização"[20] da área. Ao mesmo tempo, uma série de ameaças cibernéticas (por exemplo, espionagem, vazamento de informações, malware, ataques de negação de serviço) passaram a ser enquadradas como prioridades para a segurança nacional. Ao reunir turistas, delegações, empresas e representantes governamentais, os megaeventos também contribuíram para maiores preocupações relacionadas ao terrorismo. Nesse contexto, o ciberterrorismo e os riscos associados a infraestruturas críticas[21] (por exemplo, hidrelétricas, torres de eletricidade, rede de comunicações de aeroportos) foram priorizados em detrimento de ameaças não diretamente relacionadas à segurança nacional.

Este contexto foi marcado também por uma série de insatisfações populares que antecederam a Copa do Mundo de 2014 e as Olimpíadas de 2016, inclusive com a atuação de redes de hacktivistas. Por exemplo, o grupo Anonymous, conhecido por promover ataques cibernéticos relacionados a questões políticas, se dedicou ao ataque e comprometimento de sites governamentais,[22] o que acabou por reforçar o processo de securitização. Entre os órgãos envolvidos na formulação e execução da resposta a esses ataques estavam o Centro de Monitoramento Cibernético, o CDCiber, as Forças Armadas, a Polícia Federal,[23] o CERT.br e o CTIR.gov.[24] Estes últimos responsáveis pela notificação e alerta de órgãos públicos e privados.[25]

---

20 CEPIK; CANABARRO; BORNE (2014); DINIZ; MUGGAH; GLENNY (2014); LOBATO; KENKEL (2015); HUREL (2018).

21 "Instalações, serviços e bens que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional"(GSI-PR, 2010).

22 R7 (2013).

23 ROHR (2012).

24 CERTs e CSIRTs geralmente operam por meio de sistemas colaborativos de respostas a incidentes de segurança. O CERT.br, por exemplo, é central para as notificações de incidentes de segurança no Brasil. CSIRTs possuem composições bastante diversas, que incluem desde grupos "ad hoc" voltados para o âmbito local até grupos regionais, nacional e/ou de caráter privado (HUREL, 2018).

25 BRAUN (2012).

Além disso, a instauração de uma Comissão Parlamentar de Inquérito da Espionagem, ("CPI da Espionagem"), com o objetivo de "investigar a denúncia de existência de um sistema de espionagem, estruturado pelo governo dos Estados Unidos"[26], reforçou a abordagem pautada pela necessidade de proteger a segurança nacional. O principal resultado desta CPI foi o lançamento, pelo Departamento de Segurança da Informação e Comunicações do GSI (DSIC-GSI), da "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética para a Administração Pública Federal 2015-2018".[27] Ao mesmo tempo em que se verificou maior preocupação com o tema da segurança nacional, a CPI da Espionagem e a visibilidade que o tema da insegurança cibernética ganhou tornaram o contexto nacional favorável à adoção de medidas administrativas dedicadas ao aumento da segurança nas redes.

Ao final do ciclo de megaeventos, a competência para a implementação da estratégia e da política de segurança cibernética no país se viu compartilhada pelas seguintes organizações: (i) o Conselho Nacional de Defesa, que coordena a política e estratégia de defesa no âmbito nacional; (ii) o GSI-PR, que, por meio do Departamento de Segurança da Informação e Comunicações, é responsável por ações de segurança da informação e comunicações no âmbito da Administração Pública Federal (APF); (iii) a ABIN, encarregada das atividades de inteligência e do desenvolvimento de sistemas e comunicações seguros para a APF; (iv) as Forças Armadas, a partir do ComDCiber e CDCiber, encarregadas da coordenação e integração dos esforços de defesa cibernética no país; e (v) o Ministério da Justiça, a partir da atuação da Polícia Federal nas investigações a crimes cibernéticos contra a APF ou relativos a matérias protegidas por convenções internacionais com as quais o país tenha se comprometido.

Fora do âmbito da Administração Pública Federal pôde-se, ainda, verificar a atuação de uma série de organizações de natureza acadêmica e técnica - como universidades, CERTs e CSIRTs - e privada - como pequenas e médias empresas, além de grandes corporações no setor de tecnologia.

Observa-se, assim, que a consolidação da segurança e defesa cibernéticas no âmbito nacional é fruto de uma combinação de fatores. Em primeiro lugar, das tentativas de promover maior coordenação entre as distintas instituições domésticas destinadas a sua governança. Em segundo, da necessidade de responder órgãos destinados aos desafios apresentados pelos megaeventos ocorridos no país e às ameaças externas.[28]

26 FERRAÇO (2014).

27 Portaria CDN nº 14, de 11 de maio de 2015.

28 HUREL (2018).

3. Principais desafios para a cooperação

Como demonstrado nas seções anteriores, há, no âmbito da APF, uma grande quantidade de instituições que lidam com a segurança e defesa cibernéticas. Por essa razão, a abordagem utilizada por cada uma delas, muitas vezes, transpassa o caráter técnico-operacional e se reflete no nível político e jurídico. Tal diversificação trouxe consigo uma série de desafios - e também oportunidades - para a cooperação e coordenação nesse âmbito.

Há pelo menos quatro desafios que merecem destaque - e que também resultam das consultas realizadas ao longo do projeto: (i) o risco de excessiva securitização e de uma acentuada militarização da segurança cibernética; (ii) o risco de exclusão de atores não-estatais da governança da segurança cibernética no Brasil, desde a definição de prioridades até a elaboração e implementação de políticas; (iii) a preferência, cada vez maior, por soluções que buscam o bloqueio de aplicações, remoção de conteúdo e criminalização de comportamentos na Internet; e (iv) problemas de coordenação no âmbito da Administração Pública Federal.

O risco de "securitização"[29] e potencial "militarização" da estrutura é fruto do contexto dos megaeventos no país. Nesse contexto, a criação das soluções para os diversos problemas de segurança foram alocadas para o setor militar. A criação de órgãos especializados, vinculados às Forças Armadas, bem como a atribuição e ampliação de responsabilidades da ABIN e Polícia Federal evidenciam os esforços para lidar com questões de (in)segurança cibernética a partir da ampliação das competências de órgãos dos aparatos militar e de inteligência do Estado. Esses esforços resultaram, por sua vez, em uma maior alocação de tempo e recursos para o combate a ameaças como o terrorismo, a sabotagem industrial e a guerra cibernética, e um reforço do "aparato de vigilância" do Estado[30].

A ausência de canais para inclusão de atores não-estatais no processo de elaboração de políticas também resulta de processos de securitização e militarização, que acabam retirando da esfera do debate público determinados assuntos avaliados como estratégicos para o país. Com isso, o processo de elaboração de políticas sobre o tema se torna mais restrito aos órgãos de segurança e inteligência. O tratamento e resposta a ameaças por meio de uma lógica securitizante "reacende o trade-off normativo entre a segurança e o respeito a liberdades e direitos fundamentais"[31], colocando-os em pólos opostos, ao invés de encará-

29 CEPIK; CANABARRO; BORNE (2014); DINIZ; MUGGAH; GLENNY (2014); LOBATO; KENKEL (2015); HUREL (2018).

30 O chamado aparato de vigilância do Estado corresponde às instituições dedicadas a práticas e ao desenvolvimento de sistemas e estratégia de espionagem e vigilância doméstica e externa.

31 CEPIK; CANABARRO; BORNE (2014).

los como princípios que devem caminhar conjuntamente no processo de elaboração de políticas para a segurança cibernética.[32] Diante desse contexto, representantes da academia e a sociedade civil[33] chamaram a atenção para a importância da inclusão do multissetorialismo às diretrizes, a estruturação de órgãos pertencentes ao regime nacional de segurança cibernética, e para o processo de elaboração de políticas para o setor.[34]

Observou-se, também, uma tendência a responder aos desafios de segurança pelas vias do bloqueio, remoção de conteúdo e criminalização. Um sinal disso foi a proposta do projeto de lei 215/15, também chamado de PL Espião, que autorizava o bloqueio de aplicativos e websites, além da tentativa de criminalizar uma série de condutas - entre elas, crimes de direitos autorais e o acesso indevido a computadores e sistemas - conforme destacado no relatório final da CPI dos Crimes Cibernéticos (CPICiber). Estes processos tornaram-se evidentes em uma série de decisões judiciais, entre os anos de 2015 e 2016, que determinaram o bloqueio de aplicações[35] e foram motivadas pela dificuldade ou impossibilidade de acessar dados criptografados de redes sociais e aplicativos de mensagens. Estes episódios contribuíram para elevar a tensão entre, de um lado, abordagens com foco na criminalização de condutas e, do outro, aquelas com foco na proteção de direitos e garantias legais no tocante à Internet.

Os desafios de coordenação são bastante evidentes no âmbito da Administração Pública Federal, em virtude da carência de mecanismos efetivos de governança da segurança da informação e comunicações, segurança cibernética e ativos de informação críticos. Somando-se a isto, encontra-se a dificuldade de adaptar políticas nos campos da segurança da informação e cibernética, elaboradas em um âmbito estratégico, para o nível operacional. Em outras palavras, diretrizes e orientações de segurança feitas pelo DSIC e GSI tendem a ser apenas parcialmente implementadas. Somam-se à lista de desafios a ausência de um orgão central responsável pela coordenação executiva de forma sistêmica e participativa entre as áreas de segurança da informação, segurança cibernética e ativos de informação críticos, e de uma rubrica orçamentária própria e adequada ao tamanho do problema.[36]

De um ponto de vista mais técnico, os megaeventos, que tanto contribuíram para a consolidação de uma estrutura (ainda em desenvolvimento) para a segurança cibernética no país, também trouxeram o desafio de uma ação conjunta (entre órgãos de naturezas diversas) para a proteção e resiliência das redes. Nesse sentido, o compartilhamento de informações entre grupos organizadores, técnicos de operadores de sistemas e redes, e os CSIRTs foi visto como fundamental para esses esforços de coordenação durante a Copa do Mundo de 2014[37] e as Olimpíadas de 2016.[38]

32 CEPIK; CANABARRO; BORNE (2014), p.181.

33 ARTIGO 19 (2016); LOBATO; KENKEL (2015); DINIZ; MUGGAH; GLENNY (2014).

34 ARTIGO 19 (2016); HUREL (2018).

35 ITS RIO (2016).

36 BRASIL (2015).

37 HOEPERS (2014).

38 EB (2016).

Ao mesmo tempo, no entanto, práticas de respostas a incidentes dentro e entre organismos contribuíram para guiar e, potencialmente, redefinir a relação entre diferentes regimes e estruturas da arquitetura brasileira de governança cibernética durante os eventos.[39] Neste período, ações de respostas a incidentes incluíram a estrutura militar do CDCiber e também a atuação de parceiros externos, como o CERT.br, empresas privadas e outros órgãos da APF. Assim, apesar da limitação de acesso a informações sobre os atores envolvidos na promoção da segurança cibernética, estruturas menos hierarquizadas como o CERT.br protagonizaram o processo de capacitação e colaboração no pós-Rio+20,[40] por exemplo.

Essas estruturas também chamam a atenção para a interdependência entre os setores público, privado e da sociedade civil no processo de governança da segurança cibernética. Uma resposta adequada aos desafios apresentados nesse campo perpassa, fundamentalmente, pela criação de espaços formais e informais de diálogo, que possibilitem maior interação entre representantes destes setores.[41]

4. Considerações finais e recomendações

A análise mostrou que a segurança cibernética não possui espaço exclusivo no âmbito do governo brasileiro e que diferentes atribuições competem a atores diversos, o incluindo, governo, setor privado, academia e sociedade civil. Buscou-se identificar os diferentes grupos e instituições engajados com a temática, bem como a forma como atuam e as possibilidades (e desafios) para que cooperem entre si. Foi mostrado que o ciclo de megaeventos e o escândalo da espionagem em massa dos Estados Unidos potencializaram e aceleraram a consolidação de um processo de estruturação já em curso, que é marcado pela institucionalização da segurança cibernética no âmbito da APF e do Ministério da Defesa e por uma concentração do regime de segurança cibernética na figura do Estado.

Observou-se, também, que os processos de coordenação entre atores que compõem a estrutura de governança da segurança cibernética não estão necessariamente atrelados a mecanismos convencionais de regulação. Contextos extraordinários, como os megaeventos, contribuíram para a promoção de pontos de contato e espaços de coordenação e colaboração entre as diferentes partes, particularmente através de parcerias entre organismos técnicos não governamentais e o setor militar. Isso indica

39 HUREL (2018).

40 Idem, Ibidem.

41 MANDARINO JÚNIOR; CANONGIA (2010).

que oportunidades de cooperação e diálogo podem ocorrer a partir de contextos e processos específicos. Deve-se, no entanto, garantir que os esforços de colaboração sobrevivam a esses períodos extraordinários e componham uma estrutura de governança mais perene.

A partir dos diálogos multissetoriais organizados ao longo do projeto, identificou-se alguns dos pontos de convergência que favoreceram a cooperação e o diálogo, e que devem ser promovidos para o avanço da governança da segurança cibernética no Brasil:

Promoção de uma estrutura de governança da segurança cibernética participativa e multissetorial

A governança da segurança cibernética deve contemplar a complexidade técnica, temática e conceitual, e incluir todo o ecossistema de atores associados a ela. O modelo nacional de governança da Internet, encabeçado pelo CGI.br, serve de exemplo para o desenvolvimento e incorporação de princípios como transparência, multidisciplinaridade, e o próprio modelo multissetorial. Para um efetivo sistema de governança da segurança cibernética, deve-se propor a operacionalização e a harmonização entre iniciativas que ainda são setorializadas. Recomendam-se também a formulação de uma estratégia nacional para segurança da informação e a criação de uma agência nacional para geri-la, bem como o uso responsável de técnicas de análise/monitoramento de redes sociais para adquirir informações sobre o cotidiano urbano e eventuais problemas de segurança pública.

Participação da academia e da sociedade civil na governança da segurança cibernética e da informação

Apesar de haver espaço para cooperação entre organismos técnicos, faz-se necessário o estabelecimento de canais de cooperação que assegure a participação cidadã ampla e efetiva. Deve-se melhor compreender e relacionar a segurança da informação e a proteção de dados à segurança cibernética, evitando interpretações que restrinjam o acesso de grupos da sociedade civil e da academia à sua governança.

Esses grupos devem ser continuamente consultados e incluídos nesta estrutura. Além de desempenharem papel fundamental garantindo a continuidade de políticas e advogando por uma abordagem centrada na proteção do indivíduo e de seus dados pessoais, contribuem para o combate à desinformação e para o desenvolvimento de padrões éticos para coleta e análise de dados. Além disso, informam debates e, por vezes, trabalham com programas de capacitação e campanhas de conscientização a respeito de riscos online. Com relação a esses riscos, deve-se atentar para temas como (i) a garantia da integridade da informação política; (ii) a proteção a informações públicas e industriais sensíveis no contexto de atividades de espionagem estrangeiras; e (iii) mecanismos de produção e reprodução, humana ou automatizada, de *fake news*; e (iv) campanhas de desinformação na web.

Fomento a cooperação técnica para segurança cibernética

Os setores público e privado devem investir em cooperação na área técnica, a exemplo de respostas a incidentes de segurança e desenvolvimento e operação de sistemas e estandartes como criptografia. Centros de Estudo, Resposta e Tratamento de Incidentes (CERTs) e Grupos de Respostas a Incidentes de Segurança Cibernética (CSIRTs) devem intensificar a colaboração com os setores público e privado para a troca de informações sobre ataques cibernéticos e vulnerabilidades em sistemas, além de colaborarem para o treinamento de equipes de respostas a incidentes. Entidades da administração pública, por sua vez, devem investir na parceria com CERTs e CSIRTs para a difusão da "higiene digital", ou seja, boas práticas de segurança cibernética e manutenção de sistemas em instituições públicas. União, estados e municípios devem, ademais, priorizar a implementação de tecnologias de segurança existentes em suas páginas na web, e sistemas de computadores devem ser atualizados regularmente. Estados e municípios devem assegurar que as redes, sistemas e dispositivos de internet utilizados na administração do cotidiano urbano estejam fortificados contra ataques cibernéticos. Estes mesmos atores devem garantir que os dados coletados, compilados e analisados sejam tratados em observância a parâmetros internacionais de proteção de dados e em respeito a padrões éticos que atentem para o uso finalístico dos dados coletados.

Elaboração de legislação e marcos regulatórios

As propostas de legislação e regulação devem levar em consideração os princípios estabelecidos no Marco Civil da Internet. Além disso, os mecanismos regulatórios e normativos devem ser suficientemente flexíveis para acompanhar o desenvolvimento tecnológico, ou seja, não devem estar vinculados a uma tecnologia específica.

Conscientização, educação e combate à desinformação na internet

O governo deve investir em campanhas educacionais e de conscientização acerca do uso da internet, da difusão da desinformação online, e dos riscos de segurança que determinados comportamentos podem incorrer. É fundamental que as medidas adotadas não resultem em violações aos direitos de liberdade de expressão e outros direitos fundamentais previstos na Constituição Federal e no Marco Civil da Internet. Ademais, é importante que o governo também atue em conjunto com a sociedade civil, criando novos canais de diálogo e de confiança para um debate aberto sobre as diferentes dimensões da segurança cibernética, para além da segurança e defesa nacional. Para tanto, deve incluir abordagens centradas e dedicadas à proteção de usuários e à divulgação de boas práticas online. Deve-se estimular a difusão, para indivíduos e grupos, de informação sobre direitos, crimes e ferramentas técnicas e institucionais para lidar com ataques cibernéticos e campanhas de desinformação na internet. Plataformas e mídias sociais devem se comprometer com a revisão dos algoritmos de priorização de conteúdo e com a sua transparência, indicando, por exemplo, quando um conteúdo, independentemente de sua natureza, tiver sido removido. A comunidade acadêmica, por sua vez, deve colaborar com

a construção de evidências que possibilitem o mapeamento de situações e fenômenos de segurança, bem como com a realização e divulgação de estudos sobre o impacto real de fenômenos na web.

Desenvolvimento de padrões éticos para o monitoramento de redes

Entidades da administração pública, setor privado, academia e sociedade civil devem desenvolver padrões éticos para a pesquisa, análise e monitoramento de redes, de modo a evitar que esse tipo de atividade resulte em investigações direcionadas a pessoas e grupos específicos. Instituições e organizações dedicadas à prática devem ainda observar o princípio da finalidade da coleta de dados na Internet: dados pessoais coletados para um determinado fim não devem ser utilizados para um fim distinto daquele originário. Os atores também devem esclarecer o tipo de monitoramento realizado e se o objetivo consiste na investigação de um problema - isto é, identificar pessoas, seus comportamentos e ou objetos - ou de um fenômeno mais amplamente compreendido, a exemplo de uma investigação sobre o alcance de notícias falsas. Considerando que investigações de fenômeno podem levar à coleta de dados sensíveis, as informações compiladas devem ser protegidas contra usos indevidos ou equivocados. Aqueles que utilizam o monitoramento de redes para esse fim também devem estabelecer parâmetros de coleta, como anonimização dos dados das pessoas envolvidas e, sempre que possível, preferir o uso de dados disponíveis publicamente.

As cinco áreas identificadas acima compreendem potenciais níveis de cooperação e diálogo e refletem preocupações comuns entre integrantes do setor privado, da sociedade civil e do governo. Elas sugerem que, a despeito da variedade de atores e instituições, bem como de seus interesses e prioridades, é possível encontrar pontos de contato e oportunidades de colaboração que possibilitem a construção e a consolidação de uma arquitetura de governança para a segurança cibernética que seja coerente com os anseios e possibilidades dos diferentes setores brasileiros.

Referências

ABDENUR, A. (2014). "Brazil and cybersecurity in the aftermath of the Snowden revelations". In: Dane, F. (ed.). *International security: a European-South American dialogue*. Rio de Janeiro: Konrad Adenauer Siftung, p. 229-283.

ARTIGO 19 (2016). *Brasil: análise da estratégia de cibersegurança*. São Paulo: Artigo 19.

BRASIL. Decreto n.° 3.505, DE 13 DE JUNHO DE 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 13 de junho de 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/d305.htm>. Acesso em: 15 abr. 2018.

_____. (2008). *Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa.

_____. (2012). *Política Cibernética de Defesa*. Brasília: Ministério da Defesa.

_____. (2015). *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018*. Brasília: Gabinete de Segurança Institucional da Presidência de República.

BRAUN, D. (2012). *Exército prepara defesa cibernética da Copa das Confederações*. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/08/exercito-prepara-defesa-cibernetica-da-copa-das-confederacoes.html>. Acesso em: 27 mai. 2018.

CDCIBER (2014). *CDCIBER: perspectivas em face da espionagem eletrônica*. VIII Curso de Extensão em Defesa Nacional UNAMA. Disponível em: <https://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviicedn.pdf>. Acesso em: 5 jun. 2018.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. (2014). "A securitização do ciberespaço e o terrorismo: uma abordagem crítica". In: SOUZA, A. M.; NASSER, R.M.; MORAES, R. F. (eds.). *Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI*. Brasília: IPEA, p. 161-186.

CERT.BR. (2018). *Estatísticas dos incidentes reportados ao CERT.br*. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 27 mai. 2018.

CTIR.GOV. (2011). *Sobre o CTIR Gov*. Disponível em: <http://www.ctir.gov.br/sobre-CTIR-gov.html>. Acesso em: 26 mai. 2011.

DINIZ, G.; MUGGAH, R.; GLENNY, M. (2014*). Deconstructing cyber security in Brazil: Threats and responses*. Rio de Janeiro: Instituto Igarapé, p. 3-32. (Strategic Paper 11).

EXÉRCITO Brasileiro (2016). *Exército, Abin e CGI.br farão a defesa cibernética nas Olimpíadas Rio 2016*. Escritório de Projetos do Exército Brasileiro. Disponível em: <http://www.epex.eb.mil.br/index.php/ultimas-noticias/220-exercito-abin-e-cgi-br-farao-a-defesa-cibernetica-nas-olimpiadas-rio-2016>. Acesso em: 14 abr. 2018.

GOMIDE, A. C.; PINHEIRO, C. A. C.; VAZQUEZ, P. A. M. (1996). *Grupos de trabalho – documento GT-S: rumo a criação de uma coordenadoria de segurança de redes na internet Brasil*. NIC.BR. Disponível em: < http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169#5>. Acesso em: 18 abr. 2018.

HOEPERS, C. (2014). *Desafios e lições aprendidas no tratamento de Incidentes em grandes eventos*. CERT.br. Disponível em: < https://www.cert.br/docs/palestras/certbr- forum-csirts2014-02.pdf >. Acesso em 23 mai. 2018.

HUREL, L. M. (2018). "Securitização e governança da Segurança Cibernética no Brasil". In: *Horizonte presente: tecnologia e sociedade em Debate*. Belo Horizonte: Letramento.

ITS Rio (2016). *Bloqueio do WhatsApp viola a Constituição e os direitos humanos. Instituto de Tecnologia e Sociedade do Rio*. Disponível em: <https://feed. itsrio.org/bloqueio-do-whatsapp-viola-a-constitui%C3%A7%C3%A3o-e-os-direitos-humanos-aeaa0d94f2ae>. Acesso em 17 abr. 2018.

LOBATO, L. C.; KENKEL, K. M. (2015). *Discourses of cyberspace securitization in Brazil and in the United States*. Revista brasileira de política internacional, Brasília, v.*n* 58, n. 2, p. 23-43, Dez. Disponível em: <http://www.scielo. br/scielo.php?script=sci_=arttext&pid=S0034-73292015000200023&lng=en&nrm=iso>. Acesso: 18 abr. 2018.

MANDARINO JUNIOR, R.; CANONGIA, C. (2010). *Livro verde: segurança cibernética no Brasil*. Brasília: GSIPR/SE/DSIC.

MINISTÉRIO da Defesa (2014). "Ministro acompanha trabalho de defesa cibernética na Copa do Mundo." Ministério da Defesa. Disponível em: <http://www.defesa.gov.br/index.php/noticias/13141-ministro-acompanha-trabalho-de-defesa-cibernetica-na-copa-do-mundo>.

_____ (2017). *Comando conjunto de defesa cibernética. Ministério da Defesa*. Disponível em: <https://www.defesa.gov.br/noticias/30417-comando-conjunto-na-defesa-cibernetica>. Acesso em: 02 jun. 2018.

MUGGAH, R.; THOMPSON, N. B. (2016). *Brazil must rebalance Its approach to cybersecurity*. Council on Foreign Relations. Disponível em: <https://www.cfr.org/blog/brazil-must-rebalance-its-approach-cybersecurity> Acesso: 19 abr. 2018.

NIC (1996). *Rumo à criação de uma coordenadoria de segurança de redes na internet no Brasil*. NIC.br. Disponível em: <http://www.nic.br/pagina/grupos-de-trabalho-documento-gt-s/169#4>. Acesso: 27 mai. 2018.

R7 (2013*). Anonymous invade site do governo para apoiar protesto do Movimento Passe Livre*. Disponível em: <https://noticias.r7.com/sao-paulo/anonymous-invade-site-do-governo-para-apoiar-protesto-do-movimento-passe-livre-19062013>. Acesso em 16 mai. 2018.

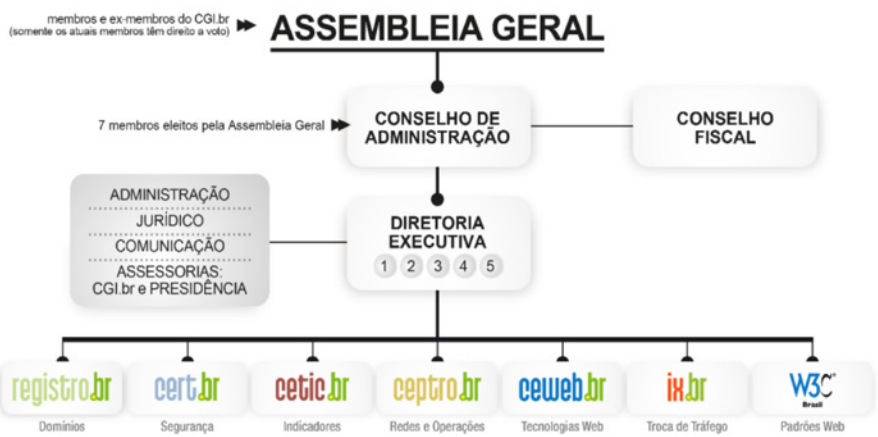
RNP (s.d.). *A história por trás dos 20 Anos da internet comercial no Brasil*. Rede Nacional de Pesquisa. Disponível em: <https://www.rnp.br/destaques/historia-por-tras-20-anos-internet-comercial-brasil>. Acesso: 27 mai. 2018.

ROHR, A. (2012). *Anonymous ataca sites ligados ao governo em protesto contra a Rio+20*. G1. Disponível em:<http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20. html>. Acesso em: 27 mai. 2018.

FERRAÇO, R. (2014). *CPI da Espionagem*. Senado Federal. Disponível em: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Acesso em 02 jun. 2018.

SOPRANA, P. (2016). *Robert Muggah: o governo brasileiro não é inocente quando o assunto é espionagem*. Época. Disponível em: <https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/06/robert-muggah-o-governo-brasileiro-espionou-seus-cidadaos.html> Acesso em: 17 abr. 2018.

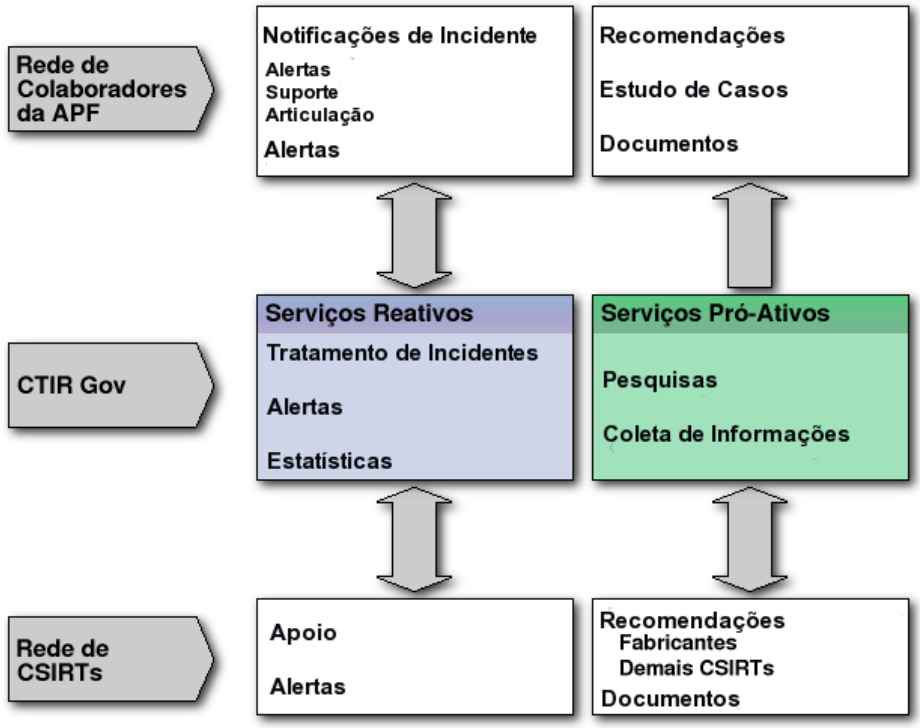
Anexo 1: Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br

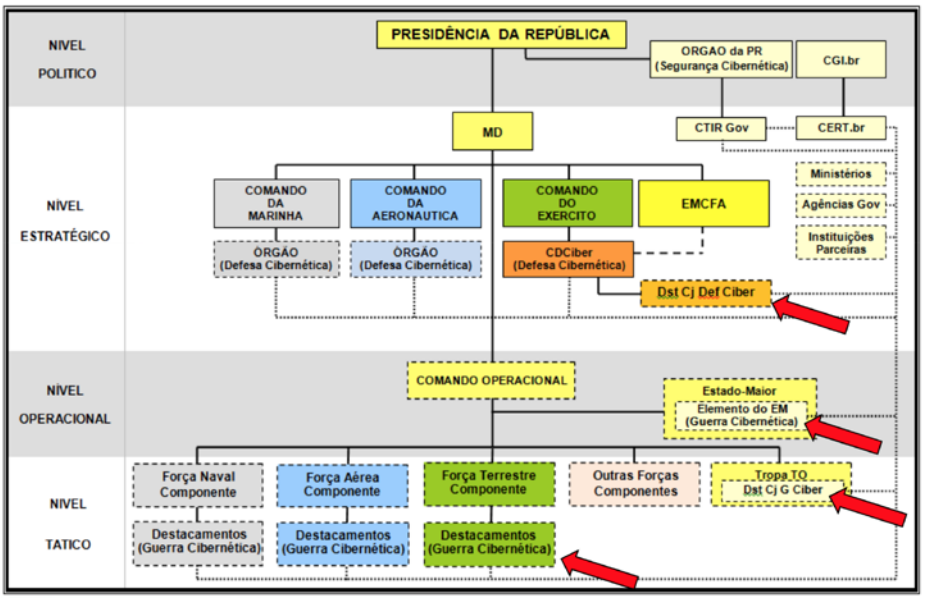
Fonte: NIC.br

Anexo 2: Estrutura de Colaboração CTIR.gov



Fonte: CTIR.gov

Anexo 3: Estrutura do Sistema Militar de Defesa Cibernética



Fonte: CDCiber, 2014

Sobre a Série

A série de artigos estratégicos integra o projeto ***Segurança Cibernética e Liberdades Digitais*** do Instituto Igarapé, com o suporte da Open Society Foundations (OSF). Esta reúne um conjunto de artigos e notas estratégicas que visam proporcionar uma reflexão crítica sobre os desafios principais que permeiam a relação entre segurança, privacidade e o emprego de novas tecnologias no Brasil. As notas estratégicas foram desenvolvidas pela equipe com base em uma série de diálogos organizados entre 2017 e 2018 com representantes do setor privado, governo, sociedade civil, comunidade técnica e academia. Visando abarcar diferentes leituras e perspectivas sobre o balanço entre abordagens criminalizantes e o fortalecimento de direitos (tal como o direito à privacidade), a série também conta com artigos de especialistas para analisar o pós-Marco Civil à luz dos desafios supracitados.

Outras publicações do Instituto Igarapé

ARTIGOS ESTRATÉGICOS

ARTIGO ESTRATÉGICO 34 - Colômbia e as FARC: cenários pós-conflito e repercussões regionais
Guilherme Damasceno Fonseca e Christian Vianna de Azevedo
(Maio 2018)

ARTIGO ESTRATÉGICO 33 - Citizen security in Latin America: facts and figures
Robert Muggah e Katherine Aguirre Tobón
(Março 2018)

ARTIGO ESTRATÉGICO 32 - A agenda sobre mulheres, paz e segurança no contexto latino-americano: desafios e oportunidades
Renata Avelar Giannini, Ana Paula Pellegrino, Carol Viviana Porto, Luisa Lobato, Maiara Folly e Mariana Gomes da Rocha
(Março 2018)

ARTIGO ESTRATÉGICO 31 - Implementando a agenda sobre "Mulheres, paz e segurança" no Brasil: uma revisão do Plano Nacional de Ação
Paula Drumond e Tamya Rebelo
(Março 2018)

ARTIGO ESTRATÉGICO 30 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Indice de Segurança da Criança em uma escola
Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck e Willian Vinícius Silva
(Maio 2017)

ARTIGO ESTRATÉGICO 29 - Migrantes invisíveis: a crise de deslocamento forçado no Brasil
Maiara Folly
(Março 2018)

ARTIGO ESTRATÉGICO 28 - Salas de Consumo de Drogas: situando o debate no Brasil
Rafael Tobias de Freitas Alloni e Luiz Guilherme Mendes de Paiva
(Outubro 2017)

ARTIGO ESTRATÉGICO 27 - Situações extraordinárias: a entrada das mulheres na linha de frente das forças armadas
Renata Avelar Giannini, Maiara Folly, Mariana Fonseca Lima (Agosto 2017)

ARTIGO ESTRATÉGICO 26 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Indice de Segurança da Criança em uma escola
Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck e Willian Vinícius Silva
(Maio 2017)

ARTIGO ESTRATÉGICO 25 - Brazil, the internet and the Digital Bill of Rights Reviewing the state of Brazilian internet governance
Daniel Arnaudo
(Abril 2017)

ARTIGO ESTRATÉGICO 24 - Confiança em desenvolvimento: o Brasil e os projetos de impacto rápido
Eduarda Hamann, Henrique Garbino e Maiara Folly
(Abril 2017)

ARTIGO ESTRATÉGICO 23 - Controlando el territorio y construyendo seguridad y justicia en el posconflicto colombiano. Edición especial de los Diálogos por la Seguridad Ciudadana
(Dezembro 2016)

ARTIGO ESTRATÉGICO 22 - Durões contra os fracos; fracos frente aos durões: as leis de drogas e a prática da ação policial
Juan Carlos Garzón Vergara
(Outubro 2016)

ARTIGO ESTRATÉGICO 21 - Infância e Segurança: um estudo sobre a percepção da violência por crianças e adolescentes do Complexo do Muquiço, Rio de Janeiro
Renata A. Giannini, Maiara Folly, Victor Ladeira, Andressa Werneck e Renata Siqueira
(Julho 2016)

ARTIGO ESTRATÉGICO 20 - Making cities safer: Citizen security innovations from Latin America
Robert Muggah, Ilona Szabo de Carvalho, Nathalie Alvarado, Lina Marmolejo e Ruddy Wang
(Junho 2016)

ARTIGO ESTRATÉGICO 19 - Construindo planos nacionais de ação eficazes: coletânea de boas práticas
Renata A. Giannini
(Março 2016)

ARTIGO ESTRATÉGICO 18 - “When kids call the shots” children’s perceptions on violence in Recife, Brazil, as per the ‘Child Security Index’
Helen Moestue, Katherine Aguirre e Renata A. Giannini
(Dezembro 2015)

ARTIGO ESTRATÉGICO 17 - Where is Latin America? Reflections on peace, security, justice and governance in the post-2015 sustainable development agenda
Renata A. Giannini
(Outubro 2015)

ARTIGO ESTRATÉGICO 16 - Políticas de drogas no Brasil: a mudança já começou
Ilona Szabó de Carvalho e Ana Paula Pellegrino
(Março 2015)

ARTIGO ESTRATÉGICO 15 - Nuevos retos y nuevas concepciones de la seguridad en México
Edición especial de los Diálogos por la Seguridad Ciudadana
(Março 2015)

ARTIGO ESTRATÉGICO 14 - A 'Third Umpire' for policing in South Africa – Applying body cameras in the Western Cape
David Bruce e Sean Tait
(Março 2015)

ARTIGO ESTRATÉGICO 13 - Brazil and Haiti: Reflections on 10 Years of peacekeeping and the future of post-2016 cooperation
Eduarda Passarelli Hamann (org.)
(Janeiro 2015)

ARTIGO ESTRATÉGICO 12 - Measurement matters: Designing new metrics for a drug policy that works
Robert Muggah, Katherine Aguirre e Ilona Szabó de Carvalho
(Janeiro 2015)

ARTIGO ESTRATÉGICO 11 - Desconstruindo a segurança cibernética no Brasil: ameaças e respostas
Gustavo Diniz, Robert Muggah e Misha Glenny
(Dezembro de 2014)

ARTIGO ESTRATÉGICO 10 - Expansão digital: como as novas tecnologias podem prevenir a violência contra crianças nos países do hemisfério sul
Helen Mostue e Robert Muggah
(Novembro 2014)

ARTIGO ESTRATÉGICO 9 - Promover gênero e consolidar a paz: a experiência brasileira
Renata A. Giannini
(Setembro 2014)

ARTIGO ESTRATÉGICO 8 - Tornando as cidades brasileiras mais seguras: edição especial dos diálogos de segurança cidadã
Michele dos Ramos, Robert Muggah, José Luiz Ratton, Clarissa Galvão, Michelle Fernandez, Claudio Beato, Andréa Maria Silveira, Melina Ingrid Risso e Robson Rodrigues
(Julho 2014)

ARTIGO ESTRATÉGICO 7 - Changes in the neighborhood: Reviewing citizen security cooperation in Latin America
Robert Muggah e Ilona Szabó de Carvalho
(Março 2014)

ARTIGO ESTRATÉGICO 6 - Prevenindo a violência na América Latina por meio de novas tecnologias
Robert Muggah e Gustavo Diniz
(Janeiro 2014)

ARTIGO ESTRATÉGICO 5 - Protegendo as fronteiras: o Brasil e sua estratégia "América do Sul como prioridade" contra o crime organizado transnacional
Robert Muggah e Gustavo Diniz
(Outubro 2013)

ARTIGO ESTRATÉGICO 4 - To save succeeding generations: UN Security Council Reform and the protection of civilians
Conor Foley
(Agosto 2013)

ARTIGO ESTRATÉGICO 3 - Momento oportuno: revisão da capacidade brasileira para desdobrar especialistas civis em missões internacionais
Eduarda Passarelli Hamann
(Janeiro 2013)

ARTIGO ESTRATÉGICO 2 - A fine balance: Mapping cyber (in)security in Latin America
Gustavo Diniz e Robert Muggah
(Junho 2012)

ARTIGO ESTRATÉGICO 1 - Mecanismos nacionais de recrutamento, preparo e emprego de especialistas civis em missões internacionais
Eduarda Passarelli Hamann
(Maio 2012)

NOTAS ESTRATÉGICAS

NOTA ESTRATÉGICA 29 - Will Cuba update its drug policy for the Twenty First Century?
Isabella Bellezza-Smull
(Dezembro 2017)

NOTA ESTRATÉGICA 28 - Desafios e boas práticas para implementação da agenda sobre mulheres, paz e segurança
Renata Avelar Giannini e Maiara Folly
(Novembro 2017)

NOTA ESTRATÉGICA 27 - À margem do perigo: preparo de civis brasileiros para atuação em países instáveis
Eduarda Passarelli Hamann
(Junho 2017)

NOTA ESTRATÉGICA 26 - Haitian women's experiences of recovery from Hurricane Matthew
Athena Kolbe, Marie Puccio, Sophonie M. Joseph, Robert Muggah and Alison Joersz
(Junho 2017)

NOTA ESTRATÉGICA 25 - O futuro das operações de manutenção da paz das Nações Unidas: uma perspectiva brasileira (implementação do relatório HIPPO)
Eduarda Hamann e Adriana Erthal Abdenur
(Março 2017)

NOTA ESTRATÉGICA 24 - Em busca da igualdade de gênero: boas práticas para a implementação da agenda sobre mulheres, paz e segurança
Maiara Folly e Renata Avelar Giannini
(Março 2017)

NOTA ESTRATÉGICA 23 - Filling the accountability gap: principles and practices for implementing body cameras for law enforcement
Robert Muggah, Emile Badran, Bruno Siqueira e Justin Kosslyn
(Novembro 2016)

NOTA ESTRATÉGICA 22 - Latin American dialogue on international peace and security reviewing the prospects for peace operations, peacebuilding and women, peace and security
(Maio 2016)

NOTA ESTRATÉGICA 21 - Assessing Haiti's electoral legitimacy crisis – Results of a 2016 survey
Athena R. Kolbe e Robert Muggah
(Fevereiro 2016)

NOTA ESTRATÉGICA 20 - Impact of perceived electoral fraud on Haitian voter's beliefs about democracy
Athena R. Kolbe, Nicole I. Cesnales, Marie N. Puccio e Robert Muggah
(Novembro 2015)

NOTA ESTRATÉGICA 19 - A força de uma trajetória: o Brasil e as operações de paz da ONU (1948-2015)
Eduarda Passarelli Hamann
(Outubro 2015)

NOTA ESTRATÉGICA 18 - Implementing UNSC resolution 1325 in Brazil: surmounting challenges and promoting equality
Renata A. Giannini, Mariana Lima e Pérola Pereira
(Outubro 2015)

NOTA ESTRATÉGICA 17 - A reforma do Conselho de Segurança da ONU: visão de mundo e narrativas do Brasil
Eduarda Passarelli Hamann
(Maio 2015)

NOTA ESTRATÉGICA 16 - Break your bones: mortality and morbidity associated with Haiti's Chikungunya epidemic
Athena R. Kolbe, Augusta Herman e Robert Muggah
(Julho 2014)

NOTA ESTRATÉGICA 15 - New technologies for improving old public security challenges in Nairobi
Mads Frilander, Jamie Lundine, David Kutalek e Luchetu Likaka
(Junho 2014)

NOTA ESTRATÉGICA 14 - O despertar da América Latina: uma revisão do novo debate sobre politica de drogas
Ilona Szabó de Carvalho
(Fevereiro 2014)

NOTA ESTRATÉGICA 13 - The changing face of technology use in pacified communities
Graham Denyer Willis, Robert Muggah, Justin Kossyln e Felipe Leusin
(Fevereiro 2014)

NOTA ESTRATÉGICA 12 - A inserção de civis brasileiros no Sistema ONU: oportunidades e desafios
Renata Avelar Giannini
(Janeiro 2014)

NOTA ESTRATÉGICA 11 - A diáspora criminal: o alastramento transnacional do crime organizado e as medidas para conter sua expansão
Juan Carlos Garzón Vergara
(Novembro 2013)

NOTA ESTRATÉGICA 10 - Smarter policing: tracking the influence of new information technology in Rio de Janeiro
Graham Denyer Willis, Robert Muggah, Justin Kosslyn e Felipe Leusin
(Novembro 2013)

NOTA ESTRATÉGICA 9 - Is tourism Haiti's magic bullet? An empirical treatment of Haiti's tourism potential
Athena R. Kolbe, Keely Brookes and Robert Muggah (Junho 2013)

NOTA ESTRATÉGICA 8 - Violencia, drogas y armas ¿Otro futuro posible?
Ilona Szabó de Carvalho, Juan Carlos Garzón e Robert Muggah
(Julho 2013)

NOTA ESTRATÉGICA 7 - A promoção da paz no contexto pós-2015: o papel das potências emergentes
Robert Muggah, Ivan Campbell, Eduarda Hamann, Gustavo Diniz e Marina Motta
(Fevereiro 2013)

NOTA ESTRATÉGICA 6 - After the storm: Haiti's coming food crisis
Athena Kolbe, Marie Puccio e Robert Muggah
(Dezembro 2012)

NOTA ESTRATÉGICA 5 - Brazil's experience in unstable settings
Eduarda Passarelli Hamann e Iara Costa Leite
(Novembro 2012)

NOTA ESTRATÉGICA 4 - Cooperação técnica brasileira
Iara Costa Leite e Eduarda Passarelli Hamann
(Setembro 2012)

NOTA ESTRATÉGICA 3 - A experiência do Brasil em contextos instáveis
Eduarda Passarelli Hamann e Iara Costa Leite
(Agosto 2012)

NOTA ESTRATÉGICA 2 - The economic costs of violent crime in urban Haiti (Aug 2011 - Jul 2012)
Athena R. Kolbe, Robert Muggah e Marie N. Puccio (Agosto 2012)

NOTA ESTRATÉGICA 1 - Haiti's urban crime wave? Results from monthly households surveys (Aug 2011 - Feb 2012)
Athena R. Kolbe e Robert Muggah
(Março 2012)

INSTITUTO IGARAPÉ
a think and do tank

O Instituto Igarapé é um think and do tank independente, dedicado às agendas da segurança, da justiça e do desenvolvimento. Seu objetivo é propor soluções inovadoras a desafios sociais complexos, por meio de pesquisas, novas tecnologias, influência em políticas públicas e articulação. O Instituto atualmente trabalha com cinco macrotemas: (i) política sobre drogas nacional e global; (ii) segurança cidadã; (iii) cidades seguras; (iv) consolidação da paz; e (v) segurança cibernética. O Instituto Igarapé tem sede no Rio de Janeiro, com representação em Bogotá, Cidade do México, Lisboa e outras partes do mundo.

Instituto Igarapé
Rua Miranda Valverde, 64
Botafogo, Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

www.igarape.org.br

Direção de arte:
Raphael Durão - STORM.pt

ISSN 2359-0998

INSTITUTO IGARAPÉ

a think and do tank

www.igarape.org.br