ETHICAL HACKING E LEGÍTIMA DEFESA ELETRÔNICA

Isaac Rodrigues Ramos Neto
Pós-graduando pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas)

RESUMO. Estudo sobre a possibilidade de configuração de legítima defesa eletrônica diante da atuação dos Times de Resposta a Incidentes de Segurança Computacional (CSIRT), na observância da prática do delito de invasão de dispositivo informático na modalidade qualificada, previsto no artigo 154-A, §§ 3º e 4º, do Código Penal Brasileiro. Debate acerca da prática do ethical hacking e se tal conduta amoldar-se-ia à excludente da legítima defesa. Utiliza o método dedutivo, bem como a pesquisa doutrinária, legislativa e jurisprudencial. Recorre à internet como forma de complementação dos assuntos estudados. Espera demonstrar, ao final, que o ethical hacking poderá configurar hipótese de legítima defesa eletrônica, desde que obedecidos todos os requisitos desta, sendo o caminho mais adequado para reduzir os danos gerados pela invasão, pois, uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet, causando à vítima danos de improvável reparação.

Palavras chave: Legítima defesa. Crimes eletrônicos. Invasão de dispositivo informático.

1 INTRODUÇÃO

A Revolução Informacional, iniciada nas duas últimas décadas do século XX, caracteriza-se pela introdução da geração, do processamento e da transmissão de informações como fontes fundamentais de produtividade e poder por causa das novas condições tecnológicas surgidas nesse período (CASTELLS, 2005, p. 65), criando-se, assim, um novo paradigma.

Uma das diferenças entre a Revolução Informacional e as Revoluções Industriais dos séculos XVIII e XIX é a amplitude dos seus efeitos. Com os meios de comunicação bem mais avançados do que naquela época em razão da própria revolução, pode-se afirmar que, hoje, um grande número de países já adentrou a era da informação.

Não obstante tenha trazido grandes benefícios para as mais diversas áreas do conhecimento, por exemplo, a bioengenharia, a engenharia genética, a microeletrônica e as telecomunicações, a Revolução Informacional também acarretou um crescimento na ocorrência de crimes eletrônicos. Isso se deu, especialmente, pela alteração do perfil do agente que comete tais tipos de delitos.

O criminoso eletrônico ostentava a qualidade de “exímio perito na operação de computadores e sistemas computacionais” (MONTEIRO NETO, 2003, p. 41), todavia, hoje, qualquer curioso usuário da internet pode aprender, por meio de diversos tutoriais disponibilizados na web, como realizar uma invasão. Assim, considerando que há meios técnicos e jurídicos para identificar o infrator e puni-lo devidamente e que uma vez de posse da informação subtraída, o invasor poderia facilmente espraiá-la pela internet, nascem alguns questionamentos: seria possível reconhecer a legítima defesa, amparada pelo Direito Penal como causa excludente de ilicitude, diante da observância da prática desse delito? Em que situações específicas? Quais seriam seus limites?

O objetivo aqui trazido é o de analisar, à luz do direito penal brasileiro, a possibilidade de configuração de legítima defesa diante da observância da prática do delito de invasão de dispositivo informático em sua modalidade qualificada. Perceber-se-á que toda a análise realizada é interdisciplinar, porque, se não o fosse, seria incompleta. Valer-se apenas do Direito para entender esse fenômeno seria uma atitude

falha.

A pesquisa tem especial aspecto acadêmico, pois a discussão acerca da legítima defesa eletrônica é incipiente, necessitando de análises aprofundadas. Possui, ainda, relevante aspecto social no intuito de esclarecer se determinada conduta de proteção da informação poderá ser considerada legítima defesa ou não, extravasando seus limites.

2 DESENVOLVIMENTO

Com a sanção da Lei nº 12.737/2012, o ordenamento jurídico brasileiro foi presenteado com a tipificação do primeiro delito eminentemente eletrônico: a invasão de dispositivo informático (artigo 154-A do Código Penal). Essa tipificação representa o primeiro grande passo no sentido de combater os crimes eletrônicos no Brasil, que, paulatinamente, só aumentam o seu número de incidências.

Deve-se atentar, contudo, que, em alguns casos, o Poder Judiciário não conseguirá agir de forma efetiva e eficaz para recuperar os danos sofridos em razão desse novo tipo penal, especialmente, na sua modalidade qualificada, em que há subtração de informações e eventual compartilhamento. Sabe-se que uma vez obtida a informação, se esta não for imediatamente recuperada, o agente criminoso poderá difundi-la rapidamente por toda a internet, impossibilitando, assim, qualquer justa reparação pelos prejuízos sofridos. O direito ao esquecimento, por exemplo, não passa de uma mera fantasia, visto ser impossível relegar ao oblívio dados dispersados na rede mundial de computadores.

Assim, como meio de enfrentar tais delitos, levanta-se a possibilidade de configuração da legítima defesa em meio ambiente eletrônico.

2.1 DEFINIÇÃO DE ETHICAL HACKING

O ethical hacking pode ser entendido sob dois aspectos.

De um lado, pode ser definido como uma forma de prevenção, consistindo numa série de testes de segurança, a fim de identificar as possíveis falhas nos sistemas e, assim, fortalecê-los (KNIGHT, 2009).

Por outro lado, também pode ser visto como a ação de recuperação dos dados subtraídos, agindo o profissional de segurança com a mesma técnica do agente criminoso (hacking back). É esta faceta que interessará ao presente trabalho.

O hacking back é um meio de resposta ativa contra invasões. São duas as suas principais modalidades (DENNING, 2008, p. 422). A primeira trata-se de uma invasão com a finalidade de localizar o sistema computacional que originou os ataques e, consequentemente, os agentes envolvidos. A segunda envolve contra-atacar a máquina de origem dos ataques, com a finalidade de suspender a ação invasiva, bem como, eventualmente, recuperar informações obtidas de modo indevido.

Dois acontecimentos tornaram-se famosos nos Estados Unidos pela utilização desta técnica para combater delitos eletrônicos: o primeiro, um ataque eletrônico contra o Pentágono; e o segundo, contra o site da Organização Mundial do Comércio (OMC).

Em setembro de 1998, foi documentada, pela primeira vez, a utilização da técnica do hacking back. O Pentágono reagiu a um ataque de negação de serviço, iniciado pela Eletronic Disruption Theater, uma organização hacktivista, utilizando-se de uma técnica ofensiva para interromper o funcionamento daqueles dispositivos de onde partiam as invasões (JAYASWAL; YURCIK; DOSS, 2002, p. 381).

A segunda reação documentada ocorreu em janeiro de 2000, durante uma reunião da OMC. O grupo The Electrohippies Collective, também conhecido por e-Hippies, invadiram o site da OMC, utilizando também ataques de negação de serviço (DENNING, 2008, p. 423).

Na ocorrência de uma invasão, devem ser seguidos três passos na utilização do hacking back (PINHEIRO, 2013, i. 8.37). O primei-

ro passo é identificar o causador da invasão por meio de sistemas de detecção (intrusion detection systems – IDS), como o firewall. O segundo passo é chegar ao dispositivo informático responsável pelos ataques (traceback). Atenta-se que a invasão de um dispositivo informático também poderá resultar no controle remoto deste. Um possível ataque ao computador que está apenas sendo manipulado, apesar de não configurar o delito do artigo 154-A, por ausência de dolo, não impossibilita a reparação civil pelos eventuais danos causados. O terceiro e último passo é contra-atacar, seja para interromper o funcionamento daquele sistema, cessando a invasão, ou para recuperar informações obtidas ilegalmente (KESAN; HAYES, 2012, p. 461-467).

O tempo para a tomada dessas decisões deve ser o mais curto possível, facilitando a identificação do invasor e diminuindo as perdas econômicas (JAYASWAL; YURCIK; DOSS, 2002, p. 380).

2.2 TIMES DE RESPOSTA A INCIDENTES DE SEGURANÇA COMPUTACIONAL (COMPUTER SECURITY INCIDENT RESPONSE TEAMS – CSIRT)

Com o grande número de incidentes computacionais, conforme informações do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR) e do Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov), surge a necessidade de aprimorar a segurança das empresas, bem como dos órgãos públicos, agora, com o fim de proteger as suas informações e o bom desenvolvimento de suas atividades. Tal proteção é feita pelo CSIRT.

O primeiro CSIRT surgiu em 1988, após um fato conhecido por The Morris Worm Incident (PEIXOTO, 2008, p. 2).

O CSIRT tem, como objetivo primordial, o monitoramento, “para que se possa pegar o infrator literalmente com a ‘mão na máquina’, quer ele seja de dentro, algum funcionário ou colaborador, quer seja de fora” (PINHEIRO, 2013, i. 8.37). É, assim, necessário um funcionamento incessante, sendo o CSIRT um verdadeiro guardião da rede. Os times também poderão ser um grupo ad hoc, formado exclusivamente para responder e avaliar incidentes específicos (CRESPO, 2011, p. 113), desvirtuando-se, nesses casos, de sua natureza de monitoramento.

A atuação do CSIRT no combate a incidentes pode ser resumida em seis grandes etapas (PEIXOTO, 2008, p. 36 et seq.):

a) Preparação: momento de prevenção, conscientização dos usuários e realização de auditorias;

b) Identificação, contenção e erradicação: coincidem com as três fases do hacking back anteriormente expostas;

c) Recuperação e aprendizado: essa etapa nada tem que ver com a recuperação de informações subtraídas. É um momento de evolução, em que o CSIRT irá recuperar-se dos danos eventualmente sofridos, ampliará e aperfeiçoará suas defesas, verificará se o sistema está operando corretamente e, finalmente, aprenderá com seus erros, tentando evitar novas falhas em situações futuras.

2.3 ETHICAL HACKING E LEGÍTIMA DEFESA ELETRÔNICA

A legítima defesa está prevista no Direito Penal Brasileiro, no CP, art. 23, II, como uma causa de excludente de ilicitude. Historicamente, a legítima defesa surgiu após a vingança particular cair em desuso (FIORETTI, 2002, p. 21). Pode ser definida como o uso moderado dos meios necessários, a fim de repelir injusta agressão, atual ou iminente, a direito seu ou de terceiro(s).

Pode-se afirmar que a expressão “legítima defesa” trata-se de uma redundância, um pleonasmo. Na realidade, o termo “legítima” foi acrescentado pelo Direito Romano, pois as palavras “defesa” e “agressão” eram designadas

pelo mesmo termo: o verbo fendo (FIORETTI, 2002, p. 21).

O conceito de legítima defesa sofreu abalos apenas durante a Idade Média, período no qual predominou os impérios da Igreja Católica. Segundo FIORETTI (2002, p. 39), "o exercício da legítima defesa parecia um ato lesivo da caridade para com o próximo".

A partir do conceito anteriormente descrito, infere-se seus requisitos.

O primeiro é a injusta agressão a um bem jurídico. O termo agressão deve ser entendido como toda ação que tenha a finalidade de por em perigo ou gerar dano a um bem jurídico, podendo ser violenta ou não (PRADO, 2009, p. 351; BITENCOURT, 2012, cap. XXI, i. 6.3.1). O conceito de injusto coincide com o de ilícito. Se houver afronta a um bem tutelado pelo ordenamento jurídico, mesmo não havendo um tipo penal específico, a legítima defesa poderá ser invocada, desde que a conduta obedeça aos requisitos necessários para sua configuração. Portanto, observe-se que a injustiça da agressão deverá estar relacionada a aspectos objetivos, nunca podendo estar relacionada com o seu autor.

O segundo é um requisito temporal, qual seja agressão deverá ser atual ou iminente. Iminente é a conduta que está prestes a acontecer, não admitindo, portanto, delongas na repulsa (BITENCOURT, 2012, cap. XXI, i. 6.3.1). Atual é a agressão presente, que, já iniciada, ainda não se concluiu (PRADO, 2009, p. 352) ou, simplesmente, aquela que está acontecendo (GRECO, 2015, p. 404). Portanto, é pouco provável a configuração de legítima defesa em relação ao tipo penal ora estudado quando a vítima for um usuário comum, pois este não possui, em regra, aparatos e conhecimentos técnicos para repelir a agressão no tempo adequado.

O terceiro é o uso moderado dos meios necessários. Meios necessários são os "eficazes e suficientes para repelir a agressão" (RODRIGUES, 2008, p. 68). A valoração acerca de quais meios serão os necessários para a repulsa "deve ser sempre [...] ex ante, isto é, do ponto de vista do sujeito no momento em que se defende" (ZAFFARONI; PIERANGELI, 2013, p. 523). O conceito de uso moderado leva em consideração o dano causado na ação. Assim, em nenhuma hipótese, a agressão infligida pela legítima defesa poderá ser maior que a própria agressão a qual ela combate (BITENCOURT, 2012, cap. XXI, i. 6.3.3), visto que, se assim o for, dará margem à ocorrência de legítima defesa sucessiva.

O quarto e último requisito é o animus defendendi. Ao contrário dos demais requisitos de ordem objetiva, este possui caráter subjetivo. Como assevera PRADO (2009, p. 353), o "agente deve ser portador do elemento subjetivo, consistente na ciência da agressão e no ânimo ou vontade (animus defendi) de atuar em defesa de direito seu ou de outrem".

2.4 LEGÍTIMA DEFESA ELETRÔNICA: NOVO CONCEITO OU APENAS UM NOVO CASO?

No Brasil, a legítima defesa eletrônica surgiu, primeiramente, no Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo, que definia "defesa digital", no art. 154-C, como a

manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação.

Todavia, essa definição foi duramente criticada, pois criava uma figura específica de defesa que muito se distanciava daquela respaldada no artigo 25 do Código Penal. Deixava claro, ainda, que o instituto só poderia ser utilizado por "agente técnico ou profissional habilitado". Foi finalmente retirada após avaliação feita pela

Comissão de Constituição, Justiça e Cidadania (CCJC) do Senado Federal.

A prática do ethical hacking, em sua modalidade hacking back, pelo CSIRT quando está diante da prática do delito de invasão a dispositivos informáticos em sua forma qualificada, conforme o art. 154-A, § 3º, CP, deverá ser considerada legítima defesa nos termos estabelecidos no próprio art. 25, CP.

A injusta agressão a um bem jurídico, o primeiro requisito, está configurada, pois o tipo penal previsto no CP, art. 154-A, § 3º, protege, em especial, o "conteúdo das comunicações eletrônicas privadas, segredos comerciais ou industriais e informações sigilosas, assim definidas em lei".

A resposta atual ou iminente à agressão, o segundo requisito, está relacionada à própria atuação dos CSIRTs, visto que atuam monitorando incessantemente todas as atividades nas redes de computadores de determinada empresa ou órgão, protegendo, assim, todo o fluxo de informações.

O uso moderado dos meios necessários, o terceiro requisito, também está presente, pois a técnica do hacking back foca-se na cessação da invasão, bem como na recuperação das informações subtraídas.

O animus defendendi, o quarto requisito, deverá ser avaliado caso a caso. Todavia, aqui, presumir-se-á presente, pois se está analisando a conduta de um time formado por profissionais que atuam na área de segurança da informação.

Diante do exposto, não se pode afirmar que a legítima defesa eletrônica se trata de um novo conceito. Ela é apenas um novo caso dentro da clássica previsão do Código Penal, nascida diante da necessidade de proteção das informações contra os novos agentes criminosos que se utilizam do meio ambiente eletrônico em suas empreitadas delituosas.

2.5 EXCESSOS NA PRÁTICA DO ETHICAL HACKING

O CP, art. 23, parágrafo único, prevê que "o agente, em qualquer das hipóteses deste artigo, responderá pelo excesso doloso ou culposo".

Configura o excesso quando há "flagrante desproporção entre a ofensa e a agressão, quando o agente responde com um tiro a um tapa desferido pelo agressor e quando o agente mata uma criança porque esta adentrou ao seu pomar e apanhou algumas frutas" (RODRIGUES, 2008, p. 69).

O excesso na prática do ethical hacking como legítima defesa pode ser verificado quando, por exemplo, na tentativa de recuperar os arquivos, informações além daquelas subtraídas também são obtidas, podendo ser do próprio agressor ou de um usuário diverso que tenha seu dispositivo controlado. Verifica-se nessas duas hipóteses, respectivamente, um uso imoderado e uma agressão contra terceiros.

É difícil dizer se tais excessos seriam puníveis na esfera penal, visto que tanto o delito de invasão de dispositivo informático quanto o crime de exercício arbitrário das próprias razões não preveem a modalidade culposa. Assim, para que houvesse a sanção penal nesses casos, o excesso deveria ser doloso, além de a conduta dever amoldar-se a todos os demais elementos previstos no art. 154-A, caput, do Código Penal.

2.6 JURISPRUDÊNCIA BRASILEIRA ACERCA DO TEMA

Em consulta aos sítios eletrônicos do Supremo Tribunal Federal, do Superior Tribunal de Justiça, dos cinco Tribunais Regionais Federais e dos vinte e sete Tribunais de Justiça, não foi encontrada nenhuma decisão acerca do tema desenvolvido.

As decisões, em sua maioria, são referentes a habeas corpus ou a conflito de competência. Não tratam, em nenhum caso, sobre a possibilidade de legítima defesa contra o crime de invasão de dispositivo informático.

Trata-se de uma discussão incipiente no Direito Penal e que ainda não teve a oportunida-

de de chegar aos tribunais.

3 CONCLUSÃO

Os efeitos de reconhecer ou não o ethical hacking como hipótese de legítima podem ser representados por dois extremos, respectivamente: um caminho para a devida proteção das informações ou uma trilha para um caótico cenário no melhor estilo “velho oeste”.

Na visão otimista, o ethical hacking, aqui considerado como meio de legítima defesa, representaria uma opção para a contenção dos efeitos das práticas criminosas em meio eletrônico, visto a redução dos danos sofridos pelas invasões ser seu principal objetivo.

Apesar de existirem outros recursos jurídicos capazes de punir o invasor, estes se mostram lentos devido à instantaneidade dos ataques eletrônicos, sendo uma resposta imediata no momento da invasão mais adequada para a devida proteção das informações. Lembrando, novamente, que uma vez de posse da informação, o agente criminoso pode, fácil e rapidamente, gerar diversas cópias e espraiá-las pela internet.

No contexto pessimista, o ethical hacking, aqui não considerado em nenhuma hipótese meio de legítima defesa, encorajaria a prática do vigilantismo em vez do uso de recursos jurídicos, criando-se, assim, um cenário de faroeste. As empresas contratariam outras que prestassem serviços de segurança de informação, fazendo estas o papel de verdadeiros pistoleiros.

Tais empresas praticariam o ethical hacking sem limites, pois o Poder Judiciário e a legislação penal apresentar-se-iam lentos, incapazes de solucionar plenamente os problemas advindos das invasões. O ethical hacking, longe dos parâmetros estabelecidos pela legítima defesa, seria, portanto, a medida mais eficaz para a contenção desses delitos. Sistemas invadidos e controlados remotamente por um sistema principal capaz de executar ações por meio daqueles poderiam ser considerados alvos, pois não haveria limites para o contra-ataque. As ferramentas de ethical hacking continuariam a se desenvolver e seriam utilizadas secretamente até que medidas legais e judiciais fossem implementadas. Com a ausência de fiscalização na realização do ethical hacking e o desenfreado número de ataques e contra-ataques, a integridade da internet restar-se-ia prejudicada.

É certo que alguns casos chegariam ao Poder Judiciário, mas seria uma quantidade mínima. Em outros, a própria vítima contrataria uma empresa de segurança capaz de rastrear o invasor e buscar fazer justiça com as próprias mãos, passando, agora, à verdadeira condição de criminosa, podendo sua conduta ser tipificada, a depender do caso, no crime de exercício arbitrária das próprias razões ou no próprio crime de invasão de dispositivo informático, agindo, assim, em concurso de agentes. Outra implicação desse péssimo cenário seria a proliferação de seguros contra invasões eletrônicas.

Diante do exposto, qual seria a solução mais adequada para a sociedade brasileira? Os futuros cenários de uso do ethical hacking variam da paz ao caos. Este trabalho posiciona-se no sentido de se construir uma postura ofensiva. Não se fará nenhuma propositura de inovação legislativa, pois se entende que o conceito de legítima defesa delineado no Código Penal Brasileiro, em seu art. 25, é preciso e suficiente para constatar o uso regular do ethical hacking. Sendo hipótese de legítima defesa, a indústria iria desenvolver aplicativos capazes de interromper tais ataques, chegando-se, talvez, ao ponto de os usuários domésticos serem capazes de evitar tais invasões. Verifica-se, por fim, que os obstáculos mais difíceis de serem transpostos e que envolvem diretamente o tema são aqueles de cunho social, em especial, a responsabilidade legal do invasor e daquele que age em excesso de legítima defesa.

ETHICAL HACKING AND ELECTRONIC SELF-DEFENSE

ABSTRACT. Research on the possibility of

setting up electronic self-defense in the face of Computer Security Incident Response Teams' action against a computing device invasion in the qualified form under Article 154-A, §§ 3º and 4º, of the Brazilian Criminal Code. Debates about the practice of ethical hacking and if such conduct would conform to the legal definition of self-defense. Uses deductive method and the doctrinal, legislative and judicial researches. Uses the internet as a way to complement the studied subjects. Hopes to demonstrate that the ethical hacking can configure hypothesis of electronic self-defense, since obeyed the imposed restrictions, and being the most adequate way to reduce the damage caused by the invasion, because the invader can quickly and easily generate multiple copies of the archives and spread them over the internet once in possession of the information, causing a damage difficult to repair.

Keywords: Self-defense. Electronic crimes. Computing device invasion.

REFERÊNCIAS

BRASIL. Decreto-Lei n. 2.848, de 07 de dezembro de 1940. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>. Acesso em: 25 julho 2017.

_____. Substitutivo ao PLS 76/2000, PLS 137/2000 e PLC 89/2003, apresentado pelo Senador Eduardo Azeredo. Altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 (Código Penal), o Decreto-Lei n. 1.001, de 21 de outubro de 1969 (Código Penal Militar), a Lei n. 9.296, de 24 de julho de 1996, o Decreto-Lei n. 3.689, de 3 de outubro de 1941 (Código do Processo Penal), a Lei n. 10.446, de 8 de maio de 2002, e a Lei n. 8.078, de 11 de setembro de 1990 (Código do Consumidor), para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e da outras providencias. Disponível em: <http://www.oab.org.br/pdf/substitutivoazeredo.pdf>. Acesso em: 25 julho 2017.

BITENCOURT, Cezar Roberto. Tratado de Direito Penal: Parte Geral, vol. 1. 14. ed. rev., ampl. e atual. de acordo com a Lei n. 12.550, de 2011 – São Paulo : Saraiva, 2012, epub.

CASTELLS, Manuel. A Sociedade em Rede. Vol. 1. 8ª ed. rev. e ampl. Tradução de Roneide Venâncio Majer e Klauss Brandini Gerhardt. – São Paulo: Paz e Terra, 2005.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DO BRASIL. Estatísticas dos Incidentes Reportados ao CERT.br. Brasil, 2016. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 24 setembro 2017.

CENTRO DE TRATAMENTO DE INCIDENTES DE REDES DO GOVERNO. Estatísticas de incidentes de rede no governo – 2° trimestre/2017. Brasil, 2017. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_2Trimestre_2017.pdf>. Acesso em: 24 setembro 2017.

_____. Estatísticas de incidentes de rede no governo – 1° trimestre/2017. Brasil, 2017. Disponível em: <http://www.ctir.gov.br/arquivos/estatisticas/2017/Estatisticas_CTIR_Gov_1Trimestre_2017.pdf>. Acesso em: 24 setembro 2017.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. – São Paulo : Saraiva, 2011.

DENNING, Dorothy E. The Ethics of Cyber Conflict. In: HIMMA, Kenneth Einar; TAVANI, Herman T. The Handbook of Information and Computer Ethics. Hoboken, New Jersey : Wiley, 2008. p. 407-428. Disponível em: <http://www.cems.uwe.ac.uk/~pchatter/2011/pepi/The_Handbook_of_Information_and_Computer_Ethics.pdf>. Acesso em: 24 setembro 2017.

FIORETTI, Julio. Legítima Defesa: Estudo de Criminologia. Traduzido por Fernando Bragança. – Belo Horizonte : Líder, 2002.

GRECO, Rogério. Curso de Direito Penal (parte geral). 17 ed. Rio de Janeiro : Impetus, 2015.

JAYASWAL, Vikas; YURCIK, William; DOSS, David. Internet Hack Back: Counter Attacks as Self-Defense or Vigilantism? In: IEEE 2002 International Symposium on Technology and Society (ISTAS'02): Social Implications of Information and Communication Technology. Proceedings. 2002. ISBN: 0-7803-7284-0. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1013841>. Acesso em: 24 setembro 2017.

KESAN, Jay P.; HAYES, Carol M. Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace. In: Harvard Journal of Law & Technology, Cambridge, Massachusetts, vol. 25, nº 2, Spring 2012. Disponível em: <http://jolt.law.harvard.edu/articles/pdf/v25/25HarvJLTech415.pdf>. Acesso em: 24 setembro 2017.

KNIGHT, William. License to hack? - Ethical hacking. In-

fosecurity, 16 OCT 2009. Disponível em: <http://www.info-security-magazine.com/view/4611/license-to-hack-ethical--hacking/>. Acesso em: 24 setembro 2017.

MONTEIRO NETO, João Araújo. Crimes Informáticos: uma abordagem dinâmica ao direito penal informático. Pensar (UNIFOR), v. 8, p. 39-54, 2003. Disponível em: <http://hp.unifor.br/pdfs_notitia/1690.pdf>. Acesso em: 24 setembro 2017.

PEIXOTO, Mário César Pintaudi. Criando um CSIRT: Computer Security Incident Response Team e entendendo seus desafios. – Rio de Janeiro : Brasport, 2008, p. 2.

PINHEIRO, Patrícia Peck. Direito Digital. 3ª ed. rev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737, de 2012 – São Paulo : Saraiva, 2013, epub.

PRADO, Luiz Régis. Curso de direito penal brasileiro, parte geral: arts. 1º a 120. 8ª ed. rev., atual. e ampl. – São Paulo : Editora Revista dos Tribunais, 2009, v. 1.

RODRIGUES, Arlindo Peixoto Gomes. A legítima defesa como causa excludente da responsabilidade civil. – São Paulo : Ícone, 2008.

ZAFFARONI, Eugenio Raúl; PIERANGELI, José Henrique. Manual de Direito Penal Brasileiro: parte geral. 10ª ed. rev. e atual. – São Paulo: Revista dos Tribunais, 2013.

O Autor é pós-graduando em Ciências Criminais pela Pontifícia Universidade Católica de Minas Gerais (PUC-Minas). Graduado em Direito pela Universidade Federal do Ceará (UFC). Ex-bolsista de extensão do Núcleo de Estudos em Ciências Criminais da Faculdade de Direito da UFC. Ex-estagiário da Defensoria Pública do Estado do Ceará, da Procuradoria da União, do Ministério Público junto ao Tribunal de Contas dos Municípios do Estado do Ceará e da Justiça Federal. Atualmente, é advogado em Fortaleza/CE. E pode ser contactado por intermédio do email isaacrrneto@gmail.com