CICAD.II.2018

ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

ATAQUES CIBERNÉTICOS E MEDIDAS GOVERNAMENTAIS PARA COMBATÊ-LOS

Washington Rodrigues da Silva[1], Jorge Madeira Nogueira[2]
Mestre em Economia da Defesa[1], Doutor em Economia Regional[2]

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.

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 (quatro) 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 circula-

ção 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 2000, 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 computado-

res, 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 et al. (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 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.

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 backdoors 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 facilmen-

te 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 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 Fórum Econômico 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 reconhecidas 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.

CYBER ATTACKS AND GOVERNMENT ACTIONS TO COMBAT THEM.

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.

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.

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.

Washington Rodrigues da Silva é instrutor na Escola de Comunicações do Exército Brasileiro (EsCom) é mestre em Economia da Defesa na Universidade de Brasília (UnB). Graduado em Administração pela Faculdade de Ciências da Administração da Universidade de Pernambuco (FCAP/UPE) (2010) e em Ciências Militares pela Academia Militar das Agulhas Negras na área de Comunicações (AMAN) (2004). Especialista em Administração Financeira pela Faculdade de Ciências da Administração da Universidade de Pernambuco (2010), em Ciências Militares pela Escola de Aperfeiçoamento de Oficiais (EsAO) (2012), Gestão de Sistemas Táticos de Comando e Controle pela EsCom (2014) e Guerra Eletrônica pelo Centro de Instrução de Guerra Eletrônica (CIGE) (2015). Atua na área de Defesa e Educação no Exército Brasileiro. Foi instrutor do Centro de Preparação de Oficiais da Reserva do Recife (CPOR/R) (2007 a 2011); compôs a equipe de instrução da EsCom (2013 a 2015) e foi instrutor na Escuela de Comunicaciones da Escuela de las Armas do Exército Argentino (EcCom/EDA) (2016). Pode ser contatado pelo e-mail washingtonrs@hotmail.com.

Jorge Madeira Nogueira é Professor Titular do Departamento de Economia da Universidade de Brasília (ECO/UnB). Formado em Economia pela Universidade Federal do Rio de Janeiro (1975), Jorge Madeira Nogueira obteve seu título de Mestre em Engenharia de Produção pela Coordenação dos Programas de Pós-graduação em Engenharia da Universidade Federal do Rio de Janeiro (1978), com doutorado em Desenvolvimento Agrário - University of London (1982) e Pós-doutorado em Economia Regional pela Cornell University, Estados Unidos (1992). Ingressou como professor no Departamento de Economia da Universidade de Brasília (ECO/UnB) em 1983. Entre 1991 e 1995 foi Professor Visitante na Universidade de Cornell nos Estados Unidos. Em Cornell, ele recebeu o BURNHAM KELLY AWARD FOR DISTINGUISHED TEACHING - Prêmio concedido ao melhor professor do ano, eleito por alunos e professores, do College of Planning. Sua produção acadêmica inclui pouco mais de 150 trabalhos publicados em periódicos ou em anais de congressos científicos. Jorge Madeira Nogueira foi membro do Conselho Consultivo do Fundo Vale para o Desenvolvimento Sustentável entre 2013 e 2017. Pode ser contatado pelo e-mail jmn0702@unb.br.