ESCOLA DE GUERRA NAVAL

CC JORGE HENRIQUE CORREIA DE SÁ

INCIDENTES NAS REDES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Rio de Janeiro

2018

CC JORGE HENRIQUE CORREIA DE SÁ

INCIDENTES NAS REDES DA ADMINISTRAÇÃO PÚBLICA FEDERAL

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientadores: CMG (FN-RM1) William Alves Rosa

CF Eugenio Campos Huguenin

Rio de Janeiro

Escola de Guerra Naval

2018

DEDICATÓRIA

Dedico esse trabalho à minha esposa, Maria, que com seu amor e simplicidade, contribuiu com a melhor ideia, me ajudando a concluí-lo. Aos meus filhos, Marcos Vinicios, Lucas, Maria Eduarda, André e Tiago, que me motivam a dedicar o máximo em tudo o que faço. E à Marinha do Brasil, para a qual presto diuturnamente meus serviços, em nome da Pátria.

AGRADECIMENTOS

Agradeço a Deus, que sempre me indicou o caminho, me inspirou a trilhá-lo e me protegeu em todos os momentos. E ao corpo discente da Escola de Guerra Naval, que a todo tempo esteve à disposição e transmitiu conhecimentos valiosíssimos para a confecção dessa pesquisa, em especial aos Comandantes William, Eugenio Huguenin e Nagashima.

RESUMO

Verificou-se qual o comportamento da quantidade anual de notificações de incidentes cibernéticos na Administração Pública Federal entre 2011 e 2017 na medida em que ocorria a evolução da sua estrutura de segurança cibernética. Por meio de um estudo sintético, foi possível reunir diversos dados estatísticos com marcos temporais relevantes em um gráfico e extrair a resposta desejada, além de outras conclusões. O resultado da pesquisa indicou um crescimento da quantidade absoluta de notificações, mas uma taxa de crescimento menor que a nacional, indicando um efeito positivo da evolução da estrutura de segurança cibernética na redução da quantidade de notificações em relação ao seu contexto nacional. Essa constatação permite vislumbrar uma possível aplicação na guerra cibernética: a da utilização dessa comparação para avaliar a segurança cibernética de outras organizações.

Palavras-chave: Segurança Cibernética. Defesa Cibernética. Guerra Cibernética. Notificações de Incidentes Cibernéticos.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

O espaço cibernético (ECiber), ou ciberespaço, foi definido como o conjunto de todos os dispositivos computacionais e material armazenado em meio digital, formando uma rede (LÉVY, 1994). E, no limiar da segunda década do século XXI, não há mais como conceber qualquer atividade humana que escape da interação, mesmo que indireta, com ciberespaço, que possui suas peculiaridades. É um ambiente sem fronteiras definidas (BRASIL, 2010, p. 13), no qual não se aplicam os conceitos de distâncias globais utilizados no mundo real e com uma gama própria de recursos e ameaças.

A importância do uso do ciberespaço pelas pessoas e, consequentemente, pelos Estados, levou à elaboração do conceito de segurança cibernética como a arte para garantir a existência de uma sociedade da informação continuamente, bem como a proteção dos seus ativos de informação[1] e das suas infraestruturas críticas no ECiber (BRASIL, 2014, p. 19). A motivação para este trabalho advém do crescente papel desse espaço na modernidade e visa agregar algum conhecimento que possa ser aplicado em um dos componentes da segurança cibernética: a guerra cibernética, tema central deste estudo.

A guerra cibernética é definida pela Doutrina Militar de Defesa Cibernética como uma atividade militar, do nível de operacional ou tático, que envolve a utilização ofensiva e defensiva da informação e dos sistemas de informação contra o Comando e Controle do inimigo, negando, explorando, corrompendo, degradando ou destruindo a sua capacidade (BRASIL, 2014, p. 37). Ela ocorre no ECiber, ambiente complexo e com nuances que interferem de modo direto nas perspectivas possíveis dos estudos científicos sobre o tema.

Embora exista somente nos ativos de informação, o ECiber pode ser

[1] Os ativos de informação são os dispositivos, sistemas de informação e meios para armazenar, transmitir e processar dados e informações, os sistemas utilizados para tal. Também estão incluídos os locais em que se encontram e o pessoal que acessa esses locais e meios (BRASIL, 2014, p. 18).

compreendido como uma dimensão própria, em que não se aplicam as regras sobre tempo e espaço como no mundo real. Dada à velocidade de processamento computacional, as ações deflagradas podem ter consequências quase imediatas. A estrutura da rede, que sustenta a existência da dimensão cibernética, não contempla as fronteiras de territórios definidas pelos Estados, mas apenas os endereços dos ativos e as rotas para acessar as informações armazenadas, o que pode dificultar a aplicação de jurisdição para os sistemas legais e a precisão da localização da origem de uma determinada ação no ciberespaço.

Os eventos ocorridos no ECiber podem gerar consequências no mundo físico. Por exemplo, desde simples equipamentos até grandes sistemas que dependem de computadores podem ter seu funcionamento alterado por interferências oriundas do ciberespaço. As redes sociais permitiram que pessoas transcendessem parte de sua existência para o ECiber, sob a forma de perfis ou avatares[2], e o que ocorre com essas personalidades acaba por afetar a vida real dos seus proprietários.

A capacidade de segregação de redes, física ou logicamente, e os recursos de proteção criptográfica permitem que o ECiber esteja fragmentado em várias redes, com tamanhos e regras distintas. Os usuários do mundo real também podem ter várias personalidades nesse espaço, sem o compromisso de refletir a sua própria, e dividem a existência com as aplicações de inteligência artificial, o que torna a correlação dos "habitantes" desse novo mundo com os da nossa realidade muito imprecisa.

Por essas peculiaridades, reforça-se a questão da segurança no ciberespaço, como aponta Mandarino, que também foi diretor do Departamento de Segurança da Informação e Comunicações (DSIC), em 2010, e coordenador da edição do "Livro Verde: a Segurança Cibernética no Brasil" (BRASIL, 2010):

[2] Entende-se por avatar as formas gráficas de representar os usuários das redes sociais em jogos virtuais ou outras comunidades no ECiber.

> “A nova fronteira constituída, o Espaço Cibernético, à semelhança de qualquer novo espaço ainda não perfeitamente demarcado, como o antigo "velho oeste", atraiu também pessoas mal intencionadas, que buscam vantagens e ganhos ilícitos, explorando a falta de regras e sendo acobertadas pela distância e pelo aparente anonimato. Assim, a questão da proteção das informações ganhou destaque” (MANDARINO, 2009 apud FERNANDES, 2009).

Um caso que ilustra como podem se desenrolar os eventos no ECiber é o do ataque às redes da Estônia, em fevereiro de 2007. Após uma crise entre esse Estado e a Rússia, envolvendo a remoção de um monumento em homenagem aos mortos do Exército Vermelho na Segunda Guerra Mundial (1939-1945), na cidade de Tallin, a Estônia começou a sofrer ataques cibernéticos que afetaram o sistema bancário, telefônico e as operações comerciais, em uma escala que ainda não havia sido vista. Mesmo após a descoberta de indícios que apontavam a Rússia como local de origem dos ataques, o governo russo negou qualquer participação no evento (KLARLE; KNAKE, 2010, p. 13-14).

Essencialmente, verifica-se que o anonimato nos principais casos de ataques cibernéticos direcionados contra os Estados e a carência de fontes primárias que confirmem a origem dos atacantes tornam o estudo científico da segurança cibernética e, consequentemente da guerra cibernética, mais consistente se conduzido pela perspectiva da defensiva. E essa será a perspectiva escolhida para a pesquisa.

O presente trabalho versa sobre aspectos da segurança cibernética e buscará obter conclusões com aplicação na guerra cibernética. Pela grande complexidade do assunto, foi escolhido, como objeto de pesquisa, o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov), órgão subordinado ao DSIC do Gabinete de Segurança Institucional da Presidência da República (GSI/PR). O objeto será delimitado no tempo pelo período entre 2011 a 2017, que compreende desde a sua criação até a última divulgação de suas estatísticas. O CTIR Gov é um dos elementos da estrutura de segurança cibernética da administração pública federal do Brasil (APF) e foi selecionado por ser o repositório das notificações de incidentes na rede da APF.

O propósito dessa dissertação será identificar as possíveis conexões entre a evolução da estrutura de segurança cibernética da APF e a quantidade de notificações de incidentes na rede relatados ao CTIR Gov. Será admitida como questão qual o comportamento da quantidade de notificações de incidentes na rede da APF relatados ao CTIR Gov no decorrer da evolução da estrutura de segurança cibernética da APF.

As evidências aqui coletadas e considerações decorrentes tratarão de matéria essencialmente técnica, acarretando na necessidade da explicação de vários conceitos relativos à terminologia. Foram selecionados, portanto, como apoio para a compreensão, dois documentos elaborados no âmbito da APF, a saber, o "Livro Verde: a Segurança Cibernética no Brasil" (BRASIL, 2010), doravante chamado apenas por livro verde, e a Doutrina Militar de Defesa Cibernética (BRASIL, 2014), cujos pontos de maior interesse para o estudo serão detalhados no decorrer do próximo capítulo e permitirão o correto entendimento de cada termo a ser empregado.

Para desenvolver um raciocínio compatível com os objetivos traçados, foi selecionado como desenho de pesquisa o estudo sintético (CERVO, BERVIAN e SILVA, 2011, p. 33-35), a fim de buscar a inserção dos elementos verificados em um sistema comum, no qual será possível a identificação da relação que fazem entre si e obter conclusões que tenham aplicação útil na guerra cibernética. Complementarmente será utilizado um gráfico com os dados coletados para facilitar a identificação das evidências que permitirão construir a síntese e retirar as devidas conclusões.

O trabalho está dividido em quatro capítulos, sendo o primeiro para a apresentação do tema e sua relevância, motivação para a pesquisa, definição do objeto a estudar, do propósito e da questão levantada, bem como para uma breve explanação da perspectiva escolhida, da metodologia científica adotada e da ideia de trabalho; o segundo, para elucidar os conceitos a serem utilizados, retirados do livro verde e da Doutrina Militar de

Defesa Cibernética, para descrever a estrutura de segurança cibernética na APF e o CTIR Gov, apresentar o padrão para notificação de incidentes de segurança ao CTIR Gov, os parâmetros para avaliar e caracterizar a evolução da estrutura de segurança cibernética da APF e apresentar um pressuposto que embasará um raciocínio no capítulo seguinte; o terceiro para o estabelecimento de relações entre a evolução da estrutura de segurança cibernética e as notificações registradas pelo CTIR Gov, por meio da identificação dos marcos de evolução da estrutura e sua correlação com os dados estatísticos das notificações e outros, com o intuito de extrair conclusões utilizando o apoio da síntese gráfica dos dados e também para verificar a possibilidade de aplicação do conhecimento obtido na guerra cibernética; e o quarto para responder à questão formulada, tomando por fundamento as deliberações anteriores e apontar o que se concluiu de aplicação do resultado do trabalho na guerra cibernética.

A fim de permitir a síntese dos elementos pesquisados, serão expostos a seguir os conceitos e arranjos teóricos relativos ao objeto do estudo.

2 CONCEITOS

2.1 Livro verde

Livros verdes são documentos publicados para estimular a discussão de determinados tópicos em alto nível[3]. Eles convidam atores relevantes, individuais ou coletivos, a participar de um processo consultivo e debater propostas que servirão de base para desenvolvimento de legislação que será delineada em livros brancos. Os livros brancos, por sua vez, lançam o debate ao público, *stakeholders*[4] e governo para chegar a um consenso político[5].

A partir do lançamento da Estratégia Nacional de Defesa, em 2008, houve um aumento na preocupação do Estado brasileiro com a segurança cibernética e o DSIC do GSI/PR elaborou o livro verde, em 2010, abrindo a discussão para o lançamento de um livro branco e, posteriormente, a aprovação de uma política nacional que orientasse a estratégia nacional de segurança cibernética.

A importância do livro verde para o estudo reside em vários aspectos, dentre eles: a publicação do livro em si é um dos marcos no desenvolvimento da estrutura de segurança cibernética no Brasil e na APF, por diversos motivos, como expor os conceitos de espaço cibernético e segurança cibernética, já apresentados no capítulo anterior; registrar a participação do Brasil em iniciativas e fóruns internacionais, que serve de evidência do amadurecimento da mentalidade de segurança; considerar os CERT[6] e CTIR como elementos

[3] Disponível em: <https://eu-lex.europa.eu/summary/glossary/green_paper.htm>. Acesso em: 30 jul. 2018.
[4] O PMBOK (PMI, 2013) define *stakeholder* como um indivíduo, grupo ou organização que pode afetar, ser afetado por ou perceber a si mesmo como afetado por uma decisão, atividade ou resultado de um projeto.
[5] Disponível em: <https://eu-lex.europa.eu/summary/glossary/white_paper.htm>. Acesso em: 30 jul. 2018.
[6] *Computer Emergency Response Team* ou Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança é uma organização para tratar incidentes de segurança em ativos computacionais ligados à Internet, de acordo com o conteúdo do próprio sítio do CERT brasileiro na Internet. Disponível em: <https://www.cert.br/sobre/>. Acesso em: 22 jul. 2018.

prioritários para a promoção da segurança; e relevar a importância de documentos de alto nível como a estratégia nacional de segurança cibernética. Em suma, levanta a necessidade de formalizar a estrutura de segurança cibernética:

> "Urge formalizar, portanto, a estrutura da Segurança Cibernética no País, bem como apoiar e fortalecer suas atividades, de forma a viabilizar e agilizar tanto a formulação de políticas, normas e regulação, a pesquisa e o desenvolvimento de metodologias e tecnologias, quanto à cooperação internacional e a implantação e promoção de uma macro-coordenação (sic) que propicie a integração de processos, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações de interesse do Estado brasileiro e da sociedade, bem como a resiliência de suas infraestruturas críticas" (BRASIL, 2010, p.25).

Esses pontos serão utilizados nas variáveis para justificar a adoção desse documento como um marco da evolução estrutura de segurança cibernética da APF.

Apesar da lacuna nos documentos de alto nível, até o momento da realização deste estudo, causada por ainda não ter sido concluído o livro branco, outras normas foram publicadas, como a Doutrina Militar de Defesa Cibernética, que será útil para a apropriação de conceitos.

2.2 Doutrina Militar de Defesa Cibernética

A defesa envolve as ações em prol da segurança, seja obtendo, resguardando ou recompondo uma condição segura, ou ainda, reagindo a contra-ataques (BRASIL, 2010, p. 18). Já a guerra cibernética envolve as ações ofensivas e defensivas utilizando informações e sistemas de informações para a negação, exploração, corrupção ou destruição de valores de oponentes sob a forma de informações, sistemas de informação e redes de computadores (BRASIL, 2010, p. 19). De acordo com a Doutrina Militar de Defesa Cibernética, a guerra cibernética está inserida na defesa, que por sua vez é conduzida no âmbito da segurança (BRASIL, 2010, p. 17), como apresentado na FIG. 1.

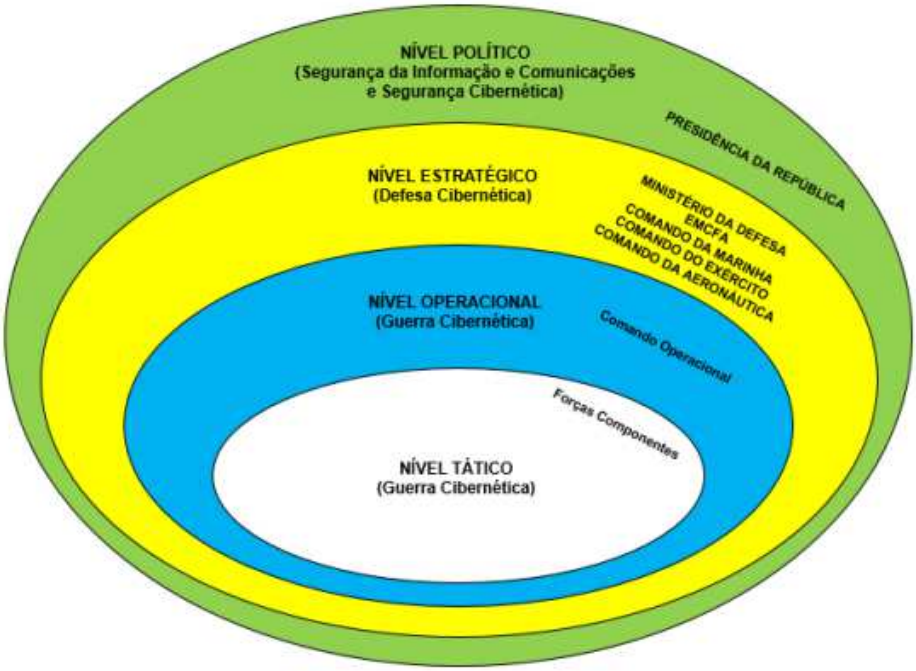

FIGURA 1 – Níveis de decisão e esquema da segurança cibernética
Fonte: BRASIL, 2010, p. 17

Essa arquitetura demonstra como a escolha de um objeto relacionado ao nível político pode ser fonte de conclusões com aplicações na guerra cibernética. E a seleção do CTIR Gov se prestará a esse objetivo.

2.3 CTIR Gov

O CTIR Gov é o órgão governamental responsável pelo atendimento dos incidentes ocorridos nas redes de computadores da APF, também conhecida como "domínio.gov". Sua criação remonta a um processo gradual que começou com a instituição da Política de Segurança da Informação[7] (PNSI), em 2000. Na ocasião, já havia alguns grupos de resposta a incidentes cibernéticos na APF, mas trabalhavam isoladamente, ou seja, não aproveitavam as oportunidades de correlacionar as ameaças detectadas, o que dificultava a

[7] Decreto n. 3505, de 13 de junho de 2000. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-normaatualizada-pe.html>. Acesso em 27 jul. 2018.

solução dos problemas e a adoção de medidas protetivas[8].

Em vista da crescente demanda no âmbito do ciberespaço, foi instituído em 2003 um grupo para estudar a criação de um *Computer Security Incident Response Team*[9] (CSIRT)[10], entre outras providências, que redundou em outro grupo específico para implantar as medidas administrativas necessárias à sua criação[11] e, ao final dos trabalhos, em 2004, concluiu-se que esse centro contribuiria para o fortalecimento da segurança da informação e serviria como repositório de dados e subsídios para a criação de políticas e normas, seguindo o exemplo de outros países que já adotavam a facilidade. As atividades de coordenação geral de tratamento de incidentes na rede da APF começaram, portanto, informalmente em 2004, tendo sido formalizadas em 2006, com a criação do DSIC. Finalmente, a partir de uma revisão do regimento interno do GSI/PR[12], em 2009, foi organizado o CTIR Gov com as características que definem o objeto desta pesquisa.

O CTIR Gov, no período estudado, sofreu alterações de atribuições, emitiu algumas normas e documentos que configuram a evolução da sua estrutura de segurança cibernética ao longo do tempo. Para que se possa ter uma melhor ideia do papel desse órgão, o ANEXO A contém uma ilustração das interações que faz com a sua rede de colaboradores e outros CSIRT. O detalhamento dos documentos que marcam essa evolução será apresentado no próximo capítulo, para a síntese com as quantidades de notificações de incidentes.

As notificações de incidentes seguem um padrão, cujo conhecimento é necessário

---

[8] Disponível em: <http://www.ctir.gov.br /sobre-CTIR-gov.html#historico>. Acesso em: 27 jul. 2018.

[9] CSIRT ou Grupo de Resposta a Incidentes de Segurança é um órgão com a finalidade responder e analisar notificações de incidentes cibernéticos. Sua atuação abrange uma comunidade específica, como uma empresa, um órgão governamental ou acadêmico. Pode ainda atender um Estado, grupo de pesquisa ou clientes pagantes. Os CERT são um tipo de CSIRT que utilizam essa denominação por meio de credenciamento junto à Universidade *Carnegie Mellon*, detentora do direito de uso da marca. Disponível em: <https://www.cert.br/certcc/csirts/csirt_faq-br.html>. Acesso em: 23 jul. 2018.

[10] Portaria n. 12 do GSI/PR, de 27 de junho de 2003. Disponível em: <http://dsic.planalto.gov.br/legislacao/port _1227 _jun_2003.pdf>. Acesso em: 27 jul. 2018.

[11] Portaria n. 17 do GSI/PR, de 18 de maio de 2004. Disponível em: <https://www.jusbrasil.com.br/diarios/ 585244/pg-12-secao-1-diario-oficial-da-uniao-dou-de-19-05-2004>. Acesso em 27 jul. 2018.

[12] Portaria n. 56 do GSI/PR, de 05 de novembro de 2009. Disponível em: < http://pesquisa.in.gov.br/imprensa/jsp /visualiza/index.jsp?data=09/11/2009&jornal=1&pagina=13&totalArquivos=204>. Acesso em: 27 jul. 2018.

para que se possam tirar conclusões úteis para esse estudo.

2.4 Padrões para notificação de incidentes de segurança ao CTIR Gov

Para a exposição do padrão para as notificações ao CTIR Gov, primeiramente será delimitado do que tratam os incidentes de segurança. De acordo com a norma complementar n° 05/IN01/DSIC/GSIPR[13], esses incidentes são as ocorrências, mesmo as não confirmadas, que envolvem a segurança dos ativos de informação. A mesma norma complementar prevê a formação de equipes de tratamento e resposta a incidentes em redes computacionais (ETIR) nos órgãos da APF e a designação formal de agentes responsáveis, que também atuam como elementos de ligação entre as equipes e o CTIR, além dos demais deveres estabelecidos pelos seus respectivos órgãos.

A rede de tratamento dos incidentes de segurança está organizada, portanto, em camadas, de forma mais ou menos centralizada em cada órgão da APF, dependendo das suas peculiaridades. Esse é o sistema que permite detectar e registrar, após um processo de triagem, ataques cibernéticos[14] que obtiveram sucesso, ou seja, venceram a defesa cibernética da APF. Sobre esse aspecto, cabe ainda ressaltar dois pontos: que a triagem é necessária para confirmar a classificação do incidente e evitar registros em duplicidade; e nem todos os ataques são detectados e notificados pelas ETIR, pois alguns artefatos[15] possuem sofisticação que ultrapassa a capacidade dos sistemas de defesa e não são percebidos.

O padrão de notificações de incidentes[16] estabelece que a comunicação deve partir

---

[13] Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Acesso em: 27 jul. 2018.

[14] A Doutrina Militar de Defesa Cibernética define ataque cibernético como aquele que compreende as ações para interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente (BRASIL, 2014, p. 23).

[15] Artefato cibernético é o equipamento ou sistema empregado no espaço cibernético para execução de ações de proteção, exploração e ataque cibernéticos (BRASIL, 2014, p. 18).

[16] Disponível em: <http://www.ctir.gov.br/arquivos/publicacoes/Padronizacao_Notificacao_CTIRGov.pdf>. Acesso em: 27 jul. 2018.

de uma ETIR, responsável por concentrar os registros de incidentes de seu órgão de competência, por nota transmitida via correio eletrônico institucional destinado ao CTIR Gov. O endereço eletrônico deve ser, preferencialmente, no formato abuse@orgao.gov.br e a nota deve conter o nome do órgão da APF e o tipo de incidente no assunto e descrever a ocorrência, incluindo os dados técnicos no corpo. Poderão ser incluídos destinatários afetados pelo incidente e anexos com conteúdo que facilite a análise. O CTIR Gov, ao receber o comunicado, realiza um processo de validação e triagem para finalmente proceder ao tratamento, se ainda não tiver sido procedido pela ETIR. Finalmente, depois de sanado o problema, o evento é incluído nas estatísticas.

Estabelecido o padrão de notificações, cujos montantes a serem incluídos na síntese serão extraídos das estatísticas divulgadas pelo CTIR Gov[17], resta apresentar as variáveis para parametrizar a evolução da estrutura de segurança cibernética.

2.5 Variáveis para avaliação da evolução da estrutura de segurança cibernética

Considerando a complexidade e diversidade das estruturas de segurança cibernética, é necessário estabelecer parâmetros que permitirão verificar a evolução da respectiva estrutura da APF. Nesse estudo, apropriar-se-á da definição de evolução como progresso, ou seja, a mudança de estado que leva a um patamar mais adiantado (FERREIRA, 2010). Souza e Almeida (2016) apresentaram o arcabouço político-administrativo do ciberespaço no Brasil, ilustrado na FIG. 2.

Nesse contexto, serão eleitos os aspectos considerados mais relevantes, mostrados a seguir, como caracterizadores da evolução da estrutura de segurança cibernética, a serem observados em uma sequência indicadora da progressão do nível mais básico até o mais

[17] Disponível em: <http://www.ctir.gov.br/estatisticas.html>. Acesso em: 27 jul. 2018.

avançado. Tais marcos serão apresentados no formato de linha do tempo, distinta da apresentada na FIG. 2, no APÊNDICE A, para auxiliar o entendimento do modelo escolhido para caracterizar a evolução da estrutura de segurança cibernética da APF. Esse modelo foi simplificado por conter os marcos considerados suficientes para a composição da síntese e permitir a elaboração de conclusões.

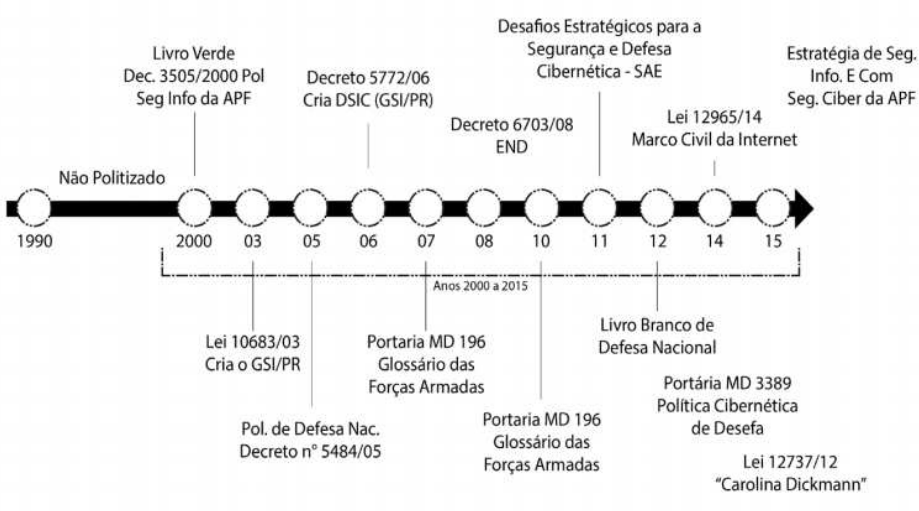

FIGURA 2 – Arcabouço Politico-Administrativo do Espaço Cibernético Brasileiro
Fonte: SOUZA, Eduardo André Araújo; ALMEIDA, Nival Nunes, 2016.

O primeiro parâmetro escolhido é o da existência de um documento oficial do governo que debata o tema da segurança cibernética e aponte a necessidade de se estabelecer diretrizes legais para tratar o assunto. Nesse quesito enquadram-se os livros verdes, brancos ou publicações similares e, no sistema estudado, o livro verde (BRASIL, 2010). Embora sua criação seja anterior ao período da pesquisa, o livro será considerado, pois sua vigência abrange todo o período pesquisado. Isso será válido para os demais documentos enquadrados nos próximos parâmetros.

O segundo parâmetro, geralmente decorrente do primeiro, é o estabelecimento de uma política nacional de segurança cibernética, com as efetivas diretrizes para o delineamento

das ações em todos os setores da sociedade no intuito de construir uma segurança compatível com as necessidades globais. A frequência de atualização dessa política servirá como subcritério para medição, tendo em vista que, de acordo com o descrito no livro verde, o aumento das ameaças e os avanços na área da tecnologia da informação são fenômenos que permeiam esse ambiente (BRASIL, 2010, p. 14). Nesse parâmetro será enquadrada a PNSI, decreto já citado e promulgado no ano 2000.

O terceiro parâmetro é o estabelecimento de uma estratégia nacional de segurança cibernética, documento em que são apresentadas as ameaças consideradas e descritas as ações decorrentes para contrapô-las, respeitando as diretrizes superiores. Do mesmo modo, a frequência de revisão dessa estratégia também é um subcritério importante, pelo mesmo motivo exposto no parágrafo anterior. Será aqui enquadrada a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal – 2015/2018, versão 1.0[18].

Além dos documentos condicionantes, o quarto parâmetro é o da existência de legislação própria para regular o uso das redes e os crimes cibernéticos, diferenciando estes dos demais e fornecendo as ferramentas adequadas para a aplicação das sanções correspondentes à gravidade dos danos que os ataques cibernéticos podem causar. Enquadram-se nesse caso a lei de crimes de informática[19] e o marco civil da Internet[20].

Como quinto parâmetro, ainda sobre a documentação de referência, segue a expedição de normas técnicas para instituir as medidas de segurança, classificação das ameaças, alarmes e tipos de ataques, reportes de incidentes, registros históricos, produção de

---

[18] Portaria n. 14 do Conselho de Defesa Nacional, de 11 de maio de 2015. Disponível em: <http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=12/05/2015>. Acesso em: 27 jul. 2018.

[19] Lei n. 12.737, de 30 de novembro de 2012, dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n° 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 27 jul. 2018.

[20] Lei n. 12.965, de 23 de abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 jul. 2018.

estatísticas e outros que contribuam para executar as ações previstas na estratégia. Será considerado como atendido se houver uma coletânea dessas normas expedidas por um órgão do governo de alcance nacional. Para esse parâmetro, serão enquadradas a Instrução Normativa GSI Nº 1[21], de 13 de junho de 2008, e as normas complementares à Instrução Normativa GSI n° 1/2008: nº 05[22], 08[23] e nº 21[24].

O sexto e último parâmetro, não menos importante, será escolhido por sua relevância na contribuição para a segurança cibernética: a existência de um CSIRT formalmente instituído e organizado, com a competência e responsabilidade de prover a resposta a eventuais ataques cibernéticos de nível nacional. O CTIR Gov é o CSIRT que atende a esses requisitos.

Vale ressaltar que os seis parâmetros, ou quesitos, listados servirão ao propósito de identificar o estágio de evolução da estrutura, como marcos em uma linha do tempo. Não há intenção de aprofundar-se no aspecto qualitativo, por se considerar desnecessário para o tipo de síntese proposta.

Descrito o objeto do CTIR Gov e como será caracterizada a evolução da estrutura de segurança da APF, ainda será necessário adotar um pressuposto que será útil na obtenção de conclusões sobre a síntese desse estudo, um paradigma de segurança.

---

[21] Disciplina a Gestão de SIC na APF, direta e indireta, e dá outras providências (publicada no DOU nº 115, de 18 de junho de 2008 - Seção 1). Disponível em: <http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf>. Acesso em: 27 jul. 2018.

[22] Disciplina a criação de ETIR nos órgãos e entidades da APF (publicada no DOU nº 156, de 17 de agosto de 2009 - Seção 1). Disponível em: <http://dsic.planalto.gov.br/legislacao/ nc_05_etir.pdf>. Acesso em: 27 jul. 2018.

[23] Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da APF (publicada no DOU nº 162, de 24 de agosto de 2010 - Seção 1). Disponível em: <http://dsic.planalto.gov.br/legislacao/ nc_8_gestao_etir.pdf>. Acesso em: 27 jul. 2018.

[24] Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da APF, direta e indireta (publicada no DOU nº196, de 10 de outubro de 2014 - Seção 1). Disponível em: <http://dsic.planalto.gov.br/legislacao/ nc_21_preservacao_de_evidencias.pdf>. Acesso em: 27 jul. 2018.

2.5 Paradigma de segurança

A síntese trabalhada nessa pesquisa envolve, em um dos seus pontos, as notificações de incidentes cibernéticos na rede de computadores da APF. Nessa rede, cada órgão possui sua estrutura de segurança, seguindo os padrões estabelecidos pelo DSIC e com medidas de defesa complementares, de acordo com suas necessidades. Pode-se admitir, portanto, que somente serão passíveis de registro como incidentes os resultados de ataques cibernéticos que obtiverem algum grau de sucesso, sendo ignorados aqueles que não conseguirem ultrapassar as defesas, o que se espera ser a maioria, para um sistema de proteção eficiente.

Um aspecto importante para prosseguir com esse raciocínio é o da dualidade da evolução dos ataques e das defesas. Ao surgirem novas ameaças, são criadas defesas para neutralizá-las. Na medida em que as ameaças são contidas, seus desenvolvedores criam outras novas, que novamente são estudadas e combatidas, em um ciclo reativo. Algumas defesas só podem ser criadas após a percepção dos sintomas de uma nova ameaça, como por exemplo, vírus com códigos específicos. Para essas ameaças, são utilizados programas antivírus com rotinas de varreduras em buscas dos códigos já conhecidos e presentes em seus bancos de dados, ou seja, novos vírus não são detectados até que seus efeitos sejam notados, o que motiva suas análises e inserção das suas características nos parâmetros de busca dos sistemas de defesa.

Adota-se, portanto, como paradigma de segurança a afirmação, corroborada pelo testamento de Giuseppe Janino[25], de que nenhum sistema de proteção cibernética será completamente seguro, seja pelas razões técnicas descritas nesse item ou por falhas das

[25] Secretário de Tecnologia da Informação do Tribunal Superior Eleitoral. Declarou em entrevista ao Portal EBC de notícias, que admite não haver sistema inviolável, ao tratar do tema das urnas eletrônicas utilizadas nas eleições brasileiras. Disponível em: <http://www.ebc.com.br/tecnologia/2016/03/nao-existe-sistema-inviolavel-diz-criador-da-urna-eletronica>. Acesso em 13 jul. 2018.

pessoas que integram os sistemas. Desse paradigma concluiremos que alguns ataques vencerão os sistemas de defesa cibernética da APF, mas seus efeitos serão percebidos, e redundarão em registros de notificações de incidentes; contudo, do mesmo modo, alguns ataques também terão sucesso e não serão detectados. E daí, pode-se dizer que as estatísticas de notificações de incidentes das APF apresentarão uma quantidade que tenderá a ser menor que o da totalidade das ocorrências envolvendo a segurança das redes. Esse raciocínio advindo do paradigma de segurança será estendido a outros sistemas fora da APF, como o do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil[26] (CERT.br).

Esse paradigma reforçará a ideia de que as estatísticas de notificações de incidentes em rede apresentadas por qualquer órgão, se observadas isoladamente, conduzirão a conclusões deficientes, visto que as quantidades registradas não corresponderão exatamente à realidade. Mas a perspectiva de interação com um sistema maior, possível com a síntese escolhida para este estudo, poderá mitigar as lacunas geradas pelo paradigma adotado.

Delineados os conceitos, variáveis e o paradigma de segurança, será procedida a síntese das evidências para responder à questão formulada e extrair as conclusões e suas possíveis aplicações na guerra cibernética.

[26] Órgão responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Disponível em: <https://www.cert.br/sobre/>. Acesso em: 23 jul. 2018.

3 RELAÇÕES ENTRE A EVOLUÇÃO DA ESTRUTURA E AS NOTIFICAÇÕES REGISTRADAS

3.1 Contexto histórico do período observado

Dentro do período selecionado para o estudo, é interessante enumerar alguns pontos que irão sobrepor-se aos marcos de evolução da estrutura de segurança cibernética da APF e à quantidade de notificações de incidentes, facilitando a retirada de conclusões da síntese a ser procedida neste capítulo.

Segundo o Ministério da Defesa[27], a partir de 2011, no âmbito do Estado-Maior Conjunto das Forças Armadas (EMCFA), entrou em uso o termo "grandes eventos" nos compromissos nacionais firmados para a realização de competições e conferências de alcance internacional que envolvessem grande fluxo de turistas ou autoridades estrangeiras, assim como a atenção da mídia internacional para o Brasil. Foram enquadrados nessa categoria os Jogos Mundiais Militares (JMM), em 2011; a Conferência das Nações Unidas para Desenvolvimento Sustentável (Rio+20), em 2012; a Copa das Confederações da FIFA (Copa Conf) e a Jornada Mundial da Juventude (JMJ), em 2013, a partir de quando se incrementou a atenção na questão da segurança cibernética; a Copa do Mundo da FIFA (Copa Mundo), em 2014; e os Jogos Olímpicos e Paralímpicos no Rio de Janeiro (JO), em 2016; pois se estimou que esses eventos, pelo seu apelo global, possuíam um potencial de atrair mais ameaças cibernéticas, o que se buscará identificar na síntese gráfica. Do mesmo modo, a cada grande evento há a tendência do acúmulo de lições aprendidas que servirão para reforçar o sistema de defesa para os próximos, diminuindo a probabilidade de um possível aumento de tentativas de ataques.

[27] Disponível em: <www.defesa.gov.br>. Acesso em: 29 jun. 2018.

Outro aspecto relevante é o do investimento governamental em segurança cibernética. No caso do Brasil, desde 2013 há uma ação orçamentária[28] – 147F, Implantação do Sistema de Defesa Cibernética Nacional – específica para a implantação do sistema de defesa cibernética, da qual se espera um impacto direto na redução da taxa de crescimento da quantidade de incidentes proporcional ao montante alocado a cada ano. Esses dados também serão buscados na síntese gráfica.

Cabe acrescentar mais um aspecto com influência em todo o período investigado, o da constante evolução tecnológica na área cibernética, que assim como trouxe novas técnicas, ativos de informação e benefícios, gerou também novos tipos de ameaças. E, com a proliferação do acesso ao ciberespaço, cada vez mais pessoas têm acesso a um número maior de ameaças (MACHADO et al, 2017, p.1). Isso por si só acarreta na tendência de aumento dos incidentes, caso não haja nenhuma alteração na estrutura de segurança cibernética de qualquer órgão. Ao desenvolver essa estrutura, espera-se uma tendência de decréscimo na taxa de aumento dos incidentes, sem necessariamente alcançar a diminuição em relação às medidas anteriores, o que seria um desempenho ideal. A ocorrência de tal tendência também será procurada na síntese gráfica.

Enumerados os pontos relevantes da janela temporal da pesquisa, também será útil descrever os eventos que caracterizam a ocorrência dos marcos de evolução da estrutura de segurança cibernética, para estimular a compreensão dos resultados da síntese.

3.2 Descrição dos marcos de evolução da estrutura de segurança cibernética

Os marcos de evolução da estrutura de segurança cibernética selecionados para

[28] De acordo com o glossário do orçamento federal, ação orçamentária é um projeto, atividade ou operação especial decorrente de um programa para consecução de objetos especificados no planejamento do governo. Disponível em: <https://www12.senado.leg.br/orcamento/glossario>. Acesso em: 29 jun. 2018.

compor a síntese correspondem aos parâmetros listados no capítulo anterior. Para que se possa compreender melhor a influência de cada um na quantidade de notificações de incidentes, serão relatados os principais pontos desses marcos.

A política nacional de segurança cibernética, promulgada como a PNSI, no ano 2000, abriu o caminho para todos os avanços na estrutura de segurança cibernética, termo ainda não consagrado na época do decreto. Trata-se de um documento condicionante bem amplo, para o estabelecimento de diretrizes, mas desde sua expedição houve um amadurecimento sobre a dimensão da importância do espaço cibernético, principalmente por causa da criação do Comitê Gestor de Segurança da Informação[29] (CGSI), cuja composição foi revisada em 2013[30].

Como explicado sobre o desenvolvimento do CTIR Gov, no capítulo anterior, em 2008 foi publicada a Instrução Normativa GSI Nº 1. Nesse documento, ficaram estabelecidas definições de termos utilizados na Gestão de Segurança da Informação e as atribuições do DSIC, do CGSI, dos demais órgãos e entidades da APF, dos gestores e comitês de segurança da informação e comunicações. No ano seguinte, foi elaborada a Norma Complementar n° 5 e formalizada a estrutura do CTIR Gov. Essa norma complementar especificou os procedimentos para criação das ETIR, que, em conjunto com a ação de coordenação do CTIR, formaram a "espinha dorsal" da estrutura de segurança cibernética da APF. Por ocasião do ponto de partida da investigação dos registros de incidentes desse estudo, em 2011, essa estrutura já funcionava seus processos regulados.

---

[29] Comitê para assessoria da Secretaria-Executiva do Conselho de Defesa Nacional, no que diz respeitos às medidas para alcançar o cumprimento do previsto na PNSI e também para análise de assuntos relacionados a essa política.

[30] Decreto n. 8.097, de 4 de setembro de 2013, estabelece a alteração da composição do CGSI, com um representante de cada Ministério ou órgão listado a seguir. Ministérios: da Justiça; da Defesa; das Relações Exteriores; da Fazenda; da Previdência Social; da Saúde; do Desenvolvimento, Indústria e Comércio Exterior; do Planejamento, Orçamento e Gestão; das Comunicações; da Ciência, Tecnologia e Inovação; de Minas e Energia. Casa Civil da Presidência da República; GSIPR; Secretaria de Comunicação Social da Presidência da República; Controladoria-Geral da União; Advocacia-Geral da União; e Secretaria-Geral da Presidência da República. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8097.htm>. Acesso em: 27 jul. 2018.

O livro verde, publicado em 2010, já bem delineado no segundo capítulo, demandou um esforço de pesquisa sobre o tema e estimulou a participação em eventos de alcance internacional, como medida para reunir as condições para o lançamento de um livro branco acerca do mesmo assunto (BRASIL, 2010). Embora, até o final do período da pesquisa, não tenha sido publicado esse livro branco, os preparativos retornaram conhecimento para o pessoal diretamente envolvido com a segurança cibernética a nível nacional. No ano seguinte à publicação do livro verde, começaram os registros de notificações de incidentes na rede da APF.

O marco civil da Internet estabeleceu os direitos dos usuários, principalmente no que diz respeito à privacidade, e as principais regras de relacionamento com prestadores de serviço e acesso à rede. Seu advento deu suporte às atividades de fiscalização do uso do ciberespaço no Brasil e amparo ao emprego judicial e policial das informações armazenadas nas redes brasileiras. A lei de crimes de informática, que alterou o código penal a partir de 2012, municiou as autoridades governamentais de um instrumento de punição para tratar os responsáveis pelas ameaças cibernéticas adequadamente e de modo distinto dos criminosos comuns. A simples tipificação de crimes no ECiber criou um elemento de repressão às ameaças e acarretou na criação de delegacias de polícia com pessoal especializado nos crimes de informática, o que reforçou a estrutura de segurança cibernética não só da APF, mas de todo o Brasil. As penas para esses crimes variam, podendo chegar até três anos e quatro meses de reclusão[31] ou multa, nos casos mais graves.

A Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF 2015-2018 foi publicada em 2015 e deriva da PNSI e da Instrução Normativa GSI Nº 1. Nela são estabelecidos os objetivos estratégicos[32] e metas[33], que

[31] Parágrafo 4° do Art. 154-A do Código Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm>. Acesso em: 27 jul. 2018.

[32] São os dez objetivos estratégicos: OE-I institucionalizar o tema de SIC e de SegCiber no planejamento e

contribuem para orientar a direção dos esforços para evoluir a estrutura de segurança cibernética da APF. Com o advento de uma estratégia foi possível refinar o planejamento, a partir de uma metodologia, entretanto seus efeitos só poderão ser efetivamente avaliados após o término do quadriênio em que vigora. Desse modo, sua publicação servirá apenas para caracterizar o atendimento de mais um parâmetro da evolução da estrutura de segurança cibernética, sem que se busque uma interferência na síntese com a quantidade de notificações de incidentes registrados.

A seguir, serão expostos os dados estatísticos que integrarão a síntese, como etapa necessária para estudo do gráfico. Cabe ressaltar que serão integrados outros dados que extrapolam o objeto de estudo, por ter sido considerado durante a pesquisa que contribuiriam para o melhor entendimento das relações.

3.3 Dados estatísticos

Serão apresentados os dados que irão compor a síntese dessa pesquisa, a começar pela quantidade de notificações de incidentes. Cabe ressaltar que, no primeiro ano da observação, em 2011, o registro estatístico divulgado apresenta os dados somente a partir do mês de abril. Ainda nos dois primeiros anos, foram realizados ajustes nos processos das notificações recebidas pelas ETIR, o que causou uma depuração e tendência de diminuição da

---

Orçamento Federal; OE-II garantir continuamente o aprimoramento do quadro de pessoal da APF em SIC e SegCiber, de forma qualitativa e quantitativa; OE-III garantir continuamente a pesquisa, o desenvolvimento e a inovação em SIC e SegCiber na APF; OE-IV instituir modelo de governança sistêmica de SIC e de SegCiber na APF, com coordenação executiva, acompanhamento e avaliação do órgão central (GSI/PR); OE-V alinhar o planejamento de SIC e de SegCiber ao planejamento estratégico dos órgãos e entidades da APF; OE-VI ampliar e fortalecer ações colaborativas em SIC e SegCiber com a academia, setores público, privado e terceiro setor, no País e no exterior; OE-VII elevar o nível de maturidade de SIC e de SegCiber na APF; OE-VIII reforçar a SIC e a SegCiber como alta prioridade na agenda de governo; OE-IX valorizar e ampliar ações que fortaleçam a segurança das infraestruturas críticas da informação; e OE-X promover mecanismos de conscientização da sociedade sobre SIC e SegCiber. Disponível em: <http://www.gsi.gov.br/arquivos/4_estrategia_de_sic.pdf>. Acesso em: 27 jul. 2018.

[33] São vinte e três metas decorrentes, divididas temporalmente, entre 2015 e 2018, e de alcance contínuo, para todo o período. Disponível em: < http://www.gsi.gov.br/arquivos/4_estrategia_de_sic.pdf>. Acesso em: 27 jul. 2018.

quantidade[34] em relação ao que seria registrado sem as modificações. Os dados foram compilados por ano, de modo a facilitar as interações com as demais informações e estão listados na tabela a seguir.

TABELA 1
Quantidade de notificações de incidentes por ano do CTIR Gov

ANO	2011	2012	2013	2014	2015	2016	2017
Incidentes	11.192	13.825	16.003	22.167	19.854	23.625	28.183

Fonte: disponível em <http://www.ctir.gov.br/arquivos/estatisticas>. Acesso em: 27 jul. 2018

Pode se verificar uma tendência de aumento a cada ano, coerente com o que se concluiu no exame do contexto histórico, no início deste capítulo. Há, ainda, um pico no ano de 2014, cujas causas serão propostas durante a síntese com os demais dados. Sobre a tabela 1, de acordo com o paradigma de segurança, depreende-se que a quantidade de notificações de incidentes registrados é provavelmente inferior ao total realmente ocorrido, informação desconhecida. A observação dos registros, portanto, carece de referência precisa para averiguação qualitativa da tendência de crescimento. Ou seja, para produção de um juízo dos dados é necessário escolher uma referência, preferencialmente compatível com o objeto estudado.

Dentro do ambiente em que se insere a APF, podemos obter dados com utilidade de comparação por meio do CERT.br. Esse centro possui estatísticas sobre incidentes ocorridos no domínio brasileiro do ECiber[35], também conhecido como “domínio.br”, sujeito a condicionantes similares às da APF. As informações de incidentes são coletadas por um

[34] De acordo com o relatório de estatísticas de tratamento de incidentes de rede na APF relativo ao período de doze meses compreendido entre abril de 2011 e março de 2012. Disponível em: <http://www.ctir.gov.br/arquivos/ estatisticas/2011/Estatisticas_CTIR_20120409.pdf>. Acesso em: 23 jul. 2018.

[35] Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 23 jul. 2018.

processo de adesão voluntária, porém com um vulto muito maior, como se pode observar na tabela 2.

TABELA 2
Quantidade de notificações de incidentes por ano do CERT.br

ANO	2011	2012	2013	2014	2015	2016	2017
Incidentes	399.515	466.029	352.925	1.047.031	722.205	647.112	833.775

Fonte: disponível em: <https://www.cert.br/stats/incidentes>. Acesso em: 27 jul. 2018.

As notificações de incidentes do CERT.br também possuem uma tendência de aumento ao longo dos anos, com um pico em 2014. O comportamento da quantidade de notificações do Brasil análogo ao da APF reforça a sujeição às mesmas condicionantes, o que evidencia a pertinência do uso desses dados como referência satisfatória para a síntese. Chega-se a uma conclusão importante sobre o estudo das estruturas de segurança cibernética, defesa cibernética e guerra cibernética. A avaliação da tendência de aumento ou queda da quantidade de notificações é facilitada se o critério for o de comparação com estruturas semelhantes.

No caso do CTIR Gov, mesmo que a tendência da quantidade de notificações seja de aumento, será possível concluir que houve uma melhora, em termos de qualidade, na quantidade de incidentes na rede caso a taxa de crescimento seja menor que a do CERT.br, que contabiliza os incidentes dentro do mesmo ambiente regional. Isso também indicará um resultado positivo das inovações na estrutura de segurança cibernética, que terá sido reforçada. Com esse artifício, seria possível comparar a diferença de tendências entre o CERT e o CSIRT de dois Estados diferentes, para avaliar qual possui a estrutura de segurança mais robusta.

Outro dado relevante, como já comentado, é o montante de recursos financeiros

destinados à estrutura de segurança cibernética. Para compor a síntese, serão considerados os recursos destinados à ação orçamentária n° 147F – Implantação do Sistema de Defesa Cibernética Nacional, cujos dados constam no portal da transparência[36], a partir de 2014. Os valores são demonstrados na tabela 3.

TABELA 3
Montante realizado na ação orçamentária 147F, por ano

ANO	2014	2015	2016	2017
Realizado	R$ 23.596.824,38	R$ 4.227.554,84	R$ 22.061.147,42	R$ 18.921.592,36

Fonte: disponível em: <http://portaltransparencia.gov.br/orcamento/despesas>. Acesso em 27 jul. 2018.

Os valores realizados são relativamente baixos, se comparados ao total anual médio, da ordem de dois trilhões de reais[37], além de haver um pico de queda em 2015. É possível encontrar montantes ainda mais baixos se filtrarmos as despesas com investimentos a cada ano, que teriam relação direta com a evolução da estrutura de segurança cibernética. Os dados são mostrados na tabela 4.

TABELA 4
Investimentos na ação orçamentária 147F, por ano

ANO	2014	2015	2016	2017
Realizado	R$ 19.646.575,76	R$ 1.337.371,46	R$ 7.837.839,49	R$ 4.614.254,54

Fonte: disponível em: <http://portaltransparencia.gov.br/orcamento/despesas>. Acesso em: 27 jul. 2018.

Essa informação também será confrontada na síntese para buscar se há alguma relação perceptível entre os gastos com a estrutura de segurança cibernética da APF e a

[36] Disponível em: <http://portaltransparencia.gov.br/ orcamento/despesas ? paginacaoSimples = true & tamanho Pagina=&offset=&direcaoOrdenacao=asc&colunasSelecionadas=ano%2CorgaoSuperior%2Corgao Vinculado%2Cfuncao%2CsubFuncao%2Cprograma%2Cacao%2CcategoriaEconomica%2CgrupoDespesa% 2CelementoDespesa%2CorcamentoInicial%2CorcamentoAtualizado%2CorcamentoRealizado%2Cpercentual Realizado&de=2013&ate=2017&acao=147F&ordenarPor=ano&direcao=desc>. Acesso em: 23 jul. 2018.

[37] Disponível em: <http://portaltransparencia.gov.br/orcamento>. Acesso em: 23 jul. 2018.

quantidade de notificações de incidentes registrados. Finalmente, foram reunidas as evidências para compor a síntese gráfica, que será iniciada a seguir.

3.4 Síntese gráfica

Os dados estatísticos e informações do contexto histórico serão agrupados, de modo a obter a síntese das evidências sobre o objeto de estudo e responder à questão formulada, extraindo as conclusões adicionais e aplicações possíveis para a guerra cibernética, caso houver. Antes de proceder ao gráfico, os principais dados citados serão reunidos em uma única tabela, o que auxiliará na interpretação da síntese gráfica. A TAB. 5 reúne os dados de interesse.

TABELA 5
Dados estatísticos compilados no período de 2011-2017

ANO	Investimentos	CERT.br	CTIR Gov
2011	...	399.520	11.192
2012	...	466.030	13.825
2013	...	352.930	16.003
2014	R$ 19.646.575,76	1.047.030	22.167
2015	R$ 1.337.371,46	722.210	19.854
2016	R$ 7.837.839,49	647.110	23.625
2017	R$ 4.614.254,54	833.780	28.183

Fonte: TAB. 1, 2 e 4.

Serão apresentados graficamente os investimentos em milhares de reais e as notificações do CERT.br em dezenas, para uma melhor visualização na escala em conjunto com os demais dados. Assim, finalmente é possível estudar a síntese sob a forma gráfica. O GRAF. 1 contém os dados da TAB. 5, os marcos de evolução da estrutura de segurança cibernética e os grandes eventos reunidos, para a obtenção das conclusões. As quantidades

anuais de notificações de incidentes do CERT.br são mostrados na linha preta grossa, com traços e pontos. Uma linha preta pontilhada e mais fina mostra a tendência crescente ao longo dos anos. As quantidades anuais de notificações de incidentes da APF, compilados pelo CTIR Gov, são indicados por uma linha verde grossa. Do mesmo modo, uma linha verde pontilhada e mais fina marca a tendência, também crescente. Os dados dos recursos realizados com investimentos na implantação do sistema de defesa cibernética nacional são colocados sob a forma de barras azuis, para diferenciá-los das quantidades de notificações.

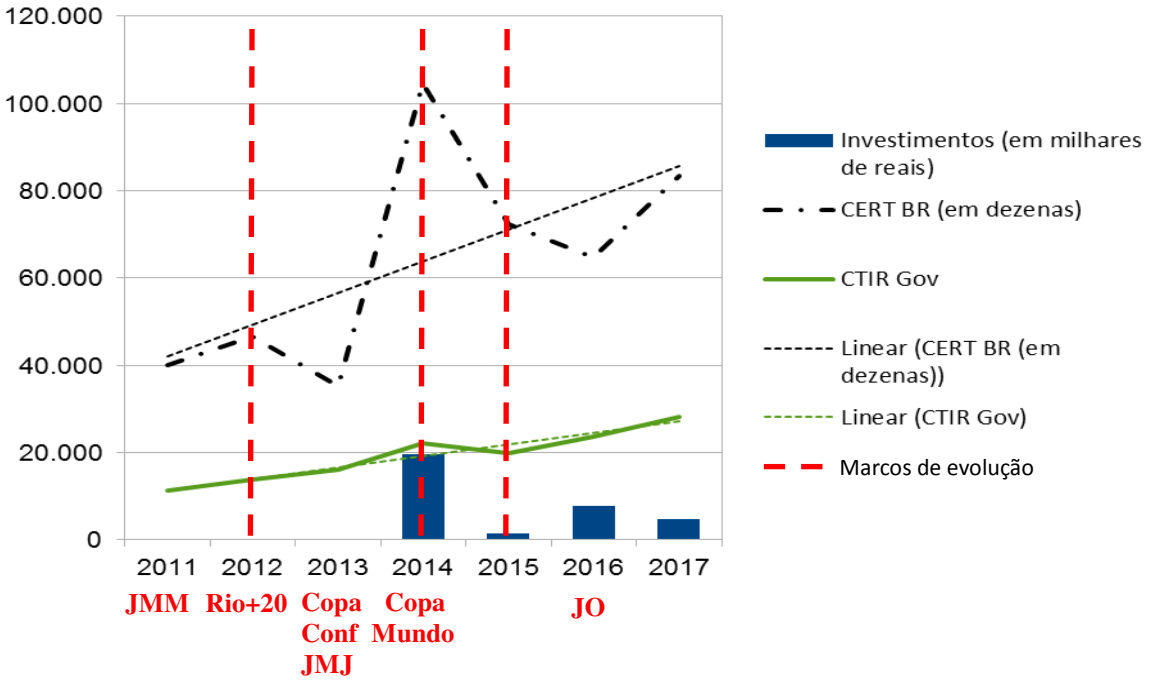

GRÁFICO 1 – Síntese gráfica dos dados pesquisados
Fonte: elaborado pelo autor.

A primeira interação observada no gráfico é a comparação entre a taxa de variação das notificações de incidente do CTIR Gov e do CERT.br. Antes de proceder à verificação, convém lembrar que os registros do ano de 2011 na APF só foram realizados a partir do mês de abril, consequentemente utilizar a quantidade bruta irá gerar uma distorção indesejada. Para calcular a taxa do CTIR Gov, será feita uma correção, extrapolando a tendência do valor

do primeiro ano de 11.192, referente a nove meses (abril a dezembro), para 14.923, que corresponderia ao total nos doze meses caso a média permanecesse a mesma.

No período delimitado para a pesquisa, ambos os órgãos tiveram um aumento na quantidade de incidentes, como já comentado. O CTIR Gov obteve uma taxa positiva de 89%, enquanto o CERT.br obteve uma taxa positiva de 109%. Nesse caso, é possível constatar que, em período e conjuntura similares, houve melhora na estrutura de segurança cibernética da APF em relação ao Brasil. Essa melhora no âmbito governamental, na verdade, reflete o desenvolvimento do seu sistema de defesa cibernética, que é a barreira para os ataques e ações de guerra cibernética.

A segunda interação que pode ser observada é a do impacto dos grandes eventos nas flutuações das quantidades de incidentes. Dos eventos listados, os de maior alcance foram a Copa do Mundo da FIFA e os Jogos Olímpicos, pelo apelo das competições nos Estados participantes. Em 2014, na ocasião do primeiro evento, é notável o aumento de notificações, tanto no Brasil quanto na APF, que sofreram um incremento de 197% e 39%, respectivamente. Isso representou uma mudança brusca de comportamento, considerando os incrementos do ano anterior, que foram de 24% negativos e 16%, respectivamente. No gráfico, a anomalia é detectável como um pico nos registros de notificações, em ambos os Centros.

Seguindo essa relação, era de se esperar que o pico fosse repetido em 2016, ano dos Jogos Olímpicos. Entretanto, o que se observa é uma queda de na quantidade de notificações no Brasil e um aumento na APF, que seguiu próximo da linha de tendência, com taxas de 10% negativos e 19%, respectivamente. Uma possível explicação é o resultado do acúmulo de lições aprendidas na Copa do Mundo, que podem ter gerado medidas adicionais de defesa cibernética, neutralizando os efeitos de atração de ameaças nos grandes eventos de maior apelo internacional.

A terceira interação é entre as quantidades de notificações de incidentes do CTIR Gov e o montante investido no sistema de defesa cibernética. Os valores de investimentos executados no primeiro ano registrado no gráfico foram os maiores, seguindo uma queda brusca no ano seguinte, alternando com novo aumento no ano subsequente e, por último, um decréscimo no montante. Entretanto, as variações das notificações não seguiram um padrão que possibilite estabelecer uma relação consistente com os recursos investidos. Uma informação adicional sobre a ação governamental medida é a discrepância entre o montante subsidiado e o efetivamente realizado[38], ou seja, é possível que o fato de os recursos aplicados na melhoria da defesa cibernética terem sido aquém do subsidiado explique o impacto imperceptível dos investimentos na mudança da quantidade das notificações. No entanto, seria necessária a ocorrência de um exercício financeiro em que o investimento fosse correspondente ao previsto no orçamento base para reforçar ou descartar a pertinência dessa explicação. Os dados da diferença entre o previsto e o realizado na ação orçamentária em questão são apresentados na TAB. 6, todos da ordem de dezenas de milhões de reais.

TABELA 6
Diferença entre os investimentos previstos e realizados na ação orçamentária 147F

ANO	Investimentos previstos	Investimentos realizados	Diferença
2014	R$ 56.000.000,00	R$ 19.646.575,76	R$ 36.353.424,24
2015	R$ 63.899.757,00	R$ 1.337.371,46	R$ 62.562.385,54
2016	R$ 18.603.689,00	R$ 7.837.839,49	R$ 10.765.849,51
2017	R$ 17.195.001,00	R$ 4.614.254,44	R$ 12.580.746,56

Fonte: disponível em: <http://portaltransparencia.gov.br/orcamento/despesas>. Acesso em: 27 jul. 2018.

[38] Disponível em: <http://portaltransparencia.gov.br/ orcamento/despesas ? paginacaoSimples = true & tamanho Pagina=&offset=&direcaoOrdenacao=asc&colunasSelecionadas=ano%2CorgaoSuperior%2CorgaoVinculado%2Cfuncao%2CsubFuncao%2Cprograma%2Cacao%2CcategoriaEconomica%2CgrupoDespesa%2CelementoDespesa%2CorcamentoInicial%2CorcamentoAtualizado%2CorcamentoRealizado%2CpercentualRealizado&de=2013&ate=2017&acao=147F&ordenarPor=ano&direcao=desc>. Acesso em: 27 jul. 2018.

A quarta interação se observa entre os marcos de evolução da estrutura de segurança e o comportamento das quantidades de notificações do CERT.br e CTIR Gov. O que se verifica é uma queda nos incidentes de rede registrados em todo o Brasil nos anos que seguem a instituição de leis e regulamentos para aumentar a segurança, mas o mesmo efeito não pode ser notado nas estatísticas da APF. Assim, é possível supor uma correlação positiva entre o estabelecimento de regulamentos de nível nacional com a melhoria os recursos de defesa cibernética em geral no Estado em que são instituídos. Quanto à relação com a rede da APF, pela sua estrutura já organizada e hierarquizada, com pessoal técnico trabalhando em equipe, sob a coordenação de um elemento central, no caso, o CTIR Gov, a publicação de documentos normativos acaba por formalizar procedimentos muitas vezes já adotados na prática. Dessa forma, o mais provável é que a experiência adquirida com o trato das ameaças na rede da APF gere subsídios para a elaboração das leis e regulamentos que beneficiam as demais redes do Brasil, o que explicaria não ser possível estabelecer uma conexão de reação das notificações de incidentes na rede da APF após o surgimento das leis e regulamentos.

Outra dedução que pode ser elaborada do GRAF. 1 é a diferença das taxas de variação das quantidades de notificações a cada ano no Brasil e na APF. As alterações da quantidade de incidentes no Brasil mudam mais bruscamente do que as da APF. A TAB. 7 demonstra o percentual de aumento ou diminuição em relação ao ano anterior dos registros de notificação do CERT.br e do CTIR Gov.

TABELA 7
Taxas de variação da quantidade de notificações em relação ao ano anterior

ANO	2012	2013	2014	2015	2016	2017
CERT.br	14,27%	-32,05%	66,29%	-44,98%	-11,60%	22,39%
CTIR Gov	-7,94%	15,75%	38,52%	-10,43%	18,99%	19,29%

Fonte: TAB. 5

Dentre as possíveis causas para a maior estabilidade da variação da quantidade de notificações de incidentes na rede da APF em torno da linha de tendência, também assinalada no GRAF. 1, adota-se a do resultado positivo da coordenação do sistema de defesa cibernética conduzida pelo CTIR Gov. A correlação dos efeitos gerados pelas ameaças em uma rede e a realização da divulgação de alertas de forma sistemática, quando bem exploradas, deve aumentar a segurança cibernética por meio da criação de novos procedimentos de defesa oriundos das lições aprendidas com essas ameaças. O padrão da linha referente às notificações do CTIR Gov é compatível com a explicação escolhida. Seguindo esse raciocínio, em uma situação considerada ótima, a taxa de crescimento da linha de tendência da APF acompanharia o aumento esperado das ameaças já enunciado no segundo capítulo (BRASIL, 2010, p. 14). O CERT.br, por sua vez, apesar de também possuir a capacidade de correlação das ameaças, apenas emite alertas, sem poder de realizar coordenação de ações ou determinar a adoção de alguma medida de defesa, acarretando em um descontrole nas ocorrências de incidentes. Isso também explicaria o comportamento mais brusco da linha do CERT.br no GRAF. 1. Ou seja, é possível observar o efeito positivo do CTIR Gov na segurança cibernética da rede da APF.

Dos resultados da síntese, é possível agora buscar aplicações dos conhecimentos na guerra cibernética, o que será discutido a seguir.

3.5 Aplicações da relação observada

A síntese realizada permitiu a elaboração de conclusões nos níveis da segurança e da defesa cibernética. Entretanto, a guerra cibernética está inserida nesse contexto, em um nível abaixo dos demais. Serão extraídos, a partir deste ponto, os desdobramentos das conclusões que possuem potencial de aplicação na guerra cibernética, tema central da pesquisa. Convém

apontar que a escolha pela busca de evidências nos níveis superiores trouxe maior riqueza à síntese e a possibilidade de verificar, em um contexto mais amplo, a relação procurada e outras decorrentes, das quais poderão ser retiradas mais facilmente as aplicações no âmbito da guerra cibernética.

A guerra cibernética, como definida, em seu caráter defensivo e ofensivo, impacta reforçando a própria defesa e segurança cibernética e se contrapondo às defesas e seguranças inimigas, respectivamente. Os patamares em que se encontram a nossa segurança cibernética e as inimigas, no que diz respeito à capacidade de resistir às ameaças do ciberespaço, são conhecimentos úteis para a condução dessa guerra. Nesse sentido, após o estudo da síntese gráfica foi possível concluir que a tendência de melhoria do sistema de defesa cibernética ou o seu enfraquecimento pode ser medida utilizando a comparação entre a quantidade de incidentes observados no nível nacional e governamental, dentro do mesmo contexto regional.

Isso pode ser utilizado para subsidiar uma decisão envolvendo a seleção de um parceiro ou alvo por um oponente, ao identificar qual deles é o mais forte ou mais fraco. Serve também para a autoavaliação de um órgão, comparando a tendência das suas próprias notificações ao longo do tempo com a tendência de outros órgãos de abrangência mais ampla, mas na mesma região. De posse dessa conclusão, para testá-la, foi procedida uma pesquisa entre os CERT de responsabilidade nacional e CSIRT governamentais, cuja lista consta no sítio do Instituto de Engenharia de Programas da Universidade *Carnegie Mellon*[39] e está replicada no APÊNDICE B. Dos 99 Estados que possuem centros registrados, somente doze estão organizados com um CERT para atendimento nacional e um CSIRT para a sua administração governamental, disponível para acesso público. Os demais dispõem na Internet de apenas um centro de abrangência nacional, sendo alguns complementados por agências especializadas ou de inteligência, que fazem parte das suas estruturas de segurança

[39] Disponível em: <https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/index.cfm>. Acesso em: 27 jul. 2018.

cibernética. Dentre os doze Estados que trabalham com centros distintos para toda a sua rede e para a rede da administração pública, somente o Brasil apresenta suas estatísticas anuais para acesso livre.

Não foi possível, portanto, listar nessa pesquisa nenhum teste comparativo entre o Brasil e outro Estado. Essa restrição não serve para negar a utilidade da aplicação que foi proposta nesse estudo, mas para apontar a necessidade de buscar esses dados, que não são abertos ao público em outros Estados. Finalmente, após a reunião das evidências para responder a questão formulada no inicio deste trabalho e da proposição de uma possível aplicação do resultado encontrado, encontram-se as condições para a sua conclusão.

A seguir, será realizada uma breve revisão das conclusões advindas desta pesquisa e exposto o comportamento da quantidade de notificações de incidentes na rede da APF relatados ao CTIR Gov no decorrer da evolução da estrutura de segurança cibernética da APF.

4 CONCLUSÃO

Esse trabalho buscou a geração de conhecimento científico envolvendo o tema da guerra cibernética. Para isso, optou-se por estudar a relação entre as notificações de incidentes na rede da APF, registradas no CTIR Gov e a evolução da estrutura de segurança cibernética da APF.

Antes da apresentação das evidências com ligação direta na pesquisa, foram vistos pontos de apoio contidos no livro verde de defesa cibernética, como os conceitos de espaço cibernético e segurança cibernética. A iniciativa desse livro demonstra o estado maduro da mentalidade de segurança, a importância do CERT.br, do CTIR Gov e dos documentos de alto nível que oficializam a estrutura de segurança cibernética. Foram destacados também aspectos da Doutrina Militar de Defesa Cibernética, como a relação entre a guerra, a defesa e a segurança cibernética, o que explica a pertinência da escolha por este nível para a obtenção de conclusões com aplicação dentro do tema proposto.

Para se compreender como são processados as quantidades de notificações de incidentes, foram apresentados os dados sobre o CTIR Gov e procedimentos para o tratamento dos incidentes de segurança, dentre os quais se destacam a triagem e a coordenação das atividades com as ETIR. Em seguida, foi necessário caracterizar a evolução da estrutura de segurança cibernética, por meio da identificação do arcabouço político-administrativo do espaço cibernético de Souza e Almeida (2016) e, seguindo os principais documentos que impactaram no reforço dessa estrutura, da seleção dos marcos correspondentes: documento oficial do governo que debata o tema da segurança cibernética; política nacional de segurança cibernética; estratégia nacional de segurança cibernética; legislação própria para regular o uso das redes e os crimes cibernéticos; normas técnicas; e existência de um CSIRT de responsabilidade nacional.

A adoção do pressuposto do paradigma de segurança de que não haveria sistema totalmente seguro permitiu vislumbrar a necessidade de interagir as quantidades de notificações de incidentes na rede da APF com dados mais amplos de um ambiente com contexto compatível, no caso, do Brasil, por meio da extração das estatísticas do CERT.br.

Listados os pontos de apoio para a pesquisa, foram apresentadas as evidências, retiradas dos objetos de estudo e de outras fontes das quais se percebeu alguma possibilidade de influência no sistema que se desejava compor. O desenho da síntese, pela fórmula de reunião dos fatos, se prestou adequadamente para alcançar o resultado, ou seja, as conclusões que serão compiladas nesse capítulo.

As conexões entre a quantidade de notificações de incidentes cibernéticos na rede da APF e a evolução da estrutura de segurança cibernética passam por muitos pontos, dentre os que puderam ser observados na pesquisa deste trabalho e foram reunidos na síntese. Acontecimentos que atraem a atenção da sociedade nacional e internacional, também atraem ameaças cibernéticas. Daí, concluiu-se que a ocorrência dos grandes eventos acarreta na tendência de interferir na quantidade da ocorrência dos incidentes nas redes, se não for adotada nenhuma medida de prevenção. Os investimentos na área da defesa cibernética poderiam ter efeito positivo na redução dos incidentes, entretanto, não foi possível concluir essa relação, pois se constatou uma demanda reprimida na aplicação dos recursos do governo, ou seja, não foram aplicados os recursos orçamentários considerados necessários para avaliação do efeito esperado. Naturalmente, a evolução tecnológica na área cibernética, por acarretar no desenvolvimento de novas ameaças, também insere um efeito esperado de permanente aumento da quantidade de incidentes a cada ano e obriga a evolução da estrutura de segurança cibernética, na tentativa de alcançar um ritmo de incremento das defesas maior do que o de surgimento das ameaças.

A compreensão desses efeitos facilitou a transcrição das conclusões extraídas da

síntese, que também serão reunidas a partir de agora. O aumento das notificações de incidentes na rede da APF é absoluto, a despeito da evolução da estrutura de segurança cibernética. Esse dado estatístico é construído por diversos fatores, dentre os quais podem ser destacados o refino dos instrumentos de detecção, o aumento da quantidade de ameaças e as ocorrências de apelo nacional e internacional, como os grandes eventos. Isso, por si só, direcionaria a resposta da questão formulada simplesmente para um comportamento de aumento das notificações à medida que a estrutura de segurança evolui.

No entanto, ao encaixar os dados da APF em um contexto mais abrangente, como o nacional, o que se observou foi uma redução relativa. Essa medição comparativa é mais facilmente visualizada quando calculada a partir da taxa de variação no período, que figura graficamente como uma linha de tendência. Mesmo que as quantidades de notificações de incidentes nacionais, do CERT.br, não garantam a totalidade dos incidentes realmente ocorridos, o seu comportamento segue um padrão semelhante ao longo do tempo, o que aponta a possibilidade de uso para comparação de forma satisfatória. Ou seja, a evolução da estrutura de segurança cibernética acarretou em resultados positivos, como a redução relativa das notificações de incidentes da rede da APF. Esse efeito se explica porque a evolução da estrutura, na verdade, é caracterizada pela instituição de regulamentos, instrumentos legais e organizações, que contribuem, cada um do seu modo, para o reforço do sistema de defesa cibernética.

Os regulamentos são a materialização de procedimentos elaborados com as lições aprendidas de ocorrências anteriores; os instrumentos legais dão amparo à execução de atividades de repressão e punição dos agentes causadores dos incidentes, tendo um resultado mais sensível no ambiente externo à APF, já amparada pelos procedimentos; as organizações, em especial as especializadas em atividades em prol da segurança, defesa e guerra cibernética, facilitam a concentração de pessoal capacitado, ferramentas e dispositivos de coordenação das

ações que contribuem para diminuição da quantidade de incidentes na rede.

Quanto ao efeito dos investimentos orçamentários no sistema de defesa cibernética, que dá suporte à estrutura de segurança, não foi possível chegar a qualquer conclusão, pois o montante executado foi muito inferior ao estimado como necessário para resultar em um impacto significativo.

Após as interações elucidadas na síntese e exposição das conclusões reunidas, há evidências suficientes para responder à questão formulada sobre a relação entre o comportamento da quantidade de notificações de incidentes na rede da APF relatados ao CTIR Gov no decorrer da evolução da estrutura de segurança cibernética da APF, caracterizada por marcos definidos a partir de um arcabouço político-administrativo do ECiber brasileiro. Foi observado que a quantidade de notificações sofreu um aumento frente à evolução da estrutura de segurança. No entanto, apesar do crescimento absoluto, também foi possível constatar que houve uma redução relativa ao contexto regional brasileiro, após comparação com as quantidades de incidentes registrados pelo CERT.br. Essa diminuição permite considerar a eliminação do efeito esperado de crescimento das ameaças e um possível refino da capacidade de detecção advinda da melhoria dos processos do CTIR Gov e suas ETIR subordinadas e perceber o comportamento de redução no contexto do local geográfico, como resultado da evolução da estrutura de segurança cibernética.

Além de responder a questão, é oportuno atentar para as aplicações do conhecimento produzido. A pesquisa realizada só logrou em concluir uma possibilidade de uso da comparação entre a quantidade de notificações de incidentes de dois órgãos para auxiliar a avaliação do nível em que se encontra a estrutura de segurança cibernética com relação a outros órgãos porque os dados estatísticos e os demais utilizados na síntese estavam disponíveis publicamente, ou seja, para acesso a qualquer pessoal no planeta. Entretanto, dentre todos os Estados que possuem CSIRT, o Brasil é o único a divulgar tão facilmente tais

dados, permitindo a exploração cibernética por qualquer agente e, consequentemente, a elaboração de conclusões semelhantes às deste trabalho quanto ao estado da estrutura de segurança cibernética brasileira.

Essa peculiaridade, inclusive, traz à reflexão outra questão, que envolve o real benefício para a sociedade brasileira da publicação das estatísticas de incidentes na rede da APF, considerando as conclusões que foram obtidas nessa pesquisa com a síntese das informações disponíveis ostensivamente e podem ser replicadas por um agente malicioso que deseje estudar as vulnerabilidades da rede governamental brasileira. De qualquer modo, permanece a possível aplicação nas ETIR da APF, para verificar o estado de seus níveis de segurança cibernética em relação ao do CTIR Gov.

REFERÊNCIAS

Acesso ao Direito da União Europeia. Desenvolvido pela União Europeia, 2011. Faculta acesso aos documentos da União Europeia. Disponível em: <https://eu-lex.europa.eu/>. Acesso em: 27 jul. 2018.

BERVIAN, Pedro A.; CERVO, Amado L.; e SILVA, Roberto. **Metodologia Científica**. 6 ed. São Paulo: Editora Person, 2011. 242 p.

BRASIL. Congresso Nacional. 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. *Diário Oficial [da República Federativa do Brasil]*, Poder Executivo, Brasília, DF, 14 jun. 2000. Seção 1. p. 2. Disponível em: <http://www2.camara.leg.br/legin/fed/decret/2000/decreto-3505-13-junho-2000-368759-normaatualizada-pe.html>. Acesso em 27 jul. 2018.

_____. _____. Decreto n. 8.097 de 04 de setembro de 2013. Altera o Decreto n. 3.505, de 13 de junho de 2000, para incluir a Secretaria-Geral da Presidência da República no Comitê Gestor da Segurança da Informação. *Diário Oficial [da República Federativa do Brasil]*, Poder Executivo, Brasília, DF, 05 set. 2013. Seção 1. p. 7. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8097.htm>. Acesso em 27 jul. 2018.

_____. _____. Lei n. 12.737 de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. *Diário Oficial [da República Federativa do Brasil]*,

Poder Executivo, Brasília, DF, 03 dez. 2012. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 27 jul. 2018.

_____. _____. Lei n. 12.965 de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial [da República Federativa do Brasil]*, Poder Executivo, Brasília, DF, 24 abr. 2014. Seção 1. p. 1. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 jul. 2018.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014. 38 p.

_____. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018**. v. 1.0. Brasília, 2015. 82 p.

_____. _____. _____. IN 01/2008: disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Brasília, 2008. Disponível em: <http://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf>. Acesso em: 27 jul. 2018.

_____. _____. _____. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, 2010. 63 p.

_____. _____. _____. NC 05/IN01/DSIC/GSIPR: criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR. Brasília, 2009. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf>. Acesso em: 27 jul. 2018.

_____. _____. _____. NC 08/IN01/DSIC/GSIPR: criação de equipes de tratamento e resposta a incidentes em redes computacionais - ETIR. Brasília, 2010. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_8_gestao_etir.pdf>. Acesso em: 27 jul. 2018.

_____. _____. _____. NC 21/IN01/DSIC/GSIPR: diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes. Brasília, 2014. Disponível em: <http://dsic.planalto.gov.br/legislacao/nc_21_preservacao_de_ evidencias.pdf>. Acesso em: 27 jul. 2018.

Carnegie Mellon University Software Engineering Institute. Desenvolvido pela Universidade *Carnegie Mellon*, 2018. Portal de acesso às informações sobre o Instituto de Engenharia de Programação da Universidade Carnegie Mellon. Disponível em: <https://www.sei.cmu.edu/>. Acesso em: 27 jul. 2018.

Centro de Tratamento de Incidentes de Redes do Governo. Desenvolvido pelo CTIR Gov, 2011. Atende aos incidentes em rede dos computadores da rede da APF. Disponível em: <https://www.ctir.gov.br/>. Acesso em: 27 jul. 2018.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desenvolvido pelo Comitê Gestor da Internet no Brasil, 1998. Trata incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil. Disponível em: <https://www.cert.br/>. Acesso em: 27 jul. 2018.

CLARKE, R. A.; KNAKE, R. K. ***Cyber War: The Next Threat to National Security and What to Do About It***. Nova Iorque: HarperCollins e-books, 2010. 140 p.

FERNANDES, J. H. C (Org.). **Gestão da segurança da informação e comunicações**. v. 1. Brasília: Universidade de Brasília, 2010. 125 p.

FERREIRA, Aurélio B. H. **Mini Aurélio: o dicionário da língua portuguesa**. 8 Ed. Curitiba: Positivo, 2010. 960 p.

FESTIVAL USINA DE ARTE E CULTURA, 1994, Porto Alegre. **Palestra de Pierre Levy sobre a emergência do ciberespaço e as mutações culturais**. Disponível em: <https://www.nescon.medicina.ufmg.br/biblioteca/imagem/2514.pdf>. Acesso em: 30 jul. 2018.

MACHADO, A. V. B. C. S. et al. **Defesa Cibernética Comparada: Um Estudo do Brasil e da África do Sul**. In: CONGRESSO ACADÊMICO SOBRE DEFESA NACIONAL, 14., 2017, Resende. 16 p.

Portal da Transparência. Desenvolvido pelo Ministério da Transparência e Controladoria-Geral da União, 2018. Integra e apresenta dados de diversos sistemas utilizados pelo Governo

Federal para a sua gestão financeira e administrativa. Disponível em: <http://www.portaltransparencia.gov.br/>. Acesso em: 27 jul. 2018.

Portal do Ministério da Defesa. Desenvolvido pelo Ministério da Defesa, 2018. Presta informações sobre o Ministério da Defesa. Disponível em: <https://www.defesa.gov.br/>. Acesso em: 27 jul. 2018.

Portal do Orçamento Federal. Desenvolvido pelo Senado Federal, 2018. Presta informações sobre o orçamento do Governo Federal brasileiro. Disponível em: <https://www12.senado.leg.br/orcamento>. Acesso em: 27 jul. 2018.

PROJECT MANAGEMENT INSTITUTE. **Guia PMBOK**. Pensilvânia, 2013. 567 p.

SOUZA, Eduardo André Araújo; ALMEIDA, Nival Nunes. **A Questão da Segurança e Defesa do Espaço Cibernético Brasileiro, e o Esforço Político-Administrativo do Estado**. R. Esc. Guerra Naval, Rio de Janeiro, v.22 n.2, p. 381 - 410, mai./ago. 2016.

APÊNDICE A – Linha do Tempo dos marcos de evolução da estrutura de segurança cibernética selecionados

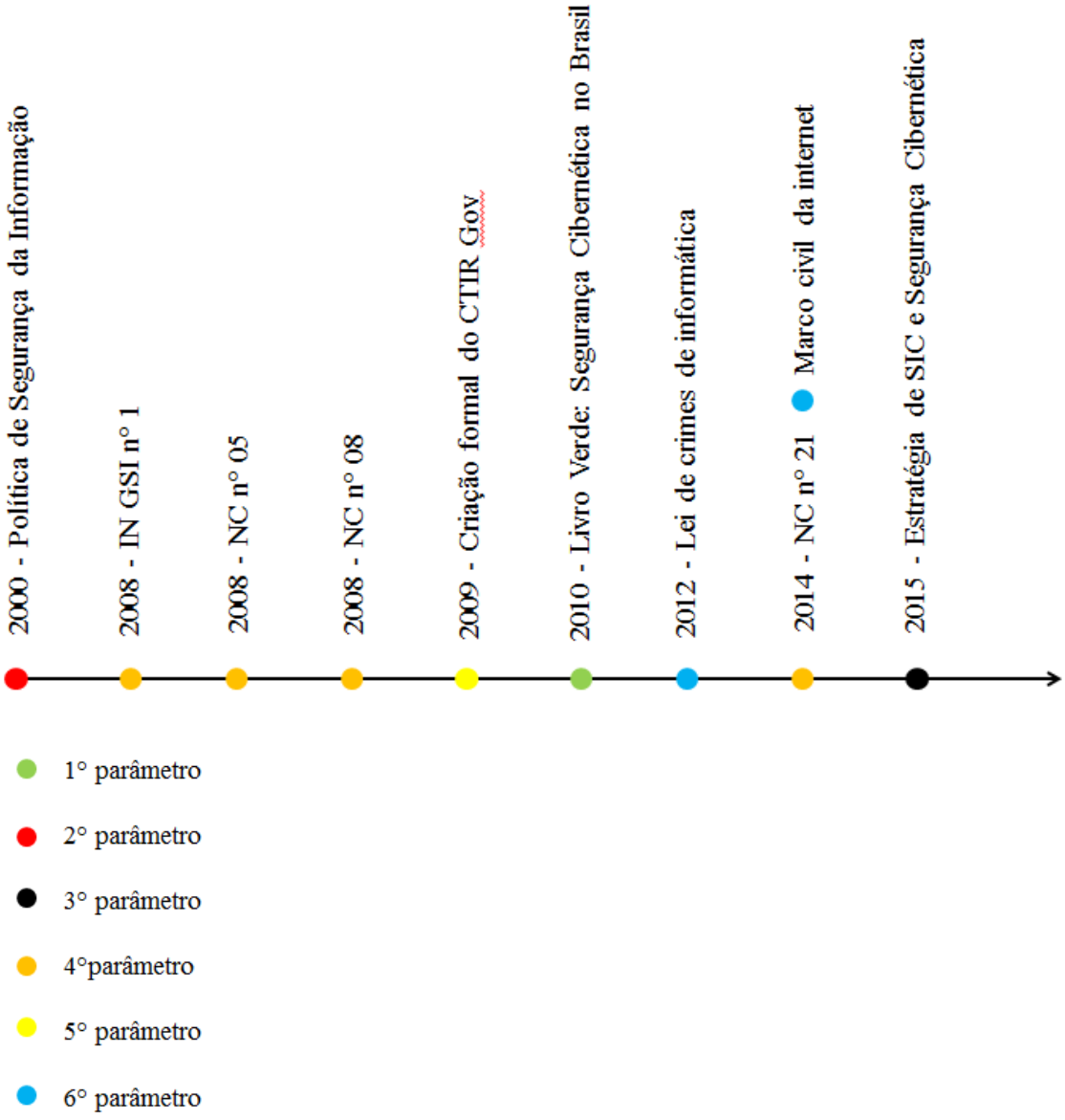

FIGURA 3 – Marcos da evolução da estrutura de segurança cibernética selecionados
Fonte: elaborada pelo autor.

APÊNDICE B – Lista dos CSIRT com responsabilidade nacional

TABELA 8
CSIRT com responsabilidade nacional

(Continua)

N°	Estado	Nome	Abreviatura
1	Albânia	*National Security Computer Agency* ALCIRT	ALCIRT
2	Argéria	*Algerian Computer Emergency Response Team*	DZ-CERT
3	Argentina	ICIC CERT	ICIC CERT
4	Armênia	*Computer Emergency Response Team Armenia*	CERT AM
5	Austrália	*Computer Emergency Response Team Australia*	CERT Australia
6	Áustria	*Austrian Government Computer Emergency Response Team*	GovCERT.AT
		National Computer Emergency Response Team of Austria	CERT.at
7	Azerbaijão	*Azerbaijan Government* CERT	CERT.GOV.AZ
8	Bangladesh*	*Bangladesh Computer Emergency Response Team*	bdCERT
		Bangladesh e-Government Computer Incident Response Team	BGD e-GOV CIRT
9	Bélgica	*The Federal Cyber Emergency Team of Belgium*	CERT.be
10	Brasil*	*Center for the Treatment of Security Incidents on Computer Networks*	CTIR Gov
		Computer Emergency Response Team Brazil	CERT.br
11	Brunei	*Brunei Computer Emergency Response Team*	BruCERT
12	Bulgária	*Bulgarian Computer Security Incidents Response Team*	CERT Bulgaria
13	Burkina Faso	CIRT *Burkina Faso*	CIRT.BF
14	Camboja	*National Cambodia Computer Emergency Response Team*	CamCERT
15	Canadá	*Canadian Cyber Incident Response Center*	CCIRC
16	Chile	*Chilean Computer Emergency Response Team*	CLCERT
17	China	*National Computer Network Emergency Response Technical Team/Coordination Center of China*	CNCERT/CC
18	Colômbia	colCERT	colCERT
19	Costa do Marfim	*Cote d'Ivoire Computer Emergency Response Team*	CI-CERT
20	Croácia	*Croatian National Computer Emergency Response Team*	HR-CERT
21	Curaçao	*Caribbean* CERT	CARICERT
22	Chipre	*Cyprus National* CSIRT	CSIRT-CY
23	República Tcheca*	*Computer Security Incident Response Team of the Czech Republic*	CSIRT.CZ
		Government CERT *of the Czech Republic*	GovCERT.CZ
24	Dinamarca	*Danish Centre for Cyber Security*	GovCERT.DK

TABELA 8
CSIRT com responsabilidade nacional

(Continua)

N°	Estado	Nome	Abreviatura
25	Equador	EcuCERT	EcuCERT
26	Egito	*Egyptian* CERT	EG-CERT
27	Estônia	*Computer Emergency Response Team Estonia*	CERT-EE
28	Etiópia	*Ethiopian Cyber Emergency Readiness and Response Team*	Ethio-CER2T
29	Finlândia	*National Cyber Security Centre Finland*	NCSC-FI
30	França	*French Government* CSIRT	CERT-FR
31	Geórgia	*Computer Emergency Response Team-Georgia*	CERT.GOV.GE
32	Alemanha	*Computer Emergency Response Team* - CERT-*Bund*	CERT-Bund
33	Gana	*Ghana National* CERT	CERT-GH
34	Guatemala	*Guatemala* CERT	CERT-GT
35	Hong Kong	*Government* CERT *Hong Kong*	GovCERT.HK
		Hong Kong Computer Emergency Response Coordination Centre	HKCERT
36	Islândia	*Computer Emergency Response Team Iceland*	CERT-IS
37	Índia	*Indian Computer Emergency Response Team*	CERT-IN
38	Indonésia	*Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center*	ID-SIRTII/CC
39	Irã	*Iran Computer Emergency Response Team/ Coordination Center*	CERTCC MAHER
40	Israel	*The Israel National Computer Emergency Response Team*	CERT-IL
41	Itália*	CERT *Nazionale Italia*	IT-CERT
		CERT *Publica Amministrazione*	CERT-PA
42	Japão*	*Japan Computer Emergency Response Team*	JPCERT/CC
		National Center of Incident Readiness and Strategy for Cybersecurity	NISC
43	Casaquistão	*Kazakhstan* CERT	KZ-CERT
44	Quênia	*Kenya Computer Incident Response Team Coordination Centre*	KE-CIRT/CC
45	Coreia do Sul*	CERT *Coordination Center of Korea*	KrCERT/CC
		Korea National Computer Emergency Response Team	KN-CERT
46	Kosovo	*National Unit for Cyber Security*	KOS-CERT
47	Laos	*Lao Computer Emergency Response Team*	LaoCERT
48	Letônia	*Information Technologies Security Incidents Response Institution Latvia*	CERT.LV

TABELA 8
CSIRT com responsabilidade nacional

(Continua)

N°	Estado	Nome	Abreviatura
49	Lituânia	*Lithuania* CERT	LT-CERT
		Lithuanian National Computer Emergency Response Team	CERT-LT
50	Luxemburgo*	CERT *Gouvernemental*	GOVCERT.LU
		Computer Incident Response Center Luxembourg	CIRCL
		National CERT *of Luxembourg*	NCERT.LU
51	Macau	*Macau Computer Emergency Response Team - Coordination Centre*	MOCERT
52	Malásia	*Malaysian Computer Emergency Response Team*	MyCERT
53	Malta	*Malta National* CSIRT	CSIRTMalta
54	Maurício	*Mauritian National Computer Security Incident Response Team*	CERT-MU
55	México	*Computer Emergency Response Team Mexico*	CERT-MX
		TIC *Defense* CERT	TIC CERT
56	Moldávia	*Cyber Security Center*	CERT-GOV-MD
57	Mônaco	CERT *Monaco*	CERT-MC
58	Montenegro	*National Montenegrin Computer Incident Response Team*	CIRT.ME
59	Marrocos	*Moroccan National Computer Emergency Response Team*	maCERT
60	Myanmar	*Myanmar Computer Emergency Response Team*	mmCERT
61	Holanda	*National Cyber Security Center - Netherlands*	NCSC-NL
62	Nova Zelândia*	CERT *New Zealand*	CERT NZ
		New Zealand National Cyber Security Centre	NCSC
63	Nigéria	*Nigeria* CERT	NgCERT
64	Noruega	*Miljodirektoratet* CERT	MiljoCERT
		Norwegian Communications Authority	EkomCERT
		Norwegian Computer Emergency Response Team	NorCERT
		Norwegian Police ICT *Services*	JustisCERT
65	Omã	*Oman National* CERT	OCERT
66	Panamá	*Computer Security Incident Response Team Panama*	CSIRT Panama
67	Paraguai	*Paraguay Equipo de Respuesta ante Incidentes Ciberneticos*	CERT-Py
68	Peru	*Peru* CERT	PeCERT
69	Filipinas	*Department of Information and Communications Technology-Cybersecurity Bureau*	CERT-PH
70	Polônia*	CERT *Polska*	CERT.PL
		Republic of Poland Governmental Computer Security Incident Response Team	CERT.Gov.PL

TABELA 8
CSIRT com responsabilidade nacional

(Continua)

N°	Estado	Nome	Abreviatura
71	Portugal*	*Computer Emergency Response Team Portugal*	CERT.PT
		Portuguese National Cybersecurity Center	CNCS
72	Qatar	*Qatar Computer Emergency Security Team*	Q-CERT
73	Romênia	*Computer Emergency Response Team Romania*	CERT-RO
74	Rússia	*Cyber Security and Incident Response Team for the governmental networks of the Russian Federation*	GOV-CERT.RU
75	Arábia Saudita	*Computer Emergency Response Team Saudi Arabia*	CERT-SA
76	Singapura	*Singapore Computer Emergency Response Team*	SingCERT
77	Eslováquia*	*Computer Security Incident Response Team Slovakia*	CSIRT.SK
		National Agency for Network and Electronic Services	GOV CERT SK
		National Security Authority of the Slovak Republic CERT	SK-CERT
		SK-CERT	SK-CERT
78	Eslovênia	*Slovenian Computer Emergency Response Team*	SI-CERT
79	África do Sul	ECS-CSIRT	ECS-CSIRT
80	Espanha	CERT - *Mando Conjunto De Ciberdefensa*	ESP DEF CERT
		Cryptology National Center Computer Emergency Response Team	CCN-CERT
		National Cybersecurity Institute of Spain (INCIBE)	CERT-SeguridadIndustria
81	Sri Lanka	*Sri Lanka Computer Emergency Readiness Team/Coordination Center*	Sri Lanka CERT/CC
82	Suécia	CERT-SE	CERT-SE
83	Suíça*	*Swiss Education and Research Network Computer Emergency Response Team*	SWITCH-CERT
		Swiss Government Computer Emergency Response Team	GovCERT.ch
84	Taiwan	*Taiwan National Computer Emergency Response Team*	TWNCERT
85	Tanzânia	*Tanzania* CERT	TZ-CERT
86	Tailândia	*Thailand Computer Emergency Response Team*	ThaiCERT
87	Tonga	*Tonga National* CERT	CERT.to
88	Tunísia	*Tunisian Computer Emergency Response Team*	tunCERT
89	Turquia	*Turkish Computer Emergency Response Team*	TR-CERT
90	Uganda	*Uganda Computer Emergency Response Team*	Ug-CERT
91	Ucrânia	*Computer Emergency Response Team of Ukraine*	CERT-UA
92	Emirados Árabes Unidos	*Arab Emirates Computer Emergency Response Team*	aeCERT
93	Reino Unido	*Computer Emergency Response Team* (CERT) *for* UK *Government*	GovCertUK
		National Cyber Security Centre (UK)	NCSC UK

TABELA 8
CSIRT com responsabilidade nacional

N°	Estado	Nome	Abreviatura
94	Estados Unidos da América	*Department of Homeland Security United States Computer Emergency Readiness Team*	US-CERT
95	Uruguai	*Incident Response Center of Information Security Uruguay*	CERTuy
96	Uzbequistão	*Uzbekistan Computerization and Information Technologies Developing Center*	UZ-CERT
97	Venezuela	*Venezuelan Bolivarian Government* CSIRT	VenCERT
98	Vietnã	*Vietnam Computer Emergency Response Team*	VNCERT
99	Zâmbia	*Zambia Computer Incident Response Team*	ZM CIRT

Fonte: disponível em: < https://www.sei.cmu.edu/education-outreach/computer-security-incident-response-teams/national-csirts/index.cfm>. Acesso em: 25 jul. 2018.

* - Estados com CSIRT nacionais e governamentais.

ANEXO A – Interações do CTIR Gov

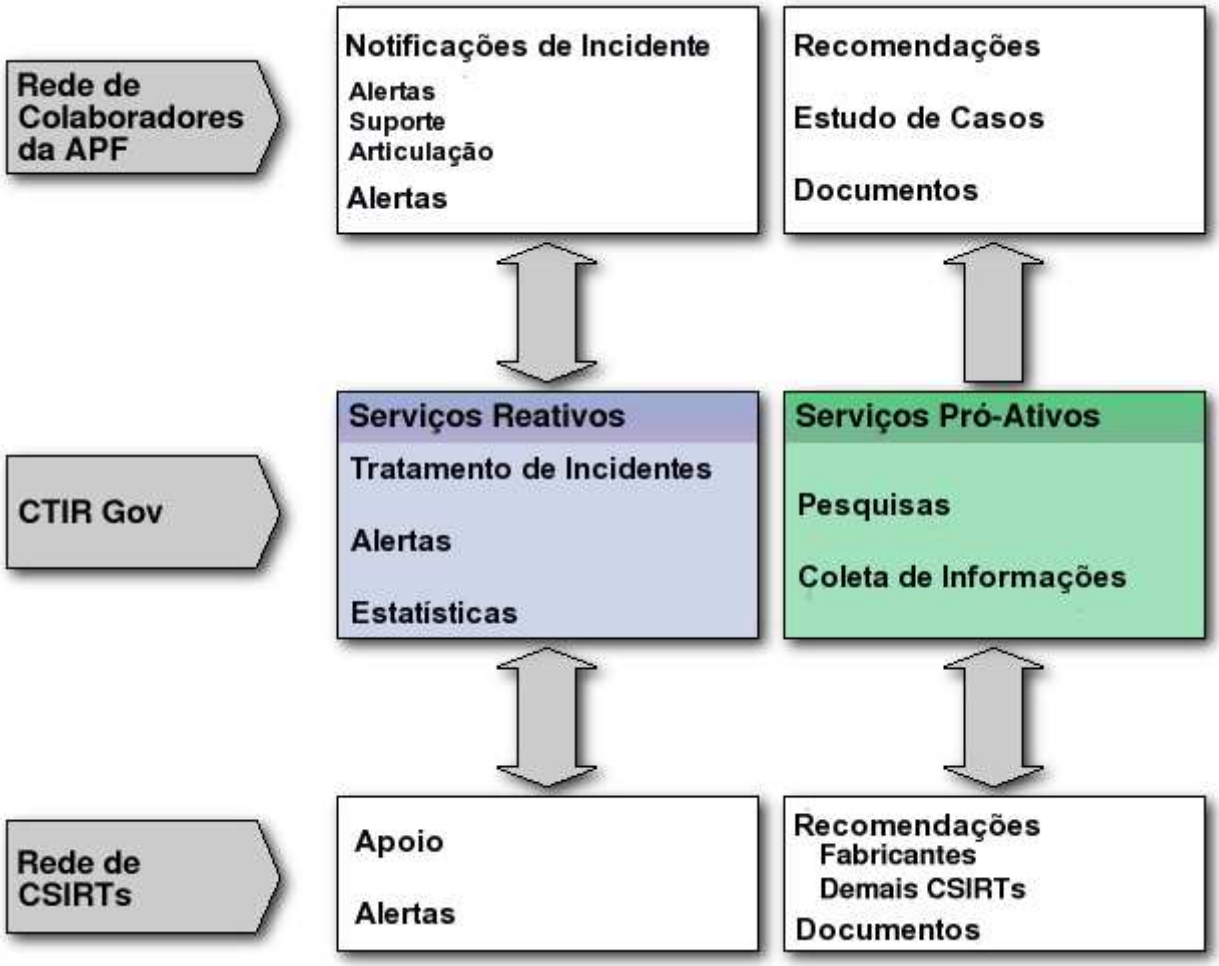

FIGURA 4 – Esquema de interações do CTIR Gov
Fonte: Sítio do CTIR Gov. Disponível em: <http://www.ctir.gov.br/sobre-CTIR-gov.html#interacoes>. Acesso em 25 jul. 2018.