UNIVERSIDADE DE BRASÍLIA
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO, CONTABILIDADE
E GESTÃO DE POLÍTICAS PÚBLICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM ECONOMIA
MESTRADO EM ECONOMIA

WASHINGTON RODRIGUES DA SILVA

ANÁLISE ECONÔMICA DOS IMPACTOS DE ATAQUES CIBERNÉTICOS

BRASÍLIA
2018

WASHINGTON RODRIGUES DA SILVA

ANÁLISE ECONÔMICA DOS IMPACTOS DE ATAQUES CIBERNÉTICOS

Dissertação apresentada à Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas no Programa de Pós-Graduação em Economia – FACE/PPGE, como requisito parcial para a obtenção do título de Mestre em Economia, área de concentração: Economia de Defesa sob orientação do Professor Dr. Jorge Madeira Nogueira.

BRASÍLIA

2018

FICHA CATALOGRÁFICA

Silva, Washington Rodrigues da

S586a Análise econômica dos impactos de ataques cibernéticos / Washington Rodrigues da Silva; orientador Jorge Madeira Nogueira. -- Brasília, 2018.

107 p. IL; (possui apêndice e anexo)

Dissertação (Mestrado - Mestrado em Economia) -- Universidade de Brasília, 2018.

1. Ataques cibernéticos. 2. Custos financeiros e econômicos. 3. Defesa. 4. Setor financeiro. I. Nogueira, Jorge Madeira, orient. II. Título.

WASHINGTON RODRIGUES DA SILVA

ANÁLISE ECONÔMICA DOS IMPACTOS DE ATAQUES CIBERNÉTICOS

Dissertação apresentada à Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas no Programa de Pós-Graduação em Economia – FACE/PPGE, como requisito parcial para a obtenção do título de Mestre em Economia, área de concentração: Economia de Defesa.

Brasília-DF, 30 de novembro de 2018.

APROVADA POR:

_____
Prof. Dr. Jorge Madeira Nogueira
Departamento de Economia – FACE – UnB

_____
Prof. Dr. Pedro Henrique Zuchi da Conceição
Departamento de Economia – FACE – UnB

_____
Prof. Dr. José Carneiro da Cunha Oliveira Neto
Departamento de Administração – FACE – UnB

_____
Prof. Dr. Helder de Barros Guimarães
Exército Brasileiro – Ministério da Defesa

Dedico este trabalho a todos que buscam, com esforço e honestidade, tornar o mundo melhor para a sua geração e as vindouras.

AGRADECIMENTOS

A Deus, pela perfeição a qual representa e pelos dons da vida e do livre arbítrio que nos concedeu.

A minha esposa e minha filha, Simone e Amanda, pela compreensão nos momentos dedicados ao estudo.

A minha mãe, “Dona Cici”, por haver feito tudo o que lhe foi possível para que seus filhos estudassem como meio de buscar uma vida melhor.

A meu avô Lucas, pelo apoio incondicional que sempre me deu e pelos ensinamentos de honestidade profissional que me foram transmitidos.

A meu estimado orientador Jorge Nogueira, por aceitar o desafio de realizarmos este trabalho, por sua paciência, apoio e orientação.

Aos professores da FACE/UNB, por compartilharem seus conhecimentos, sendo fundamentais para a realização do primeiro mestrado em Economia de Defesa do Brasil.

Aos estimados amigos Ricardo Férre, Ricardo Dondoni, Cel De La Vega, Robson Bezerra, Tony Moura, Carla Madsen e Rôber Yamashita pelas colaborações dadas durante a confecção desta dissertação.

Aos colegas de turma, pelos momentos de estudos que vivemos nos dois últimos anos.

E a todos que, de alguma forma, contribuíram para a realização deste trabalho.

“*Never, never, never give up*!”

Winston Churchill

SILVA, W. R. **Análise econômica dos impactos de ataques cibernéticos.** 2018. Dissertação (Mestrado em Economia) – Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da UNB, Brasília, 2018.

RESUMO

O uso do espaço cibernético cresce a cada dia, possibilitando acesso a milhões de usuários. Os ataques cibernéticos acompanham esse crescimento, apresentando-se como ameaça constante e mutável. Esses ataques comprometem a confidencialidade, integridade e/ou disponibilidade de dados, sistemas e serviços, com reflexos negativos em variados setores da economia. Objetivou-se estudar os impactos econômicos causados por ataques cibernéticos ao setor financeiro no Brasil. Foram utilizadas fontes secundárias de pesquisa bibliográfica. Identificou-se que os ataques cibernéticos são percebidos como prováveis e de elevado impacto. Eles possuem motivações diversas como, por exemplo, política e ideológica. Todavia, quando destinados ao setor financeiro, a maior parte dos ataques tem objetivo de ganhos monetários. Propôs-se a fórmula para calcular impactos causados por ataques cibernéticos direcionados ao setor financeiro. Essa considera os fatores levantados pelo diagrama de ciclo causal aplicado a ataques cibernéticos propostos por Lagazio, Sherif e Cushman (2014). Identificou-se, ainda, que o Brasil se encontra em nível intermediário de segurança cibernética, segundo critérios da União Internacional de Telecomunicações. Foi identificado também que a maior parte dos ataques cibernéticos sofridos no Brasil reportados ao CERT.br originam-se no próprio país, o que pode ser uma consequência da falta de leis específicas e sensação de impunidade pelos infratores. Concluiu-se que deve haver atuação do governo para combater a subnotificação de ataques sofridos. Nesse sentido, há necessidade de legislações específicas e fiscalização. Há tendência de crescimento de seguros para cobrir perdas por ataques cibernéticos no Brasil. Por fim, conclui-se que o tema apresenta amplo espaço para estudos futuros, sendo afeto a vários campos do conhecimento.

Palavras-chave: Ataques cibernéticos, custos financeiros e econômicos, Defesa, setor financeiro.

SILVA, W. R. **Economic analysis of the impacts of cyber-attacks.** 2018. Dissertation (master's degree in economics) – Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas da UNB, Brasília, 2018. Portuguese.

ABSTRACT

The use of cyberspace has grown every day, enabling access to millions of users. The cyber attacks have accompanied this growth with constant threat. These attacks compromise the confidentiality, integrity and/or availability of data, systems and services. These aspects have had negative reflections upon varied sectors of the economy. In this context, the objective of this study is to analyze economic impacts caused by cyber attacks to the financial sector in Brazil. Data from secondary sources were used. We have identified that cyber attacks are probable and generate high impact. They have various motivations, such as political and ideological. However, when intended for the financial sector, most of the attacks have monetary gains as their goal. We propose a formula to estimate impacts caused by cyber attacks directed to the financial sector. This formula considers the factors identified by the causal loop diagram applied to cyber attacks proposed by Lagazio, Sherif and Cushman (2014). It was emphasized that Brazil is in the intermediate level of cyber security, according to criteria of the International Telecommunications Union. It was identified that the majority of cyber attacks suffered in Brazil reported to the CERT.br originate from inside the country, which may be a consequence of the lack of specific laws to eliminate the impunity of offenders. As our main conclusion there should be action by the Government to combat underreporting of attacks. In this sense, there is a need for specific legislation and supervision, as well as a tendency of insurance diffusion to cover losses due to cyber attacks in Brazil. Finally, it is concluded that the theme offers ample room for future studies, with affection to various fields of knowledge.

Key words: Cyber attacks, financial and economic costs, Defense, financial sector.

LISTA DE TERMOS

TERMO	SIGNIFICADO
Backdoor	Código malicioso que se instala em um computador para permitir o acesso de um invasor.
Black-hat	Sinônimo de cracker.
Bot herder	Atacante que está no controle dos sistemas comprometidos (*bots*).
Botnet	Semelhante ao *backdoor*, com a diferença de que apenas um equipamento é capaz de controlar todas as máquinas infectadas simultaneamente.
Cavalo de Tróia	Programa malicioso que entra em sistemas simulando ser outro.
Cracker	*Hackers* que utilizam seus conhecimentos com fins ilícitos.
Hacker	Pessoa possuidora de grande habilidade em computação. Neste trabalho, o termo é utilizado, independentemente do fim a que essa pessoa utiliza seus conhecimentos.
Malware	Programa criado com fim de se infiltrar em sistemas computacionais de forma ilícita, para causar danos, alterações ou roubo de informações.
Phishing	Ataque que busca acesso, de forma fraudulenta, a informações financeiras ou pessoais, utilizando códigos eletrônicos maliciosos.
Ransomware	*Malware* que impede o acesso a arquivos digitais valiosos, com isso, os criminosos cobram um resgate para tornar os dados acessíveis novamente
Scrit kiddies	Sinônimo de cracker.
Software	É um conjunto de procedimentos lógicos que controlam as atividades de sistemas computacionais. São genericamente chamados de programas.
Spear phishing	*Phishing* destinado a alvos específicos.
Spyware	Programas capazes de subtrair informações de computadores e modificar suas configurações.
Stuxnet	*Malware* projetado especificamente para atacar os sistemas de automação industrial.
Trojan	Expressão em língua inglesa para o termo Cavalo de Tróia.
Vírus	Programas desenvolvidos para infectar sistemas computacionais que se autorreplicam e com capacidade de rápida propagação, necessitando de um sistema hospedeiro para sobreviver.
Worm	Semelhante ao vírus, com a diferença que não necessita de um hospedeiro para se replicar.

LISTA DE ABREVIATURAS

ABREVIATURA	SIGNIFICADO
BCB	Banco Central do Brasil
CDCiber	Centro de Defesa Cibernética
CERT.br	Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil
ComDCiber	Comando de Defesa Cibernética
ICS	Industrial *Control Systems* (Sistemas de Controle Industrial)
ICS-CERT	*Industrial Control Systems Cyber Emergency Response Team* (Equipe de Resposta a Emergências Cibernéticas e Sistemas de Controle Industrial dos Estados Unidos da América)
DSIC/GSI-PR	Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República
END	Estratégia Nacional de Defesa
ENaDCiber	Escola Nacional de Defesa Cibernética
FBI	*Federal Bureau of Investigation*
£	Libra esterlina
MD	Ministério da Defesa do Brasil
NCCIC	*National Cybersecurity and Communications Integration Center's* (Centro de Integração Nacional de Segurança Cibernética e Comunicações dos Estados Unidos da América)
NCSC	*National Cyber Security Centre* (Centro Nacional de Segurança Cibernética da União Européia)
R$	Real brasileiro
SCADA	*Supervisory Control and Data Acquisition*
SCEA	*Sony Computer Entertainment American*
SIMOC	Simulador de Operações de Guerra Cibernética
TIC	Tecnologia da Informação e Comunicação
US$	Dólar americano

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS

SUMÁRIO

CONSIDERAÇÕES INICIAIS

A criação dos computadores, em meados do século XX, elevou a capacidade de processamento e proporcionou benefícios como aumento da capacidade produtiva em variados setores da economia.

A partir do início do século XXI, além da informatização, que possibilitou a automatização de diversos processos industriais, houve a facilitação do acesso à rede mundial de computadores (internet) ao público em geral, em razão da ampliação de empresas de telecomunicações e da redução de preço dos dispositivos finais (computadores, *tablets*, *smartphones*, entre outros).

As facilidades proporcionadas pelos sistemas de tecnologia da informação e comunicação (TIC) (o que inclui a internet) trouxeram consigo oportunidades para pessoas, instituições e até governos explorarem um novo ambiente, chamado espaço cibernético, para usos benéficos ou prejudiciais. Atualmente, o mundo apresenta crescente dependência de sistemas de TIC.

Barreto (2007) aponta que a TIC desempenha papel crítico na gestão e operação de sistemas, como os de telecomunicações, geração e distribuição de energia, controle aéreo, instituições financeiras, defesa, logística e abastecimento de bens, água e alimentos. Ademais, as novas TIC trouxeram desafios e efeitos negativos. Por exemplo, por meio delas, criaram-se possibilidades de explorações para fins de crimes financeiros, espionagem industrial e até ataques entre Nações.

Nesse cenário, governos e instituições de diversos países passaram a tomar providências para se protegerem. Como o resto do mundo, o Brasil tem, diante de si, semelhantes desafios. Como destacam Cashell et al. (2004), o mundo moderno apresenta níveis significativos de dependência dos sistemas computacionais. De maneira que, se houvesse sua parada, por qualquer razão, praticamente todos os setores seriam afetados, desde os produtivos (como fabris, logísticos, etc), passando pelo comércio e até serviços públicos vitais, como defesa nacional e saúde.

Ainda segundo Cashell et al. (2004), há a concepção de que a segurança da informação é um tema crítico de política nacional. Dois fatores indicam o crescimento da importância do assunto. O primeiro é que a integração de sistemas é crescente e abarca diversas áreas. O segundo é que o número de ataques cibernéticos (violações de segurança) aumenta a cada dia e seus danos crescem de maneira imprevisível.

A temática do espaço cibernético e da sua capacidade de permear por variados setores, benefícios, vulnerabilidades, assim como sua defesa apresenta vasto espaço

para exploração. E, por sua importância, são cada vez mais discutidos nos meios empresariais, governamentais e acadêmicos.

Do exposto, levantou-se a seguinte problemática: quais são os impactos econômicos de ataques cibernéticos? Em virtude da elevada amplitude do tema, buscou-se delimitar o estudo ao setor financeiro. Assim, o objetivo central desta dissertação é estudar os impactos econômicos que ataques cibernéticos causam quando são destinados contra alvos do setor financeiro.

O presente trabalho faz-se relevante por apresentar um estudo das dimensões econômicas de ameaças cibernéticas e destacar quão importante é a atuação, tanto do Estado, por meio de políticas públicas, quanto do setor privado para prevenir, ou mesmo, reduzir os efeitos negativos decorrentes de ataques cibernéticos em áreas que são fundamentais para o funcionamento saudável da economia.

A fim de conduzir o estudo de maneira lógica e facilitar a compreensão, adotou-se a sequência de abordagem tratando do amplo para o específico, dessa forma, a dissertação foi dividida em 5 (cinco) seções, além destas considerações iniciais e das conclusões.

A primeira seção trata sobre ameaças cibernéticas. Nela é feita uma explicitação sobre o espaço cibernético e suas definições, são apresentados os tipos de ameaças encontrados atualmente e explicado dentro da classificação de ataques contra a confidencialidade, integridade e disponibilidade.

A segunda seção aborda as dimensões econômicas de ataques cibernéticos que são de conhecimento público. Ela apresenta casos práticos de ataques contra a confidencialidade, integridade e disponibilidade, os quais exemplificam como estes podem criar transtornos à estabilidade dos entes econômicos, como fornecedores, compradores, agentes financeiros, órgãos governamentais ou mesmo, o cidadão comum. Ao final, é exposto, por meio de um quadro, um resumo dos tipos de ataques cibernéticos e suas possíveis consequências.

A terceira seção trata, especificamente, sobre as consequências de ataques cibernéticos ao setor financeiro. A delimitação do estudo ocorreu nesse setor, onde são feitas aproximações, estimando-se os prejuízos causados por ataques cibernéticos. Tal escolha deu-se por entender que esse setor é fundamental para a economia como um todo.

A quarta seção aborda como outros países estão enfrentando o atual cenário de ataques cibernéticos e quais estruturas foram criadas para tal. Em seguida, na

quinta seção, há semelhante abordagem sobre como o Brasil está nesse cenário, apresentando o passado, presente e prospecções do futuro em relação ao setor financeiro e o espaço cibernético.

Metodologicamente, para o desenvolvimento desta investigação, utilizou-se dados de fontes secundárias, obtidos por meio de uma pesquisa bibliográfica aplicada. Buscaram-se dados e informações em livros especializados e artigos científicos em Economia e Tecnologia da Informação, além de sítios de instituições oficiais, tais como os brasileiros Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Federação Brasileira de Bancos (FEBRABAN), Banco Central do Brasil (BCB), Exército Brasileiro e Ministério da Defesa; os estadunidenses *Federal Bureau of Investigation* (FBI), *The Council of Economic Advisers* (CEA), *National Cybersecurity and Communications Integration Center's* (NCCIC), Organização dos Estados Americanos (OEA), os britânicos *Action Fraud, National Cyber Security Centre* (NCSC) e o *UK Cabinet Office*, a página do Escritório do Primeiro Ministro da Austrália e da União Internacional de Telecomunicações (ITU), com sede na Suíça. A esses foram adicionadas consultas a portais de jornais de grande circulação no Brasil como a Folha de São Paulo, G1, Valor Econômico, Correio Braziliense e jornais internacionais como o Europress-Reuters e The New York Times.

No intento de estimar os prejuízos causados por ataques cibernéticos ao setor financeiro, utilizaram-se os documentos pesquisados, assim como notícias divulgadas nos sítios de jornais, buscando dados sobre perdas de empesas do setor. Em seguida, relacionou-se quais foram os tipos de perdas e como essas fazem parte da composição do impacto causado pelos ataques cibernéticos. Por fim, foi proposta a fórmula para estimar o referido impacto ao setor financeiro.

Ademais, a pesquisa por fontes incluiu conteúdos redigidos em língua portuguesa, inglesa e espanhola, publicadas a partir do ano 2002, dando-se preferência a publicações recentes, principalmente a partir de 2013. Dessas, a maior parte das fontes de referências obtidas fora do Brasil é oriunda dos Estados Unidos da América, país onde foram encontrados os estudos disponíveis em maior número. Em seguida, fontes do Reino Unido, Austrália, Argentina e Peru.

1 AMEAÇAS CIBERNÉTICAS: suas inúmeras dimensões

1.1 O espaço cibernético

O surgimento da internet foi o primeiro passo para o atingimento do grau de compartilhamento de informações vivenciados atualmente. Impressiona ao observador contemporâneo a velocidade com que os dados fluem até chegarem a seus destinatários. Meios de comunicações, hospitais, hidrelétricas, bancos, escolas, comércio, indústrias, governos, enfim, praticamente todos os setores têm algum nível de dependência dos sistemas de TIC.

Nesse contexto, surge uma nova dimensão, o espaço cibernético. Esse espaço apresenta, segundo Oliveira et al. (2017), três características: a primeira é que se encontra em uma dimensão intangível e abstrata; a segunda refere-se a ser considerado importante desde o início de sua existência; e a terceira é de ser transversal, esta última em consonância com Ventre (2011), o qual adiciona que o espaço cibernético permeia todos os espaços geográficos, permitindo controlar desde satélites e radares marítimos até metrôs em grandes cidades, assim, as ações geradas no campo virtual são capazes de criar consequências no mundo real.

O espaço cibernético e a internet apresentam semelhanças, contudo eles são fenômenos distintos, apesar de haver discordância sobre suas diferenças e semelhanças. Cebrowski (2004) afirma que o espaço cibernético é maior do que a internet. Autores como Carvalho (2011) e Oliveira et al. (2017) concordam com essa concepção e incluem que o espaço cibernético é composto por dispositivos computacionais, conectados em redes ou não, com trânsito ou armazenamento de informações. Há, ainda, autores que incluem os usuários na composição do espaço cibernético, como é o caso de Klimburg (2012), ao afirmar que “o espaço cibernético é mais que internet, inclui não somente *hardware*, *software* e sistemas informacionais, mas também pessoas e suas interações sociais nas redes de computadores”[1].

Vale destacar que os *hardwares* tratados por Klimburg não são apenas computadores e sim todos dispositivos com capacidade de processamento ou armazenamento, direta ou indiretamente e conectáveis a redes. Dessa forma, os *hardwares* incluem televisores (*smart tv*), decodificadores de canais por assinatura, *smatphones,* impressoras, *tablets*, relógios inteligentes, equipamentos controlados

[1] Neste estudo, adotou-se a definição de espaço cibernético de Klimburg, por entender que as ações realizadas pelos usuários influenciam diretamente no mesmo. Ademais, o espaço cibernético não faria sentido sem o fator humano, pois não seria possível sua existência.

por meio de automação, especialmente nos dias atuais em que a chamada “Internet das Coisas”[2] é um tema que cresce de importância.

1.2 Tipos e instrumentos de ameaças no espaço cibernético

As principais ameaças aos usuários do meio digital são os ataques cibernéticos. Klinburg (2012) afirma que o termo ataque cibernético não é internacionalmente definido, havendo diferenças substanciais entre a definição do governo estadunidense e de outros países. A definição mais genérica de ataque cibernético é a que afirma tratar-se de uma tentativa maliciosa premeditada de ataque para quebrar a confidencialidade, integridade ou disponibilidade de informações existentes em computadores ou redes computacionais. Vianna e Fernandes (2015) definem ataques cibernéticos, de forma simplificada, como ações cibernéticas hostis. Nessa óptica, os ataques podem ocorrer por ações intencionais ou involuntárias, os quais serão exemplificados posteriormente neste trabalho.

A definição genérica de Klinburg (2012) de ataques cibernéticos põe como seus principais objetivos, comprometer os princípios da segurança da informação (confidencialidade, integridade e disponibilidade). Na prática, o comprometimento de confidencialidade significa que o atacante pode obter acesso a dados que lhe são negados. Quanto a alterar a integridade, entende-se que o atacante consegue obter meios de modificar dados da vítima. Por fim, a afirmação de que um atacante cibernético obtém êxito sobre a disponibilidade significa que ele é capaz de tornar dados, informações e equipamentos indisponíveis a seus usuários legítimos por meio de ações cibernéticas.

O governo dos Estados Unidos da América (EUA) trata ataques cibernéticos como “atividade cibernética maliciosa” e as definem da seguinte forma:

> Atividade cibernética maliciosa é qualquer atividade, desautorizada ou em desacordo com a lei dos EUA, que busca comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de computadores, sistemas de informação ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informação, ou as informações nele contidos (CEA, 2018, p. 2).

Já o Ministério da Defesa (MD) do Brasil entende como ataque cibernético quaisquer “ações que objetivam interromper, negar, degradar, corromper ou destruir

[2] Atzori et al. (2010) afirmam que a ideia básica de “Internet das Coisas”, ou como é conhecido em inglês “*Internet of Things*” (*IoT*), é que objetos dotados de sensores sejam capazes de interagir com o ambiente e trocarem informações entre si, cooperando mutuamente para realizarem uma atividade que lhes fora programada como objetivo.

informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente" (BRASIL, 2014a, p. 23).

Os agentes cibernéticos são classificados de acordo com os fins de suas atuações. O termo *hacker*, bastante utilizado cotidianamente como uma generalização de usuários criminosos, não significa exatamente isso. Ramalho Terceiro (2002) aponta *hacker*[3], genericamente, como alguém possuidor de grande habilidade em computação. Já os *crackers, black-hats* ou *scrit kiddies* são *hackers* que utilizam seus conhecimentos para atacar computadores. Dessa forma, *hackers* podem utilizar seus conhecimentos para análise de vulnerabilidades e, inclusive, trabalhar em parcerias com empresas de segurança cibernética. Já os *crackers* são os verdadeiros criminosos, pois utilizam seus potenciais cognitivos para cometerem atos ilícitos.

Raposo (2007) destaca a existência de um grupo formado por *hackers* com motivações políticas ou religiosas, contratados por extremistas com o objetivo de realizarem ataques para geração de pânico, mortes, acidentes, contaminação ambiental ou perdas econômicas. Esses *hackers* são denominados de terroristas cibernéticos[4]. *The Council of Economic Advisers* (CEA), um órgão do governo estadunidense, ratifica esse conceito classificando esses indivíduos que efetuam ataques cibernéticos por razões ideológicas como hacktivistas (CEA, 2018).

Além dos terroristas cibernéticos, Moresi et al. (2012) afirmam que há mais três categorias de infratores: os ciberdelinquentes, os cibercriminosos e os ciberespiões. Essas denominações são dadas pela finalidade dos ataques realizados. Há, segundo Moresi et al. (2012), casos documentados de associação entre eles, visando benefícios mútuos, onde ciberterroristas contrataram cibercriminosos para roubar informações de cartão de crédito e apoiar traficantes de drogas, todos com o objetivo de financiar operações terroristas tradicionais. CEA (2018) afirma que diversas fontes do governo dos EUA, inclusive o Pentágono, apontam o governo da China como um grande ator governamental responsável por ataques cibernéticos contra setores públicos e privados norte-americanos.

Há diversas formas com as quais os atacantes cibernéticos podem buscar seus objetivos. Caldas (2016) afirma que parte considerável das ações criminosas em

---

[3] Este parágrafo explicou o conceito *hacker* e *cracker* esclarecendo que não são exatamente o mesmo. A partir deste momento, ambos serão tratados indistintamente com o sentido de *crackers*, especialmente por haver tal indistinção em grande parte das literaturas utilizadas como referência neste trabalho.

[4] Também chamados de cyber-terroristas, ciberterroristas ou racktivistas.

redes computacionais são praticadas com uso de *softwares* maliciosos, conhecidos por *malwares* e os define como programas criados com a intenção de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações.

Um dos elementos usualmente presentes em ataques cibernéticos são os *vírus*. Sikorski e Honing (2012) apresentam vírus e *worms* como tipos de *malwares*[5] e Easttom (2016) afirma que, por definição, os vírus são programas que se autorreplicam e possuem capacidade de rápida propagação. Já Gaspar (2007) explica que os vírus são partes de códigos maliciosos desenvolvidos para infectar sistemas computacionais. O vírus de computador, análogo ao vírus biológico, infecta o sistema, cria cópia de si mesmo e tenta se espalhar para outros computadores (organismos). No entanto, ele necessita de uma aplicação hospedeira para se replicar e infectar outros sistemas.

Outra ferramenta de ataque cibernético são os vermes, conhecidos no meio cibernético como *worms*. Gaspar (2007) diferencia os *worms* dos vírus pois não necessitam de um portador para se replicarem. Eles se autorreplicam, espalhando-se de um computador para outro podendo, inclusive, conter vírus para infectar os sistemas. Os vermes exploram as vulnerabilidades e utilizam quaisquer mecanismos para se propagarem como, por exemplo, e-mails, serviços de internet, compartilhamento de arquivos, mídias removíveis, entre outros.

Por vezes, nos deparamos com a expressão Cavalo de Tróia[6]. Ela se refere a programas de finalidades gerais que trazem consigo outro, oculto, com capacidades nocivas ao recebedor (usuário), sua classificação como Cavalo de Tróia é uma alusão à clássica história grega Ilíada[7], de autoria de Homero. Segundo Gaspar (2007), Cavalos de Tróia são programas maliciosos que entram no sistema simulando ser outros, aparentemente inofensivos para o usuário e supostamente úteis, entretanto possibilitam a criação de brechas de segurança para outras formas de ataques, abrindo portas para permitir que o invasor controle remotamente as máquinas contaminadas. Eles não se propagam sendo, assim, distintos dos vírus e vermes.

---

[5] Além desses, os autores incluem como tipos de *malwares: backdoor, botnets, downloader, information-stealing, launcher, rootkit, shareware, spam-sending*.

[6] Também conhecidos como *trojan horse* ou, simplesmente, *trojan*.

[7] Livro disponível na versão em língua portuguesa. Editora Penguin e Companhia das Letras, tradução Frederico Loureço, 1ed., São Paulo: 2013. ISBN 9788563560568.

Os *backdoors*, segundo Sikorski e Honing (2012), são códigos maliciosos que se instalam em um computador para permitir o acesso de um invasor. Normalmente, permitem ao atacante se conectar a um computador com pouca ou nenhuma autenticação e executar comandos no seu sistema. Os *botnets,* ainda segundo Sikorski e Honing (2012), são similares aos *backdoors* quanto à capacidade de permitir ao atacante acessar o sistema. Entretanto, os *botnets* permitem que todas as máquinas infectadas com o mesmo *botnet* recebam as mesmas instruções do um único servidor de comando e controle, ou seja, uma única máquina atacante comanda todas as infectadas com comando único.

Somando-se aos *malwares*, Gaspar (2007) destaca a existência de outro tipo de ameaça, os *spywares*. Estes foram criados, inicialmente, com fins comerciais, para monitorar o comportamento de usuários da internet, sem seus consentimentos, permitindo a venda dessas informações. Atualmente, os *spywares* têm sido utilizados para subtrair informações financeiras e alterar as configurações do computador, instalando outros tipos de *softwares* ou redirecionando o tráfego *web* para *sites* com propagandas.

Segundo Pais, Moreira e Varajão (2013), os *spywares* podem ser instalados em um computador por meio de *trojans,* ao acessar sites com aplicações capazes de explorar vulnerabilidades de navegadores de internet. Podem, ainda, ser instalados por meio de *shareware* e *freeware*[8], em que o *spyware* está incluído na aplicação de instalação do *software*. E, ainda, segundo os autores, os *spywares* podem ser instalados com ou sem consentimento do usuário, podem disponibilizar ou não o tipo de informação que coleta, bem como a sua finalidade.

Para Gaspar (2007), o *spyware* era, à época, a ameaça mais preeminente da internet e representava uma grande fatia dos crimes cibernéticos, sendo utilizado por *crackers*, em conjunto com *malwares*, para invadir computadores, roubar dados financeiros e pessoais dos usuários, obter informações sensíveis das empresas, entre outros.

---

[8] *Sharewares* e *freewares* são programas que possuem algum tipo de restrição. Leister e Christophersen (2012) indicam que os *sharewares* são desenvolvidos por entusiastas que comercializam seus programas. Tais programas podem ser usados gratuitamente por um período de avaliação, mas estão sujeitos ao pagamento posterior de uma taxa, caso o usuário ainda deseje utilizá-los. Já os *freewares* são *softwares* podem ser usados sem custos. No entanto, desde que o código fonte não esteja livremente disponível. Os autores de *freewares* normalmente restringem um ou mais direitos para copiar, distribuir e fazer trabalhos derivados dos *softwares*. As licenças desses *softwares* podem impor restrições sobre o tipo de uso, por exemplo, uso pessoal, individual, sem fins lucrativos, não comercial ou acadêmico.

Segundo o FBI (2018), outro tipo de ataque que se encontra entre os mais incidentes, atualmente, é o *ransomware*[9]. Segundo o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), esse consiste em um tipo de *malware* que impede o acesso a arquivos digitais valiosos, com isso, os criminosos cobram um resgate para tornar os dados acessíveis novamente (CERT.br, 2018a). O *ransomware* pode gerar perdas que vão desde fotos com algum valor sentimental a fortunas em segredos industriais e pesquisas de elevada complexidade de setores de tecnologia, o que, por vezes, induz ao atacado pagar pelo resgate para evitar maiores prejuízos.

Como, na definição aqui adotada, o ser humano é parte do espaço cibernético, suas vulnerabilidades devem ser consideradas. Sobre esse tema, Singer e Friedman (2014) afirmam que é justamente o fator mais débil, pois permite várias formas de ataques em razão de procedimentos inadequados.

Uma das possíveis formas de atuação sobre os usuários é a Engenharia Social. Em relação a isso, Mitnick e Simon (2002) dizem que a Engenharia Social usa a capacidade de pessoas de influenciar e persuadir para enganar a terceiros, convencendo-os que são confiáveis e obtendo, assim, informações, com ou sem o uso de tecnologia. Essas informações, obtidas pelo engenheiro social, são a porta de entrada para alguém desautorizado obter informações sobre a rede ou o sistema de uma organização.

Para Pais, Moreira e Varajão (2013), a maior fonte de risco para a segurança são as vulnerabilidades dos indivíduos que compõem uma organização visada. Em razão da simplicidade e engenho, a Engenharia Social é a maneira mais fácil e eficaz de um atacante superar os obstáculos impostos pelos sistemas de segurança. Os autores adicionam que há níveis de preocupação e medidas que robustecem os sistemas de defesa cibernética. Entretanto a parte humana, por eles chamada de “social”, da segurança tem sido deixada para traz como se não fosse essencial para o processo de proteção dos sistemas de informação.

Outro tipo de ataque é o *phishing*. Este é definido por Pais, Moreira e Varajão (2013), como um ataque que busca obter acesso, de forma fraudulenta, a informações financeiras ou pessoais. São normalmente iniciados por e-mail, chamadas telefônicas ou mensagens instantâneas (em redes sociais na internet, como *Facebook*,

[9] Segundo o CERT.br (2018a), existem dois tipos de *ransomware:* o *locker*, que impede o acesso ao equipamento infectado; e o *crypto*, que impede o acesso aos dados armazenados no equipamento.

aplicações de *smartphones*, como *Whatsapp*, ou mesmo por mensagens de texto de telefones celulares, por meio de SMS[10]). Ainda, segundo o Pais, Moreira e Varajão (2013), a diferença entre *phishing* e Engenharia Social é tênue e na maioria das vezes cruzam-se. O *phishing*, em geral, realiza ataques maciços buscando dados de usuários indistintamente.

Pais, Moreira e Varajão (2013) apontam que o *phishing* apresenta variações, a depender de como atua. Uma delas é o *spear phishing*, que muda do *phishing* tradicional por ser direcionado a vítimas específicas e do tipo de conteúdo que coleta, que são dados de acesso aos sistemas de informação aos quais as vítimas utilizam, sendo assim, mais perigosos por buscar ganhos econômicos, dados classificados, como segredos industriais ou informações militares.

Uma pessoa pode comprometer a segurança cibernética involuntariamente, por desconhecimento, realizando atos como conectar mídias móveis em equipamentos infectados ou clicando em *links* maliciosos recebidos por e-mails ou mensagens de aplicações de *smartphones,* contraindo vírus.

Oppermann (2013) reforça a ideia de que até usuários frequentes da internet e sabedores da existência de *malwares* cometem erros primários como clicar em links desconhecidos em rede sociais, e-mails ou em mensagens recebidas em aplicativos de conversação em *smartphones*. Tais atos podem entregar um computador[11] em casa, no trabalho ou na escola a um *bot herder*[12] ou a outro tipo de criminoso cibernético e acabar como um componente em um sistema de amplitude nacional de fraudes bancárias *on-line* ou um conflito internacional em qualquer parte do planeta.

1.3 Ataques cibernéticos contra a confidencialidade

Os ataques cibernéticos contra a confidencialidade possuem, em geral, o objetivo de conceder, ao atacante, acesso a dados que lhes são negados. Os ataques podem possuir fins diversos, como inteligência, espionagem industrial, espionagem governamental ou, simplesmente, testar vulnerabilidade de sistemas.

A preocupação com a manutenção da confidencialidade de dados computacionais é crescente. Novas tecnologias de armazenamento surgem com

---

[10] SMS é a abreviatura do termo em inglês *Short Message Service,* que são mensagens curtas enviadas por telefones celulares. Este serviço é oferecido por empresas de telefonia móvel em geral.

[11] Nesse caso, computador poderia ser qualquer máquina de usuário (*host*), como um *tablet* ou *smartphone*.

[12] *Bot herder*, segundo Ianelli e Hackworth (2007), refere-se ao atacante que está no controle dos sistemas comprometidos (*bots*).

relativa velocidade como, por exemplo, a de armazenamentos em nuvem[13] que, por sua praticidade[14], é cada dia mais utilizada como meio principal de armazenamento e para *backup*. Assim, tanto os dados armazenados localmente, quanto em unidades remotas são passíveis de tentativas de ataques.

Barreto (2007) afirma que ataques cibernéticos podem ser gerados por atacantes individuais ou por grupos, coordenados, especializados, com recursos materiais e financeiros expressivos e com disponibilidade de tempo e conhecimento. Denomina-se tais grupos de terroristas cibernéticos. Apesar dos terroristas cibernéticos apresentarem potencial ofensivo muito maior, os *hackers* individuais, não patrocinados, mas possuidores de talento com os computadores, não devem ser desconsiderados.

Vianna e Fernandes (2015) destacam que países como Brasil, EUA e Alemanha foram expostos a ações de vigilância e espionagem cibernética, comprometendo a privacidade de pessoas e organizações e, quiçá, até as soberanias dessas nações. Esses não são os únicos, ataques cibernéticos com o fim de espionagem ocorrem em todas as regiões houver conteúdos passíveis de gerar algum benefício, seja financeiro, político ou outro qualquer.

Ainda segundo Vianna e Fernandes (2015), em 2013, a situação conhecida como caso Snowden[15] foi um marco emblemático por revelar a atuação do governo dos EUA em espionagem de dados, dentro e fora do seu território. Nesse sentido foi exposto como o governo estadunidense obtinha acesso a e-mails e outros arquivos eletrônicos de usuários, por meio de empresas como Google, Microsoft e Facebook.

---

[13] Armazenamento em nuvem é um tipo de serviço em que dados computacionais são enviados de dispositivos finais como, por exemplo, computadores e smartphones, por meio da internet, a dispositivos de armazenamento remotos, podendo ser utilizado pelo usuário quando seu dispositivo final estiver conectado à internet.

[14] Segundo Rodrigues (2014), os sistemas de armazenamento em nuvem são atrativos, por permitirem opções de acesso, recuperação e armazenamento de arquivos de qualquer lugar e a qualquer hora.

[15] Segundo Pilati e Olivo (2014), o caso Snowden foi como ficou mundialmente conhecido o evento de divulgação de denúncias, com provas, de que o governo dos EUA coletava informações de dados eletrônicos de pessoas, órgãos e governos em todo mundo. Tais denúncias foram realizadas, em 2013, por Edward Snowden, um ex-funcionário da National Security Agency (NSA). Estima-se que Snowden fez cópias (*downloads*), enquanto trabalhava na NSA, de cerca de 1,7 milhões de documentos. Em entrevistas a periódicos de grande circulação (o britânico, The Guardian e o norte-americano, The Washington Post), Snowden apresentou provas de que a NSA monitorava milhares de telefones e dados de usuários conectados nos EUA e no exterior, inclusive de autoridades como a chanceler alemã Angela Merkel e Dilma Rousseff, então presidente do Brasil, com acessos a servidores de empresas como Google, Facebook, Skype e Apple. Tais denúncias criaram elevada repercussão, tanto por meio da imprensa mundial, quanto de representantes de governos, como os da Alemanha e do Brasil.

Dentre esses, estavam a Presidência da República Federativa do Brasil e empresas como a Petrobras.

O peso dos ataques contra confidencialidade tem mais relação com a importância da informação obtida do que com os sistemas computacionais. Assim, a perda da confidencialidade pode gerar instabilidades diplomáticas, como ocorreu no caso Snowden entre o governo dos EUA e os dos países por eles espionados.

A quebra de sigilo sobre conhecimentos restritos, como propriedade intelectual, projetos, tecnologias, *know how* e afins é a maior ameaça para os setores industriais, acadêmicos e de pesquisa, desenvolvimento e inovação (P&DI). Esses são os setores em que a informação possibilita a criação de riquezas de elevado valor agregado. Soma-se a isso, o interesse dos concorrentes em descobrir os diferenciais dos demais atores envolvidos. Por essa razão, ataques cibernéticos contra a confidencialidade são preocupações constantes nesses meios.

É comum haver elevados níveis de precauções como estabelecimentos de estruturas de segurança, *softwares* preventivos como antivírus e *antispywares* nos ambientes de desenvolvimento de P&DI. Mas não apenas a proteção lógica deve ser considerada. O caso Snowden é um exemplo de que o elemento humano, fisicamente tem um potencial de acesso a sistemas que não pode ser descartado, pelo contrário, não pode deixar de haver proteções contra os chamados ataques físicos, ou seja, em que alguém, presencialmente, acessa a informações constantes em sistemas de armazenamento computacionais.

Martins e Santos (2005) destacam que no aspecto segurança física, áreas críticas como servidores só devem ser acessadas por pessoas autorizadas e, ainda assim, sob controle de entrada e saída, tanto de pessoas quanto de equipamentos. Recomendando-se a criação de normatizações de controles internos referente ao assunto, os quais devem sofrer auditoria periodicamente.

Percebe-se que se houvesse o impedimento de Snowden sair do seu ambiente de trabalho, com mídias de armazenamento, o mesmo não lograria êxito em divulgar as informações coletadas pela NSA. De qualquer forma, quando se trata de confidencialidade, a seleção de recurso humano é fundamental. Se esse não mantiver a confidencialidade dos dados, qualquer sistema de proteção de dados torna-se vulnerável.

Outros dois ataques cibernéticos que chamaram a atenção devido a falhas humanas, que vieram a corromper a confidencialidade são destacados por Singer e

Friedman (2014). O primeiro caso citado pelos autores remota a 2008, quando um soldado dos EUA que passava por um estacionamento fora de uma base militar norte-americana no Oriente Médio encontrou um *pendrive*. Esse soldado inseriu o achado em um computador que estava conectado à rede militar de Comando Central americana e desencadeou uma das maiores brechas cibernéticas da história militar dos EUA, conhecida como *Buckshot Yankee*. Essa falha levou ao escaneamento de computadores da rede militar, a abertura de diversas portas de saída de dados e levou cerca de quatorze meses para ser sanada completamente pelo Pentágono.

O segundo caso destacado por Singer e Fiedman (2014) foi o de um executivo de uma companhia de Tecnologia da Informação que encontrou um CD que continha *malware* no banheiro masculino e resolveu verificar o conteúdo do referido disco. Desavisadamente, o executivo compartilhou projetos da aviônica do helicóptero presidencial norte-americano com *hackers* iranianos.

CEA (2018) destaca, ainda, a atuação de Estados, como China, Rússia, Coreia do Norte e Irã, no campo da espionagem cibernética, especialmente, direcionados aos EUA. Nesse aspecto, CEA (2018) lista uma série de empresas atacadas nos Estados Unidos em 2014 como, por exemplo, Westinghouse Electric Company, SolarWorld e Allegheny Technologies Inc*,* sendo a primeira vez que o governo dos EUA acusou autoridades estrangeiras de crimes de espionagem cibernética.

1.4 Ataques cibernéticos contra a integridade

Machado et al. (2016) destacam que o objetivo da integridade, em segurança cibernética, é a proteção contra modificação imprópria ou destruição de informação, incluindo a garantia de autenticidade das informações. Assim, a perda de integridade ocorre com a modificação ou destruição de informações de forma não autorizada. Ataques contra a integridade ocorrem, em geral, como atividade meio não como um fim. Ao modificar algum dado, o atacante, normalmente, busca inserir algum *backdoor* para coletar informações, ou ainda, modificar a configuração de sistemas de automação para danificar ou obter controle das máquinas por eles controladas.

Podem haver ataques contra a integridade em que o atacante modifique dados existentes e essas modificações criem benefícios indevidos para alguém. Por exemplo, em um sistema financeiro haver, eletronicamente, a modificação do número da conta bancária de destino de pagamentos ou transferências.

1.5 Ataques cibernéticos contra a disponibilidade

Machado et al. (2016) afirmam que a disponibilidade visa garantir o acesso sempre que necessário. Ou seja, o ataque cibernético contra a disponibilidade ocorre quando impossibilita o acesso a um sistema de informação, o uso de dados nele contido ou o torna inoperante. O uso crescente de automatização de sistemas é notório em diversas áreas, como indústrias, usinas de geração de energia, sistemas de vigilância e monitoramento remoto, entre outros. Nesses setores, a inoperância dos sistemas controladores pode indisponibilizar linhas de produção, câmeras de vigilância e até motores de turbinas responsáveis por geração elétrica. Muitos sistemas controladores são informatizados, ou seja, passíveis de sofrer ataques cibernéticos.

Ataques cibernéticos contra sistemas controladores de processos produtivos já ocorreram. Um caso conhecido é o *Stuxnet,* em que um *malware* foi utilizado para atuar sobre os computadores que controlavam centrífugas de uma usina de enriquecimento de urânio, tornando o processo produtivo dessa usina inoperante. Esse caso será tratado com maiores detalhes na seção 2.4.

Outro setor que é alvo de constante ameaça de perda de disponibilidade é o comercial. Grande parte dos sistemas de vendas é informatizado. Redes de varejo estão passíveis a prejuízos em volumes elevados se seus computadores ou servidores tornarem-se indisponíveis, assim como pequenas empresas podem tê-los, em razões percentuais consideráveis.

Não apenas as vendas são afetadas com possíveis indisponibilidades causadas por ataques cibernéticos, setores relacionados a serviços também são dependentes dos meios informacionais como, por exemplo, o sistema financeiro, assim como empresas de telecomunicações de diversas plataformas e serviços *on-line* em geral como provedores de internet, de vídeos por *streaming* e instituições de ensino a distância.

Finalmente, setores relacionados à gestão de mobilidade como o controle de trafego aéreo, trânsito e linhas férreas são exemplos de áreas em que ataques cibernéticos causadores de indisponibilidade dos sistemas computacionais são capazes de criar transtornos de elevadas magnitudes, tanto para os cidadãos comuns, quanto para empresas e governos, afetando, direta ou indiretamente, a economia da área atacada.

2 ATAQUES CIBERNÉTICOS: dimensões econômicas

2.1 A difícil transição do qualitativo para o quantitativo

Tratar economicamente aspectos relacionados a ataques cibernéticos não é tarefa trivial. Sua qualificação é de fácil percepção pois visualizam-se os prejuízos causados por possíveis danos a sistemas computacionais. Contudo, a quantificação não é banal e apresenta elevados níveis de complexidade. Não obstante, há estudiosos que têm enfrentado esse desafio.

Nesse contexto, há autores apresentam estimativas. Hale (2002) afirma que os crimes cibernéticos no mundo atingiam, aproximadamente, a quantia de US$ 50 bilhões em 2002. Lewis (2018) destaca que, dentre os crimes praticados globalmente, os cibernéticos estão em terceiro lugar em geração de custos, atrás apenas de corrupção nos governos e do narcotráfico. Ele adiciona que as estimativas existentes dos custos dos crimes cibernéticos apresentam variações significativas, indo de US$ 10 bilhões a mais de US$ 1 trilhão, o que reflete a reduzida confiabilidade dos dados e nas diferentes metodologias de cálculo. Lewis (2018), por exemplo, utilizou a metodologia *economic history research*, chegando à estimativa de custo global dos crimes cibernéticos de até US$ 600 bilhões.

Por outro lado, Cashell et al. (2004) verificaram que a obtenção de dados precisos sobre ataques cibernéticos sofridos por empresas e seus impactos exigiria a divulgação de informações omitidas por parte das atacadas. E, nesse aspecto, há incentivos[16] para as organizações não revelarem tais informações pois, ao exporem possíveis vulnerabilidades, por meio de ataques sofridos ou prejuízos deles decorrentes, essas empresas poderiam ser consideradas inseguras ou possuidoras de sistemas pouco confiáveis, criando uma imagem negativa perante seus mercados. Sob tal perspectiva, há uma tendência de as empresas não divulgarem dados sobre ataques cibernéticos sofridos.

A dificuldade de obtenção de dados precisos e representativos é exposta por CEA (2018) que afirma que houve elevada relutância das empresas em relatar informações negativas. Pode-se reforçar os baixos níveis de relatos oficiais de ataques sofridos com a estimativa feita por Scott (2016) que aponta apenas 13,2%

[16] Mankiw (2009) aponta que um dos princípios da Economia é que os agentes econômicos (pessoas e instituições) reagem à incentivos. Nesse aspecto, para a ciência econômica, tem-se que os agentes tendem a tomar decisões por meio de comparação de custos e benefícios. Como os custos de divulgar informações sobre ataques cibernéticos sofridos são interpretados pelos atacados como maiores do que os benefícios, há a tendência de que esses optem por não os divulgar.

dos crimes cibernéticos ocorridos no Reino Unido como reportados às autoridades policiais ou ao *Action Fraud*[17].

Assim, Cashell et al. (2004) concluem que modelos teóricos que descrevem os retornos dos gastos em segurança da informação fornecem alguma ideia sobre o tamanho das perdas potenciais, mas a ausência de dados estatísticos melhores faz com que a determinação, de modo geral, dos custos dos ataques cibernéticos continue sendo especulativa. Essa percepção é coerente com a posição de CEA (2018) que afirma que as estatísticas divulgadas podem apresentar posições tendenciosas em razão dos dados obtidos.

CEA (2018) destaca que apesar de, normalmente, não divulgarem as perdas sofridas por ataques cibernéticos, as empresas ofertantes de seguros são as que provavelmente possuem as melhores condições de avaliar em que níveis essas perdas encontram-se, uma vez que ressarcem a seus clientes quando sofrem tais danos. Isso certamente é considerado pelas seguradoras para avaliar os riscos aos quais seus clientes estão expostos e quanto devem cobrar pelos seus seguros contra danos causados por ataques cibernéticos. Cabe o destaque de que, segundo a *National Association of Insurance Commissioners* (*NAIC*), o valor das apólices de seguro cibernético é estimado em cerca de US$ 2,49 bilhões, com dados atualizados a partir de 2016 (NAIC, 2018).

Essas dificuldades de estimativas fornecem o panorama em que se insere a caracterização das consequências econômicas de ataques cibernéticos. Muitas vezes, analistas dessa problemática precisam basear-se em considerações qualitativas sobre diferentes tipos de ataques cibernéticos identificados e sobre casos práticos ocorridos em variados setores ao redor do mundo.

Apesar dos números difusos, é notório que os ataques cibernéticos apresentam crescimento significativo, o que pode ser inferido pelo aumento progressivo das estimativas como, por exemplo, dos ataques de *ransomware* que, segundo Microsoft (2016), somaram US$ 325 milhões em 2015. Adicionalmente, Morgan (2017a) estima que esse valor foi de, aproximadamente, US$ 1 bilhão em 2016 e com previsão de cerca de US$ 5 bilhões em 2017.

Tal cenário é tão preocupante que os riscos de ataques cibernéticos figuram entre os 10 maiores riscos de colapsos globais de 2018, do Fórum Econômico Mundial

[17] *Action Fraud* é o centro nacional de denúncias de fraudes e crimes cibernéticos do Reino Unido (ACTION FRAUD, 2018a).

(WEF, sigla em inglês), classificado em terceiro em probabilidade de ocorrência e em sexto em termos de impactos (WEF, 2018), o gráfico 1 mostra a relação entre a probabilidade de ocorrência e possíveis níveis de impacto dos eventos de risco da WEF.

O gráfico 1 chama a atenção, pois mostra que o Banco Mundial coloca os ataques cibernéticos atrás apenas de eventos climáticos extremos e desastres da natureza, no critério de análise probabilidade. Quando se consideram os impactos gerados, ficam abaixo dos dois anteriores somados a armas de destruição em massa, fracasso na mitigação/adaptação às mudanças climáticas e crises relacionadas à água. Assim, os ataques cibernéticos foram entendidos como causadores de impactos maiores do que relevantes ameaças como conflitos entre Estados, ataques terroristas, desemprego e crises relacionadas à fome.

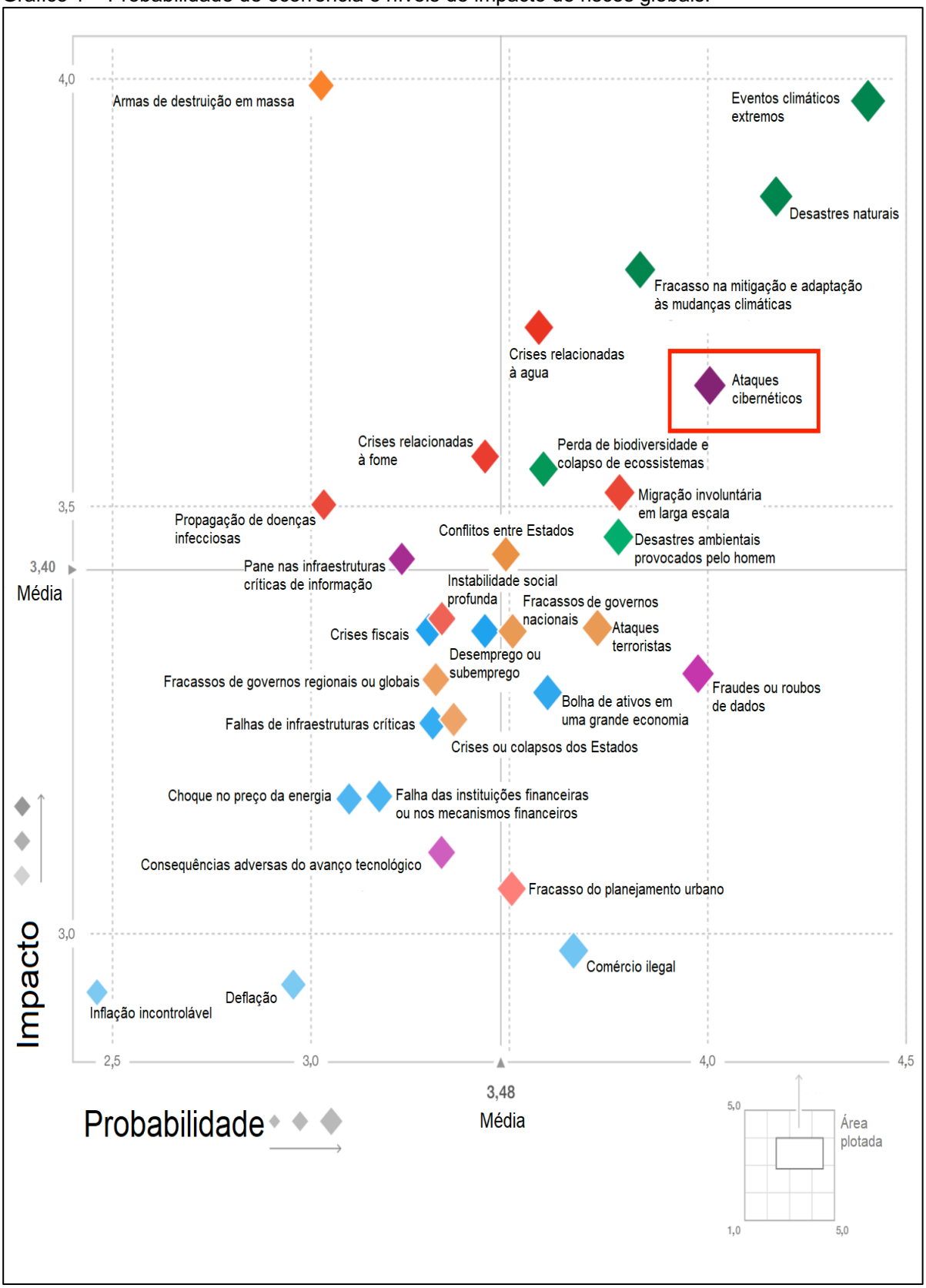
Esses elevados impactos são ratificados por Morgan (2017b) quando destaca que há previsão de que os crimes cibernéticos gerem um custo mundial[18] acima de US$ 6 trilhões anuais em 2021, o que representaria o dobro de 2015.

Com tais níveis de relevância, surge a indagação: como ocorrem tantos incidentes cibernéticos? Uma resposta parcial é que muitos tipos de ataques estão diretamente relacionados a procedimentos inadequados dos usuários, como nos casos já mencionados do soldado norte-americano no Oriente Médio e do executivo que inseriu um CD de procedência desconhecida em sua máquina. Contudo, a maior parte dos ataques é iniciada por meio de *links* enviados às vítimas. Sobre esse aspecto, Zetter (2015) estima que 91% dos ataques sofisticados são iniciados por *phishing* ou *spear phishing* enviados por e-mail. Obviamente, se o usuário clicar nos *links* desconhecidos recebidos por correio eletrônico, estará contribuindo para o aumento da vulnerabilidade da rede a que participa.

Como resposta ao aumento das ameaças, as instituições passaram a investir cada vez mais em medidas preventivas, como contratação de prestadores de serviços de segurança cibernética e treinamento de funcionários. A respeito disso, Mello Júnior (2017) estima que esse treinamento preventivo dos colaboradores pode criar um mercado com cifras que estarão em torno de US$ 10 bilhões em 2027.

[18] Nesse cálculo, Morgan (2017b) incluiu os danos causados por destruição de dados, dinheiro roubado, perda de produtividade, roubo de propriedade intelectual, roubo de dados pessoais e financeiros, peculato, fraudes, interrupção das atividades normais de negócio após o ataque, investigação forense, restauração e limpeza dos sistemas, e danos à reputação.

Gráfico 1 – Probabilidade de ocorrência e níveis de impacto de riscos globais.



Fonte: WEF, 2018.

A seguir, serão expostos alguns casos de conhecimento público de ataques ocorridos contra a confidencialidade, integridade e disponibilidade. Certamente são uma parcela ínfima dos ataques ocorridos no mundo, contudo, suficientemente ilustrativos quanto à abrangência de setores que podem ser afetados e de que forma.

2.2 Casos de ataques cibernéticos contra a confidencialidade

2.2.1 Invasão do banco de dados do Playstation em 2011

Silva, Azevedo e Rufato (2014) tratam sobre uma ação movida nos EUA, por usuários do vídeo game Playstation, de propriedade da *Sony Computer Entertainment American Inc* (SCEA), uma das subsidiárias da japonesa Sony Corporation. Nesse incidente, a própria SCEA admitiu que, em junho de 2011, seu o banco de dados sofreu uma violação, permitindo que informações de usuários fossem expostas ao invasor.

Silva, Azevedo e Rufato (2014) relatam que foram movidas 65 ações (*class actions*[19]) em consequência da invasão do banco de dados da SCEA em vários tribunais dos EUA. Todas as ações foram encaminhadas e julgadas em tribunal único na Corte Distrital do Sul da Califórnia e consolidados em uma só *class action.* Depois de várias audiências, em 2014, chegou-se a um acordo entre as partes em que a SCEA se comprometeu a pagar uma série de benefícios aos usuários do Playstation, no valor de US$ 17,17 milhões.

Pode-se perceber que o ataque cibernético sofrido pela Sony criou um custo indireto em razão das ações movidas. Não se restringindo ao pagamento do acordo, incluem-se custos advocatícios e o intangível da imagem da empresa e de seu produto.

2.2.2 Noite do dragão

Said (2016) destaca que um ataque cibernético contra diversas empresas de diferentes setores produtivos foi divulgado em fevereiro de 2011. McAfee (2011) expôs esse ataque por meio de um documento intitulado *Global Energy Cyberattacks: Night Dragon.* Nele informa-se que, foram realizados ataques cibernéticos encobertos e direcionados a empresas globais de petróleo, energia e petroquímica em 2009.

---

[19] *Class action* é um tipo de ação coletiva existente nos EUA. Daudt (2014) diz que a "*class action,* no direito norte-americano, é um procedimento em que uma pessoa considerada individualmente, ou um pequeno grupo de pessoas, enquanto tal passa a representar um grupo maior ou classe de pessoas, desde que compartilhem, entre si, um interesse comum".

Esses ataques envolveram engenharia social, ataques de *spear phishing*, exploração de vulnerabilidades do sistema operacional Microsoft Windows e ferramentas de administração remota para direcionar e colher operações proprietárias competitivas sensíveis e informações de financiamento de projetos relacionados licitações e operações de campos de petróleo e gás. Segundo McAfee (2011), os ataques eram provenientes de diversas localidades na China, que buscavam comprometer servidores na Holanda para realizar ataques contra empresas globais daqueles setores, bem como indivíduos e executivos no Cazaquistão, Taiwan, Grécia e Estados Unidos para ter acesso a informações confidenciais.

Nesse exemplo, tem-se o típico custo de espionagem industrial. Nele a vítima depara-se com um concorrente de posse de um produto novo, contabiliza os investimentos em P&DI e que o criminoso o obteve sem tais custos, além dos prejuízos relacionados às patentes.

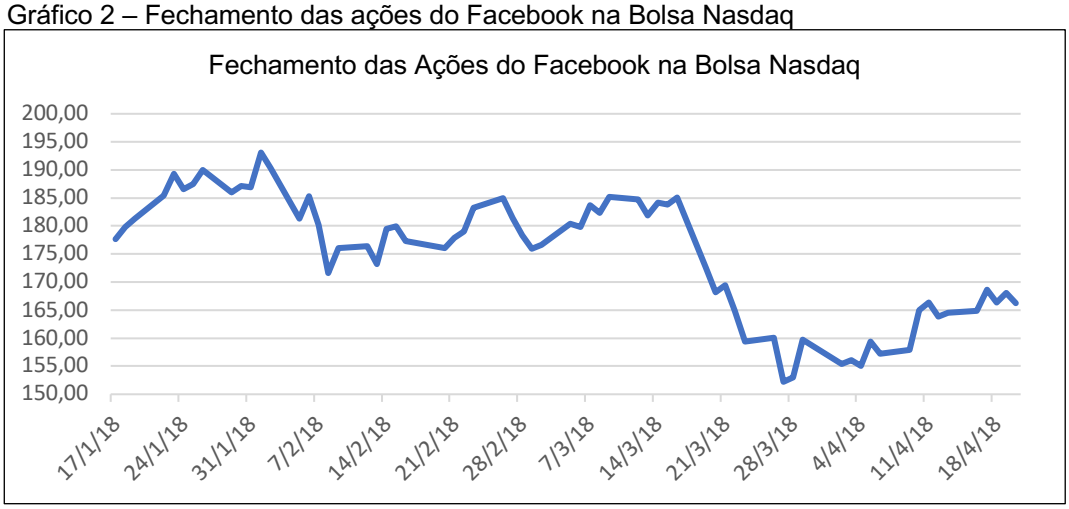
2.2.3 Uso de informações de usuários do Facebook pela *Cambridge Analytica*

Rosenberg, Confessore e Cadwalladr (2018) publicaram em 17 de março de 2018, nos jornais *The New York Times*, dos EUA e *The Guardian*, da Grã-Bretanha a denúncia de um ex-funcionário da empresa *Cambridge Analytica* de que a mesma utilizava, indevidamente, dados de usuários do *Facebook* para fazer análises de seus perfis em favor de campanhas políticas como a do presidente norte-americano Donald Trump em 2016. Carazzai (2018) chama a atenção que, em 10 de abril de 2018, o CEO e fundador do Facebook, Mark Zukerberg compareceu ao congresso estadunidense para esclarecer o uso de dados provenientes da empresa. Na oportunidade reconheceu que houve o uso indevido de dados pela *Cambridge Analytica.* Sobre o fato, Agrela (2018) destacou que Zukerberg admitiu que 87 milhões de usuários foram afetados, destes 443 mil localizados no Brasil.

Esse cenário de perda de confidencialidade dos dados pelo Facebook criou algumas consequências imediatas, como pedidos de indenização, dentro e fora dos Estados Unidos. Como exemplo, pode-se citar Stempel (2018) que trata sobre a primeira *class action* movida nos EUA em razão do caso em pauta que foi impetrada por uma moradora de Maryland, no dia 20 de março de 2018 e Oliveira (2018) que destaca a entrada de um pedido de indenização por danos morais, na 7ª Vara Cível de São Paulo, no dia 20 de abril de 2018, no valor de R$ 10 milhões, referentes aos dados dos 443 mil brasileiros.

Outro aspecto importante quanto ao caso da *Cambridge Analytica* com o Facebook foi o reflexo nas ações desta última na Bolsa Nasdaq, que é a bolsa que negocia ações de empresas do ramo de tecnologia nos Estados Unidos. Segundo Stempel (2018), esse evento criou uma desvalorização de mercado de cerca de 50 bilhões de dólares em dois dias. O gráfico 2, confeccionado pelo autor com dados da referida bolsa, mostra a evolução das cotações das ações Facebook, Inc. *Class A*, código FB.

Gráfico 2 – Fechamento das ações do Facebook na Bolsa Nasdaq



Fonte: NASDAQ, 2018.

Pode-se extrair algumas informações por meio do gráfico 2. Uma delas é que no dia 16 de março de 2018, as ações da empresa fecharam o pregão cotadas a US$ 185,09. Dois pregões após a divulgação do uso indevido dos dados, no dia 20 de março, as ações fecharam com cotação de US$ 168,15 e continuaram caindo para níveis abaixo dos US$ 160,00 até Zukerberg depor no congresso, assumindo a responsabilidade da empresa e anunciando que haveria mudanças na política de gestão dos dados sob guarda do Facebook. Após as declarações do CEO, houve uma recuperação na cotação da empresa, mas com níveis consideravelmente inferiores aos anteriores a março de 2018.

Nesse caso, as perdas identificadas foram semelhantes às da Sony (tratadas na seção 2.2.1), envolvendo custos advocatícios e os intangíveis da imagem da empresa, que nesse caso pôde-se ter uma ideia da dimensão por meio das cotações de suas ações.

2.2.4 *Duqu* e *Duqu* 2.0

Segundo Symantec (2011), um *worm* chamado *Duqu* foi identificado em ataques de espionagem industrial em 2011. O objetivo do *Duqu* era de reunir dados

de inteligência e ativos de entidades, como fabricantes de sistemas de controle industrial, a fim de conduzir com mais facilidade um futuro ataque contra terceiros. Os alvos eram informações como documentos de projeto que poderiam ajudá-los a montar um futuro ataque em instalações de controle industrial.

Já em 2015, uma nova versão do *Duqu* foi identificada em ataques direcionados a empresas de telecomunicações. Segundo Sysmantec (2015), dentre as organizações visadas havia uma operadora europeia de telecomunicações, uma operadora de telecomunicações do norte da África e uma fabricante de equipamentos eletrônicos do sudeste asiático. Ademais, foram encontradas infecções do *worm* em computadores localizados nos EUA, Reino Unido, Suécia, Índia e Hong Kong. De acordo com Sysmantec (2015), *Duqu* 2.0, como foi chamada a segunda versão do *worm*, possuía funcionalidades como coleta de informações no computador infectado, descoberta de rede, infecção de rede e comunicação com comando e controle.

Nesse exemplo, verifica-se que podem ser contabilizados custos relativos à acessos desautorizados a informações classificadas, o que seria mensurado a depender do que foi acessado, podendo ser desde informações empresariais até conteúdos de Estados.

2.3 Casos de ataques cibernéticos contra a integridade

2.3.1 Intrusão à rede do World Bank Group em 2008

No ano de 2008, de acordo com Olowu (2009), a rede de computadores do banco europeu World Bank Group teve quarenta servidores de dados comprometidos por criminosos cibernéticos. Foram realizados seis ataques que ocasionaram perdas financeiras a contas de diversos clientes, dentre eles, o então presidente francês, Nicolas Sarkozy.

Nesse episódio, contabiliza-se o custo direto dos valores subtraídos das contas dos clientes e gastos com contratação de seguros para casos de ataques desse tipo. Além desses, devem ser considerados os custos indiretos relacionados à investigação policial para o Estado, possíveis ações contra o banco e o intangível prejuízo vinculado à imagem do banco.

2.3.2 Fraude contra o sistema de pagamento por meio de boleto bancário

Outro caso de ataque cibernético contra a integridade ocorreu no Brasil. Esse caso será tratado com profundidade na seção 3.2. Entretanto, pode-se adiantar, resumidamente, que foi um ataque, descoberto por uma empresa de segurança cibernética norte-americana, onde um *malware* identificava boletos recebidos na

máquina infectada, modificando-o de forma que, quando a vítima pagava o boleto, os recursos eram depositados na conta dos fraudadores. Nesse exemplo, têm-se os mesmos tipos de custos relacionados ao caso tratado na seção 2.3.1.

2.3.3 Fraude por meio de aplicativos de *smartphones*

Brito (2018) relata um alerta emitido pela empresa de antivírus Avast destinado a usuários do Brasil. Segundo o autor, a empresa descobriu um trojan bancário oculto em aplicativos de *smartphone* na *Google Play Store*, tendo como alvos os clientes do banco Santander. Ao instalar o aplicativo, o trojan exibia uma tela falsa a qual simulava a verdadeira do banco, capturando as credenciais de acesso dos usuários.

2.4 Casos de ataques cibernéticos contra a disponibilidade

2.4.1 *Stuxnet*

A atual dependência de diversos sistemas aos meios computacionais cria a possibilidade de torná-los indisponíveis ao serem atacados. Um caso emblemático foi o ataque conhecido como *Stuxnet.*

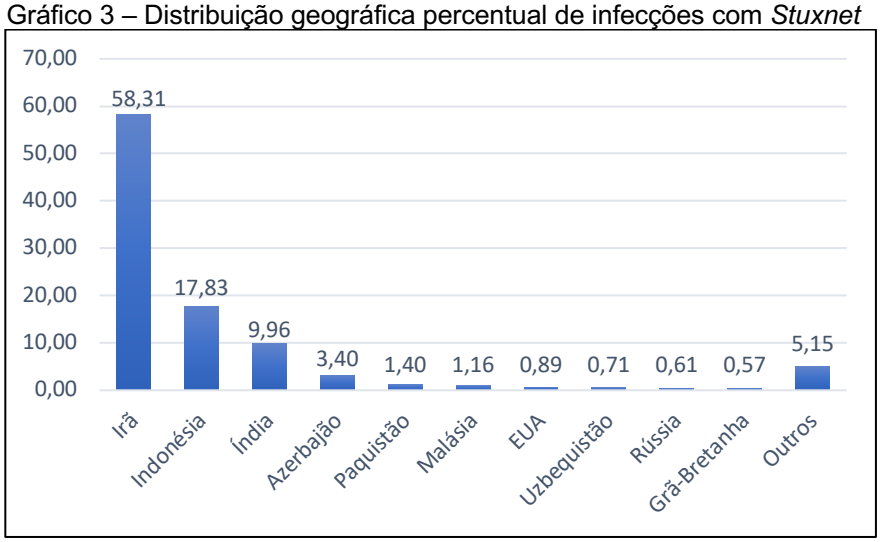
Stuxnet foi o nome atribuído a tipo específico de *worm* que se espalhou por vários países em 2010 e 2011. No entanto, sua história é anterior, pouco menos de uma década, em 2002, quando, segundo Lopes e Oliveira (2014), o governo estadunidense descobriu que o Irã construíra, secretamente, uma instalação enriquecimento de urânio na cidade de Natanz. Assim, o governo dos EUA levantou hipóteses de neutralizar o programa nuclear iraniano sem realizar ataques militares convencionais.

Com o objetivo de atuar na defesa e segurança nacional, conforme Clarke e Knake (2010), houve a criação do *U.S. Cyber Command,* o qual passou a desenvolver a capacidade cibernética dos EUA, trabalhando em conjunto com outros órgãos do governo. Lopes e Oliveira (2014) explicam que foi estabelecida uma parceria entre Israel e os EUA em que a Agência Nacional de Segurança de Israel e compartilhou com os EUA, um *malware* por eles desenvolvido para atuar no sistema das centrífugas iranianas. Esse *malware* foi chamado de *Stuxnet*.

Segundo Said (2016), o *Stuxnet* foi projetado especificamente para atacar os produtos de automação da Siemens, sendo capaz de baixar informações sobre processos, modificar lógicas de programação e, em seguida, encobrir suas evidências. Assim, *Stuxnet* foi capaz de tomar o controle do sistema de automação, controlando a configuração da centrífuga de forma que operasse em um ritmo que executasse lentamente sua autodestruição.

Lopes e Oliveira (2014) destacam que foi o primeiro ataque que se tem conhecimento em que um governo atacou ciberneticamente alguma instalação de outro país. Sua fama difundiu-se amplamente, pois o *Stuxnet* apresentou efeito colateral, comportando-se de forma inesperada, ele propagou-se e atingiu mecanismos de automação de várias regiões do planeta, conforme pode ser observado no gráfico 3.

Gráfico 3 – Distribuição geográfica percentual de infecções com *Stuxnet*



Fonte: FALLIERE, MURCHU e CHIEN, 2011.

Segundo Said (2016), após a divulgação do *Stuxnet,* os sistemas SCADA/ICS[20] passaram a ser vistos como atrativos e compensadores, tornando-se alvos de hackers e criminosos. Segundo o autor, dados do ICS-CERT[21] indicavam que, em 2011, houve cento e quatro avisos de tentativas de ataques a SCADA/ICS e antes da divulgação do ataque, haviam sido apenas cinco.

Nesses casos, percebe-se que os custos dos ataques cibernéticos são relacionados ao tempo de indisponibilidade das máquinas controladas pelos sistemas de automação, ademais, se houver danos físicos aos equipamentos, somam-se os

[20] Supervisory Control and Data Acquisition (SCADA) ou os Sistemas de Controle Industrial (ICS, em inglês) são sistemas utilizados para automação de máquinas nas indústrias. Esses tipos de sistemas utilizam computadores para seu gerenciamento e controle.

[21] ICS-CERT é a abreviatura de Industrial Control Systems Cyber Emergency Response Team. Segundo o National Cybersecurity and Communications Integration Center's (NCCIC) (2018), faz parte do Departamento de Segurança Interna dos Estados Unidos (Department of Homeland Security) como um de seus subordinados. Ele contribui na missão de coordenação de incidentes de segurança relacionados a sistemas de controle e troca de informações com agências e organizações federais, estaduais e locais, a comunidade de inteligência e constituintes do setor privado, incluindo fornecedores, proprietários e operadores, e CERTs do setor privado e internacional.

custos de suas manutenções e se vier a ocorrer algum dano às instalações e pessoal, os custos de reparo e gastos de saúde.

2.4.2 *WannaCry*

O *WannaCry* foi um ataque cibernético do tipo *ransomware* ocorrido em 2017. Segundo WEF (2018), esse ataque cibernético afetou cerca de 300 mil computadores no ano de seu lançamento em, aproximadamente, 150 países. Dentre as vítimas, encontram-se infraestruturas críticas e empresas de energia.

Para WEF (2018), o impacto do *WannaCry* foi considerado relativamente limitado, mas revelou a vulnerabilidade de um número considerável de organizações de infraestruturas críticas ao redor do mundo.

Os custos de ataques desse tipo são os de perder o acesso a dados e sistemas empresariais, caso não haja uma política de *backup* adequada. Pode-se contabilizar, ainda, o valor do pagamento do resgate, mesmo que essa seja uma medida contraindicada pelos especialistas pois, mesmo havendo o pagamento, não há garantias de que os criminosos devolverão o acesso à vítima.

2.5 Resumo dos possíveis tipos de ataques cibernéticos

Após os ataques cibernéticos haverem sido apresentados e mostrado como podem causar custos financeiros, econômicos, sociais e políticos em variados setores, apresentamos alguns dos possíveis ataques cibernéticos e reflexos econômicos em decorrência dos mesmos. Esses encontram-se sintetizados no quadro 1.

Quadro 1 – Resumo dos tipos de ataques cibernéticos e seus reflexos econômicos.

Possíveis tipos de ataques cibernéticos		**Possíveis consequências econômicas**
Contra a disponibilidade	Ataques com *malwares*	Redução ou atraso de produção, afetando renda e emprego.
		Redução da oferta energética, produzindo reflexos em toda cadeia produtiva, como atrasos na produção, perda de produtos que dependem de refrigeração, colapsos generalizados.
		Distúrbios na infraestrutura rodoviária, criando reflexos nos meios de transporte e na circulação de pessoas e produtos.
		Distúrbios no controle de tráfego aéreo, influenciando na circulação de pessoas e produtos, com reflexos diretos em setores como logística e turismo.
		Indisponibilidades em infraestruturas de telecomunicações como telefonia e internet, causando, por exemplo, redução de sistemas produtivos por falta de comunicação entre setores interdependentes com reflexos em variados áreas da economia.
		Problemas de indisponibilidades do sistema financeiro causando indisponibilidade de crédito e efeitos em todos os setores econômicos.
		Em uma visão macro, pode afetar os níveis de confiança nos sistemas que se tornaram indisponíveis em decorrência dos ataques.
	Ataques do tipo *ransomware*	Perda de pesquisas de elevado valor agregado, segredos industriais, dados de clientes e fornecedores, entre outros, criando reflexos em setores como de P&DI. Afetando produtividade, empregos, mercados e renda.
Contra a confidencialidade	Ataques com *malwares*, *spywares, phishing e spear phishing*	Perdas financeiras por quebras de patentes e espionagem industrial. Elevação de custos de proteção cibernética e seguros, custos decorrentes de ações judiciais, etc., afetando produtividade, empregos, mercados e renda.
	Ataques de Engenharia Social e espionagem cibernética	
Contra a integridade	Ataques com vírus, *worms, backdoors,* Cavalos de Tróia e *botnets*	Podem paralisar produção, prejudicar sistemas de pagamentos, criar fraudes financeiras, danificar sistema de automação, etc., afetando produtividade, empregos, mercados e renda.

Fonte: Elaborado pelo autor com base nos eventos apresentados no capítulo 2.

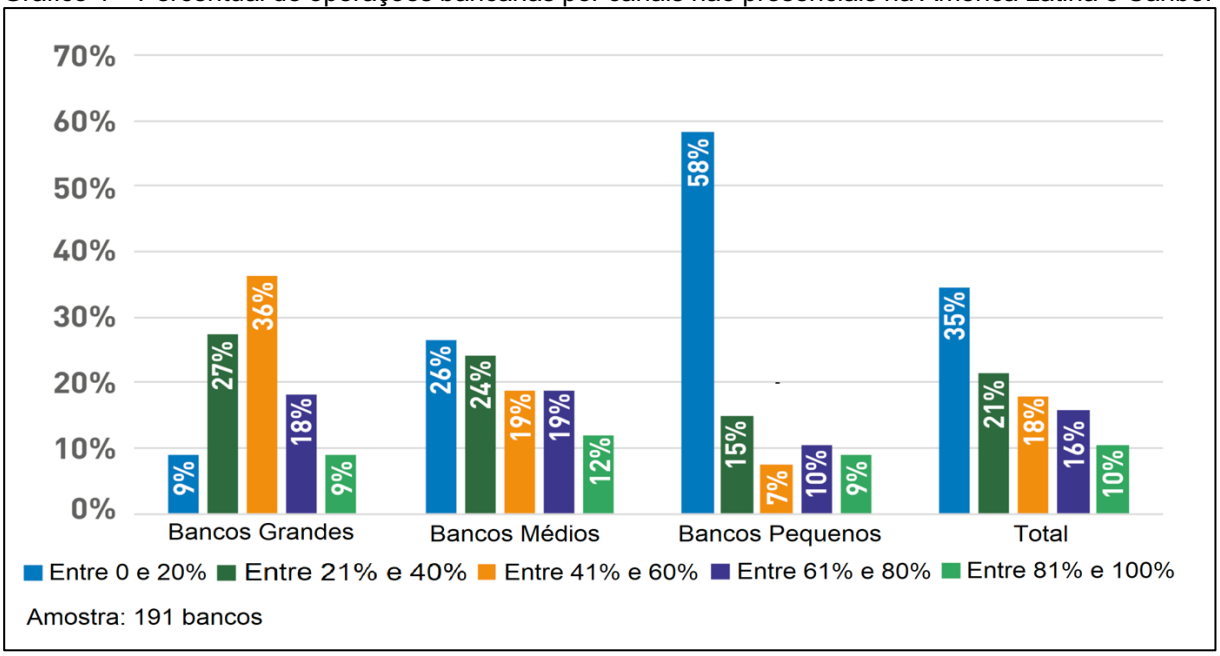
3 VULNERABILIDADES ECONÔMICAS NO SETOR FINANCEIRO: uma aproximação

3.1 Dimensões do meio cibernético pelo setor financeiro

O uso de recursos eletrônicos na internet para fins relacionados a atividades financeiras é elevado e crescente. A esse respeito, Olmstead e Smith (2017) mostram que 55% dos norte-americanos relatam possuir conta *on-line* com bancos ou outros prestadores de serviços financeiros e 39% possuem algum tipo de conta *on-line* que envolve pagamentos de faturas.

Segundo a OEA (2018), as operações bancárias não presencias[22] na América Latina e Caribe está distribuída conforme o gráfico 4.

Gráfico 4 – Percentual de operações bancárias por canais não presenciais na América Latina e Caribe.



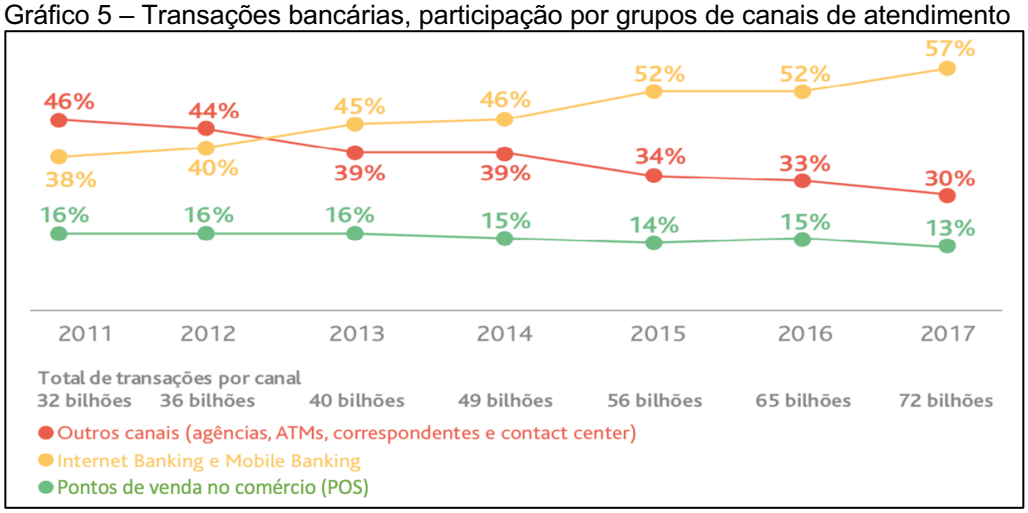
Fonte: OEA, 2018.

Analisando o gráfico 4, percebe-se que o uso dos canais não presenciais nos bancos latino-americanos é mais significativo entre os bancos médios e grandes, o que indica uma possibilidade de crescimento na região para os bancos pequenos. Quando são considerados os valores totais, verifica-se que 44% dos bancos da América Latina e Caribe apresentam mais de 41% de suas transações realizadas por meio de acesso remoto.

[22] Esse estudo considera os seguintes meios não presenciais para realização de transações bancárias: internet, transações eletrônicas, caixas eletrônicos (ATM), pagamentos automáticos, telefones celulares e por meio telefônico convencional.

Já no Brasil, o uso de meios conectados à internet (computadores e *smartphones*) é próximo, percentualmente, aos números dos Estados Unidos. Deloitte (2018)[23] indica que em 2017, no Brasil, as transações realizadas por meio de *Internet Banking* e *Mobile Banking*[24] representaram 57% do total, sendo, inclusive um pouco maior do que nos EUA. O gráfico 5 apresenta o número total de transações bancárias brasileiras e suas participações percentuais por grupos de canais de atendimento.

Gráfico 5 – Transações bancárias, participação por grupos de canais de atendimento



Fonte: DELOITTE, 2018.

O gráfico 5 mostra uma clara tendência de substituição do atendimento classificado na categoria “outros” (como agências e caixas eletrônicos) por i*nternet banking* e *mobile banking*, além de uma leve redução do atendimento em pontos de venda no comércio. Tal crescimento, oferece oportunidades aos agentes financeiros de ofertarem serviços compatíveis com as novas demandas. Assim, os bancos brasileiros passaram a oferecer novas modalidades de contas em que os clientes, basicamente, têm acesso aos serviços bancários por meio de computadores e/ou *smartphones*. Segundo Deloitte (2018), essas contas, em 2017, igualaram-se em número no Brasil, totalizando 59 milhões cada.

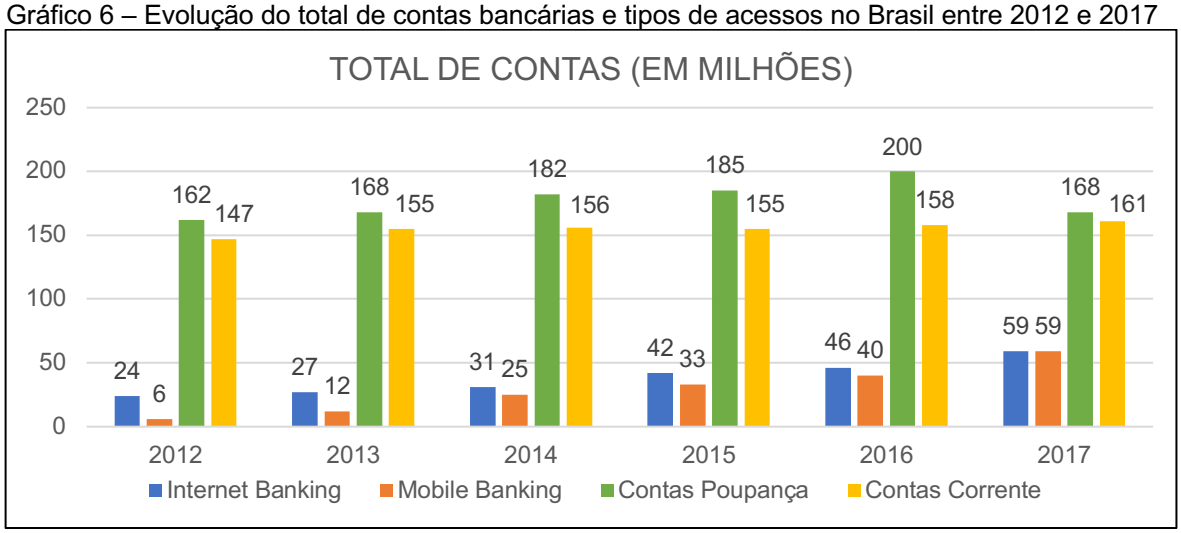
O gráfico 6 mostra o total de contas no Brasil, de uma amostra que contou com 21 bancos, no período entre 2012 e 2017. Nele é possível visualizar o crescimento

[23] A Deloitte é uma empresa que oferece serviços de auditoria, consultoria, assessoria financeira, gestão de riscos e consultoria tributária para consumidores públicos e privados dos mais diversos setores (DELOITTE, 2018). Ela realiza, anualmente, para a Federação Brasileira de Bancos (FEBRABAN), uma pesquisa denominada “Pesquisa FEBRABAN de Tecnologia Bancária” na qual são abordados temas relevantes ao setor de TIC relacionados ao setor bancário no Brasil.

[24] *Mobile Banking* refere-se ao uso de aplicativos de *smartphones* dedicados à prestação de serviços bancários.

dos meios de acesso *internet banking* (por meio de computadores) e *mobile banking* (por meio de smartphones), especialmente esta última.

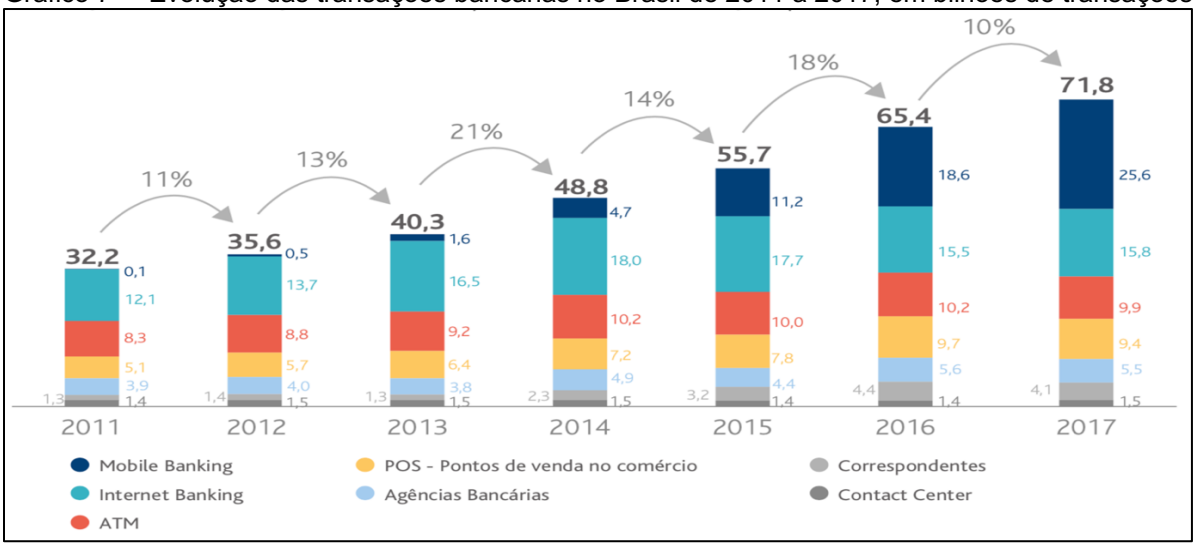
Gráfico 6 – Evolução do total de contas bancárias e tipos de acessos no Brasil entre 2012 e 2017



Fonte: DELLOITE, 2018.

A tendência de aumento do uso de meios eletrônicos para fins financeiros ocorre no mercado brasileiro, com destaque para os *smartphones*. Deloitte (2017) destaca que houve um significativo crescimento no uso do *mobile banking*, de 2011 (ano em tornou-se um meio para transações bancárias no Brasil) a 2016, de 21.800%. E há manutenção dessa tendência, pois em 2017, segundo Deloitte (2018) houve aumento de 37% no número de transações por meio do *mobile banking* em relação ao ano anterior. O gráfico 7 mostra a evolução das transações bancárias no Brasil de 2011 a 2017, em bilhões de transações.

Gráfico 7 – Evolução das transações bancárias no Brasil de 2011 a 2017, em bilhões de transações



Fonte: DELOITTE, 2018.

Diante desses números, pode surgir o questionamento: como esses dados relacionam-se aos ataques cibernéticos? O evidente crescimento dos meios digitais pelo setor financeiro (tanto internamente quanto pelos seus clientes e parceiros ao acessarem os serviços), eleva a exposição dos sistemas a vulnerabilidades e ao risco de ataques pois, em muitos casos, basta o atacante conseguir acessar o dispositivo de um usuário da rede para conseguir realizar ações fraudulentas.

3.2 Casos de perdas do setor financeiro por ataques cibernéticos no exterior

Lewis (2018) destaca que os crimes cibernéticos produzem várias formas de perdas, dentre as quais, as listadas no quadro 2 podem afetar diretamente ao setor financeiro:

Quadro 2 – Perdas causadas ao setor financeiro por ataques cibernéticos

Principais perdas do setor bancário em decorrência de ataques cibernéticos
Roubo de registros pessoais
Manipulação do mercado financeiro[25]
Redução de confiança nas atividades *on-line*
Interrupção de serviços
Custos para proteção das redes
Contratação de seguros contra crimes cibernéticos
Danos à reputação da empresa invadida
Riscos de responsabilização para a empresa invadida
Riscos à marca da empresa
Danos temporários no valor da ação em bolsa de valores

Fonte: LEWIS, 2018.

Ainda segundo Lews (2018), os bancos são os principais alvos de cibercriminosos qualificados há mais de uma década, isso faz com que o setor financeiro invista o triplo da média dos demais.

A esse respeito, Action Fraud (2018b) relata que, entre outubro de 2017 e março de 2018, foram reportadas 51.677 infecções em computadores com Cavalos de Tróia relacionados a bancos no Reino Unido, havendo, nesse período, perdas por crimes cibernéticos na casa de £ 11 milhões.

Action Fraud (2018b) destaca que há indícios de que haja grupos com apoio de governos atuando diretamente contra instituições financeiras, como bancos e a rede

[25] As perdas listadas no Quadro 2 são autoexplicativas, todavia, jugou-se pertinente elucidar que a "manipulação do mercado financeiro" pode ocorrer em razão do uso de informações sigilosas de negócios sobre possíveis fusões ou conhecimento antecipado de relatórios de desempenho de empresas de capital aberto obtidas por meio de ataques cibernéticos.

SWIFT[26], nesse sentido, aponta o governo da chinês como patrocinador de ações de espionagem cibernética; enquanto Rússia, Coreia do Norte e Irã como patrocinadores de instituições organizadas de hackers que agem contra bancos e a rede SWIFT. Sobre esses ataques à rede SWIFT, estima-se que foram roubados cerca de US$ 81 milhões do Banco Central de Bangladesh (WEF, 2018).

Rodríguez (2018) aponta que o roubo de identidade em compras não presenciais, clonagem de cartões de crédito, ataques de *phishing* foram os principais riscos enfrentados pelos bancos da América Latina e Caribe. Afirma, ainda, que esses crimes contribuíram para o surgimento de um mercado ilegal de venda de números de contas, cartões e senhas, tendo a Rússia como a principal origem dos ataques.

A segurança cibernética segue o princípio de que uma corrente é tão forte quanto o seu elo mais fraco. Por essa razão, todos que participam de alguma forma de redes corporativas, sejam funcionários, parceiros ou clientes devem possuir mecanismos de proteção sob o risco de comprometer toda a rede. Nesse sentido, Kaspersky (2017) aponta uma pesquisa que abrangeu empresas de 15 países. A mesma identificou que 60% das empresas do setor financeiro necessitam implementar medidas que fortaleçam a proteção a terceiros que acessam a seus sistemas. Isso, segundo Kaspersky (2017), afeta o tempo no qual os bancos precisam para detectar uma ameaça, tanto que 24% dessas organizações financeiras relataram que haviam descoberto sofrer algum incidente por meio da informação de seus clientes.

Por outro lado, o compartilhamento de informações por meio da formação de parcerias entre membros do setor financeiro pode beneficiar a proteção do sistema como um todo. Bazo (2018) destaca que o sistema bancário peruano obteve êxito em defender-se de uma série de ataques cibernéticos no dia 17 de agosto de 2018. Tal logro deveu-se a um alerta de segurança emitido por outros agentes do sistema financeiro mundial. Em consequência desse alerta, as instituições financeiras do Peru iniciaram seus protocolos de segurança, suspendendo ou limitando temporariamente determinados serviços. Nesse evento, percebe-se que, mesmo havendo o sucesso

[26] SWIFT é a abreviatura em inglês de *Society for Worldwide Interbank Financial Telecommunications*. A Sociedade de Telecomunicações Financeiras Interbancárias Mundiais (SWIFT) é uma instituição com sede na Bélgica e oferece, entre outros, o serviço de interligação entre redes bancárias de todo mundo. Ela possibilita a realização transferências entre bancos de diferentes países, por meio da chamada Rede SWIFT que, atualmente, conta com mais de 11.000 instituições bancárias, em mais de 200 países em todos os continentes (SWIFT, 2018).

em evitar-se a fraude bancária, houve perdas indiretas como o tempo sem a oferta dos serviços financeiros.

Bazo (2018) ainda aborda o evento no qual o Banco do Chile sofreu ataques cibernéticos em maio de 2018, tendo cerca de US$ 10 milhões transferidos para contas em Hong Kong.

Stefanko (2018) relata que foi descoberto um grupo de aplicativos bancários falsos para smartphones com sistema operacional Android disponíveis na loja oficial da Google Play entre junho e julho de 2018. Os aplicativos ofereciam aumento de limite do cartão de crédito e solicitava dados pessoais e de acesso a serviços bancários de três bancos da Índia. Casos parecidos já haviam sido reportados, como Alves (2017) expõe, nos Estados Unidos, Austrália, Alemanha, França, Espanha e Portugal, mas não se tratavam de aplicativos baixados na loja oficial do Google e nesses casos eram outros tipos de aplicativos que continham o Cavalo de Tróia que roubava os dados das contas das vítimas.

3.3 Casos de perdas do setor financeiro por ataques cibernéticos no Brasil

Os primeiros exemplos expõem três formas parecidas, entretanto distintas de obter acesso a dados bancários de clientes para, em seguida, executar transações financeiras nas contas das vítimas.

O primeiro foi a criação de uma página falsa na internet de um grande banco brasileiro em 2012. Nesse caso, Catoira (2012) relata que quando os clientes entravam na página falsa, os dados inseridos eram enviados para os fraudadores e em seguida, encaminhados para a página verdadeira do banco para que não houvesse suspeita por parte do usuário.

Outro caso é reportado por Camurça (2016) em que a página na internet do Banco do Estado do Rio Grande do Sul (BANRISUL) foi atacada por cibercriminosos e modificada, fazendo com que os clientes que acessavam à página verdadeira fossem redirecionados a uma falsa. Uma vez na página fraudulenta, era oferecido o download de um arquivo que continha um Cavalo de Tróia o qual roubava as senhas bancárias e desinstalava o antivírus das vítimas.

E o terceiro exemplo é tratado por Harán (2018) em que, entre junho e agosto de 2018, criminosos modificaram, remotamente, as configurações de roteadores de um fabricante específico fazendo com que os usuários, ao acessarem as páginas do Banco do Brasil e do Itaú, fossem redirecionados para páginas falsas, onde seus

dados eram roubados, permitindo o acesso em suas contas pelos criminosos. Nesses três exemplos, não foram relatados os valores envolvidos.

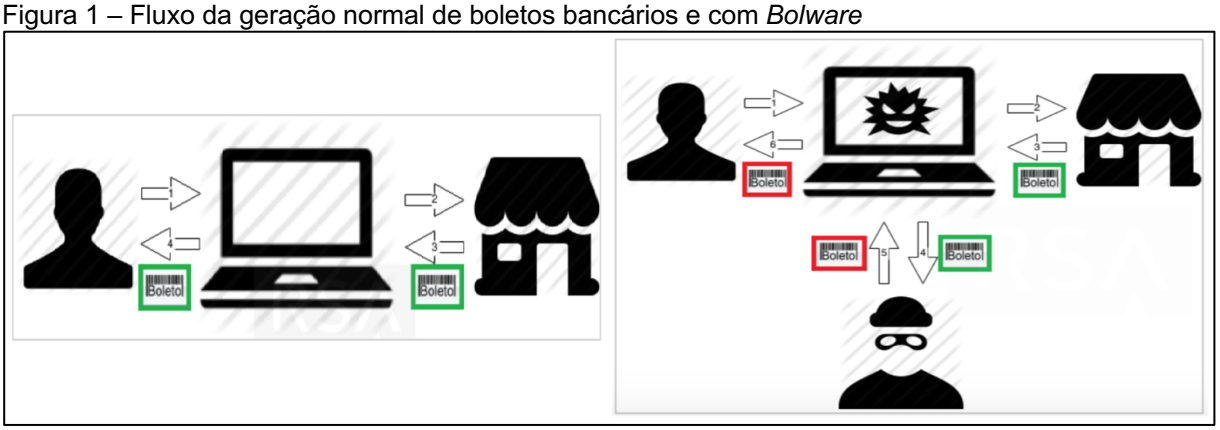
Brito (2018) relata que, em 29 de outubro de 2018, uma fraude semelhante à dos bancos indianos relatados na seção 3.2, com disponibilização de aplicativos falsos na Google Play, destinadas a clientes do banco Santander, foi detectada no Brasil, conforme já explicado na seção 2.3.3. Nesses quatro casos, não há indicação de valores envolvidos.

Um ataque de grandes dimensões que se tem conhecimento no Brasil foi tratado por Kerner e Winston (2014) que reportam a descoberta pela RSA[27] de um *malware* atuando em computadores do país que foi chamado de *Bolware*, uma fusão das palavras boleto e *malware.*

Conhecia-se o *Bolware* desde o 2013, mas a descoberta da RSA foi que, entre março e junho de 2014, mais de 30 bancos do Brasil haviam sido afetados por essa ferramenta criminosa, criando a estimativa de perdas que pode chegar a R$ 8,57 bilhões, o que na época estava em torno dos US$ 3,75 bilhões.

Nas transações normais, os clientes que desejam pagar por produtos e serviços, geram uma solicitação, por meio do computador e esta é enviada para o vendedor. Este último possui uma aplicação de seu banco que lhe permite gerar um boleto que é enviado para o cliente, como pode ser visualizado na ilustração à esquerda da figura 1. O *Bolware* atuava como um elemento no meio da transação normal, instalando-se no computador do cliente, conforme a ilustração à direita da figura 1.

Figura 1 – Fluxo da geração normal de boletos bancários e com *Bolware*



Fonte: KERNER e WINSTON, 2014.

[27] *RSA Security* é uma empresa norte-americana especializada em serviços de proteção cibernética e gerenciamento de risco digital (RSA, 2018).

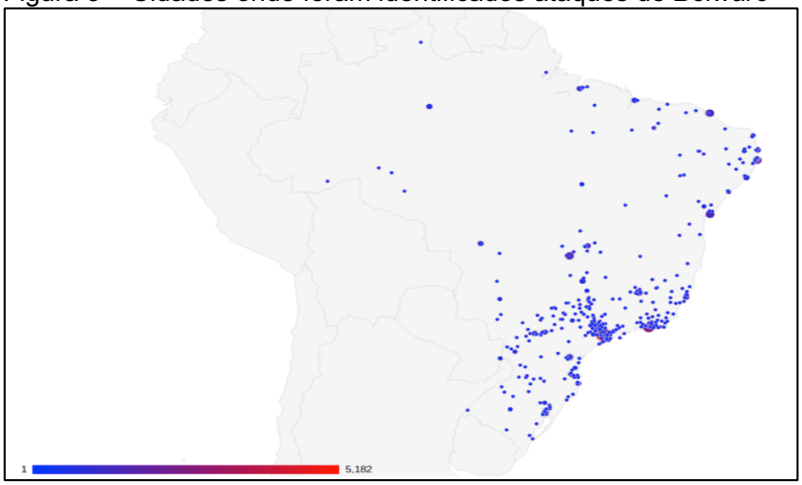
Segundo Kerner e Winston (2014), o *Bolware* atacava computadores com sistema operacional *Windows,* inserido por meio de um Cavalo de Tróia. Ele identificava quando boletos eram recebidos pelo computador infectado, desviava-os para um servidor externo onde os boletos eram modificados e reenviados ao cliente. Esses boletos fraudulentos continham, basicamente, as mesmas informações dos originais, contudo, o número da conta na qual valor seria depositado e o código de barras eram as informações modificadas pelo *malware*, conforme a figura 2.

Figura 2 – Boleto verdadeiro e gerado pelo *Bolware*

Fonte: KERNER e WINSTON, 2014.

Como se tratavam de modificações muito sutis, eram de difícil detecção, o que gerou um número significativo de vítimas. Outro aspecto que contribuiu foi que, no período em questão, o boleto era o segundo maior meio de pagamentos utilizado no Brasil, o que possibilitou a atuação do *malware* em todas as regiões do país, principalmente nos grandes centros urbanos, como pode ser visualizado na figura 3.

Figura 3 – Cidades onde foram identificados ataques de *Bolware*



Fonte: KERNER e WINSTON, 2014.

Ademais, Kerner e Winston (2014) identificaram que o *Bolware* coletava dados das contas de usuários da *Microsoft* e de seus serviços de *e-mail* como *live.com, hotmail.com e outlook.com*, provavelmente para acessar a computadores de novas vítimas por meio das listas de contatos dos atacados. O Quadro 3 apresenta uma visão geral da descoberta do *Bolware:*

Quadro 3 – Dados da atuação do malware "Bolware" no Brasil

Dados da atuação do malware "Bolware" no Brasil	
Ano que foi descoberto	2013
Sistema Operacional afetado	Windows
Bancos afetados	Mais de 30
Perda potencial relacionada ao *Bolware*	R$ 8.572.513.355,59 (US$ 3,75 bilhões)
Número de boletos identificados com a modificação causada pelo *Bolware*	8.095
Número potencial de transações com fraude causada pelo *Bolware*	495.753
Número de credenciais de usuários coletados	83.506
Total de computadores infectados	192.227

Fonte: KERNER e WINSTON, 2014.

Ao analisar-se o volume de transações identificadas como fraudulentas em razão do Bolware (495.753) e compará-lo ao de transações em 2013 (40,3 bilhões) obtêm-se uma proporção pequena. No entanto, o valor subtraído, ainda assim, é relevante (cerca de US$ 3,75 bilhões), assim como o número de bancos afetados (mais de 30), o que mostra a permeabilidade do *malware* no país.

Há inúmeros casos de atuações de agentes maliciosos envolvendo valores menores, o que não os torna insignificantes. O portal G1 (2017) relata um em que dois homens foram presos em flagrante sacando uma quantia de R$ 700 mil em Itajaí-SC. O grupo era compostos por *hackers* que acessavam remotamente a rede de instituições bancárias, com um sistema que simulava um computador válido do banco. Assim, quebravam os sistemas de segurança e obtinham de informações e dados de transações, o que lhes permitia redirecionar valores para as suas contas bancárias. Segundo a Polícia Civil, apenas um dos investigados no caso desviou mais de R$ 1,4 milhão para sua conta.

Payão (2018a) relata a tentativa de extorsão de um *hacker* que invadiu o sistema do Banco Inter em 2018. No evento, o invasor expões ao banco, o qual estava

prestes a se lançar como empresa de capital aberto na Bolsa de Valores de São Paulo (BOVESPA), que invadiu o sistema do banco (que é totalmente digital), possuía informações pessoais e bancárias de cerca de 300 mil clientes, como números de cartão de crédito, contas e senhas, caso não fosse pago o valor solicitado (não revelado) o criminoso venderia tais dados, além de divulgar parte deles para denegrir a imagem do banco ante sua pretensão de ingressar na BOVESPA. O banco não pagou e o *hacker* divulgou ao sítio especializado Techmundo. Em seguida, houve a abertura de um inquérito civil público, conforme Payão (2018b), e o Ministério Público do Distrito Federal e Territórios (MPDFT) constatou o comprometimento de dados de 19.961 correntistas do banco, dos quais cerca de 13 mil foram dados bancários. Segundo Agência Estado (2018), tal informação foi confirmada pelo banco cerca de 3 meses depois, e segundo o mesmo, houve a participação de um funcionário.

Como consequência da ação do *hacker* ao Banco Inter, segundo Payão (2018b), o MPDFT moveu uma ação civil pública por danos morais coletivos contra o banco pedindo uma indenização no valor de R$ 10 milhões, em razão de não haver tomado os cuidados necessários para garantir a segurança de dados dos clientes.

O nível de sofisticação dos ataques no Brasil é tão elevado que, segundo Loubak (2018), chegam a apresentar métodos capazes de driblar mecanismos de autenticação biométrica. Esse *malware* foi descoberto em agosto de 2018 por pesquisadores do IBM X-Force[28].

Visto os exemplos expostos, tanto no exterior quanto no Brasil, pode-se verificar o quanto os ataques cibernéticos são significativos e relevantes para as economias atacadas. Com isso, o questionamento de qual é o impacto causado pelos ataques cibernéticos ao setor financeiro torna-se inevitável.

3.4 Diagrama de ciclo causal aplicado a ataques cibernéticos

Como já foi tratado na seção 1.2, os ataques cibernéticos podem ser gerados por diversas razões. Quando ocorrem, criam efeitos que extrapolam ao recebedor do ataque, podendo afetar atores que se relacionam à vítima, como clientes, parceiros, concorrentes e o governo (pois em uma visão macro deve intervir quando surgem falhas de mercado).

Por haver uma relação de causa e efeito em vários participantes do mercado, Lagazio, Sherif e Cushman (2014) aperfeiçoaram o modelo de Anderson et al

[28] IBM X-Force Reserch é uma equipe de pesquisa em segurança comercial, o qual faz parte do grupo IBM. (IBM, 2018).

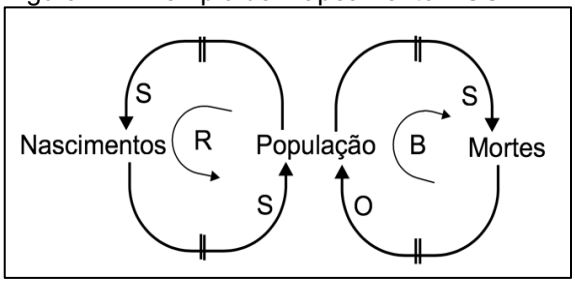
apresentado em *Mesuring the Cost of Cyber Crime* em 2012 para dimensionar os custos causados pelos crimes cibernéticos. Trata-se do diagrama de ciclo causal[29] (DCC). Esse método é um tipo de sistema dinâmico que, segundo os autores, é uma convenção de diagramação que ajuda a representar estruturas de *feedbacks* em problemas, mostrando como uma ação cria reflexos em outras relacionadas ao problema analisado.

Esse modelo é aplicável aos atacantes cibernéticos que agem de forma racional, ou seja, que realizam uma análise de custo-benefício em suas ações e decidem pela linha de ação que mais benefícios lhes traz. Assim, excluem-se os que agem por fins ideológicos (como os hacktivistas), vingança e passionais pois, nesses casos, a lógica de ação leva em conta benefícios psicológicos e ideológicos.

O DCC faz uma representação, por meio de figuras, da relação causa-efeito de forma simplificada, mas bastante ilustrativa e considera diversas variáveis sobre o objeto em análise. Para melhor entendimento, será utilizada a explicação do método feita por Lagazio, Sherif e Cushman (2014). Eles exemplificam o mapeamento utilizando DCC para analisar a população de uma localidade, para tal, consideram dois fatores: nascimentos e mortes, em um cenário em que há retardo (*delay*) em algumas consequências e outras são imediatas.

Assim, ambos fatores atuam diretamente na quantidade da população. Por haver uma população, há tendência de nascerem crianças no futuro (ação retardada), ao ocorrer o nascimento, imediatamente, há o aumento da população. Esse é um caso de fato que cria um reforço na população. Por outro lado, havendo uma população, no futuro (ação retardada), as pessoas morrerão. Nesse momento, há um decréscimo na população. É evidente que ambos fatores são independentes, mas influenciam diretamente na população. Esse exemplo pode ser visualizado na figura 4.

Figura 4 – Exemplo de mapeamento DCC



Fonte: LAGAZIO, SHERIF e CUSHMAN, 2014.

[29] Em inglês, *causal loop diagrams (CLD).*

A simbologia utilizada no DCC tem o seguinte significado: quando um fator possui relação causal positiva sobre o efeito, é representado por (S); quando possui relação negativa, por (O); quando a consequência ocorre com efeito retardado, é representada por (||); quando a ação cria um reforço, é representada por (R); e quando gera um decréscimo, é representada por (B).

Lagazio, Sherif e Cushman (2014) concluíram que os crimes cibernéticos influenciam e são influenciados por uma série de fatores que criam várias relações de causa e efeito. Por essa razão elegeram o DCC como metodologia para análise dos custos criados pelos crimes cibernéticos ao setor financeiro. Os autores identificaram que esses custos podem ser divididos em três grupos:

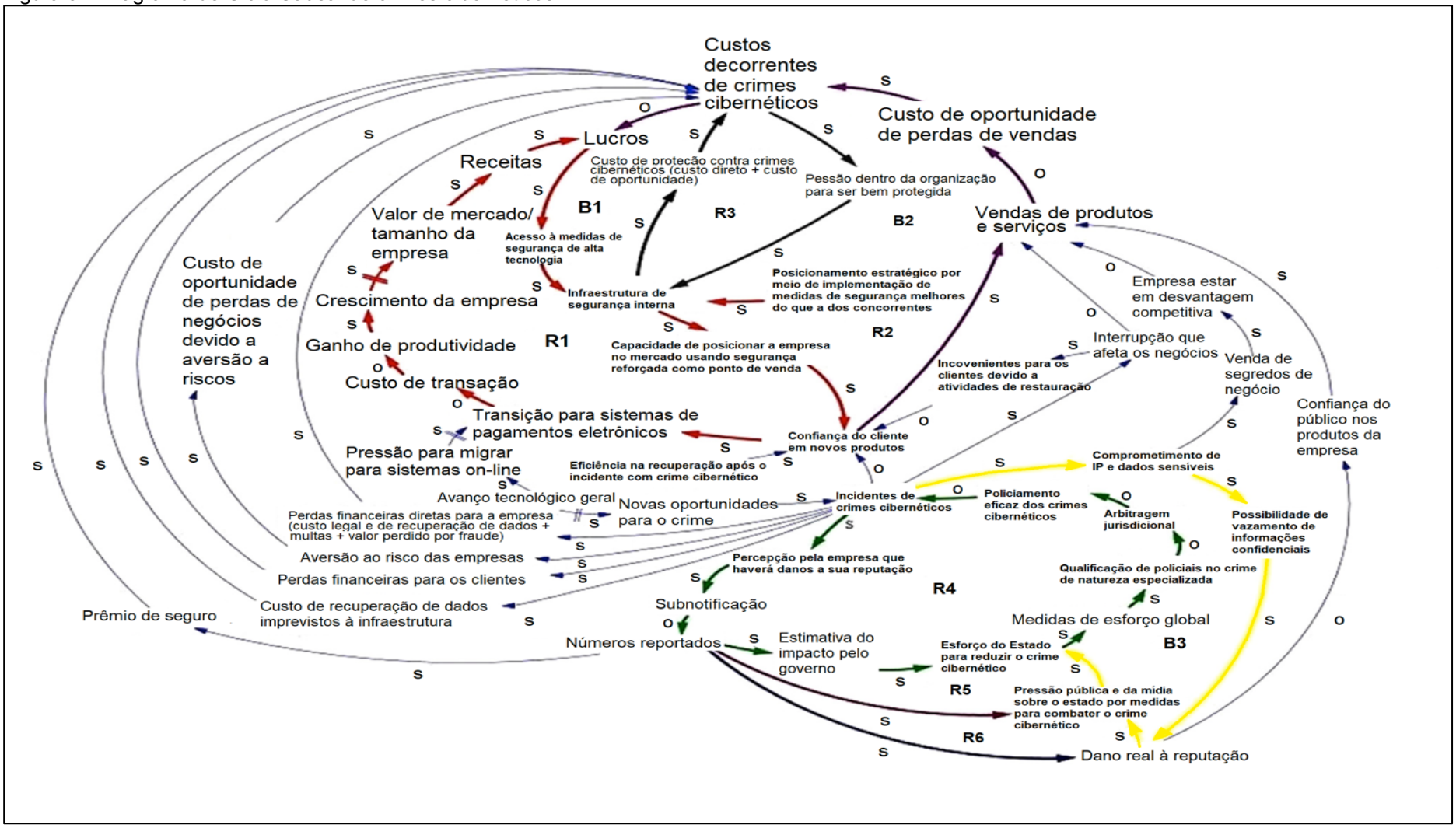
a – custos diretos (perdas monetárias, danos a sistemas, gastos com limpeza e recuperação dos sistemas, custos legais, perda de confiança e fechamento de contas de clientes);

b – custos indiretos (relacionados ao custo de oportunidade impostos à organização ou à sociedade, onde esses consideram a possibilidade de haver redução de vendas de serviços, recuperação de danos imprevistos nas infraestruturas, dano global à reputação que se estenda além dos próprios clientes da empresa, perda de confiança dos cidadãos em geral no setor, desvantagem competitiva devido a roubos de propriedade intelectual e custos de oportunidades por mudanças de prioridades e estratégias em resposta ao crime cibernético); e

c – custos de proteção (contratação de seguros, contratação de medidas de proteção cibernética, treinamento e conscientização de pessoal e todos os custos relacionados com segurança cibernética em detrimento das atividades geradoras de receita).

Assim como a maior parte dos que buscaram quantificar os custos criados pelos ataques e crimes cibernéticos, Lagazio, Sherif e Cushman (2014) também se depararam com a escassez de dados referentes à ataques sofridos, o que chamaram de subnotificação. Tal aspecto torna-se um impeditivo para realizar uma análise sobre o assunto com precisão. Entretanto, a abordagem com o método do diagrama de ciclo causal permite inferir os aspectos relacionados aos ataques cibernéticos direcionados ao setor financeiro. Utilizando essa análise, será feita uma proposta de medição dos impactos causados por esses ataques. Os autores chegaram ao diagrama expresso na figura 5.

Figura 5 – Diagrama de Ciclo Causal de crimes cibernéticos



Fonte: LAGAZIO, SHERIF e CUSHMAN, 2014.

Para o entendimento detalhado da análise dos autores, sugere-se a leitura do artigo dos mesmos. No entanto, apenas visualizando a figura 5, pode-se verificar diversos fatores que influenciam no número de ataques cibernéticos, por exemplo, o ciclo R4 (representado pelas setas verdes) permite concluir que se as informações sobre ataques sofridos pelas empresas do setor financeiro forem reportadas às autoridades competentes, essas poderão estimar o problema na dimensão adequada. Em consequência, haverá um esforço para especializar a quantidade necessária de agentes para combater tal crime. Possuindo maior especialização, as autoridades do governo (policiais e judiciárias) tenderão a ser mais eficazes contra os criminosos, o que contribui para a redução dos crimes cibernéticos. Por outro lado, se as empresas não notificarem os ataques sofridos, pela percepção de que tal informação criaria danos à sua imagem, o inverso ocorre, chegando-se a um cenário de aumento de crimes cibernéticos no final do ciclo. Análises semelhantes são feitas em todos os ciclos da figura 5 considerando os outros fatores.

3.5 Proposta de fórmula para quantificação dos custos causados por ataques cibernéticos ao setor financeiro

A dificuldade de obtenção de dados sobre os custos das instituições do setor financeiro decorrentes de ataques cibernéticos tornou-se um impeditivo para a determinação adequada do impacto econômico causado ao setor nesta investigação. No entanto, pôde-se contribuir com a proposição de como fazê-lo, assim, alguém possuidor da base de dados adequada, poderá alimentá-la e chegar à estimativa dos custos causados ao setor e seu respectivo impacto econômico.

Nossa proposição é simples, para determinar o custo total (C_T), deve-se somar os custos diretos (C_d) com os custos indiretos (C_i) e os custos de proteção (C_p) em um espaço de tempo (t), que é o valor, medido em dias ou meses, do período compreendido entre a percepção da ocorrência do ataque cibernético até a eliminação de seus efeitos, conforme a fórmula (1). Esse cálculo nos dá o custo de forma simplificada para cada ente envolvido, sejam as empresas do setor financeiro, seja o governo com medidas visando o combate aos ataques cibernéticos, ou ainda, seguradoras e em última instância, os clientes.

$$C_T = \sum_{i=1}^{t} \left(C_d + C_i + C_p \right) \quad (1)$$

Os custos diretos, indiretos e de proteção são os indicados por Lagazio, Sherif e Cushman (2014) e mostrados na seção 3.4 deste trabalho. Desses, certamente, os custos indiretos são os mais difíceis de serem mensurados, principalmente, os custos de perda de credibilidade e de desvantagem competitiva devido a roubos de propriedade intelectual.

Do exposto, têm-se que o custo total do setor financeiro ($C_{T(fi)}$) é a soma do custo total (C_T), de todas as empresas do setor, conforme a fórmula (2).

$$C_{T(fi)} = \sum_{i=1}^{t} \left(C_{T(fi1)} + C_{T(fi2)} + C_{T(fi3)} + \cdots + C_{T(fin)} \right) \quad (2)$$

Da mesma forma, o setor de seguros sofre perdas quando o ataque cibernético é exitoso sobre o setor financeiro, se este possuir uma apólice contra os mesmos. Assim, esses valores devem compor o cálculo do impacto de ataques cibernéticos ao setor financeiro. E esse valor é dado pelo somatório de prêmios de apólices ($C_{T(se)}$) pagos pelas seguradoras aos segurados, conforme a fórmula (3).

$$C_{T(se)} = \sum_{i=1}^{t} \left(C_{T(se1)} + C_{T(se2)} + C_{T(se3)} + \cdots + C_{T(sen)} \right) \quad (3)$$

Outro ator que compõe o cálculo do impacto dos ataques cibernéticos sofridos pelo setor financeiro é o governo, principalmente por meio de gastos no combate aos criminosos, como treinamento de pessoal especializado em investigação cibernética, gastos com estruturas policiais e jurídicas especializadas, gastos para prevenir ataques (que indiretamente contribuem para o reduzir as perdas do setor financeiro), além de perdas indiretas, como redução da arrecadação fiscal por parte do setor financeiro face aos prejuízos tidos pelos ataques cibernéticos. Dessa forma, o valor do custo total do governo ($C_{T(go)}$) é a soma dos custos diretos para combater os ataques cibernéticos ($C_{d(go)}$) e os custos indiretos ($C_{i(go)}$), conforme a fórmula (4).

$$C_{T(go)} = \sum_{i=1}^{t} \left(C_{d(go)} + C_{i(go)} \right) \quad (4)$$

Por fim, os custos dos clientes do setor financeiro em razão de ataques cibernéticos devem compor o cálculo do impacto sofrido pelo setor. Da mesma forma

que os demais atores, o custo total dos clientes ($C_{T(cl)}$) é o somatório de todos os custos diretos ($C_{d(cl)}$), indiretos ($C_{i(cl)}$) e de proteção ($C_{p(cl)}$) que os clientes tiveram em decorrência de ataques cibernéticos ao setor financeiro como, por exemplo, indisponibilidade de serviços como saques e transferências, constrangimentos por falta indevida de saldos, atrasos em negócios, aquisição de mecanismos de defesa como antivírus para acessar a serviços bancários, etc. Assim, o custo total dos clientes ($C_{T(cl)}$) pode ser visto na fórmula (5).

$$C_{T(cl)} = \sum_{i=1}^{t} \left(C_{T(cl1)} + C_{T(cl2)} + C_{T(cl3)} + \cdots + C_{T(cln)} \right) \quad (5)$$

Dessa forma, o impacto (I) dos ataques cibernéticos ao setor financeiro é o somatório do custo total de todas as empresas do setor financeiro ($C_{T(fi)}$), com o custo total de todas as empresas do setor de seguros que pagaram prêmios referentes à ataques cibernéticos ao setor financeiro ($C_{T(se)}$), com os custos do governo para combater os ataques cibernéticos e suas perdas de arrecadação ($C_{T(go)}$), e o custo total que os clientes do setor financeiro ($C_{T(cl)}$) tiveram em decorrência de ataques cibernéticos ao setor. Tudo isso em um determinado período de tempo (t) que pode ser em dias ou meses, conforme pode ser visto na fórmula (6).

$$I = \sum_{i=1}^{t} \left(C_{T(fi)} + C_{T(se)} + C_{T(go)} + C_{T(cl)} \right) \quad (6)$$

Do exposto, torna-se evidente que os ataques cibernéticos oferecem iminente ameaça aos diversos países, tanto em setores produtivos, quanto nos financeiros, ou ainda, à segurança nacional. Por essa razão, diversos Estados criaram ou estão em processo de criação de mecanismos para fortalecerem suas capacidades de defesa nesse campo.

4 COMBATE E PREVENÇÃO AOS ATAQUES CIBERNÉTICOS

Tendo conhecimento das capacidades criadas e o quão danoso pode ser o advento cibernético, os países passaram a buscar soluções para prevenirem-se de possíveis ataques nos níveis governamentais, ou ainda, para desenvolverem capacidades ofensivas, caso necessário, em um cenário denominado Guerra Cibernética. Da mesma forma, o setor privado busca proteger-se dos ataques cibernéticos, tendo em vista que é o principal alvo dos criminosos em tempos de paz.

O advento do espaço cibernético criou o conceito de segurança cibernética que, para o Ministério da Defesa do Brasil, “é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas” (BRASIL, 2014a, p. 19).

Outro conceito surgido foi o de defesa cibernética que, para Oliveira et al. (2017, p. 13), é o “ato de defender o sistema crítico das TIC de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país”. Já para o MD brasileiro, esse é um conceito mais restrito, assim definido:

> Defesa cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (BRASIL, 2014a, p. 18)

O conceito de proteção cibernética é, para o MD, uma atividade de caráter permanente que abrange ações para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de computadores e de comunicações (BRASIL, 2014a, p. 23). Esse último conceito é o que melhor se adequa aos setores da iniciativa privada, o que não significa que lhe é exclusivo, uma vez que todos devem buscar fazê-lo. Por fim, o conceito de Guerra Cibernética que é, em resumo, o uso do espaço cibernético em operações militares.

4.1 Segurança e Defesa Cibernética pelo mundo

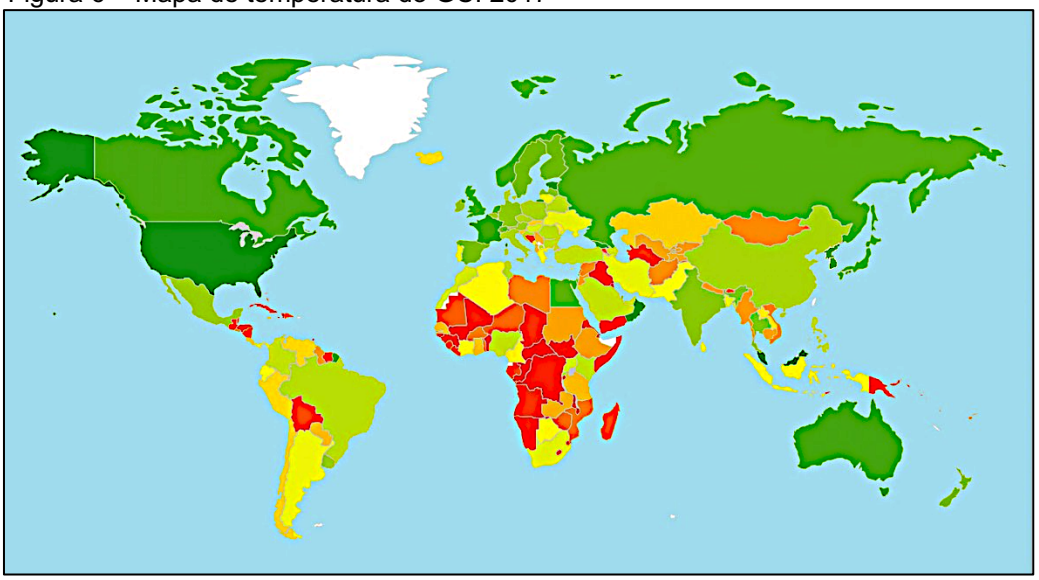
A União Internacional de Telecomunicações (ITU, sigla em inglês) publicou o Índice Global de Segurança Cibernética (GCI, sigla em inglês) 2017. Esse índice considera 25 parâmetros que compõem 5 pilares: legal, técnico, organizacional, capacitação e cooperação (ITU, 2017).

Em linhas gerais, os pilares do GCI são descritos da seguinte maneira:

> 1. Legal: Medido com base na existência de instituições legais e estruturas que lidam com segurança cibernética e crimes cibernéticos.
> 2. Técnico: Medido com base na existência de instituições técnicas e estruturas relacionadas à segurança cibernética.
> 3. Organizacional: Medido com base na existência de instituições de coordenação de políticas e estratégias para o desenvolvimento de segurança cibernética em nível nacional.
> 4. Capacitação: Medido com base na existência de programas de pesquisa e desenvolvimento, educação e treinamento; profissionais certificados e agências do setor público promovendo a capacitação.
> 5. Cooperação: Medido com base na existência de parcerias, quadros cooperativos e redes de partilha de informação. (ITU, 2017, p. 4)

O índice avaliou 193 países e chegou ao mapeamento global conforme a figura 6, onde a cor verde com tonalidade mais escura sinaliza os maiores índices e os vermelhos mais escuros indicam os menores.

Figura 6 – Mapa de temperatura do GCI 2017



Fonte: ITU, 2017.

Os dez países que obtiveram os maiores índices no GCI foram Singapura, EUA, Malásia, Omã, Estônia, Maurícias, Austrália, Geórgia, França e Canadá. No anexo A encontra-se *scorecard* da região das Américas, onde é possível verificar as menções atribuídas aos países do continente. Na classificação global, o Brasil aparece na 38ª posição, com índice 0,59338, figurando como o quinto das Américas, atrás de Estados Unidos, Canadá, México e Uruguai. Nessa análise, o Brasil foi classificado pela ITU como “em fase de amadurecimento”.

Analisando-se o GCI, é possível verificar os distintos níveis dos países em relação à temática cibernética. Além disso, há distintos modelos para tratar de segurança cibernética e defesa cibernética. Segundo Oliveira et al. (2017), há basicamente três deles, com uma pequena variação no terceiro modelo. O primeiro,

adotado por países como Estados Unidos, Colômbia e Venezuela, utiliza estruturas militares como responsáveis tanto pela defesa cibernética quanto pela segurança cibernética. O segundo, adotado no Paraguai, utiliza estruturas civis que também tratam incidentes cibernéticos na esfera militar. E o terceiro modelo é o adotado por países como Brasil e Argentina, que possuem estruturas civis para lidar com a segurança cibernética e estruturas militares para a defesa cibernética. Por fim, há uma variação do último modelo, adotada pelo Uruguai. Nele existem estruturas distintas bem definidas para os setores civil e militar, que são responsáveis, respectivamente, pela segurança cibernética e pela defesa cibernética. Contudo, a política de Defesa uruguaia prevê a atuação das estruturas militares de defesa cibernética também no setor privado.

A temática relacionada a crimes cibernéticos é tratada como relevante à segurança nacional pelo governo brasileiro e por outros como o dos EUA. Os norte-americanos, por meio da Divisão Cibernética do FBI, investigam casos de invasão de computadores, contraterrorismo e contrainteligência como as principais prioridades do programa cibernético devido à sua possível relação com a segurança nacional (FBI, 2018). Segundo FBI (2018), foi criada, recentemente, uma força-tarefa composta por diversas agências do governo, dentre elas o Departamento de Defesa, o Departamento de Segurança Interna e o próprio FBI, com o objetivo de trabalharem em conjunto para combater os crimes cibernéticos.

Algo semelhante ocorre na Austrália, onde, segundo Office of Prime Minister (2017), o governo australiano investiu US$ 230 milhões na Estratégia Nacional Segurança Cibernética em 2016 e o Livro Branco de Defesa da Austrália prevê incremento de até US$ 400 milhões para melhoria das capacidades de defesa cibernética do país.

Na Europa, segundo o *National Cyber Security Centre* (NCSC, sigla em inglês), a União Europeia (UE) reconheceu que qualquer incidente de segurança cibernética poderia afetar vários Estados-Membros e, em 2013, apresentou uma proposta para melhorar a sua preparação para ataques cibernéticos. Esta proposta tornou-se, em 2016, uma diretiva denominada *The UE directive on the security of Network and Information Systems* (NIS, sigla em inglês), dando aos Estados-Membros 21 meses para integrarem a diretiva nas respetivas legislações nacionais (NCSC, 2018).

O Reino Unido, segundo o UK Cabinet Office (2016), elevou o orçamento em defesa cibernética de £ 860 milhões para £ 1,9 bilhão, entre 2016 e 2021, com ênfase

em três áreas: defesa de estruturas críticas nacionais como energia e transporte; retaliação a atacantes; e formação de uma geração de especialistas, com ênfase no investimentos em centros de pesquisa e ensino de segurança cibernética nas escolas.

Segundo o NCSC (2018), serão implementadas mudanças na legislação do Reino Unido, conforme a Diretiva de Segurança de Redes e Sistemas de Informação da União Europeia, visando aumentar os níveis de segurança e resiliência globais dos sistemas de rede e de informação, obtendo, assim, base jurídica para:

> Dispor de um quadro nacional equipado para gerir incidentes de segurança cibernética. Isso inclui uma Estratégia Nacional de Segurança Cibernética, uma Equipe de Resposta a Incidentes de Segurança da Computação (CSIRT, sigla em inglês) e uma autoridade nacional de Segurança de Redes e Sistemas de Informação.
> Criar um Grupo de Cooperação com os membros da UE para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações, participando de uma rede de CSIRT para promover uma cooperação operacional rápida e eficaz em incidentes específicos de segurança de redes e sistemas de informação, bem como partilhar informações sobre os riscos. (NCSC, 2018)

Hakmeh (2017) afirma que nos países do Conselho de Cooperação do Golfo (GCC, sigla em inglês) há significativa diferença da forma com que seus países membros tratam legalmente os crimes cibernéticos. A autora põe como fundamental a existência de aspectos legais definidos nas legislações dos países para que o combate aos crimes cibernéticos seja efetivo, como a definição de leis sobre o tema, tipificação criminal, regulação de interação entre Estados com fins cooperativos, definição de poderes processuais, definição de termos e os parâmetros de sua aplicação, estabelecimento de regras para provas eletrônicas, definição de sua jurisdição, e descrever a responsabilidade dos prestadores de serviços. O quadro 4 apresenta como estão os países do GCC nesses aspectos.

Quadro 4 – Estado das leis sobre crimes cibernéticos nos países do Conselho de Cooperação do Golfo

País / Característica-chave	Barein	Kuwait	Omã	Catar	Arábia Saudita	Emirados Árabes Unidos
Definição	x	x	x	x	x	x
Criminalização	x	x	x	x	x	x
Poderes processuais	x			x		
Evidência eletrônica						
Jurisdição						
Cooperação internacional				x		
Responsabilização do provedor de serviços				x		
Crimes adicionais não previstos em outros instrumentos internacionais		x	x	x	x	x

Fonte: HAKMER, 2017.

Analisando o quadro 4, percebe-se que todos os países do Conselho de Cooperação do Golfo possuem leis sobre crimes cibernéticos, porém, segundo Hakmer (2017), essas, em sua maioria, apenas concentram-se na criminalização. Ademais, nota-se que o Catar é o país da região com maior avanço nas suas leis, denotando maior adequação ao cenário atual.

Hakmer (2017) enfatiza que a melhor forma de combater os crimes cibernéticos é a cooperação internacional, sem a qual a efetiva atuação tende a ser ineficiente, pois as técnicas de atuação dos atacantes mudam com elevada velocidade. Assim, a autora destaca que é necessário haver compartilhamento de informações, inteligência, experiências e lições aprendidas para encontrar as melhores maneiras de conter o crime cibernético e abordar seus desafios, para tanto, ferramentas regulatórias, legais e tecnológicas precisam ser desenvolvidas coletivamente e atualizadas continuamente.

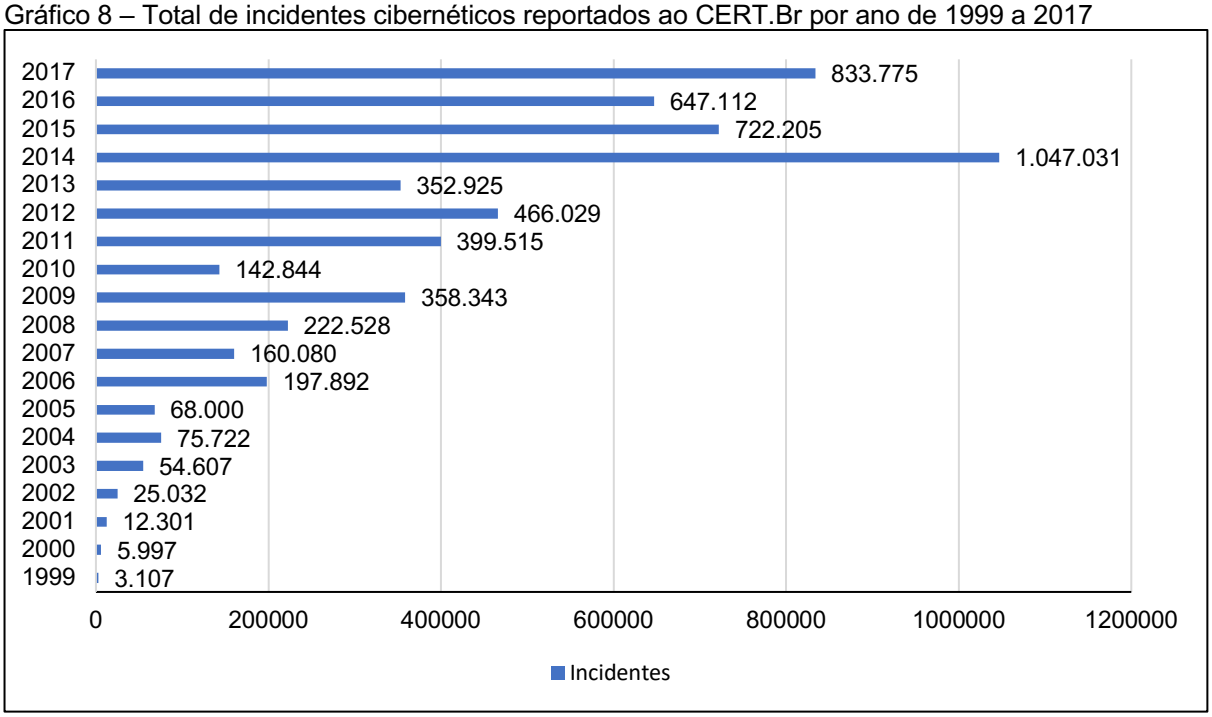
Dessa forma, pôde-se verificar que nas diversas regiões do mundo, o tema da defesa cibernética consta da pauta governamental.

5 PASSADO PRESENTE E FUTURO DE ATAQUES CIBERNÉTICOS NO BRASIL

5.1 Passado

Desde 2006, o Brasil rompeu a barreira de mais de 100 mil incidentes cibernéticos reportados ao CERT.br em um ano. Desde então, apresentou uma forte tendência de crescimento desse número, com um pico em 2014, com mais de 1 milhão de incidentes reportados, como pode-se observar no gráfico 8. Esses números são menores do que os reais, pois nem todos os incidentes são reportados. Entretanto, ainda assim, permitem a obtenção de um panorama geral.

Gráfico 8 – Total de incidentes cibernéticos reportados ao CERT.Br por ano de 1999 a 2017



Fonte: CERT.br, 2018b.

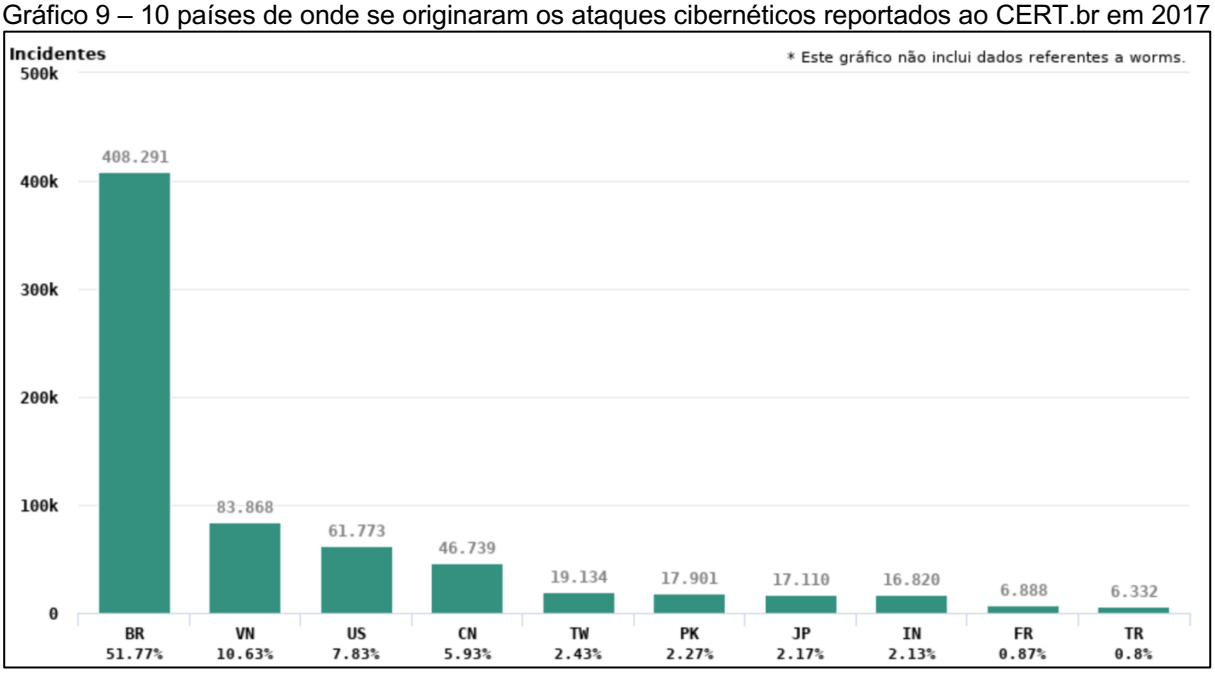
Como pode-se perceber no gráfico 8, o Brasil é um alvo relevante de ataques cibernéticos. A esse respeito, há estudos que indicam o destaque para os ataques com finalidade de obtenção de vantagens financeiras. Lewis (2018), em sua análise para a Mcafee, identificou o impacto econômico de crimes cibernéticos em alguns países como Austrália, Brasil, Canadá, Alemanha, Japão, México, Reino Unido e Emirados Árabes Unidos. Nesse estudo, Lewis (2018) aponta o Brasil como um dos novos centros de crimes cibernéticos, juntamente com a Índia, Coreia do Norte e Vietnã.

Lewis (2018) apresenta o Brasil como caso único no mundo em que existem fatores facilitadores à existência do crime cibernético. Isso faz com que o país esteja

em segundo lugar no número de ataques cibernéticos originados no território e seja o terceiro principal alvo de ataques dessa natureza.

Lewis (2018) aponta que as leis brandas poderiam ser uma das causas de que 54% dos ataques cibernéticos reportados no Brasil são originários de dentro do próprio país, tendo como principal alvo, os bancos e instituições financeiras. Esse dado é coerente com os apresentados pelo CERT.br (2018c) em que 51,77% dos ataques que lhe foram reportados procederam do Brasil, conforme o gráfico 9, onde constam o "*top10*" da origem dos ataques sofridos no Brasil.

Gráfico 9 – 10 países de onde se originaram os ataques cibernéticos reportados ao CERT.br em 2017



Fonte: CERT.br, 2018c.

O gráfico 9 mostra que o maior risco cibernético enfrentado pelas instituições brasileiras originam-se do próprio território nacional. Nesse sentido, têm-se, segundo Lewis (2018), que 95% das perdas sofridas pelos bancos brasileiros foram causados por ataques cibernéticos.

No Brasil existem leis que tratam sobre o tema, como a Lei nº 12.737, de 30 de novembro de 2012, conhecida popularmente como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Código Penal Brasileiro (BRASIL, 2012a) e a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecida como Marco Civil da Internet (BRASIL, 2014b). Assim, ao aceitarmos a análise de Lewis (2018) é possível que tais leis não obtenham a eficácia adequada para inibir a

criminalidade em razão de seu grau de rigidez, pois na primeira lei, as penas não passam de três anos de prisão e a segunda não contempla penalidades aos infratores.

A possibilidade de ganhos elevados com os ataques cibernéticos e percepção de impunidade, cria uma relação de custo-benefício para os criminosos em que incentiva a realização do ataque. Mesmo havendo iniciativas por parte do setor privado para proteger-se, há uma notória falha de mercado, pois os criminosos, quando obtêm êxito em suas ações cibernéticas, geram externalidades[30] negativas para suas vítimas, como perdas financeiras para clientes e bancos, elevação de custos de prevenção, etc.

Outro aspecto que indica a existência de falha de mercado, no tocante aos ataques cibernéticos, é a assimetria de informações, pois conforme já tratado, é um campo no qual há elevadas incertezas sobre as suas reais dimensões e não há incentivos para que haja o compartilhamento de informações que verdadeiramente permitam fazer tal dimensionamento.

Ademais, já foi mostrado que o espaço cibernético pode ser utilizado em ações cibernéticas com fins militares entre Estados, como ocorreu na usina nuclear iraniana com o uso do *Stuxnet*, assim a atuação governamental no sentido de fortalecer as capacidades de proteção cibernética para o país pode, indiretamente, contribuir para a redução da falha de mercado criada pelos ataques cibernéticos, se forem criadas medidas que incentivem ações conjuntas entre os setores públicos e privados. Uma vez que os conhecimentos necessários para proteger instalações críticas, como hidrelétricas apresentam semelhanças aos de proteger bancos de dados de instituições financeiras, seria viável a atuação conjunta. Tal parceria contribuiria tanto para reduzir as falhas de mercado, quanto para fortalecer a defesa nacional que, por definição, é um bem público.

Em virtude de aspectos como os acima mencionados, a atuação do Estado é importante e desejável. Esta, visando tornar o país menos vulnerável a ilicitudes e agressões por meio do espaço cibernético. Assim, medidas foram tomadas para adequar o Brasil ao cenário enfrentado.

---

[30] Os economistas chamam de externalidade o efeito que não se reflete nos custos e nos benefícios dos agentes, tampouco nos mecanismos de preço. No entanto, esse efeito gera consequências a terceiros. Quando esse reflete, no terceiro, de forma benéfica, é denominado de externalidade positiva, caso contrário, de externalidade negativa.

Ao criar a Política Nacional de Defesa em 2008, com revisão em 2012, o Brasil classificou o setor cibernético, juntamente com o nuclear e o espacial como estratégicos (BRASIL, 2012b). Isso permitiu a inclusão do setor cibernético na Estratégia Nacional de Defesa (END) o que, segundo Brasil (2014a), permitiu que a segurança cibernética e a defesa cibernética passassem a ser reconhecidos como campos sob responsabilidade de atuação do Estado.

Em 2009, segundo Brasil (2018a), o Ministério da Defesa designou o Exército Brasileiro como responsável pelo estabelecimento do setor cibernético, em consequência, foi criado o Projeto de Defesa Cibernética. Esse projeto deu início ao Centro de Defesa Cibernética (CDCiber), órgão destinado a concentrar pessoal capacitado na área. Além do núcleo da Escola Nacional de Defesa Cibernética (ENaDCiber), para implementar pesquisas científicas voltadas ao tema e coordenar com instituições civis, acadêmicas e empresariais atividades conjuntas.

O Projeto de Defesa Cibernética ganhou maiores proporções, sendo substituído pelo Programa Estratégico do Exército Defesa Cibernética em 2016. Moury (2017) complementa que a prioridade do governo brasileiro com a defesa e a proteção cibernética levaram ao surgimento do Comando de Defesa Cibernética (ComDCiber) em 2016. Esse comando passou a englobar o CDCiber e funcionar com pessoal das três Forças Armadas, além de especialistas civis.

A END apresentou entre seus objetivos: promover ações conjuntas entre os Ministérios da Defesa e da Ciência, Tecnologia e Inovação contemplando o incentivo à multidisciplinaridade e dualidade de aplicações, fomento da Base Industrial de Defesa, aquisição de conhecimentos, geração de emprego e proteção das infraestruturas estratégicas do Brasil (BRASIL, 2012b). Esse contexto permitiu a estruturação do Estado Brasileiro na formatação adotada em 2018, conforme será tratado a seguir.

5.2 Presente

No Brasil, atualmente, a responsabilidade de proteger os ativos nacionais no espaço cibernético são divididas para os setores civil e militar. Tal divisão ocorre de acordo com nível de atuação dos agentes públicos.

Segundo Brasil (2017a), a responsabilidade do planejamento, coordenação e desenvolvimento de ações de segurança cibernética é do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR).

Já a defesa cibernética age no nível estratégico. Na prática, tal divisão põe a segurança cibernética em um nível superior à Defesa Cibernética. Assim a primeira engloba a segunda, conforme pode-se visualizar na figura 7, onde são representados os níveis de decisão referentes ao espaço cibernético que foram adotados pelo governo brasileiro.

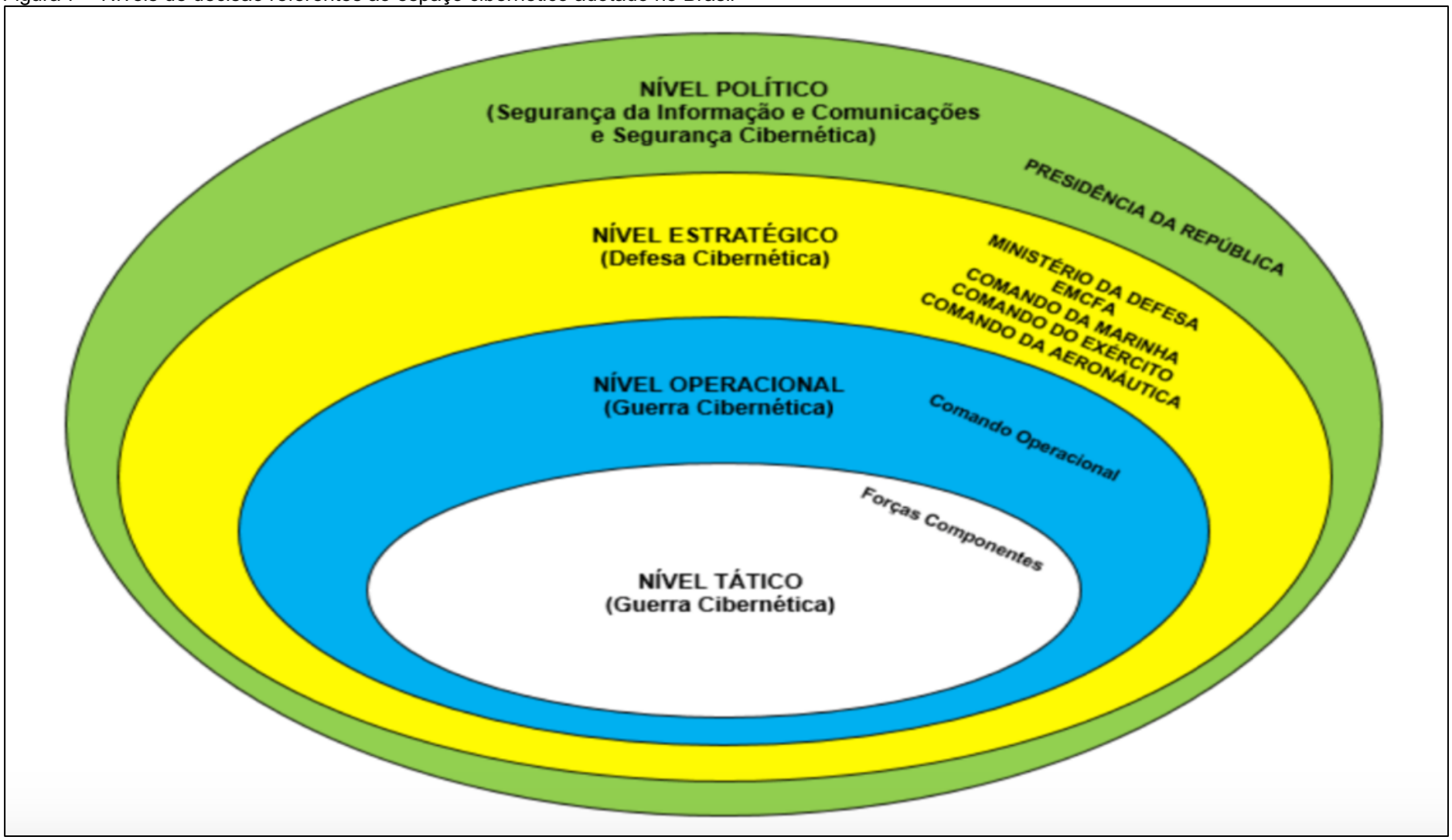
A figura 7 resume o que é tratado em cada nível de decisão quanto a ataques cibernéticos e qual órgão possui essa responsabilidade. Assim, o DSIC/GSI-PR é encarregado pelo nível político; o ComDCiber pelo estratégico; o CDCiber pelo operacional e unidades militares das forças componentes pelo nível tático.

Alguns objetivos da END explicitados no item 5.1 já ocorrem, como a aquisição de conhecimentos, produzindo o desenvolvimento de ferramentas com aplicação dual (tanto para fins militares como para o mercado) na área de cibernética. Pode-se citar o Simulador de Operações de Guerra Cibernética (SIMOC) que é um simulador virtual que foi desenvolvido com tecnologia 100% nacional, pelo Exército Brasileiro em parceria com uma empresa de Tecnologia da Informação. O SIMOC destina-se ao treinamento e simulação de situações para as tropas contra possíveis ataques cibernéticos (BRASIL, 2018b).

Conforme já tratado, segundo ITU (2017), o Brasil encontra-se em um nível intermediário no tocante à segurança cibernética, ocupando a 38ª posição, com GCI 0,59338. Até o término deste trabalho, o índice de 2018 não havia sido publicado. No entanto, é evidente que estar em uma condição intermediária, significa que há oportunidades de melhoria.

Na busca pelo fortalecimento das capacidades de defesa cibernética, o Governo brasileiro trabalha conjuntamente com organizações públicas e privadas. Por exemplo, em julho de 2018, em Brasília, ocorreu o primeiro exercício de simulação de ataques em massa aos setores financeiro, nuclear e de defesa, utilizando o SIMOC. Esse exercício conjunto foi denominado Guardião Cibernético e contou com a participação de gestores de crise e técnicos da área de proteção cibernética de instituições do setor financeiro, como Banco Central, bancos públicos e privados, empresas do setor nuclear, Ministérios da Defesa, das Relações Exteriores, Presidência da República e entidades do setor cibernético (BRASIL, 2018b).

Figura 7 – Níveis de decisão referentes ao espaço cibernético adotado no Brasil



Fonte: BRASIL, 2014a.

Outro exemplo de parceria visando aumentar a resistência aos ataques cibernéticos é o acordo assinado entre a Fundação Parque Tecnológico Itaipu e o Exército Brasileiro em 2017, esse acordo trata sobre cooperação mútua no Laboratório de Segurança Eletrônica, de Comunicações e Cibernética que funciona desde 2015 no Complexo Hidrelétrico de Itaipu (BRASIL, 2017b).

A colaboração entre parceiros de outras nações faz-se necessária para o crescimento mútuo. Dessa forma, há atividades conjuntas com países que mantêm relações com o Brasil com o objetivo de trocas de conhecimentos, um exemplo é o Estágio Internacional de Defesa Cibernética, que ocorreu na sua terceira edição em 2018 no Centro de Instrução de Guerra Eletrônica do Exército, na cidade de Brasília, com participação de representantes de vários países (BRASIL, 2018c).

Por fim, ainda sobre as parcerias internacionais, segundo (ITU, 2017), a Polícia Federal do Brasil participa do sistema global de comunicações policiais I-24/7 desenvolvido pela Interpol para conectar policiais, incluindo crimes cibernéticos.

O Banco Central do Brasil (BCB), como órgão regulador do setor financeiro no Brasil, diante da relevância do tema, publicou a Resolução nº 4.658, de 26 de abril de 2018. Tal legislação dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo BCB (BRASIL, 2018d).

Na Resolução nº 4.658, o BCB determina que as instituições por ele autorizadas a funcionar implementem políticas de segurança com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados dos seus sistemas e o devido plano (BRASIL, 2018d). Ainda, no mesmo documento, há diversas determinações que visam à maior transparência sobre incidentes cibernéticos.

Nesse sentido, pode-se citar o “registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição”; determinar a criação de “mecanismos para disseminação da cultura de segurança cibernética”; que sejam extensivos a terceiros que acessam aos sistemas do banco (como prestadores de serviços); que seja confeccionado um relatório anual sobre o andamento do plano de ação e de respostas a incidentes, fornecendo maior fonte de dados ao BCB (BRASIL, 2018d).

Com as determinações presentes na Resolução nº 4.658, o Banco Central busca obter dados mais precisos sobre os ataques cibernéticos sofridos pelos bancos brasileiros. De posse desses dados, os entes governamentais podem tomar medidas mais adequadas para o cenário enfrentado como estimular a criação de cursos direcionados para a área de proteção cibernética, formação ou ampliação de equipes de peritos especializados, criação de leis específicas, entre outras.

5.3 Futuro

Fazer análises prospectivas não é tarefa trivial. No entanto, analisando-se as informações disponíveis é possível perceber uma tendência de crescimento do uso do espaço cibernético tanto por cidadãos quanto por criminosos. Nesse sentido, surge campo para a oferta de novos serviços relacionados aos equipamentos eletrônicos como *smartphones* e computadores pelo setor financeiro, tanto internamente quanto para seus clientes e parceiros. Essa tendência de aumento de utilização de meios *on-line*, abre espaço não apenas para o aumento do volume de ataques cibernéticos, como para o surgimento de novos tipos de ataques. Esse cenário, leva ao entendimento de que novas ações visando combater aos crimes cibernéticos deverão ser executadas, tanto pelo setor privado como pelo governo.

As medidas tomadas pelo Banco Central objetivando reduzir as subnotificações dos ataques sofridos pelo setor financeiro, somadas à percepção de que esses são verdadeiros óbices, aliados à ações conjuntas entre a iniciativa privada e órgãos públicos, conforme foram mostradas neste trabalho, nos permitem identificar a possibilidade de atuações mais efetivas, sob a condição de que se estabeleçam objetivos comuns e que haja, efetivamente, trocas de informações com colaboração mútua.

Os órgãos governamentais responsáveis pela defesa cibernética e pela segurança cibernética tendem a crescer de importância no país. Esse crescimento pode criar externalidades positivas como o fortalecimento das capacidades de reação e mesmo prevenção de ataques a diversos setores, dentre eles, o financeiro. Para tanto, faz-se necessário a criação de políticas públicas para permitir que haja maior atuação conjunta de órgãos como o CERT.br, polícias especializadas e Forças Armadas, de preferência, com a participação de órgãos de proteção ligados a setores estratégicos do país, como o de energia e o financeiro, como ocorreu no exercício conjunto Guardião Cibernético em 2018.

O setor financeiro brasileiro tende a manter fortalecendo-se contra ações hostis, especialmente em razão de encontrar nos crimes cibernéticos a maior fonte de perdas financeiras. No entanto, faz-se necessário a existência de massa crítica capacitada para trabalhar nesse setor que exige elevada capacidade de adaptabilidade e constante atualização de conhecimentos, pois a cada dia novas formas de se atacar surgem e novas medidas de defesa são necessárias.

A oferta de seguros contra perdas decorrentes de ataques cibernéticos tende a crescer. Segundo Martins (2018), desde 2012, quando a AIG passou a oferecer cobertura para ataques cibernéticos, é possível a contratação dessa modalidade de seguro no Brasil. Conforme o autor, o número de seguradoras que passaram a oferecer coberturas semelhantes aumentou, significativamente, após o ataque do *WannaCry* em 2017. Ainda assim, Martins (2018) enfatiza que a contratação de apólices ainda é baixa no Brasil (com valores aproximados de R$ 10 milhões) quando comparada à quantidade de ataques sofridos no país. E esse crescimento é uma tendência mundial, por exemplo, nos EUA esse mercado dobra a cada dois anos e gira em torno de US$ 2 bilhões.

Outra perspectiva é relacionada a formação de cidadãos com cultura de segurança cibernética. Essa medida é uma necessária para o fortalecimento dos sistemas computacionais do país. Assim, uma solução razoável é que seja promovida a inserção de conteúdos relacionados à segurança cibernética nas instituições de ensino desde os níveis mais básicos até os mais avançados. Se essa medida for adotada, os usuários terão, no mínimo, a consciência de que estão vulneráveis e que podem tomar medidas que lhes permitirá robustecer os sistemas como um todo.

Como há carência de leis específicas tratando sobre ataques cibernéticos, prospecta-se que essa deve ser uma pauta a ser discutida pelos legisladores. Por exemplo, Martins (2018) destaca que ainda não há legislação específica sobre proteção de dados no Brasil e que dois anteprojetos de lei estão em discussão no Congresso Nacional.

Verifica-se que a discussão sobre os ataques cibernéticos e medidas referentes ao tema é relativamente recente e tende a expandir-se em variados setores, pois envolve desde áreas da computação, como segurança de dados e redes, passando por questões jurídicas como leis, envolvendo até o campo econômico, pois afeta diretamente fatores como renda e produção. Dessa forma prospecta-se que no Brasil e no mundo estará na pauta de pesquisadores multidisciplinares.

CONCLUSÕES

O presente trabalho estudou os ataques cibernéticos sob uma perspectiva econômica, analisando seus reflexos no setor financeiro, com ênfase no Brasil. Após serem mostrados os conceitos relativos ao espaço cibernético, as ameaças sob as quais os usuários de sistemas computacionais e o quanto isso está presente na sociedade atual, foram exemplificados ataques cibernéticos de variados tipos em diversos setores, além de perdas sofridas pelas vítimas.

Pôde-se concluir que o uso do espaço cibernético se encontra em plena expansão, especialmente com a popularização dos *smartphones,* proporcionando acesso cada vez maior e com menores custos à internet e aos benefícios por ela oferecidos. Um desses são os aplicativos bancários que permitem realizar praticamente todas as operações que tradicionalmente só eram feitas nas agências. Esses aspectos permitiram aos bancos reduzir custos com agências, mas exigiram investimentos em infraestruturas voltadas para os serviços digitais.

Paralelamente ao crescimento da oferta de serviços por meios eletrônicos, há, tanto no Brasil quanto em outros países, a tendência de crescimento de ataques cibernéticos direcionados ao setor financeiro. Sobre esse aspecto, conclui-se que são justamente os ataques cibernéticos a maior fonte de perdas do setor bancário brasileiro. Por essa razão, o tema é relevante para considerações relacionadas a análises de risco pelos níveis decisórios dos bancos, além da necessidade da existência de uma política orçamentária prevendo a constante atualização das medidas de segurança das empresas.

Outra conclusão é que se não houver uma política criada pelo governo, as empresas vítimas de ataques cibernéticos evitarão expor os ataques por elas sofridos. Tal fato se deve à percepção das empresas de que podem perder credibilidade e haver danos à sua reputação. Esse aspecto gera subnotificação aos órgãos de controle e cria um ciclo prejudicial, pois criam uma imagem equivocada de que não são necessárias maiores ações para combater os crimes cibernéticos. Por outro lado, a existência de legislações que obriguem os bancos a informar os ataques sofridos, pode criar um ciclo virtuoso, oposto ao cenário anterior. Por essa razão, o Banco Central deu um primeiro passo ao estabelecer a Resolução nº 4.658 em 2018.

Devido à dificuldade de acesso a dados sobre ataques cibernéticos sofridos pelo setor financeiro do Brasil, não foi possível determinar o impacto desses ao referido setor. No entanto, propôs-se uma metodologia de quantificação que pode ser

utilizada por alguém que possua acesso a esses dados. Dessa forma, identificou-se que os ataques cibernéticos geram três tipos de custos: os diretos, indiretos e de proteção. Tais custos repercutem no setor financeiro propriamente dito e em elementos que se relacionam a este, como seguradoras, governo e clientes. Assim, os custos diretos, indiretos e de proteção desses envolvidos entram no cálculo do impacto dos ataques cibernéticos.

Essa metodologia pode ser resumida pela fórmula proposta. Propôs-se que o impacto (I) dos ataques cibernéticos ao setor financeiro é o somatório do custo total de todas as empresas do setor financeiro ($C_{T(fi)}$), com o custo total de prêmios pagos por empresas do setor de seguros para ataques cibernéticos ao setor financeiro ($C_{T(se)}$), com os gastos do governo para combater os ataques cibernéticos e suas perdas de arrecadação decorrentes dos ataques sofridos pelo setor financeiro ($C_{T(go)}$), e o custo total que os clientes do setor financeiro ($C_{T(cl)}$) tiveram em decorrência de ataques cibernéticos ao setor. Tudo isso em um determinado período de tempo (t), que é o valor, medido em dias ou meses, do período compreendido entre a percepção da ocorrência do ataque cibernético até a eliminação de seus efeitos. Conforme a fórmula:

$$I = \sum_{i=1}^{t} \left(C_{T(fi)} + C_{T(se)} + C_{T(go)} + C_{T(cl)} \right)$$

Por não conseguir aplicar a fórmula proposta, por falta de dados, deixa-se o seu teste como proposta para estudos futuros, a fim de contribuir com o conhecimento sobre o tema.

Conclui-se que governos de diversas regiões estão a tomar medidas que proporcionem interação entre a defesa e proteção cibernética de Estado com elementos da iniciativa privada. Assim, o modo de proteger um sistema governamental ou de infraestruturas críticas para um país, como o setor de energia, pode robustecer os sistemas bancários e vice-versa. Dessa forma, o Brasil começa a caminhar nessa direção com a aproximação de órgãos do governo, Forças Armadas e instituições como Febraban, Banco Central, bancos públicos e privados.

Por fim, conclui-se que o tema apresenta amplo espaço para estudos futuros, sendo afeto a vários campos do conhecimento. Em especial, relacionados a pesquisas

sobre políticas públicas voltadas para o setor cibernético, aspectos legais envolvendo o espaço cibernético, segurança da informação e no campo das relações internacionais como tratar sobre ataques cibernéticos gerados em outros países.

REFERÊNCIAS

ACTION FRAUD. **About us**. London: 2018a. Disponível em: <https://www.actionfraud.police.uk/about-us>. Acesso em: 7 ago. 2018.

ACTION FRAUD. **National Cyber Profile**. London: 2018b. Disponível em: <https://www.actionfraud.police.uk/sites/default/files/National%20-%20Cyber.pdf>. Acesso em: 7 ago. 2018.

AGÊNCIA ESTADO. Banco Inter confirma vazamento de dados de clientes e é investigado. **Correio Braziliense**, Economia: 17 ago. 2018. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/economia/2018/08/17/internas_economia,700663/banco-inter-confirma-vazamento-de-dados-de-clientes-e-e-investigado.shtml>. Acesso em: 20 set. 2018.

AGRELA, Lucas. O que você precisa saber sobre o vazamento de dados do Facebook. **Exame**. São Paulo: 14 abr. 2018. Disponível em: <https://exame.abril.com.br/tecnologia/o-que-voce-precisa-saber-sobre-o-vazamento-de-dados-do-facebook/>. Acesso em: 23 abr. 2018.

ALVES, Paulo. **Android é alvo de vírus que rouba dados bancários: conheça o BankBot.** Techtudo, 28 nov. 2017. Disponível em: <https://www.techtudo.com.br/noticias/2017/11/android-e-alvo-de-virus-que-rouba-dados-bancarios-conheca-o-bankbot.ghtml>. Acesso em 20 set. 2018.

ATZORI, Luigi; IERA, Antonio e MORABITO, Giacomo. The Internet of Things: A survey, **Computers Network**. Elsevier B.V. (2010). Disponível em: <https://www.cs.mun.ca/courses/cs6910/IoT-Survey-Atzori-2010.pdf>. Acesso em: 16 abr. 2018. DOI:10.1016/j.comnet.2010.05.010

BARRETO, Eduardo Müssnich. Terrorismo cibernético e cenários especulativos. **Revista Brasileira de Inteligência**/ Agência Brasileira de Inteligência. vol. 3, n. 4, set, p. 63–76. Brasília, 2007.

BAZO, Mariana. El sistema bancário en Perú repele una cadena de ciberataques y suspende sus servicios temporalmente. **Europress – Reuters**, Lima, 18 agosto, 2018. Disponível em: <http://m.europapress.es/internacional/noticia-sistema-bancario-peru-repele-cadena-ciberataques-suspende-servicios-temporalmente-20180818025655.html>. Acesso em: 20 ago. 2018.

BRASIL. Casa Civil. **Lei nº 12.737, de 30 de novembro de 2012.** Brasília: 2012a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm>. Acesso em: 25 out. 2018.

_____. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa.** Brasília: 2012b. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 14 set. 2018.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** Brasília: 2014a. Disponível em: <https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf>. Acesso em: 25 out. 2018.

_____. Casa Civil. **Lei nº 12.965, de 23 de abril de 2014.** Brasília: 2014b. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 out. 2018.

_____. Casa Civil. **Decreto Presidencial nº 9.031, de 12 de abril de 2017.** Brasília: 2017a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9031.htm>. Acesso em: 25 out. 2018.

_____. Exército Brasileiro. **Exército e Itaipu assinam acordo para incremento da segurança de estrutura estratégica vital para o país.** Noticiário do Exército. Brasília: 5 set. 2017b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercito-e-itaipu-assinam-acordo-para-incremento-da-seguranca-de-estrutura-estrategica-vital-para-o-pais->. Acesso em: 14 set. 2018.

_____. Escritório de Projetos do Exército Brasileiro. **Coordena e integra a Defesa Cibernética.** Brasília: 2018a. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. **Exercício Guardião Cibernético reúne especialistas em TI, gestores de crise e tomadores de decisão.** Noticiário do Exército. Brasília: 4 jul. 2018b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercicio-guardiao-cibernetico-reune-especialistas-em-ti-gestores-de-crise-e-tomadores-de-decisao->. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. **Cooperação internacional e defesa cibernética atuam juntos para o enfrentamento das ameaças dessa natureza.** Noticiário do Exército. Brasília: 14 mai. 2018c. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/cooperacao-internacional-e-defesa-cibernetica-atuam-juntos-para-enfrentamento-das-ameacas-dessa-natureza->. Acesso em: 14 set. 2018.

_____. Banco Central do Brasil. **Resolução nº 4.658, de 26 de abril de 2018.** Brasília: 2018d. Disponível em: <https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50581/Res_4658_v1_O.pdf>. Acesso em: 25 out. 2018.

BRITO, Paulo. Trojan oculto na Google Play mira cliente Santander. **CiberSecurity: alertas, notícias, análises.** Riscos & ameaças. 29 out. 2018. Disponível em: <https://www.cibersecurity.net.br/trojan-oculto-na-google-play-mira-cliente-santander/>. Acesso em: 3 nov. 2018.

CALDAS, Daniel Mendes. **Análise e extração de características estruturais e comportamentais para perfis de malware.** Dissertação. UnB: Brasília, 2016. Disponível em: <http://repositorio.unb.br/handle/10482/23110>. Acesso em: 23 out. 2017.

CAMURÇA, Francisco. **Site do banco Banrisul sofre ataque de cibercriminosos.** Welivesecurity. ESET, 25 out. 2016. Disponível em: <https://www.welivesecurity.com/br/2016/10/25/banrisul-sofre-ataque/>. Acesso em: 17 set. 2018.

CARAZZAI, Estelita Hass. Senado pressiona Zuckerberg em depoimento e o acusa de negligência. **Folha de São Paulo**. Ed. digital, São Paulo, 10 abr. 2018. Disponível em: <https://www1.folha.uol.com.br/mundo/2018/04/em-depoimento-de-zuckerberg-senadores-questionam-modelo-do-facebook.shtml>. Acesso em: 23 abr. 1018.

CARVALHO, Paulo Sergio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos – Revista das Ciências Militares**. Rio de Janeiro, 2011.

CASHELL, Brian; JACKSON, William D.; JICKLING, Mark e WEBEL, Baird. The Economic Impact of Cyber-Attacks. Government and Finance Division. **Congressional Research Service**. The Library of Congress. 1th Apr. 2004. n. RL32331. Disponível em: <https://fas.org/sgp/crs/misc/RL32331.pdf>. Acesso em: 12 set. 2017.

CATOIRA, Fernando. **Ataque de phishing a um importante banco brasileiro. Welivesecurity.** ESET. 20 mar. 2012. Disponível em: <https://www.welivesecurity.com/br/2012/03/20/ataque-de-phishing-a-um-importante-banco-brasileiro/>. Acesso em: 17 set. 2018.

CEA (THE COUNCIL OF ECONOMIC ADVISERS). **The Cost of Malicious Cyber Activity to th U.S Economy**. Washington, Feb. 2018. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>. Acesso em: 18 jul. 2018.

CEBROWSKI, A. K. Transformation and the Changing Character of War? **Transformation Trends**, Office of Transformation, Department of Defense. Arlington, 17 June 2004. Disponível em: <www.hsdl.org/?view&did=448180>. Acesso em: 14 out. 2017.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para Internet: ransomware.** 25 mai. 2018a. Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 8 set. 2018.

_____. **Total de incidentes reportados ao CERT.br por ano.** 2018b. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 12 set. 2018.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2017.** 2018c. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/top-cc.html>. Acesso em: 14 set. 2018.

CLARKE, Richard A.; KNAKE, Robert K. **Cyber War: the next threat to national security and what tod do about it**. New York, NY: 2010. ed. brochura (2012). ISBN 978-0-06-196224-0.

DAUDT, Simone Stabel. **Aspectos das ações coletivas no direito brasileiro e das class action no direito norte-americano.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 19, n. 3871, 5 fev. 2014. Disponível em: <https://jus.com.br/artigos/26599>. Acesso em: 22 jan. 2018.

DELOITTE. **Pesquisa FEBRABAN de Tecnologia Bancária 2017**. In: CIAB FEBRABAN – Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras, 2017. Disponível em: <http://www.ciab.org.br/download/researches/research-2017.pdf>. Acesso em 5 ago. 2018.

_____. **Pesquisa FEBRABAN de Tecnologia Bancária 2018**. In: CIAB FEBRABAN – Congresso e Exposição de Tecnologia da Informação das Instituições Financeiras, 2018. Disponível em: <http://www.ciab.org.br/download/researches/research-2018.pdf>. Acesso em 5 ago. 2018.

EASTTOM, William Chuck. **Computer Security Fundamentals**. Pearson IT Certification, 3 ed. 2016.

FEDERAL BUREAU OF INVESTIGATION (FBI). **What we investigate: Cyber Crime.** U.S. Government, U.S. Departament of Justice. 2018. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acesso em: 2 jul. 2018.

GASPAR, Philipe. **Pragas eletrônicas: ainda não estamos livres delas**. jul. 2007. Disponível em: <http://www.philipe.eti.br/artigo-003.pdf>. Acesso em: 22 out. 2017.

G1. **Dupla é presa em Itajaí com R$ 700 mil desviados de banco; um estava com R$ 100 mil dentro da calça.** Itajaí: 19 set. 2017. Disponível em: <https://g1.globo.com/sc/santa-catarina/noticia/dupla-e-presa-em-itajai-com-r-700-mil-desviados-de-banco-um-estava-com-r-100-mil-dentro-da-calca.ghtml>. Acesso em: 20 set. 2018.

HAKMER, Joyce. **Cybercrime and the Digital Economy in the GCC Countries. Chatham House.** The Royal Institute of International Affairs. International Security Departmente. London: June, 2017. Disponível em: <https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf>. Acesso em: 16 set. 2018.

HALE, Chris. Cybercrime: Facts & Figures Concerning This Global Dilemma. **Crime & Justice International.** v. 18, Issue 65, p. 5, 6, 24-26, Sep. 2002. Disponível em: <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=197384>. Acesso em: 30 jan. 2018.

HARÁN, Juan Manuel. **Campanha de hijacking afetou usuários do Banco do Brasil e do Itaú. Welivescurity**. ESET. 14 ago. 2018. Disponível em: <https://www.welivesecurity.com/br/2018/08/14/campanha-de-hijacking-afetou-usuarios-do-banco-do-brasil-e-do-itau/>. Acesso em: 17 set. 2018.

IANELLI, Nicholas; HACKWORTH, Aaron. Botnets as a Vehicle for Online Crime. **The International Journal of Forensic Computer Science.** v.2, n.1, p.19-39, Brasília, 2007.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity Index 2017.** Genebra: 2017. ISBN: 978-92-61-25071-3. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf>. Acesso em: 27 set. 2018.

IBM. **IBM X-Force**. EUA: 2018. Disponível em: <https://www.ibm.com/security/xforce>. Acesso em: 20 set. 2018.

FALLIERE, Nicolas; MURCHU, Liam O e CHIEN, Eric. W32.Stuxnet Dossier. **Symantec Security Response.** Symantec Corporation. Version 1.4, Feb. 2011. Cupertino: 2011. Disponível em: <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf>. Acesso em: 23 abr. 2018.

KASPERSKY. **Things to do before the next big thing: How the financial industry reacts to cyberthreats.** Mar. 2017. Disponível em: <https://www.kaspersky.com/blog/how-the-financial-industry-reacts-to-cyberthreats/6610/#mktoForm_10582>. Acesso em: 9 ago. 2018.

KERNER, Rotem; WINSTON, James. **RSA discovers massive boleto fraud ring in Brazil**. RSA Reseach Group. July, 2014. Disponível em: <https://www.emc.com/collateral/white-papers/h13282-report-rsa-discovers-boleto-fraud-ring.pdf>. Acesso em: 21 ago. 2018.

KLIMBURG, Alexander. **National Cyber Security Framework Manual**, NATO CCD COE Publication, Tallinn, 2012.

LAGAZIO, Monica; SHERIF, Nazneen; e CUSHMAN, Mike. A multi-level approach to understanding the impact of cyber crime on the financial sector. **Computers & Security.** v. 45, Sept. 2014, p. 58-74 ScienceDirect. Elsevier. London: 2014. DOI: http://dx.doi.org/10.1016/j.cose.2014.05.006

LEISTER, Wolfgang e CHRISTOPHERSEN, Nils. **ITLED4240 Compendium Spring 2012: Open Source, Open Collaboration and Innovation.** Norsk Regnesentral. Oslo–Norway, 2012.

LEWIS, James. **Economic Impact of Cybercrime – No Slowing Down**. Mcafee Report – CSIS. Santa Clara, CA, Feb. 2018. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email>. Acesso em: 31 jul. 2018.

LOPES, Gills e OLIVEIRA, Carolina F. Jost de. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. **Revista Brasileira de Estratégia de Defesa**. Ano 1, n. 1, jul./dez., p. 55-69, 2014. Disponível em: <https://rbed.abedef.org/rbed/article/download/39457/30874>. Acesso em: 20 set. 2017.

LOUBAK. Ana Letícia. **Golpe com vírus CamuBot usa nome de bancos e faz vítimas no Brasil.** Techtudo. 6 set. 2018. Disponível em: <https://www.techtudo.com.br/noticias/2018/09/golpe-com-virus-camubot-usa-nome-de-bancos-e-faz-vitimas-no-brasil.ghtml>. Acesso em: 20 set. 2018.

MACHADO, T. G.; MOTA, A. A.; MOTA, L. T. M.; CARVALHO, M. F. H. e PEZZUTO, C. C. Methodology For the Cybersecurity Maturity Level Identification in Smart Grids. **IEEE Latin America Transactions.** v. 14, issue 11, p. 4512-4519, Nov. 2016. Disponível em: <http://www.revistaieeela.pea.usp.br/issues/vol14issue11Nov.2016/14TLA11_14GerardMachado.pdf>. Acesso em: 22 jan. 2018. DOI: 10.1109/TLA.2016.7795822

MANKIW, N. Gregory. **Introdução à Economia**. Tradução da 3ª edição norte-americana [tradução Allan Vidigal Hastings]. São Paulo: Cengage Learning, 2009.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **JISTEM: Journal of Information Systems and Technology Management**, vol. 2, n. 2, 2005, pp. 121-136. ISSN online: 1807-1775. Universidade de São Paulo. São Paulo. Disponível em: <http://www.redalyc.org/pdf/2032/203219587002.pdf>. Acesso em: 22 jan. 2018.

MARTINS, Danylo. Invasões cibernéticas criminosas ameaçam os negócios. **Valor Econômico.** Finanças. São Paulo: 28 mai. 2018. Disponível em: <https://www.valor.com.br/financas/5552593/invasoes-ciberneticas-criminosas-ameacam-os-negocios>. Acesso em: 5 out. 2018.

MELLO JÚNIOR, John P. Security Awareness Training Explosion. **Cybersecurity Ventures.** Menlo Park, California: 6 Feb. 2017. Disponível em: <https://cybersecurityventures.com/security-awareness-training-report/>. Acesso em: 8 set. 2018.

MITNICK, Kevin D.; SIMON, William L. **The art of deception: Controlling the Human Element of Security.** 2002. Ed Wiley: 2007.

MCAFEE FOUNDSTONE PROFESSIONAL SERVICES AND MCAFEE LABS (McAfee). **Global Energy Cyberattacks: "Night Dragon"**. Santa Clara, EUA: Feb. 2011. Disponível em: <https://www.git-security.com/file/track/5246/1>. Acesso em: 23 abr. 2018.

MICROSOFT. **Helthcare Beware the Rise of Ransomware**. 31 May 2016. Disponível em: <https://cloudblogs.microsoft.com/industry-blog/industry/microsoft-in-business/healthcare-beware-the-rise-of-ransomware/>. Acesso em: 8. set. 2018.

MORESI, Eduardo A. D.; SANTINI JÚNIOR, Nelson; FRAGOLA, Rodrigo J.; BASSI, Marco C. e ALONSO, José E. T. Defesa cibernética: um estudo sobre a proteção da infraestrutura e o software e o software seguro. **Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética: CICIC 2012**. Orlando – FL – USA, 2012. Disponível em: <https://pt.slideshare.net/moresi/defesa-ciberntica-um-estudo-sobre-a-proteo-da-infraestrutura-e-o-software-seguro>. Acesso em: 22 out. 2017.

MORGAN, Steve. Global Ransomware Damage Costs Predicted to Exceed $ 5 Billion in 2017. **Cybersecurity Ventures.** Menlo Park, California: 18 May 2017a. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

_____. Cybercrime Damages $ 6 Trillion By 2021. **Cybersecurity Ventures.** Menlo Park, California: 16 Oct. 2017b. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

MOURY. Taciana. Exército Brasileiro investe em defesa cibernética. **Diálogo: Revista militar digital – Fórum das Américas**. 12 mai. 2017. Disponível em: <https://dialogo-americas.com/pt/articles/brazilian-army-invests-cyber-defense>. Acesso em: 14 set. 2018.

NASDAQ. **Facebook, Inc. Class A Common Stock Historical Stock Prices**. Disponível em: <https://www.nasdaq.com/symbol/fb/historical>. Acesso em: 23 abr. 2018.

NATIONAL ASSOCIATION OF INSURANCE COMMISSIONERS (NAIC). **Key iniciative – Cybersecurity**. EUA: July 2018. Disponível em <https://www.naic.org/cipr_topics/topic_cyber_risk.htm>. Acesso em: 9 ago. 2018.

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER'S (NCCIC). **ICS-CERT – about us.** EUA: 2018. Disponível em: <https://ics-cert.us-cert.gov/about-us>. Acesso em: 23 abr. 2018.

NATIONAL CYBER SECURITY CENTRE (NCSC). **Introduction to the NIS Directive.** London: 28 Jan. 2018. Disponível em: <https://www.ncsc.gov.uk/guidance/introduction-nis-directive>. Acesso em: 16 set. 2018.

OFFICE OF PRIME MINISTER. **Offensive Cyber Capability to Fight Cyber Criminals.** Media release. Austrália: 30 June 2017. Disponível em: <https://www.pm.gov.au/media/offensive-cyber-capability-fight-cyber-criminals>. Acesso em: 14 ago. 2018.

OLIVEIRA, Marcos A. G.; PAGLIARI, Graciete D. C.; MARQUES, Adriana A.; PORTELA, Lucas S. e FERREIRA NETO, W. B. **Guia de Defesa Cibernética na América do Sul.** Recife: Ed. UFPE, 2017.

OLMSTEAD, Kenneth e SMITH, Aaron. Americans and Cybersecurity. **Pew Reserch Center**, Jan. 2017. Disponível em: <http://assets.pewresearch.org/wp-content/uploads/sites/14/2017/01/26102016/Americans-and-Cyber-Security-final.pdf>. Acesso em 5 ago. 2018.

OLOWU, D. Cyber-Crimes and the Boundaries of Domestic Legal Responses: Case for an Inclusionary Framework for Africa. **Journal of Information, Law & Technology (JILT)**, Johannesburg, South Africa, 2009. Disponível em: <http://go.warwick.ac.uk/jilt/2009_1/olowu>. Acesso em: 30 jan. 2018.

OPPERMANN, Daniel. Governança da internet e segurança cibernética no Brasil. **Monções: Revista de Relações Internacionais da UFGD**. Dourados, v.2, n.3, jul./dez., 2013.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS (OEA). **Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.** Washington-DC: 2018. Disponível em: <http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf>. Acesso em: 5 out. 2018.

PAIS, Ricardo; MOREIRA, Fernando; VARAJÃO, João. **Engenharia Social (ou o carneiro que afinal era um lobo).** Universidade de Minho – Portugal. Ed. Almedina, p. 171–187, 2013. Disponível em: <http://hdl.handle.net/1822/26251>. Acesso em: 4 nov. 2017.

PAYÃO, Felipe. Banco Inter é extorquido e dados de clientes são expostos: invasão é negada. **Tecmundo**. 4 mai. 2018a. Disponível em: <https://www.tecmundo.com.br/seguranca/129811-exclusivo-vazam-dados-400-mil-clientes-banco-inter.htm>. Acesso em: 20 set. 2018.

_____. Ministério Público move ação contra Banco Inter por vazamento de dados. **Tecmundo**. 31 jul. 2018b. Disponível em: <https://www.tecmundo.com.br/seguranca/132760-ministerio-publico-move-acao-banco-inter-vazamento-dados.htm>. Acesso em: 20 set. 2018.

PILATI, José I.; OLIVO, Mikhail V. C. de. **Um Novo Olhar sobre o Direito à Privacidade: caso Snowden e pós-modernidade jurídica.** In: V SEMINÁRIO DIÁLOGO AMBIENTAL, CONSTITUCIONAL E INTERNACIONAL. Lisboa: out. 2014. Disponível em:<https://periodicos.ufsc.br/index.php/sequencia/article/download/2177-7055.2014v35n69p281/28392>. Acesso em: 21 jan. 2018. DOI: http://dx.doi.org/10.5007/2177-7055.2014v35n69p281.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais**. Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 7**,** n. 58**,** 1 ago. 2002**.** Disponível em: <https://jus.com.br/artigos/3186>. Acesso em: 21 out. 2017.

RAPOSO, Álisson Campos. Terrorismo e contraterrorismo: desafio do século XXI. **Revista Brasileira de Inteligência/ Agência Brasileira de Inteligência**. vol. 3, n. 4, set, p. 39–55. Brasília, 2007.

RODRIGUES, Ricardo Batista. **RecCloud: um modelo de recomendação de arquivos para sistemas de armazenamento em nuvem.** Dissertação. UFPE. Recife: 2014. Disponível em: <https://repositorio.ufpe.br/bitstream/123456789/11974/1/DISSERTAÇÃO%20Ricardo%20Batista%20Rodrigues.pdf>. Acesso em: 17 abr. 2018.

RODRÍGUEZ, Santiago F. La ciberseguridad en la banca de América Latina y el Caribe. **Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe.** Washington-DC: 2018. Disponível em: <http://www.oas.org/es/sms/cicte/sectorbancariospa.pdf>. Acesso em: 5 out. 2018.

ROSENBERG, Matthew; CONFESSORE, Nicholas e CADWALLADR, Carole. **How Trump Consultants Exploited the Facebook Data of Millions.** The New York Times. Digital Version, New York: 17 Mar. 2018. Disponível em <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html>. Acesso em: 23 abr. 2018.

RSA SECURITY. **About RSA**. 2018. Disponível em: <https://www.rsa.com/en-us/company>. Acesso em 21 ago. 2018.

SAID, Carlos Gerardo. Infraestructuras Críticas: Sectores necesitados de un modelo de ciberseguridad. **European Scientific Journal.** Edição especial. n. 1, p. 42-52, mayo, 2016. ISSN: 1857 – 7881 (Print) e - ISSN 1857- 7431. Disponível em: <https://eujournal.org/index.php/esj/article/view/7388/7116>. Acesso em: 23 abr. 2018.

SIKORSKI, Michael e HONIG, Andrew. **Practical Malware Analysis.** No Starch Press. San Francisco, 2012.

SINGER, Peter Warren; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know.** 2014. Segurança e Guerra cibernéticas: o que todos precisam saber. Tradutor Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército Editora, 2017.

SCOTT, Patrick. How much of a problem is cyber-crime in the UK? **The Telegraph.** United Kingdom, 1th Nov. 2016. Disponível em: <https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/>. Acesso em: 7 ago. 2018.

SILVA, Emerson Marcelo da; AZEVEDO, Renato Asamura e RUFATO, David de Oliveira. Confidencialidade dos Jogos em Rede. **Id on line Revista de Psicologia**. ano 8, n. 24, nov., 2014 - ISSN 1981-1179. Disponível em: <https://idonline.emnuvens.com.br/id/article/download/302/411>. Acesso em: 22 jan. 2018.

SYMANTEC SECURITY RESPONSE. **W32.Duqu: The Precursor to the Next Stuxnet**. 2011. Disponível em: <https://www.symantec.com/connect/w32_duqu_precursor_next_stuxnet>. Acesso em: 23 abr. 2018.

_____. **Duqu 2.0: Reemergence of an aggressive cyberespionage threat**. 2015. Disponível em: <https://www.symantec.com/connect/blogs/duqu-20-reemergence-aggressive-cyberespionage-threat>. Acesso em: 23 abr. 2018.

SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT). **SWIFT history**. 2018. Disponível em: <https://www.swift.com/about-us/history>. Acesso em: 13 ago. 2018.

STEFANKO, Lukas. **Apps bancários falsos descobertos no Google Play vazam dados roubados de cartões de crédito.** Welivesecurity. ESET. 26 jul. 2018. Disponível em: <https://www.welivesecurity.com/br/2018/07/26/apps-bancarios-falsos-descobertos-no-google-play-vazam-dados-roubados-de-cartoes-de-credito/>. Acesso em: 17 set. 2018.

UK CABINET OFFICE. **Britain's cyber security bolstered by world-class strategy.** United Kingdom: Nov. 2016. Disponível em: <https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy>. Acesso em: 14 ago. 2018.

VENTRE, Daniel. Ciberguerra. In: ACADEMIA GENERAL MILITAR. **Seguridad global y potencias emergentes en un mundo multipolar**. XIX Curso Internacional de Defensa. España: Universidad Zaragoza. p. 31-45, 2011. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf>. Acesso em: 1 set. 2018.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science: Research Trends**, v. 9, n. 1, Marília, 2015. DOI 10.22556/1981-1640.

WORLD ECONOMIC FORUM (WEF). **The Global Risks Report 2018, 13th Edition.** Geneva: 2018. ISBN: 978-1-944835-15-6. Disponível em: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>. Acesso em: 15 ago. 2018.

ZETTER, Kim. **Hacker Lexicon: what is phishing?** Wired. EUA: 4 July 2015. Disponível em: <https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/>. Acesso em 8 set. 2018.

APÊNDICES E ANEXOS

APÊNDICE A – PRODUÇÃO ACADÊMICA DERIVADA DA DISSERTAÇÃO

Artigo apresentado na 2ª Conferência Científica em Assuntos de Defesa da Escola de Comunicações do Exército Brasileiro, em 22 de novembro de 2018, na cidade de Brasília-DF. Aprovado para publicação na revista científica O Comunicante, da mesma instituição, com previsão de constar no volume 9, número 1, 2019.

SILVA, W. R.; NOGUEIRA, J. M. **Ataques cibernéticos e medidas governamentais para combatê-los.** Brasília, 2018.

RESUMO

O uso do espaço cibernético cresce a cada dia. Os ataques cibernéticos acompanham esse crescimento, apresentando-se como ameaça constante e mutável. Esses ataques comprometem a confidencialidade, integridade e/ou disponibilidade de dados, sistemas e serviços, com reflexos negativos em variados setores da economia. Objetivou-se estudar os ataques cibernéticos, seus riscos e como são tratados por governos ao redor do mundo e no Brasil. Foram utilizadas fontes secundárias de pesquisa bibliográfica. Identificou-se que o Brasil se encontra em nível intermediário de segurança cibernética, segundo critérios da União Internacional de Telecomunicações. Além de que a maior parte dos ataques cibernéticos sofridos no Brasil reportados ao CERT.br originam-se no próprio país, o que pode ser uma consequência da falta de leis específicas e da sensação de impunidade pelos infratores. E, que houve um início de aproximação entre órgãos do governo e da iniciativa privada para colaboração na melhoria da capacidade de proteção cibernética no Brasil.

Palavras-chave: Ataques cibernéticos, Brasil, Defesa.

SILVA, W. R.; NOGUEIRA, J. M. **Cyber-attacks and government actions to combat them.** Brasília, 2018. Portuguese.

ABSTRACT

The use of cyberspace grows every day. The cyber attacks have accompanied this growth whith constant threat. These attacks compromise the confidentiality, integrity and/or availability of data, systems and services, with negative reflections upon varied

sectors of the economy. The objective of this article is to study the cyber attacks, their risks and those being treated by governments around the world and in Brazil. Data from secondary sources were used. It was identified that Brazil is in the intermediate level of cybersecurity, according to the criteria of the International Telecommunication Union. It was identified that the majority of cyber attacks suffered in Brazil reported to CERT.br originate from inside the country, which may be a consequence of the lack of specific laws to eliminate the impunity of offenders. It was found that a process of approximation between government agencies and the private sector has started to collaborate in the improvement of cybernetic protection capacity in Brazil.

Key words: Cyber attacks, Brazil, Defense.

INTRODUÇÃO

As facilidades proporcionadas pelos sistemas de tecnologia da informação e comunicação (TIC) trouxeram consigo oportunidades para a exploração de um novo ambiente, o chamado espaço cibernético, para usos benéficos ou prejudiciais. Nesse contexto, as novas TIC criaram desafios e efeitos negativos. Por exemplo, por meio delas, surgiram novas possibilidades de explorações para fins de crimes financeiros, espionagem industrial e até ataques entre Nações. Nesse cenário, governos e instituições de diversos países passaram a tomar providências para protegerem-se. Como o resto do mundo, o Brasil tem, diante de si, semelhantes desafios.

Do exposto, levantou-se a problemática: quais são os impactos de ataques cibernéticos? Em virtude da elevada amplitude do tema, buscou-se delimitar o estudo conforme segue: este trabalho tem o objetivo de estudar os ataques cibernéticos, seus riscos e como são tratados por governos ao redor do mundo e no Brasil.

Assim, o presente trabalho faz-se relevante por destacar o quão presentes e danosos são os ataques cibernéticos e destacar a importância da atuação do Estado, por meio de políticas públicas e ações para combater essa ameaça.

Este artigo é dividido em 4 seções, além desta introdução e das conclusões. Na primeira, é tratado sobre o espaço cibernético e são os tipos de ameaças cibernéticas. A segunda seção aborda as dimensões econômicas de ataques cibernéticos. A terceira aborda como outros países estão enfrentando o atual cenário de ataques cibernéticos e quais estruturas foram criadas para tal. Na quarta seção, há semelhante abordagem sobre como está o Brasil nesse cenário.

Metodologicamente, utilizou-se dados de fontes secundárias, obtidos por meio de uma pesquisa bibliográfica aplicada. Buscou-se dados e informações em livros especializados e artigos científicos, sítios oficiais de órgãos como os brasileiros Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Exército Brasileiro (EB) e Ministério da Defesa (MD); os estadunidenses Federal Bureau of Investigation (FBI), The Council of Economic Advisers (CEA), os britânicos National Cyber Security Centre (NCSC) e o UK Cabinet Office, a página do Office of Prime Minister, da Austrália e da União Internacional de Telecomunicações (ITU, sigla em inglês), com sede na Suíça. Além de portais de jornais de grande circulação no Brasil como o Valor Econômico.

Ademais, a pesquisa por fontes incluiu conteúdos redigidos em língua portuguesa, inglesa e espanhola, publicadas a partir do ano 2002, dando-se preferência a publicações recentes, principalmente a partir de 2013. Dessas, a maior parte das fontes de referências obtidas do exterior são oriundas dos Estados Unidos da América (EUA) por haver maior disponibilidade de estudos em fontes abertas.

1 AMEAÇAS CIBERNÉTICAS: suas inúmeras dimensões

1.1 O espaço cibernético

O surgimento da internet foi o primeiro passo para o atingimento do grau de compartilhamento de informações vivenciados atualmente. Nesse contexto, surge uma nova dimensão, o espaço cibernético. Esse espaço apresenta, segundo Oliveira et al. (2017), três características: dimensão intangível e abstrata; considerado importante desde o início de sua existência; e transversal, esta última em consonância com Ventre (2011), o qual adiciona que o espaço cibernético permeia todos os espaços geográficos, permitindo controlar desde satélites e radares marítimos até metrôs em grandes cidades, assim, as ações geradas no campo virtual são capazes de criar consequências no mundo real.

O espaço cibernético e a internet apresentam semelhanças, contudo são distintos, apesar de haver discordância. Cebrowski (2004) afirma que o espaço cibernético é maior do que a internet. Autores como Carvalho (2011) e Oliveira et al. (2017) concordam com essa concepção e incluem que o espaço cibernético é composto por dispositivos computacionais, conectados em redes ou não, com trânsito ou armazenamento de informações. Há, ainda, autores que incluem os usuários na composição do espaço cibernético, como é o caso de Klimburg (2012), o qual afirma

que “o espaço cibernético é mais que internet, inclui não somente *hardware*, *software* e sistemas informacionais, mas também pessoas e suas interações sociais nas redes de computadores”.

1.2 Tipos e instrumentos de ameaças no espaço cibernético

As principais ameaças são os ataques cibernéticos. Klinburg (2012) afirma que esse não é um termo internacionalmente definido, havendo diferenças substanciais entre a definição do governo estadunidense e de outros países. A definição mais genérica de ataque cibernético é que se trata de uma tentativa maliciosa premeditada de ataque para quebrar a confidencialidade, integridade ou disponibilidade de informações existentes em computadores ou redes computacionais.

O governo dos EUA trata ataques cibernéticos como atividade cibernética maliciosa e as definem da seguinte forma:

> Atividade cibernética maliciosa é qualquer atividade, desautorizada ou em desacordo com a lei dos EUA, que busca comprometer ou prejudicar a confidencialidade, integridade ou disponibilidade de computadores, sistemas de informação ou comunicações, redes, infraestrutura física ou virtual controlada por computadores ou sistemas de informação, ou as informações nele contidos (CEA, 2018, p. 2).

Já o Ministério da Defesa do Brasil entende como ataque cibernético quaisquer “ações que objetivam interromper, negar, degradar, corromper ou destruir informações ou sistemas computacionais armazenados em dispositivos e redes computacionais e de comunicações do oponente” (BRASIL, 2014a, p. 23).

Os agentes cibernéticos são classificados de acordo com os fins de suas atuações. O termo *hacker*, bastante utilizado cotidianamente como uma generalização de usuários criminosos, não significa exatamente isso. Ramalho Terceiro (2002) aponta *hacker* como alguém possuidor de grande habilidade em computação. Já os *crackers* são *hackers* que utilizam seus conhecimentos para atacar computadores, utilizando seus potenciais cognitivos para cometer atos ilícitos, ou seja, os criminosos são, essencialmente, os *crackers*. Apesar da diferença entre os termos, o termo *hacker* será utilizado neste artigo indistintamente.

Raposo (2007) destaca a existência de um grupo formado por *hackers* com motivações políticas ou religiosas, contratados por extremistas com o objetivo de realizarem ataques para geração de pânico, mortes, acidentes, contaminação ambiental ou perdas econômicas. Esses *hackers* são denominados de terroristas cibernéticos. *The Council of Economic Advisers*, um órgão do governo estadunidense,

ratifica esse conceito classificando esses indivíduos que efetuam ataques cibernéticos por razões ideológicas como hacktivistas (CEA, 2018).

Há diversas formas com as quais os atacantes cibernéticos podem buscar seus objetivos. Caldas (2016) afirma que parte considerável das ações criminosas em redes computacionais são praticadas com uso de *softwares* maliciosos, conhecidos por *malwares* e os define como programas criados com a intenção de se infiltrar em um sistema de computador alheio de forma ilícita, para causar danos, alterações ou roubo de informações (confidenciais ou não).

Um dos elementos usualmente presentes em ataques cibernéticos são os *vírus*. Sikorski e Honing (2012) apresentam vírus e *worms* como tipos de *malwares.* Easttom (2016) explica que, por definição, os vírus são programas que se autorreplicam e possuem capacidade de rápida propagação. O vírus de computador, análogo ao vírus biológico, necessita de uma aplicação hospedeira para se replicar e infectar outros sistemas.

Outra ferramenta de ataque cibernético são os vermes, conhecidos no meio cibernético como *worms*. Gaspar (2007) diferencia os *worms* dos vírus pois não necessitam de um portador para se replicarem. Eles se autorreplicam, espalhando-se de um computador para outro. Os vermes exploram as vulnerabilidades e utilizam quaisquer mecanismos para se propagarem como, por exemplo, e-mails, serviços de internet, compartilhamento de arquivos, mídias removíveis, entre outros.

Os ataques cibernéticos podem ocorrer de diversas outras formas, como Cavalos de Tróia, *backdoors*, *botnets, spywares, phishing*, *spear phishing,* entre outros. Havendo constante surgimentos de novas formas de ataques, segundo o FBI (2018), um desses que está atualmente entre os mais incidentes é o *ransomware*. Conforme o Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT.br), esse consiste em um tipo de *malware* que impede o acesso a arquivos digitais valiosos, com isso, os criminosos cobram um resgate para tornar os dados acessíveis novamente (CERT.br, 2018a).

Como o ser humano é parte do espaço cibernético, suas vulnerabilidades devem ser consideradas. Sobre esse tema, Singer e Friedman (2014) afirmam que é justamente o fator mais débil, pois permite várias formas de ataques em razão de procedimentos inadequados.

Uma das possíveis formas de atuação sobre os usuários é a Engenharia Social. Para Pais, Moreira e Varajão (2013), a maior fonte de risco para a segurança são as

vulnerabilidades dos indivíduos que compõem uma organização visada. Em razão da simplicidade e engenho, a Engenharia Social é a maneira mais fácil e eficaz de um atacante superar os obstáculos impostos pelos sistemas de segurança.

Oppermann (2013) reforça a ideia de que até usuários frequentes da internet e sabedores da existência de *malwares* cometem erros primários como clicar em links desconhecidos em rede sociais, e-mails ou em mensagens recebidas em aplicativos de conversação em *smartphones*.

1.3 Ataques cibernéticos contra a confidencialidade

Os ataques cibernéticos contra a confidencialidade possuem, em geral, o objetivo de conceder, ao atacante, acesso a dados que lhes são negados.

Vianna e Fernandes (2015) destacam que países como Brasil, EUA e Alemanha foram expostos a ações de vigilância e espionagem cibernética, comprometendo a privacidade de pessoas e organizações e, quiçá, até as soberanias dessas nações. Esses não são os únicos, ataques cibernéticos com o fim de espionagem ocorrem em todas as regiões onde houver conteúdos passíveis de gerar algum benefício, seja financeiro, político ou outro qualquer.

Ainda segundo Vianna e Fernandes (2015), em 2013, a situação conhecida como caso Snowden foi um marco emblemático por revelar a atuação do governo dos EUA em espionagem de dados, dentro e fora do seu território. Nesse sentido foi exposto como o governo dos EUA obtinha acesso a e-mails e outros arquivos eletrônicos de usuários, por meio de empresas como Google, Microsoft e Facebook. Dentre esses, estavam a Presidência do Brasil e empresas como a Petrobras.

O peso dos ataques contra confidencialidade tem mais relação com a importância da informação obtida do que com os sistemas computacionais. Assim, a perda da confidencialidade pode gerar instabilidades diplomáticas, como ocorreu no caso Snowden entre o governo dos EUA e os dos países por eles espionados.

A quebra de sigilo sobre conhecimentos restritos, como propriedade intelectual, projetos, tecnologias, *know how* e afins é a maior ameaça para os setores industriais, acadêmicos e de pesquisa, desenvolvimento e inovação (P&DI), uma vez que neles a informação possibilita a criação de riquezas de elevado valor agregado.

É comum haver elevados níveis de precauções como estabelecimentos de estruturas de segurança, *softwares* preventivos como antivírus e *antispywares* nos ambientes de desenvolvimento de P&DI. Mas não apenas a proteção lógica deve ser considerada. O caso Snowden é um exemplo de que o elemento humano tem um

potencial de acesso a sistemas que não pode ser descartado, pelo contrário, não pode deixar de haver proteções contra os chamados ataques físicos, ou seja, em que alguém, presencialmente, acessa a sistemas computacionais.

Martins e Santos (2005) destacam que no aspecto segurança física, áreas críticas como servidores só devem ser acessadas por pessoas autorizadas e, ainda assim, sob controle de entrada e saída, tanto de pessoas quanto de equipamentos. Recomendando-se a criação de normatizações de controles internos referente ao assunto, os quais devem sofrer auditoria periodicamente. Ainda assim, tratando-se de confidencialidade, a seleção adequada de pessoal é fundamental.

Outros dois ataques cibernéticos que chamam a atenção devido a falhas humanas, corrompendo a confidencialidade, são destacados por Singer e Friedman (2014). O primeiro caso citado pelos autores remota ao ano de 2008, quando um soldado dos EUA que passava por um estacionamento fora de uma base militar norte-americana no Oriente Médio encontrou um *pen drive*. Esse soldado inseriu o achado em um computador que estava conectado à rede militar de Comando Central americana e desencadeou uma das maiores brechas cibernéticas da história militar dos EUA, conhecida como *Buckshot Yankee*. Essa falha levou ao escaneamento de computadores da rede militar, a abertura de diversas portas de saída de dados e levou cerca de quatorze meses para ser sanada completamente pelo Pentágono.

O segundo caso destacado por Singer e Fiedman (2014) foi o de um executivo de uma companhia de Tecnologia da Informação que encontrou um CD que continha *malware* no banheiro masculino e resolveu verificar o conteúdo do referido disco. Desavisadamente, o executivo compartilhou projetos da aviônica do helicóptero presidencial norte-americano com *hackers* iranianos.

1.4 Ataques cibernéticos contra a integridade

A perda de integridade ocorre com a modificação ou destruição de informações de forma não autorizada. Ataques contra a integridade ocorrem, em geral, como atividade meio, não como um fim. Ao modificar algum dado, o atacante, normalmente, busca inserir algum *backdoor* para coletar informações, ou ainda, modificar a configuração de sistemas de automação para danificar ou obter controle das máquinas por eles controladas, entre outros.

1.5 Ataques cibernéticos contra a disponibilidade

Machado et al. (2016) afirmam que a disponibilidade visa garantir o acesso sempre que necessário. Ou seja, o ataque cibernético contra a disponibilidade ocorre

quando impossibilita o acesso a um sistema de informação, o uso de dados nele contido ou o torna inoperante. O uso crescente de automatização de sistemas é notório em diversas áreas, como indústrias, usinas de geração de energia, sistemas de vigilância e monitoramento remoto, entre outros. Nesses setores, a inoperância dos sistemas controladores pode indisponibilizar linhas de produção, câmeras de vigilância e até motores turbinas responsáveis por geração elétrica. Muitos desses sistemas controladores são informatizados, ou seja, passíveis de sofrer ataques cibernéticos, de procedência interna e externa.

Ataques cibernéticos contra sistemas controladores de processos produtivos já ocorreram. Um caso conhecido é o *Stuxnet,* em que um *malware* foi utilizado para atuar sobre os computadores que controlavam centrífugas de uma usina de enriquecimento de urânio, tornando o processo produtivo dessa usina inoperante.

Setores como o comércio, o de serviços, como o financeiro e de telecomunicações são alvos de ataques cibernéticos e estão passíveis de sofrer elevadas perdas se seus computadores ou servidores tornarem-se indisponíveis.

Finalmente, setores relacionados à gestão de mobilidade como o controle de trafego aéreo, trânsito e linhas férreas são exemplos de áreas em que ataques cibernéticos causadores de indisponibilidade são capazes de criar transtornos de elevadas magnitudes, tanto para os cidadãos comuns, quanto para empresas e governos, afetando, direta ou indiretamente, a economia da área atacadas.

2 ATAQUES CIBERNÉTICOS: dimensões econômicas

Tratar economicamente aspectos relacionados a ataques cibernéticos não é tarefa trivial. Os prejuízos causados por possíveis danos a sistemas computacionais são facilmente perceptíveis, no entanto, sua quantificação não é banal e apresenta elevados níveis de complexidade. Não obstante, há estudiosos que têm enfrentado esse desafio.

Hale (2002) afirma que os crimes cibernéticos no mundo atingiam, aproximadamente, a quantia de US$ 50 bilhões em 2002. Lewis (2018) destaca que, dentre os crimes praticados globalmente, os cibernéticos estão em terceiro lugar em geração de custos, atrás da corrupção nos governos e do narcotráfico. Ele adiciona que as estimativas existentes dos custos dos crimes cibernéticos apresentam variações significativas, indo de US$ 10 bilhões a mais de US$ 1 trilhão, o que reflete a baixa confiabilidade nos dados e nas diferentes metodologias de cálculo. Lewis

(2018), por exemplo, utilizou a metodologia *economic history research*, chegando à estimativa de custo global dos crimes cibernéticos de até US$ 600 bilhões.

A dificuldade de obtenção de dados precisos e que representativos é exposta por CEA (2018) que afirma que houve elevada relutância das empresas em relatar informações negativas. Isso é reforçado por Scott (2016) que aponta apenas 13,2% dos crimes cibernéticos ocorridos no Reino Unido como reportados às autoridades policiais ou ao Action Fraud, que é o órgão britânico ao qual são informadas atuações criminosas dessa natureza.

Assim, Cashell et al. (2004) concluem que modelos teóricos que descrevem os retornos dos gastos em segurança da informação fornecem alguma ideia sobre o tamanho das perdas potenciais, mas a ausência de dados estatísticos melhores faz com que a determinação, de modo geral, dos custos dos ataques cibernéticos continue sendo especulativa. Essa percepção é coerente com a posição de CEA (2018) que afirma que as estatísticas divulgadas podem apresentar posições tendenciosas em razão dos dados obtidos.

CEA (2018) destaca que apesar de, normalmente, não divulgarem as perdas sofridas por ataques cibernéticos, as empresas ofertantes de seguros são as que provavelmente possuem as melhores condições de avaliar em que níveis essas perdas encontram-se, uma vez que ressarcem a seus clientes quando sofrem tais danos. Isso certamente é considerado pelas seguradoras para avaliar os riscos aos quais seus clientes estão expostos e quanto deve cobrar pelos seus seguros contra danos causados por ataques cibernéticos.

Essas dificuldades de estimativas fornecem o panorama em que se insere a caracterização das consequências econômicas de ataques cibernéticos. Muitas vezes, analistas dessa problemática precisam basear-se em considerações qualitativas sobre diferentes tipos de ataques cibernéticos identificados e sobre casos práticos ocorridos em variados setores ao redor do mundo.

Apesar dos números difusos, é notório que os ataques cibernéticos apresentam crescimento significativo, o que pode ser inferido pelo aumento progressivo das estimativas como, por exemplo, dos ataques de *ransomware* que, segundo Microsoft (2016), somaram US$ 325 milhões em 2015. Adicionalmente, Morgan (2017a) estima que esse valor foi de, aproximadamente, US$ 1 bilhão em 2016 e com previsão de cerca de US$ 5 bilhões em 2017.

Tal cenário é tão preocupante que os riscos de ataques cibernéticos figuram entre os 10 maiores riscos de colapsos globais de 2018, do Fórum Econômico Mundial (WEF, sigla em inglês), classificado em terceiro em probabilidade de ocorrência e em sexto em termos de impactos (WEF, 2018).

O Banco Mundial coloca os ataques cibernéticos atrás apenas de eventos climáticos extremos e desastres da natureza, no critério de análise probabilidade. Quando se consideram os impactos gerados, ficam abaixo dos dois anteriores somados a armas de destruição em massa, fracasso na adaptação às mudanças climáticas e crises relacionadas à água. Assim, os ataques cibernéticos foram entendidos como causadores de impactos maiores do que relevantes ameaças como conflitos entre Estados, ataques terroristas, desemprego e crises relacionadas à fome.

Esses elevados impactos são ratificados por Morgan (2017b) quando destaca que há previsão de que os crimes cibernéticos gerem um custo mundial acima de US$ 6 trilhões anuais em 2021, o que representaria o dobro de 2015.

Com tais níveis de relevância, surge a indagação: como ocorrem tantos incidentes cibernéticos? Uma resposta parcial é que muitos tipos de ataques estão diretamente relacionados à procedimentos inadequados dos usuários, como os caso já mencionados do soldado norte-americano no Oriente Médio e do executivo que inseriu um CD de procedência desconhecida em sua máquina. Contudo, a maior parte dos ataques é iniciada por meio de *links* enviados às vítimas. Sobre esse aspecto, Zetter (2015) estima que 91% dos ataques sofisticados são iniciados por *phishing* ou *spear phishing* enviados por e-mail. Obviamente, se o usuário clicar nos *links* desconhecidos recebidos por correio eletrônico, ele estará contribuindo para o aumento da vulnerabilidade da rede a que participa.

Como resposta ao aumento das ameaças, as instituições passaram a investir cada vez mais em medidas preventivas, como contratação de prestadores de serviços de segurança cibernética e treinamento de funcionários. A respeito disso, Mello Júnior (2017) estima que esse treinamento preventivo dos colaboradores pode criar um mercado que gira em torno de US$ 10 bilhões em 2027.

Do exposto, torna-se evidente que os ataques cibernéticos oferecem iminente ameaça a setores produtivos, financeiros e até a segurança nacional de países. Por essa razão, diversos Estados, criaram ou estão em processo de criação de mecanismos para fortalecerem suas capacidades de defesa nesse campo.

3 COMBATE E PREVENÇÃO AOS ATAQUES CIBERNÉTICOS

3.1 Conceitos relacionados à segurança e defesa cibernética

Sabendo das possibilidades criadas e o quão danoso pode ser o advento cibernético, os países passaram a buscar soluções para prevenirem-se de possíveis ataques nos níveis governamentais, ou ainda, para desenvolverem capacidades ofensivas, caso necessário, em um cenário denominado Guerra Cibernética. Da mesma forma, o setor privado busca proteger-se dos ataques cibernéticos, tendo em vista que é o principal alvo dos criminosos em tempos de paz.

O advento do espaço cibernético criou o conceito de segurança cibernética que "é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no Espaço Cibernético, seus ativos de informação e suas infraestruturas críticas" (BRASIL, 2014a, p. 19).

Outro conceito surgido foi o de defesa cibernética que, para Oliveira et al. (2017, p. 13), é o "ato de defender o sistema crítico das TIC de um Estado. Além disso, ela engloba as estruturas e questões cibernéticas que podem afetar a sobrevivência de um país". Já para o MD, esse é um conceito mais restrito, assim definido:

> Defesa cibernética é o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente. (BRASIL, 2014a, p. 18)

O conceito de proteção cibernética é, para o MD, uma atividade de caráter permanente que abrange ações para neutralizar ataques e exploração cibernética contra os dispositivos computacionais e redes de computadores e de comunicações (BRASIL, 2014a, p. 23). Esse último conceito é o que melhor se adequa aos setores da iniciativa privada, o que não significa que lhe é exclusivo, uma vez que todos devem buscar fazê-lo. Por fim, o conceito de Guerra Cibernética que é, em resumo, o uso do espaço cibernético em operações militares.

3.2 Segurança e defesa cibernética pelo mundo

A União Internacional de Telecomunicações (ITU) publicou o Índice Global de Segurança Cibernética (GCI, sigla em inglês) 2017. Esse índice é considera 25 parâmetros que compõem 5 pilares: legal, técnico, organizacional, capacitação e cooperação (ITU, 2017).

Analisando o GCI é possível verificar os distintos níveis dos países em relação à temática cibernética. O Brasil aparece na 38ª posição, com índice 0,59338, figurando como o quinto das Américas, atrás de EUA, Canadá, México e Uruguai. Nessa análise, o Brasil foi classificado pela ITU como “em fase de amadurecimento”.

Há distintos modelos para tratar de segurança cibernética e defesa cibernética. Segundo Oliveira et al. (2017), há basicamente três deles, com uma pequena variação no terceiro modelo. O primeiro, adotado por países como EUA, Colômbia e Venezuela, utiliza estruturas militares como responsáveis tanto pela defesa quanto pela segurança cibernética. O segundo, adotado no Paraguai, utiliza estruturas civis que também tratam incidentes cibernéticos na esfera militar. E o terceiro modelo é o adotado por países como Brasil e Argentina, que possuem estruturas civis para lidar com a segurança cibernética e estruturas militares para a defesa cibernética. Por fim, há uma variação do último modelo, adotada pelo Uruguai. Nele existem estruturas distintas bem definidas para os setores civil e militar, que são responsáveis, respectivamente, pela segurança e pela defesa cibernética. Contudo, a Política de Defesa uruguaia prevê a atuação das estruturas militares de defesa cibernética também no setor privado.

Os crimes cibernéticos são tratados como relevante à segurança nacional por diversos governos. Os EUA, por meio da Divisão Cibernética do FBI investigam casos de invasão de computadores, contraterrorismo e contrainteligência como as principais prioridades do programa cibernético devido à sua possível relação com a segurança nacional (FBI, 2018). Segundo FBI (2018), foi criada, recentemente, uma força-tarefa composta por diversas agências do governo, dentre elas o Departamento de Defesa, o Departamento de Segurança Interna e o próprio FBI, com o objetivo de trabalharem em conjunto para combater os crimes cibernéticos.

Algo semelhante ocorre na Austrália, onde, segundo Office of Prime Minister (2017), o governo investiu US$ 230 milhões na Estratégia Nacional Segurança Cibernética em 2016 e o Livro Branco de Defesa da Austrália prevê incremento de até US$ 400 milhões para melhoria das capacidades de defesa cibernética do país.

Na Europa, segundo o National Cyber Security Centre (NCSC), a União Europeia (UE) reconheceu que qualquer incidente de segurança cibernética poderia afetar vários Estados-Membros e, em 2013, apresentou uma proposta para melhorar a sua preparação para ataques cibernéticos. Essa proposta tornou-se, em 2016, uma diretiva denominada *The EU Directive on the security of Network and Information*

Systems, dando aos Estados-Membros 21 meses para integrarem a diretiva nas respetivas legislações nacionais (NCSC, 2018).

O Reino Unido, segundo o UK Cabinet Office (2016) elevou o orçamento em defesa cibernética de £ 860 milhões para £ 1,9 bilhões, entre 2016 e 2021, com ênfase em três áreas: defesa de estruturas críticas nacionais como energia e transporte; retaliação a atacantes; e formação de uma geração de especialistas, com ênfase no investimentos em centros de pesquisa e ensino de segurança cibernética nas escolas.

Segundo o NCSC (2018), serão implementadas mudanças na legislação do Reino Unido, conforme a Diretiva de Segurança de Redes e Sistemas de Informação da UE, visando aumentar os níveis de segurança e resiliência globais dos sistemas de rede e de informação, obtendo, assim, base jurídica para dispor de um quadro nacional para gerir incidentes de segurança cibernética e criar um grupo de cooperação com os membros da UE para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações, participando de uma rede de para promover uma cooperação operacional em incidentes específicos de segurança de redes e sistemas de informação, bem como partilhar informações sobre os riscos. (NCSC, 2018)

Hakmeh (2017) afirma que nos países do Conselho de Cooperação do Golfo (GCC, sigla em inglês) há significativa diferença da forma com que os países membros tratam legalmente os crimes cibernéticos. A autora põe como fundamental haver aspectos legais definidos nas legislações dos países para que o combate aos crimes cibernéticos seja efetivo, como a definição de leis sobre o tema, tipificação criminal, regulação de interação entre Estados com fins cooperativos, definição de poderes processuais, definição de termos e os parâmetros de sua aplicação, estabelecimento de regras para provas eletrônicas, definição de sua jurisdição e a descrição da responsabilidade dos prestadores de serviços.

Todos os países do Conselho de Cooperação do Golfo possuem leis sobre crimes cibernéticos, porém, segundo Hakmer (2017), essas, em sua maioria, apenas concentram-se na criminalização.

Hakmer (2017) enfatiza que a melhor forma de combater os crimes cibernéticos é a cooperação internacional, sem a qual, a efetiva atuação tende a ser ineficiente, pois as técnicas operativas dos atacantes mudam com elevada velocidade. Assim, a autora destaca que é necessário haver compartilhamento de informações, inteligência, experiências e lições aprendidas para encontrar as melhores maneiras

de conter o crime cibernético e abordar seus desafios, para tanto, ferramentas regulatórias, legais e tecnológicas precisam ser desenvolvidas coletivamente e atualizadas continuamente.

Dessa forma, verifica-se que o tema da defesa cibernética consta da pauta governamental nas diversas regiões do mundo.

4 PASSADO PRESENTE E FUTURO DE ATAQUES CIBERNÉTICOS NO BRASIL

4.1 Passado

Desde 2006, o Brasil rompeu a barreira de mais de 100 mil incidentes cibernéticos reportados ao CERT.br em um ano. Desde então, apresentou uma forte tendência de crescimento desse número, com um pico em 2014, com mais de 1 milhão de incidentes reportados (CERT.br, 2018b). Esses números são menores do que os reais, pois nem todos os incidentes são reportados. Entretanto, ainda assim, permitem a obtenção de um panorama geral.

O Brasil é um alvo relevante de ataques cibernéticos. A esse respeito, há estudos que indicam o destaque para os ataques com finalidade de obtenção de vantagens financeiras. Lewis (2018), em sua análise para a Mcafee, identificou o impacto econômico de crimes cibernéticos em países como Austrália, Brasil, Canadá, Alemanha, Japão, México, Reino Unido e Emirados Árabes Unidos. Nesse estudo, Lewis (2018) aponta o Brasil como um dos novos centros de crimes cibernéticos, juntamente com a Índia, Coreia do Norte e Vietnã.

Lewis (2018) classifica o Brasil em segundo lugar no número de ataques cibernéticos originados no território e o terceiro principal alvo. Assim, o autor aponta que as leis brandas poderiam ser uma das causas de que 54% dos ataques cibernéticos reportados no Brasil são originários de dentro do próprio país, tendo como principal alvo, os bancos e instituições financeiras. Esse dado é coerente com os apresentados pelo CERT.br (2018c) em que 51,77% dos ataques que lhe foram reportados procederam do Brasil.

No Brasil existem leis que tratam sobre o tema, como a Lei nº 12.737, de 30 de novembro de 2012, conhecida popularmente como Lei Carolina Dieckmann, que dispõe sobre a tipificação criminal de delitos informáticos, alterando o Código Penal Brasileiro (BRASIL, 2012a) e a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, conhecida como Marco Civil da Internet (BRASIL, 2014b). Assim, é possível que tais leis sejam

ineficazes para inibir a criminalidade pois na primeira lei, as penas não ultrapassam três anos de prisão e a segunda não contempla penalidades aos infratores.

O cenário descrito de leis brandas, associado à possibilidade de ganhos elevados com os cibernéticos e percepção de impunidade, cria uma relação de custo-benefício para os criminosos em que incentiva a realização de ataques.

A atuação governamental no sentido de fortalecer as capacidades de proteção cibernética para o país pode, indiretamente, contribuir para a redução da falha de mercado criada pelos ataques cibernéticos, se forem criadas medidas que incentivem ações conjuntas entre os setores públicos e privados. Uma vez que os conhecimentos necessários para proteger instalações críticas, como hidrelétricas apresentam semelhanças aos de proteger outros tipos de instituições, seria viável a atuação conjunta. Tal parceria contribuiria tanto para reduzir as falhas de mercado, quanto para fortalecer a defesa nacional que, por definição, é um bem público.

Em virtude de aspectos como os mencionados, a atuação do Estado é importante e desejável. Assim, medidas foram tomadas para adequar o Brasil ao cenário enfrentado. Ao criar a Política Nacional de Defesa em 2008, com revisão em 2012, o Brasil classificou o setor cibernético, juntamente com o nuclear e o espacial como estratégicos (BRASIL, 2012b). Isso permitiu a inclusão do setor cibernético na Estratégia Nacional de Defesa (END) o que, segundo Brasil (2014a), permitiu que a Segurança Cibernética e a Defesa Cibernética passassem a ser reconhecidos como campos sob responsabilidade de atuação do Estado.

Em 2009, segundo Brasil (2018a), o MD designou o EB como responsável pelo estabelecimento do setor cibernético, criando-se o Projeto de Defesa Cibernética. Esse ganhou proporções maiores, sendo substituído pelo Programa Estratégico do Exército Defesa Cibernética em 2016. Moury (2017) complementa que a prioridade do Governo Brasileiro com a defesa e a proteção cibernética levaram ao surgimento do Comando de Defesa Cibernética (ComDCiber) em 2016. Esse comando passou a funcionar com pessoal das três Forças Armadas, além de especialistas civis.

A END apresentou entre seus objetivos: promover ações conjuntas entre os Ministérios da Defesa e da Ciência, Tecnologia e Inovação contemplando o incentivo à multidisciplinaridade e dualidade de aplicações, fomento da Base Industrial de Defesa, aquisição de conhecimentos, geração de emprego e proteção das infraestruturas estratégicas do Brasil (BRASIL, 2012b). Esse contexto permitiu a estruturação do Estado Brasileiro na formatação adotada em 2018.

4.2 Presente

No Brasil, atualmente, a responsabilidade de proteger os ativos nacionais no espaço cibernético são divididas para os setores civil e militar. Tal divisão ocorre de acordo com nível de atuação dos agentes públicos.

Segundo Brasil (2017a), a responsabilidade do planejamento, coordenação e desenvolvimento de ações de segurança cibernética é do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSI-PR). Já a defesa cibernética age no nível estratégico. Assim, o DSIC/GSI-PR é encarregado pelo nível político; o ComDCiber pelo estratégico; o Centro de Defesa Cibernética pelo operacional e unidades militares das forças componentes pelo nível tático.

Alguns objetivos da END já ocorrem, como a aquisição de conhecimentos, produzindo o desenvolvimento de ferramentas com aplicação dual na área de cibernética. Pode-se citar o Simulador de Operações de Guerra Cibernética (SIMOC) que é um simulador virtual que foi desenvolvido com tecnologia 100% nacional, pelo EB em parceria com uma empresa de TIC. O SIMOC destina-se ao treinamento e simulação de situações para as tropas contra possíveis ataques cibernéticos (BRASIL, 2018b).

Na busca pelo fortalecimento das capacidades de defesa cibernética, o Governo Brasileiro trabalha conjuntamente com organizações públicas e privadas. Por exemplo, em 2018, ocorreu o primeiro exercício de simulação de ataques em massa aos setores financeiro, nuclear e de defesa, utilizando o SIMOC em Brasília. Esse exercício conjunto contou com a participação de gestores de crise e técnicos da área de proteção cibernética de instituições do setor financeiro, como Banco Central, bancos, empresas do setor nuclear, Ministérios da Defesa, das Relações Exteriores, Presidência da República e entidades do setor cibernético (BRASIL, 2018b).

Outro exemplo de parceria visando aumentar a resiliência aos ataques cibernéticos foi o acordo assinado entre a Fundação Parque Tecnológico Itaipu (FPTI) e o EB em 2017, esse acordo trata sobre cooperação mútua no Laboratório de Segurança Eletrônica, de Comunicações e Cibernética que funciona desde 2015 no Complexo Hidrelétrico de Itaipu (BRASIL, 2017b).

A colaboração entre agentes externos é necessária para o crescimento mútuo. Dessa forma, há atividades conjuntas com países que mantêm relações com o Brasil com o objetivo de trocar conhecimentos, um exemplo é o Estágio Internacional de

Defesa Cibernética conduzido pelo EB, havendo a participação de representantes de vários países (BRASIL, 2018c).

Por fim, ainda sobre as parcerias internacionais, segundo (ITU, 2017), a Polícia Federal do Brasil participa do sistema global de comunicações policiais I-24/7 desenvolvido pela Interpol para conectar policiais, incluindo crimes cibernéticos.

4.3 Futuro

Percebe-se a tendência de crescimento do uso do espaço cibernético tanto por cidadãos quanto por criminosos. Esse cenário, leva ao entendimento de que novas ações visando combater aos crimes cibernéticos deverão ser executadas, tanto pelo setor privado como pelo governo.

Os órgãos governamentais responsáveis pela defesa cibernética e pela segurança cibernética tendem a crescer de importância no país. Esse crescimento pode criar externalidades positivas como o fortalecimento das capacidades de reação e mesmo prevenção de ataques a diversos setores. Para tanto, faz-se necessário a criação de políticas públicas para permitir que haja maior atuação conjunta de órgãos como o CERT.br, polícias especializadas e Forças Armadas, de preferência, com a participação de órgãos de proteção ligados a setores estratégicos do país.

Como há carência de leis específicas tratando sobre ataques cibernéticos, prospecta-se que essa deve ser uma pauta a ser discutida pelos legisladores. Por exemplo, Martins (2018) destaca que ainda não há legislação específica sobre proteção de dados no Brasil e que dois anteprojetos de lei estão em discussão no Congresso Nacional.

CONCLUSÃO

O presente trabalho estudou os ataques cibernéticos tratando sobre seus riscos, como são tratados por governos ao redor do mundo e no Brasil.

Conclui-se que o uso do espaço cibernético se encontra em plena expansão e que Governos de diversas regiões estão a tomar medidas que proporcionem interação entre a defesa e proteção cibernética de Estado com elementos da iniciativa privada. Assim, o modo de proteger um sistema governamental ou de infraestruturas críticas para um país pode robustecer os sistemas empresariais e vice-versa. Dessa forma, o Brasil começa a caminhar nessa direção com a aproximação de órgãos do governo, Forças Armadas e instituições públicas e privadas.

Por fim, conclui-se que o tema apresenta amplo espaço para estudos futuros, sendo afeto a vários campos do conhecimento.

REFERÊNCIAS

BRASIL. Casa Civil. **Lei nº 12.737, de 30 de novembro de 2012.** Brasília: 2012a.

_____. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa.** Brasília: 2012b. Disponível em: <https://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf>. Acesso em: 14 set. 2018.

_____. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética.** Brasília: 2014a.

_____. Casa Civil. **Lei nº 12.965, de 23 de abril de 2014.** Brasília: 2014b.

_____. Casa Civil. **Decreto Presidencial nº 9.031, de 12 de abril de 2017.** Brasília: 2017a.

_____. Exército Brasileiro. **Exército e Itaipu assinam acordo para incremento da segurança de estrutura estratégica vital para o país.** Noticiário do Exército. Brasília: 5 set. 2017b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercito-e-itaipu-assinam-acordo-para-incremento-da-seguranca-de-estrutura-estrategica-vital-para-o-pais->. Acesso em: 14 set. 2018.

_____. Escritório de Projetos do Exército Brasileiro. **Coordena e integra a Defesa Cibernética.** Brasília: 2018a. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. **Exercício Guardião Cibernético reúne especialistas em TI, gestores de crise e tomadores de decisão.** Noticiário do Exército. Brasília: 4 jul. 2018b. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/exercicio-guardiao-cibernetico-reune-especialistas-em-ti-gestores-de-crise-e-tomadores-de-decisao->. Acesso em: 14 set. 2018.

_____. Exército Brasileiro. **Cooperação internacional e defesa cibernética atuam juntos para o enfrentamento das ameaças dessa natureza.** Noticiário do Exército. Brasília: 14 mai. 2018c. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/cooperacao-internacional-e-defesa-cibernetica-atuam-juntos-para-enfrentamento-das-ameacas-dessa-natureza->. Acesso em: 14 set. 2018.

CALDAS, Daniel Mendes. **Análise e extração de características estruturais e comportamentais para perfis de malware.** Dissertação. UnB: Brasília, 2016. Disponível em: <http://repositorio.unb.br/handle/10482/23110>. Acesso em: 23 out. 2017.

CARVALHO, Paulo Sergio Melo de. A defesa cibernética e as infraestruturas críticas nacionais. **Coleção Meira Mattos – Revista das Ciências Militares**. Rio de Janeiro, 2011.

CASHELL, Brian; JACKSON, William D.; JICKLING, Mark e WEBEL, Baird. The Economic Impact of Cyber-Attacks. Government and Finance Division. **Congressional Research Service**. The Library of Congress. 1th Apr, 2004. n. RL32331. Disponível em: <https://fas.org/sgp/crs/misc/RL32331.pdf>. Acesso em: 12 set. 2017.

CEA (THE COUNCIL OF ECONOMIC ADVISERS). **The Cost of Malicious Cyber Activity to th U.S Economy**. Washington, Feb, 2018. Disponível em: <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf>. Acesso em: 18 jul. 2018.

CEBROWSKI, A. K. Transformation and the Changing Character of War? **Transformation Trends**, Office of Transformation, Department of Defense. Arlington, 17 Jun. 2004. Disponível em: <www.hsdl.org/?view&did=448180>. Acesso em: 14 out. 2017.

CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Cartilha de Segurança para Internet: ransomware.** 25 mai. 2018a. Disponível em: <https://cartilha.cert.br/ransomware/>. Acesso em: 8 set. 2018.

_____. **Total de incidentes reportados ao CERT.br por ano.** 2018b. Disponível em: <https://www.cert.br/stats/incidentes/>. Acesso em: 12 set. 2018.

_____. **Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2017.** 2018c. Disponível em: <https://www.cert.br/stats/incidentes/2017-jan-dec/top-cc.html>. Acesso em: 14 set. 2018.

EASTTOM, William Chuck. **Computer Security Fundamentals**. Pearson IT Certification, 3 ed. 2016.

FEDERAL BUREAU OF INVESTIGATION (FBI). **What we investigate: Cyber Crime.** U.S. Government, U.S. Departament of Justice. 2018. Disponível em: <https://www.fbi.gov/investigate/cyber>. Acesso em: 2 jul. 2018.

GASPAR, Philipe. **Pragas eletrônicas: ainda não estamos livres delas**. jul. 2007. Disponível em: <http://www.philipe.eti.br/artigo-003.pdf>. Acesso em: 22 out. 2017.

HAKMER, Joyce. **Cybercrime and the Digital Economy in the GCC Countries. Chatham House.** The Royal Institute of International Affairs. International Security Departmente. London: Jun. 2017. Disponível em: <https://www.chathamhouse.org/sites/default/files/publications/research/2017-06-30-cybercrime-digital-economy-gcc-hakmeh.pdf>. Acesso em: 16 set. 2018.

HALE, Chris. Cybercrime: Facts & Figures Concerning This Global Dilemma. **Crime & Justice International.** v. 18, Issue 65, p. 5, 6, 24-26, Sep. 2002. Disponível em: <https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=197384>. Acesso em: 30 jan. 2018.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity Index 2017.** Genebra: 2017. ISBN: 978-92-61-25071-3. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf>. Acesso em: 27 set. 2018.

KLIMBURG, Alexander. **National Cyber Security Framework Manual**, NATO CCD COE Publication, Tallinn, 2012.

LEWIS, James. **Economic Impact of Cybercrime – No Slowing Down**. Mcafee Report – CSIS. Santa Clara, CA, February. 2018. Disponível em: <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf?utm_source=Press&utm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21&utm_medium=email>. Acesso em: 31 jul. 2018.

MACHADO, T. G.; MOTA, A. A.; MOTA, L. T. M.; CARVALHO, M. F. H. e PEZZUTO, C. C. Methodology For the Cybersecurity Maturity Level Identification in Smart Grids. **IEEE Latin America Transactions.** v. 14, issue 11, p. 4512-4519, Nov. 2016. Disponível em: <http://www.revistaieeela.pea.usp.br/issues/vol14issue11Nov.2016/14TLA11_14GerardMachado.pdf>. Acesso em: 22 jan. 2018. DOI: 10.1109/TLA.2016.7795822

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. Uma metodologia para implantação de um Sistema de Gestão de Segurança da Informação. **JISTEM: Journal of Information Systems and Technology Management**, vol. 2, n. 2, 2005, pp. 121-136. ISSN online: 1807-1775. Universidade de São Paulo. São Paulo. Disponível em: <http://www.redalyc.org/pdf/2032/203219587002.pdf>. Acesso em: 22 jan. 2018.

MARTINS, Danylo. Invasões cibernéticas criminosas ameaçam os negócios. **Valor Econômico.** Finanças. São Paulo: 28 mai. 2018. Disponível em: <https://www.valor.com.br/financas/5552593/invasoes-ciberneticas-criminosas-ameacam-os-negocios>. Acesso em: 5 out. 2018.

MELLO JÚNIOR, John P. Security Awareness Training Explosion. **Cybersecurity Ventures.** Menlo Park, California: 6 Feb. 2017. Disponível em: <https://cybersecurityventures.com/security-awareness-training-report/>. Acesso em: 8 set. 2018.

MICROSOFT. **Helthcare Beware the Rise of Ransomware**. 31 May. 2016. Disponível em: <https://cloudblogs.microsoft.com/industry-blog/industry/microsoft-in-business/healthcare-beware-the-rise-of-ransomware/>. Acesso em: 8. set. 2018.

MORGAN, Steve. Global Ransomware Damage Costs Predicted to Exceed $ 5 Billion in 2017. **Cybersecurity Ventures.** Menlo Park, California: 18 May. 2017a. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

_____. Cybercrime Damages $ 6 Trillion By 2021. **Cybersecurity Ventures.** Menlo Park, California: 16 Oct. 2017b. Disponível em: <https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>. Acesso em: 8 set. 2018.

MOURY. Taciana. Exército Brasileiro investe em defesa cibernética. **Diálogo: Revista militar digital – Fórum das Américas**. 12 mai. 2017. Disponível em: <https://dialogo-americas.com/pt/articles/brazilian-army-invests-cyber-defense>. Acesso em: 14 set. 2018.

NATIONAL CYBER SECURITY CENTRE (NCSC). **Introduction to the NIS Directive.** London: 28 Jan. 2018. Disponível em: <https://www.ncsc.gov.uk/guidance/introduction-nis-directive>. Acesso em: 16 set. 2018.

OFFICE OF PRIME MINISTER. **Offensive Cyber Capability to Fight Cyber Criminals.** Media release. Austrália: 30 Jun. 2017. Disponível em: <https://www.pm.gov.au/media/offensive-cyber-capability-fight-cyber-criminals>. Acesso em: 14 ago. 2018.

OLIVEIRA, Marcos A. G.; PAGLIARI, Graciete D. C.; MARQUES, Adriana A.; PORTELA, Lucas S. e FERREIRA NETO, W. B. **Guia de Defesa Cibernética na América do Sul.** Recife: Ed. UFPE, 2017. Disponível em: <https://pandia.defesa.gov.br/images/acervodigital/GuiaDefesaCiberneticaAmericaSul.pdf>. Acesso em: 20 jan. 2018.

OPPERMANN, Daniel. Governança da internet e segurança cibernética no Brasil. **Monções: Revista de Relações Internacionais da UFGD**. Dourados, v.2, n.3, jul./dez., 2013.

PAIS, Ricardo; MOREIRA, Fernando; VARAJÃO, João. **Engenharia Social (ou o carneiro que afinal era um lobo).** Universidade de Minho – Portugal. Ed. Almedina, p. 171–187, 2013. Disponível em: <http://hdl.handle.net/1822/26251>. Acesso em: 4 nov. 2017.

RAMALHO TERCEIRO, Cecílio da Fonseca Vieira. O problema na tipificação penal dos crimes virtuais**. Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 7**,** n. 58**,** 1 ago. 2002**.** Disponível em: <https://jus.com.br/artigos/3186>. Acesso em: 21 out. 2017.

RAPOSO, Álisson Campos. Terrorismo e contraterrorismo: desafio do século XXI. **Revista Brasileira de Inteligência/ Agência Brasileira de Inteligência**. vol. 3, n. 4, set, p. 39–55. Brasília, 2007.

SIKORSKI, Michael e HONIG, Andrew. **Practical Malware Analysis.** No Starch Press. San Francisco, 2012.

SINGER, Peter Warren; FRIEDMAN, Allan. **Cybersecurity and cyberwar: what everyone needs to know.** 2014. Segurança e Guerra cibernéticas: o que todos precisam saber. Tradutor Geraldo Alves Portilho Junior. Rio de Janeiro: Biblioteca do Exército Editora, 2017.

SCOTT, Patrick. How much of a problem is cyber-crime in the UK? **The Telegraph.** United Kingdom, 1th Nov. 2016. Disponível em: <https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/>. Acesso em: 7 ago. 2018.

UK CABINET OFFICE. **Britain's cyber security bolstered by world-class strategy.** United Kingdom: Nov. 2016. Disponível em: <https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy>. Acesso em: 14 ago. 2018.

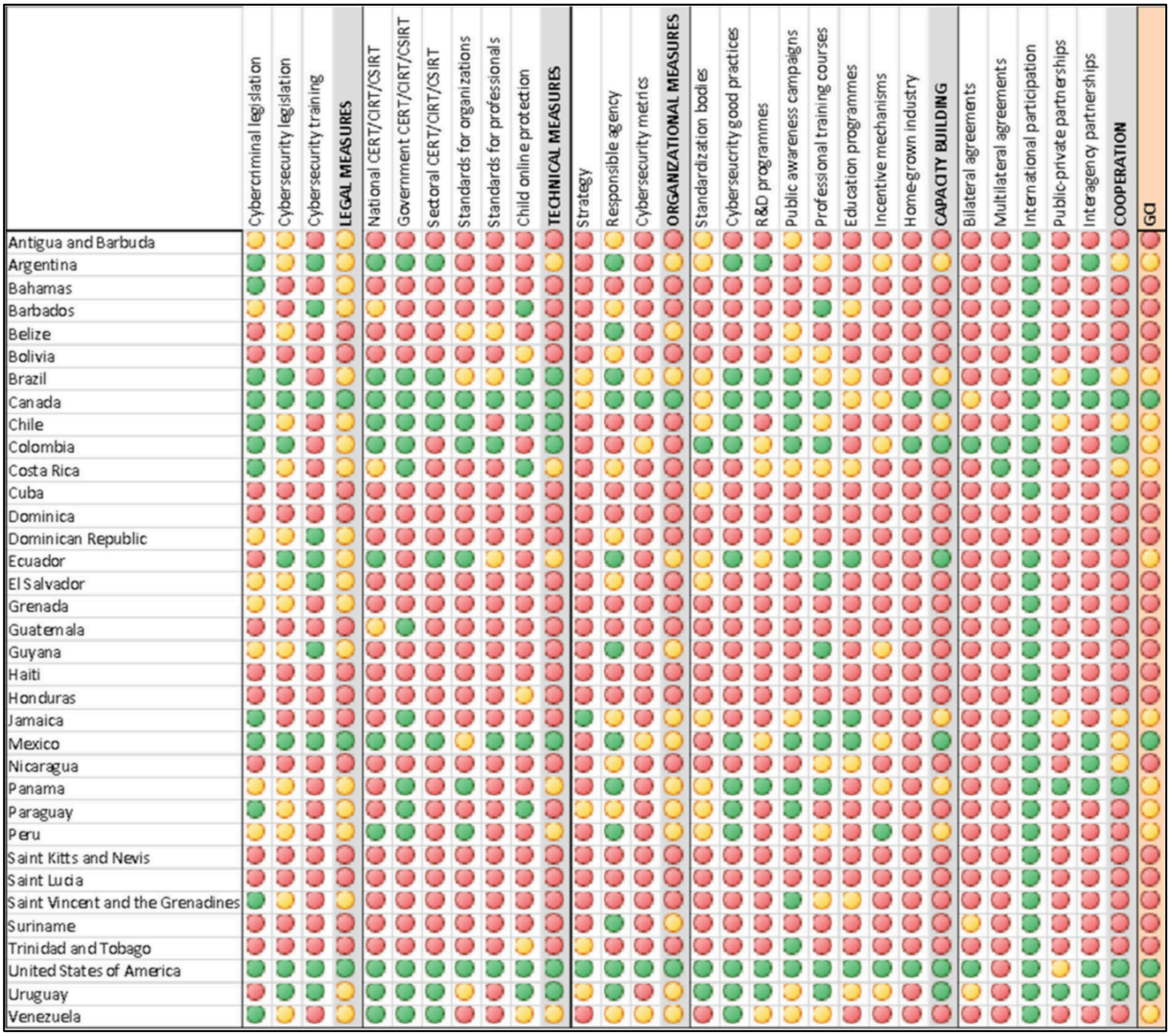
VENTRE, Daniel. Ciberguerra. In: ACADEMIA GENERAL MILITAR. **Seguridad global y potencias emergentes en un mundo multipolar**. XIX Curso Internacional de Defensa. España: Universidad Zaragoza. p. 31-45, 2011. Disponível em: <https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF48.pdf>. Acesso em: 1 set. 2018.

VIANNA, Eduardo Wallier; FERNANDES, Jorge Henrique Cabral. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science: Research Trends**, v. 9, n. 1, Marília, 2015. DOI 10.22556/1981-1640.

WORLD ECONOMIC FORUM (WEF). **The Global Risks Report 2018, 13th Edition.** Geneva: 2018. ISBN: 978-1-944835-15-6. Disponível em: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf>. Acesso em: 15 ago. 2018.

ZETTER, Kim. **Hacker Lexicon: what is phishing?** Wired. EUA: 4 jul. 2015. Disponível em: <https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/>. Acesso em 8 set. 2018.

ANEXO A – SCORECARD DO GCI 2017 DAS AMÉRICAS



Fonte: ITU, 2017.

O apêndice A apresenta *scorecard* regional das Américas. Nele são apresentadas as classificações atribuídas pela União Internacional de Telecomunicações para cada parâmetro que compõe o Índice Global de Segurança Cibernética de 2017. É exibido segundo um código de cores onde o verde representa padrão alto, amarelo significa classificação com padrão médio e vermelho para baixo. Assim, na última coluna é exibido, segundo esse código de cores, a classificação do Índice Global de Segurança Cibernética de cada país.