Stories Behind a Minuscule Chinese Chip

P. A. D. Rezende

***Abstract* – We begin by examining the context of a political media campaign launched in October of 2018 in the scope of the North Atlantic Treaty Organization military alliance, aimed at disseminating among IT managers, with backing from general public opinion, perceptions of new risks in the use of electronic microchips fabricated by Chinese companies, for use in sensitive computational platforms. We then contrast theses actions, which occur at the intersection of psychological and informational cyber fronts of the contemporary form of warfare (hybrid, 4th generation), with a similar type of risks inherent to the model for informatization of the federalized electoral process in Brazil, chosen more than twenty years ago and since frozen. Such contrast signals the presence of some form of geopolitical and/or ideological filtering, active in the mapping and evaluation of risks through scientific, legal and lay narratives on cibersecurity, regarding either embedded systems for military use, such as in weapons' controls, or for civilian purposes, such as in electronic voting systems.**

***Index terms* – computer security, embedded software, invasive software, national security, security management.**

I. INTRODUÇÃO

As duas primeiras partes deste artigo incluem extensa reedição, traduzida do inglês com a devida autorização, de um texto publicado no portal de comentário geopolítico *Moon of Alabama* [1], abordando o tema em análise e seu contexto. A saber, da intensa campanha político-midiática orquestrada no âmbito da aliança militar "Organização do Tratado do Atlântico Norte" (OTAN) no final de 2018, visando agora também disseminar percepções sobre novos riscos na utilização de componestes de microeletrônica fabricados por empresas chinesas. Na Segunda Parte descrevemos a polêmica que suscitou esta análise, sobre um minúsculo chip chinês, e na Terceira, relevantes aspectos do modelo de votação eletrônica implementado no Brasil, com destaque para detalhes da arquitetura e operação do sistema da urna eletrônica em uso desde 2013. Na Conclusão, um breve contraste em relação a riscos de tipo anteriormente abordados.

II. PRIMEIRA PARTE: CONTEXTO

Artigo submetido em 26 de março de 2019.

Pedro Antônio Dourado de Rezende (prezende@unb.br), professor da Universidade de Brasília. O autor-editor de [1], que em seu portal web se identifica por pseudônimo – bernhard –, através de uma troca privada de e-mails autorizou para este fim a tradução citada no início da Introdução.

NO dia 4 de outubro de 2018, vários países da OTAN coordenaram uma escalada na campanha de propaganda contra a Rússia, agora ampliada contra a China e o multipolarismo. O gatilho para deflagração dessa escalada foi uma reunião de cúpula da OTAN, na qual os Estados Unidos (EUA) pressionaram por uma intensificação na guerra cibernética contra a principal adversária dessa organização militar. No mesmo dia, outra vertente dessa campanha orquestrada mirou como alvo a China, voltada contra o desenvolvimento e fabricação chineses de chips eletrônicos avançados na cadeia de valor das arquiteturas de sistemas computacionais. Relacionado a isso, surge também pressão dos EUA contra Taiwan, um dos principais fornecedores de chips ao ocidente, para cortar seus laços com a China continental nessa área.

A campanha inicial anti-Rússia é tematizada com acusações de hacking, influência política ilegítima, e operações de espionagem. Na escalada, a Grã-Bretanha, a Holanda e a Bélgica largaram junto. O governo da Grã-Bretanha acusou [2] o Serviço de Inteligência Militar da Rússia (GRU) de espionagem contra a Organização para a Proibição de Armas Químicas (OPCW) em Haia, de tentativas de espionagem contra seu Ministério das Relações Exteriores (*Foreign Office*), de tocar campanhas de influência relacionadas às eleições europeias e americanas, e de hackear a Agência Internacional Anti-Doping (WADA). A mídia corporativa britânica voluntariamente apoiou isto, ajudando a exagerar as alegações. Citando, por exemplo, o The Gardian [3]:

> "*O Foreign Office atribuiu seis ataques específicos a hackers apoiados por GRU e identificou 12 nomes de grupos de hackers como frentes do GRU - Fancy Bear, Voodoo Bear, APT28, Sofacy, Pawnstorm, Sednit, CyberCalipato, Cyber Berku, BlackEnergy Actors, Stronium, Tsar Equipe e Sandworm*." (trad. do autor)

Tal "ajuda" se revela uma farsa quando se percebe que os codinomes dos "grupos de hackers" que o Gardian tenta vender como russos não se referem a grupos de hackers, mas a métodos de ataque. Após se tornarem conhecidos, qualquer desses métodos pode ser usado por qualquer grupo ou indivíduo competente. Com efeito, os métodos de codinome citados, quanto bem executados, são quase impossíveis de serem rastreados até um ponto confiável para atribuição da autoria. Além disso, *Fancybear*, *ATP28*, *Pawn Storm*, *Sofacy*, *Sednit* e

Strontium são apenas nomes diferentes para o que pode ser identificado apenas como um mesmo método de ataque [4], conhecido já há bastante tempo.

Há também codinomes listados que se referem a ferramentas antigas, utilizadas por grupos de hackers para praticar crimes comuns. A Blackenergy [5], por exemplo, tem sido usada por cibercriminosos desde 2007. Alega-se em [5] que um grupo pró-russo denominado Sandworm a teria usado na Ucrânia, mas a evidência para tal atribuição é no mínimo duvidosa, pois se baseia no idioma falado pelos indivíduos de tal grupo, quando se sabe que na Ucrânia também se fala russo. Lançar mão assim de uma lista de codinomes, sem qualquer diferenciação, aponta a possibilidade de uma operação midiática planejada para desinformar e assustar o público espalhando medo, incerteza e dúvida (FUD - *Fear, Uncertainty and Doubt*).

O governo da Holanda, por sua vez, promoveu no mesmo dia uma litania [6] sobre supostas tentativas de espionagem contra a OPCW em Haia. A narrativa começa com a história de quatro supostos agentes do GRU viajando para Haia com passaportes diplomáticos oficiais russos, alegadamente com o intuito de escanearem a rede wifi da OPCW. Ocorre que as redes wifi são notórias pela facilidade de serem escaneadas e hackeadas. Se a OPCW estiver usando essa tecnologia para comunicações sensíveis, ela estaria violando não só as melhores práticas de cibersegurança, como também as mínimas. Mas o discurso holandes só dirige sua atenção para as ações dos russos, declarando-os suspeitos, quando caberia antes indagar o óbvio: Por que enviar agentes russos com passaportes diplomáticos a Bruxelas para hackearem uma rede wifi, se qualquer um poderia e pode fazê-lo?

Atribuiu-se a suspeita por serem esses agentes muito reservados. Limpavam o próprio lixo no quarto do hotel, enquanto ao mesmo tempo transportavam laptops com dados privados, inclusive recibos de táxi mostrando sua viagem da sede da GRU para o aeroporto de embarque em Moscou. Assim como na saga Skripal/Novichok os suspeitos são pintados, nas mesmas pinceladas, como formidáveis supervilões e ao mesmo tempo como trapalhões amadores. Ocorre que espiões de agências que se prezam não são nem uma coisa nem outra. Seria mais coerente e razoável considerar que a participação desses russos nessa ladainha envolve algum tipo de *honeypot* [7].

De sua parte, o Departamento de Justiça dos EUA havia reforçado essa escalada impetrando, no dia anterior, novos indiciamentos contra supostos agentes do GRU [8], duvidosamente conectados a vários alegados incidentes de cibersegurança [9]. Mas como nenhum dos agentes russos indiciados jamais se apresentaria em um tribunal nos EUA, as acusações genéricas e vagas nesse indiciamento nunca terão sua veracidade publicamente testada.

A. Imbróglio na OTAN

Essa nova escalada foi sincronizada com o desfecho da reunião dos Ministros de Defesa dos países-membros da OTAN, encerrada nesse "dia D" (4/10/2018) [10], com uma proposta do governo dos EUA [11] na qual o mesmo 'se oferece' para usar suas armas cibernéticas sob disfarce ou à guisa da OTAN. Citando [11]:

> "*Katie Wheelbarger, a principal subsecretária adjunta de defesa para assuntos de segurança internacional, disse que os EUA estavam se comprometendo a executar operações cibernéticas ofensivas e defensivas para aliados da OTAN, mas com os Estados Unidos mantendo o controle sobre seu próprio pessoal e capacidades.*" (trad. do autor)

Se os demais membros da OTAN, sob pressão dessa escalada, concordarem com tal proposta, os resultados óbvios serão mais controle dos EUA sobre as redes e cidadãos de seus países, com mais provocações e ameaças contra potenciais adversários. Citando ainda [11]:

> *"O chefe da OTAN prometeu nesta quinta-feira [4 de outubro de 2018] fortalecer as defesas da aliança contra ataques a redes de computadores que, segundo a Grã-Bretanha, são dirigidas pela inteligência militar russa, também conclamando a Rússia a parar com seu comportamento 'imprudente'."* (trad. do autor)

Essas acusações contra a Rússia, decorrentes de nefastas operações de espionagem e supostas ações contra policiais, são hipócritas [12] frente as dimensões e imenso alcance da espionagem e americana e britânica [13], reveladas por Edward Snowden. Tornaram-se também bem conhecidas as ferramentas de hacking e ciberataque da CIA, com o vazamento do "Vault 7" para o Wikileaks.

Também é conhecido que o Pentágono realiza grandes campanhas de manipulação de mídias corporativas e sociais. A agência britânica de espionagem GHCQ, sua parceira na aliança *Five Eyes* [14], hackeou a maior empresa de telecomunicações da Bélgica [15] para espionar as várias organizações internacionais com sede em Bruxelas. Organizações como a OPCW têm sido alvo, direta ou indiretamente, também de espiões e operações clandestinas dos EUA. A Agência de Segurança Nacional dos EUA (NSA) tem invadido regularmente a OPCW pelo menos desde setembro de 2000 [16] . Citando [16]:

> "*De acordo com o vazamento do Shadow Brokers da semana passada, a NSA comprometeu um servidor DNS da Organização para a Proibição de Armas Químicas em setembro de 2000, dois anos depois da Lei de Libertação do Iraque e da Operação Raposa do Deserto, mas antes da eleição de Bush.*" (trad. do autor)

B. Pressão contra neutralidade na OPCW

Em 2002 o governo dos EUA expulsou o então dirigente da OPCW [17], por sinal um diplomata Brasileiro, porque este não concordava em propagandear as imaginárias armas químicas iraquianas. Citando [17]:

> "*José Mauricio Bustani, um diplomata brasileiro que foi reeleito por unanimidade no ano passado [2001] como diretor-geral da Organização para a Proibição de Armas Químicas, composta por 145 nações, foi eliminado do cargo hoje depois de recusar repetidas exigências dos Estados Unidos de que renunciasse por causa de seu 'estilo de gestão'. Nenhum sucessor foi selecionado.*" (trad. do autor)

O governo dos EUA organizou uma votação relâmpago contra o dirigente ameaçando deixar a OPCW se a mesma não ocorresse. John Bolton, conhecido como um burocrata irascível e predisposto ao enfrentamento, agora ocupando a função de Conselheiro de Segurança Nacional de Donald Trump, ameaçou atingir os filhos de José Bustani, para pressioná-lo a renunciar [18]. Citando [18]:

> "*'Recebi um telefonema de John Bolton – foi a primeira vez que tive contato com ele – e ele disse que tinha instruções para me dizer que eu teria que renunciar à organização, e eu perguntei por quê', disse Bustani à RT. 'Ele [Bolton] disse que o [meu] estilo de gestão não estava de acordo com Washington' ... Bustani respondeu que 'não devia nada' aos EUA, apontando que ele fora nomeado por todos os estados-membros da OPCW. Com um tom mais sinistro, Bolton disse: 'OK, então haverá retaliação. Prepare-se para aceitar as consequências. Sabemos onde estão seus filhos.'. Segundo Bustani, dois de seus filhos estavam em Nova York na época, e sua filha estava em Londres*" (trad. do autor)

Como marca deste cenário geopolítico, destacamos o emprego pelos EUA e Grã-Bretanha das mesmas abordagens que tentam retratar como *casus belli* cibernéticos se praticadas por terceiros, ou mesmo se praticáveis com ou sem evidências convincentes.

III. Segunda Parte: O Chip Chinês

Esta escalada na propaganda contra o multipolarismo teve sua largada com a publicação, bem ajustada ao contexto acima descrito, de uma matéria no portal de notícias econômicas Bloomberg, a qual vinha sendo preparada há mais de um ano. Com título que se traduz "A grande hackeada: Como a China usou um chip minúsculo para se infiltrar nas empresas dos EUA" [19], a matéria alega que empresas chinesas manipulam o hardware que fabricam para a empresa norte-americana SuperMicro, o qual é depois vendido para a Apple, Amazon e outras, para suas operações com servidores em nuvem. Ilustrada com uma foto desse chip sobre a ponta de um dedo, indicando seu tamanho equivalente (em altura e comprimento) ao de um mero grão de arroz, a matéria afirma:

> "*Aninhados nas placas-mãe dos [computadores que funcionarão como] servidores, os testadores encontraram um pequeno microchip, não muito maior que um grão de arroz, que não fazia parte do design original das placas.*" (trad. do autor)

Todavia, tanto a Apple quanto a Amazon negaram categoricamente essas alegações [20], inclusive com denúncia de má prática jornalística [21]. Eis que a matéria da Bloomberg tem mesmo graves problemas, visíveis inclusive. Para começar, ela está completamente baseada em fontes anônimas, a maioria funcionários do governo dos EUA. Sobre tais fontes, citamos a própria ([19]):

> "*As negativas das empresas [supostamente afetadas] são contraditadas por seis ex ou atuais altos funcionários nacionais de segurança, que, em conversas iniciadas durante o governo Obama e continuadas sob o governo Trump, detalharam a descoberta dos chips e a investigação das agências do governo.*" (trad. do autor)

Ainda, a forma como o funcionamento desse chip e a sua alegada manipulação sorrateira são descritos, indica que esta é teoricamente possível [22], mas não é plausível que ocorra [23]. Na opinião instruída do autor de [1], seriam necessárias múltiplas manipulações, e não apenas em um minúsculo chip, para se alcançar os efeitos descritos. Também os especialistas da confiança daquele autor, consultados [24], não estavam convencidos da veracidade da narrativa. Além de outros em posterior análise, como Joel Uchill em [25]. Ainda assim, é particularmente curioso que tais críticas estivam prontas para serem publicadas no mesmo dia que a matéria criticada, e que os mesmos modelos citados de placas-mãe para servidores ainda estejam sendo usadas em operações relevantes para a segurança nacional dos EUA. Citando [24]:

> "*Assumindo que a história da Bloomberg esteja correta, isso significa que a comunidade de inteligência dos EUA, durante um período que abrangeu duas administrações, percebeu uma ameaça estrangeira mas permitiu que essa ameaça se infiltrasse nas forças armadas. Se a história for falsa, ou incorreta em seus aspectos técnicos, então faria sentido que a Supermicro estivesse durante esse tempo equipando as forças armadas dos EUA.*" (trad. do autor)

Considerando tudo isto, pode também haver motivo financeiro por trás dessa narrativa propagada na matéria da Bloomblerg. Citando ainda [22]:

> "*Os repórteres da Bloomberg recebem bônus baseados indiretamente em quanto eles influenciam mercados com suas matérias. Esta história, sem dúvida, fez isso.*" (trad. do autor)

De fato, quando a tal matéria ([19]) foi publicada, como parte dessa blitz no dia D para escalada de propaganda contra o multipolarismo, o preço das ações da SuperMicro caiu, de US$ 21,40 para menos de $ 9,00 [26]. Ações que vinham sendo negociadas a US$ 12,60 ao tempo em que tal narrativa começou a ser escrita na Bloomberg.

Essa narrativa pode também ser uma camuflagem para algum *hack* da NSA, após este ter sido acidentalmente detectado por potencial vítima. De qualquer forma, o mais provável é que ela contenha meias-verdades, baseadas em um incidente mais antigo [27], buscando dissuadir a indústria ocidental de TI em escolher fornecedores de componentes eletrônicos na China. Esta última hipótese seria consistente com outras ações e movimentos do governo dos EUA contra a China, inclusive as que coincidentemente (ou não) ocorreram no mesmo dia D.

A. Ciberfront na guerra híbrida

Dentre essas ações concomitantes nesse dia, houve um pronunciamento belicosamente revelador do vice-presidente dos EUA [28], proferido no Instituto Hudson, *think tank* com sede em Washington, DC. Citando [28]:

> "*... Mike Pence acusou a China na quinta-feira [4/10/2018] de tentar minar o presidente Donald Trump no momento em que o governo lança uma nova e dura retórica sobre o comércio chinês, sua política econômica e política externa. ... Soando o alarme, Pence advertiu outras nações a serem cautelosas ao fazerem negócios com a China, condenando a 'diplomacia da dívida' do país asiático, que busca atrair nações em desenvolvimento para sua órbita. Pence também alertou as empresas americanas a serem vigilantes contra os esforços chineses para alavancar o acesso a seus mercados, para modificar o comportamento corporativo de acordo com o gosto deles.*" (trad. do autor)

Outra ação simultânea foi a revelação de um novo relatório do Pentágono, alertando contra a compra de equipamentos chineses. O relatório "vazou" para a Agência Reuters, que nesse dia D a divulgou [29], em apoio à vertente anti-China dessa blitz para a atual campanha psicológica contra o multipolarismo. Citando [29]:

> "*A China representa um 'risco significativo e crescente' para o suprimento de materiais vitais para os militares dos EUA, de acordo com um novo relatório liderado pelo Pentágono, que visa melhorar as deficiências das principais indústrias norte-americanas, vitais para a segurança nacional. O relatório de quase 150 páginas, divulgado pela Reuters na quinta-feira [4 de outubro], antes de seu lançamento oficial na sexta-feira, concluiu que existem cerca de 300 vulnerabilidades que podem afetar materiais e componentes essenciais para os militares norte-americanos .... 'Uma das principais conclusões deste relatório é que a China representa um risco significativo e crescente para o fornecimento de materiais e tecnologias consideradas estratégicas e críticas para a segurança nacional dos EUA', disse o relatório.*" (trad. do autor)

A narrativa da Bloomberg [19], o discurso de Pence [28], e o relatório "vazado" do Pentágono [29], concomitantes, parecem orquestrados para assustar os que contemplem utilizar fornecedores ou equipamentos eletrônicos chineses em suas cadeias de suprimentos. Entretanto, as alegações de ataques chineses via cadeia de suprimentos são tão hipócritas quanto as acusações contra a Rússia por ataques cibernéticos. Começando pelo primeiro caso conhecido desse tipo de ataque (via fornecedor de suprimentos de TI), que remonta a 1982 [30], onde agressor e vítima estavam em posição oposta à insinuada pela atual propaganda bélica. Citando [30]:

> "*Uma operação da CIA para sabotar a indústria soviética, seduzindo Moscou a usar software que estava contaminado com uma armadilhada para sabotagem, foi espetacularmente bem-sucedida quando [o uso desse software instalado em dispositivo de controle] desencadeou uma enorme explosão num gasoduto siberiano, ocorrida ontem. [em junho de 1982] ... O Sr. Reed [Thomas Reed, ex-ministro da Força Aérea e ex-assessor do Conselho Nacional de Segurança do governo Reagan] escreve que o software 'foi programado para redefinir as velocidades da bomba e as configurações da válvula para produzir pressões muito além daquelas aceitáveis para juntas de tubulações e soldas'.*" (trad. do autor)

O portal Wikileaks, em seu repositório "Valt 7", lista ainda outros 26 casos envolvendo manipulação clandestina de hardware e/ou software por agentes ou agências dos EUA, capazes de sabotar cadeias de suprimentos para viabilizar ciberataques dirigidos [31]. E uma busca por "supply chain" nos arquivos do Edward Snowden mostra 18 documentos descrevendo tais "projetos" [32].

O atual governo dos EUA, com John Bolton numa posição de destaque, replica o estilo brutal da campanha eleitoral de Donald Trump e o emprega como instrumento de política externa[2] . Seja em escala ou em coordenação,

2 - Haja vista, por exemplo, o caso contra a empresa Huawei – vide [46]

essa massiva campanha político-midiática é comparável à deflagrada em 2002 para vender a guerra contra o Iraque. Assim, seja na campanha eleitoral de 2016 nos EUA ou nessa escalada de propaganda contra o multipolarismo [33], o papel da mídia, com apoio consciente ou não, deliberado ou não de seus veículos, é fundamental para o efeito psicológico planejado nesta forma de combate, e para eficácia de operações nesse estágio da guerra híbrida.

IV. TERCEIRA PARTE: O CHIP NA URNA

NO Brasil, há um caso similar de chip que, curiosamente, não aparece no noticiário da mídia corporativa. Muito menos como foco potencial de riscos, e menos ainda na escalada da campanha político-midiática analisada acima. Trata-se de um chip denominado *Master Security Device* (MSD), ou "Dispositivo Microprocessado de Segurança", destacado em vermelho na figura a seguir.

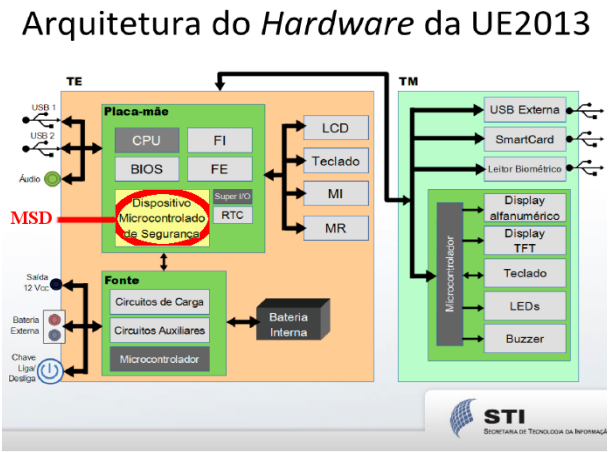

Fig. 1. Testes Públicos de Segurança – 2016. Extraída de [34].

O MSD passou a fazer parte do projeto de placa-mãe para urnas eletrônicas que o Tribunal Superior Eleitoral (TSE) atualizou em 2009, conforme o qual vem sendo licitadas e compradas urnas desde 2015 no mais tardar. Dizemos curiosamente pois o caso do MSD, que passamos a expor, parece-nos ainda mais concreto, relativo ao tipo de risco aqui discutido, que o do chip chinês denunciado em [19].

A função do MSD deve ser a de controlar a inicialização da BIOS na urna. Em tese, apenas isso, nas urnas que hoje compõem mais de 90% do estoque do TSE. O MSD foi projetado por pesquisadores do instituto Renato Archer[3], como resultado de um projeto de pesquisa contratado para 'melhorar a segurança da Urna Eletrônica'. Por esse contrato, o modelo-base para votação informatizada adotado pelo TSE não era para ser questionado, e não foi.

A proposta de 'melhoria' com o MSD seria para que o TSE pudesse controlar com mais recursos o que pode e o que não pode "dar boot" em suas urnas. A ideia isoladamente parece boa [34], já que o inquestionado[4] modelo básico adotado pelo TSE desde 1996 tem sido o *Direct-Recording Electronic* (DRE) [36], que especifica máquinas de votar de 1ª geração [37], [38], puramente eletrônicas, sem scanner e sem impressora que possibilitem o registro material de cada voto individual.

Porém, no contexto da implementação, outros aspectos passaram a ter importância no mapeamento de novos riscos, conforme o referencial de interesses e do modelo de votação "irrevogabilizado"[4] pelo TSE: eis que a fabricação e montagem do chip MSD nas placas-mãe fica a cargo da fornecedora das urnas, que antes grava um *blob* [39] na sua memória não-volátil e, depois, "atualiza" esse *blob* com "*drivers* de urna", que são entregues ao TSE, até onde se sabe [40], em código binário pouco antes da compilação do restante do software da urna, que atualiza no TSE o Sistema Operacional e aplicativos a serem instalados nas urnas, às vésperas de cada eleição.

A. *Ciberfront na disputa eleitoral*

Deixando de lado as campanhas de candidatos, focamos aqui na TI do sufrágio. A fornecedora de urnas para as últimas eleições brasileiras é, ao menos desde 2009, uma empresa que tem uma homônima transnacional, que não se sabe bem se é ou não sua matriz, mas que vem a ser ou já foi a maior fabricante de máquinas eletrônicas para jogos de azar do planeta. A mesma que já foi banida como fornecedora de urnas eletrônicas em ao menos dois estados nos EUA [41], por mentir na fase de homologação dos seus produtos, suprimentos ou serviços.

Empresa esta que atualmente é – ela e/ou sua homônima e/ou matriz – ré em ao menos cinco processos judiciais no Brasil [42], por fornecer a clientes de certos bancos software de *home banking* que funcionariam, por trás da interface, também como sorrateiros programas espiões.

Ocorre também que a instalação do software e dos dados preparados para cada eleição, necessária nas centenas de milhares dessas urnas, é feita em fase preparatória de cada turno de votação, conhecida como "carga das urnas", a qual tem sido executada nos TREs e cartórios eleitorais – ao menos em eleições recentes [43] – por empresas terceirizadas que formam consórcios envolvendo empresa estrangeira de perfil *sui generis*, e contratos muito disputados e mal especificados, descritos em [44].

Então, para um nível de cautela compatível com conhecimento das formas possíveis de se penetrar e explorar plataformas DRE, em tese é plausível que uma controladora "defeituosa" (ou maliciosa) da BIOS possa abrir passagem para software trapaceiro instalado no sistema de arquivos da urna, permitindo a este executar com permissões administrativas, subvertendo os mecanismos de controle criptográfico que o TSE implementa na camada de aplicativos de sua plataforma

3 - Oriundos do Instituto de Computação da Unicamp.

4 - Até mesmo contra decisões do Poder Legislativo – vide [35]

DRE, pois de forma invisível e indetectável a estes mecanismos.

V. CONCLUSÕES

A hipótese de risco descrita acima, que pode envolver o MSD (e melhor se camuflar com ele), tanto é verossímil que ainda é a que melhor explica estranhos eventos, como por exemplo certos registros encontrados no log da plataforma de carga das urnas no cartório eleitoral de uma zona eleitoral de Londrina na eleição municipal de 2012 [45], conforme perícia documentada nos autos do processo cível 163.24.2012.6.160157.

Para encerrar, revisitamos certos argumentos que tem sido empregados em debates sobre esse sistema de votação, por quem defende a irrevogabilidade da adoção pelo TSE do modelo básico de 1ª geração (DRE). Por aqueles que, mesmo em contextos acadêmicos, quando lhes falta argumentos técnicos ou jurídicos e os argumentos de autoridade não mais impressionam, acabam por recorrer a argumentos *ad hominem*, como o de acusar quem os crítica de serem vítimas de um "complexo de vira-latas".

Diante do que aqui se expôs, onde essa forma de debater tal tema sinaliza atuação de filtros psicológicos de teor ideológico ou geopolítico, resta então finalmente indagar: Com quem estaria mesmo o complexo de vira-latas?

REFERÊNCIAS

[1] Bernhard [pseudônimo], "How The U.S. Runs Public Relations Campaigns - Trump Style - Against Russia And China" [Online]. Artigo no portal web "Moon of Alabama", 5 de outubro de 2018. Disponível: https://www.moonofalabama.org/2018/10/how-the-us-runs-public-relations-campaigns-trump-style-against-russia-and-china.html. Acessado 6 de março de 2019.

[2] Foreign Office, "The attempted hacking of the Organisation for the Prohibition of Chemical Weapons (OPCW) by the Russian Military Intelligence Service - the GRU - part of a sustained pattern of hostile cyberspace activity" [Online]. Trilha postada em conta validada no serviço Tweeter, 4 de outubro de 2018. Disponível: https://twitter.com/foreignoffice/status/1047856886362656768. Acessado 6 de março de 2019.

[3] The Gardian, "UK accuses Kremlin of ordering series of 'reckless' cyber-attacks" [Online]. Artigo não assinado, 4 de outubro de 2018. Disponível: https://www.theguardian.com/technology/2018/oct/04/uk-accuses-kremlin-of-ordering-series-of-reckless-cyber-attacks. Acessado 6 de março de 2019.

[4] W. Webb, "Wikileaks Reveals: CIA's UMBRAGE Allows Agency to Carry out 'False Flag' Cyber Attacks" [Online]. Artigo publicado no portal Global Research, 7 de março de 2017. Disponível: https://www.globalresearch.ca/wikileaks-reveals-cias-umbrage-allows-agency-to-carry-out-false-flag-cyber-attacks/5578786. Acessado 6 de março de 2019.

[5] New Jersey Cybersecurity and Communications Integration Cell, "BlackEnergy" [Online]. Relatório, 30 de agosto de 2017. Disponível: https://www.cyber.nj.gov/threat-profiles/ics-malware-variants/blackenergy. Acessado 6 de março de 2019.

[6] Government of the Netherland, "Netherlands Defence Intelligence and Security Service disrupts Russian cyber operation targeting OPCW" [Online]. Item de notícia, 4 de outubro de 2018. Disponível: https://www.government.nl/government/members-of-cabinet/ank-bijleveld/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw. Acessado 6 de março de 2019.

[7] Wikipedia, "Honeypot (computing)" [Online]. Artigo de edição colaborativa. Disponível: https://en.wikipedia.org/wiki/Honeypot_(computing)/ Acessado 6 de março de 2019.

[8] United States Federal Court of Western District of Pensilvania, "Indictment" [Online]. Caso 2:18-cr-00263-MRH, Documento 4, 3 de outubro de 2018. Disponível: https://www.justice.gov/opa/page/file/1098481/download; Acessado 6 de março de 2019.

[9] E. Lesser, "Three Revelations From the DOJ's New Russian Hacking Indictment" [Online]. Artigo na revista Roling Stone, 04 de outubro de 2018. Disponível: https://www.rollingstone.com/politics/politics-news/russian-hacking-indictment-733162/amp/. Acessado 6 de março de 2019.

[10] North Atlantic Treaty Organization, "Defense Minister Meeting" [Online]. Programa e prospecto, 03 a 04 de outubro de 2018. Disponível: https://www.nato.int/cps/en/natohq/news_157997.htm?epslanguage=en-GB. Acessado 6 de março de 2019.

[11] L. Baldor, "US to offer cyberwar capabilities to NATO allies" [Online]. Artigo no portal Fox Business, 03 de outubro de 2018. Disponível: https://www.foxbusiness.com/features/us-to-offer-cyberwar-capabilities-to-nato-allies.amp. Acessado 6 de março de 2019.

[12] J. Bamford, "The world's best cyber army doesn't belong to Russia" [Online]. Artigo distribuído pelo serviço Reuters, 4 de agosto de 2016. Disponível: https://www.reuters.com/article/us-election-intelligence-commentary-idUSKCN10F1H5. Acessado 6 de março de 2019.

[13] L. Witt, "One of the greatest propaganda successes of US/UK Governments in recent times is to completely replace from public discourse the massive global NSA/GCHQ hacking/spying/disinfo infrastructure revealed by @Snowden just a few years ago with Russia's efforts" [Online]. Trilha postada no serviço Tweeter, 4 de outubro de 2018. Disponível: https://twitter.com/LudWitt/status/1047800238361247744. Acessado 6 de março de 2019.

[14] Wikipedia, "Five Eyes" [Online]. Artigo de edição colaborativa. Disponível: https://en.wikipedia.org/wiki/Five_Eyes/ Acessado 6 de março de 2019.

[15] R. Gallagher, "The Inside Story of how British Spies Hacked Belegium's Largest Telco" [Online]. Artigo no jornal The Intercept, 13 de dezembro de 2014. Disponível: https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/. Acessado 6 de março de 2019.

[16] C. Doctorow, "The NSA hacked the Hague-based Organization for the Prohibition of Chemical Weapons" [Online]. Artigo no portal BoingBoing, 6 de novembro de 2016. Disponível: https://boingboing.net/2016/11/06/in-2000-the-nsa-hacked-the-ha.html. Acessado 6 de março de 2019.

[17] M. Simons, "U.S. Forces Out Head of Chemical Arms Agency" [Online]. Artigo no jornal The New York Times, 23 de abril de 2002. Disponível: https://www.nytimes.com/2002/04/23/world/us-forces-out-head-of-chemical-arms-agency.html. Acessado 6 de março de 2019.

[18] RT News, "'I give you 24 hours to resign': 1st OPCW chief on how John Bolton bullied him before Iraq War" [Online]. Videontrevista exclusiva, 7 de abril de 2018. Disponível: https://www.rt.com/usa/423477-bolton-threat-opcw-iraq/. Acessado 6 março 2019.

[19] J. Robertson & M. Riley., "The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies" [Online]. Artigo no jornal The New York Times, 4 de outubro de 2018. Disponível: https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies. Acessado 6 de março de 2019.

[20] S. Schmidt, "Setting the Record Straight on Bloomberg BusinessWeek's Erroneous Article" [Online]. Artigo no blog AWS Security, 4 de outubro de 2018. Disponível: https://aws.amazon.com/pt/blogs/security/setting-the-record-straight-on-bloomberg-businessweeks-erroneous-article/. Acessado 6 de março de 2019.

[21] Applestatement, "What Businessweek got wrong about Apple" [Online]. Nota publicada no Newsroom da Apple, 4 de outubro de 2018. Disponível: https://www.apple.com/newsroom/2018/10/what-businessweek-got-wrong-about-apple/ Acessado 6 março 2019.

[22] K. McCarthy, "Decoding the Chinese Super Micro super spy-chip super-scandal: What do we know – and who is telling the truth?" [Online]. Aritgo no jornal The Register, 4 de outubro de 2018. Disponível: https://www.theregister.co.uk/2018/10/04/supermicro_bloomberg/ Acessado 6 março 2019.

[23] P. Kennedy, "Bloomberg Reports China Infiltrated the Supermicro Supply Chain We Investigate" [Online]. Artigo no portal ServeTheHome, 4 de outubro de 2018. Disponível: https://www.servethehome.com/bloomberg-reports-china-infiltrated-the-supermicro-supply-chain-we-investigate/ Acessado 6 março 2019.

[24] T. Grugq, "Supply Chain Security Speculation" [Online]. Artigo no portal de blogs Medium, 4 de outubro de 2018. Disponível: https://medium.com/@thegrugq/supply-chain-security-speculation-b7b6357a5d05. Acessado 6 março 2019.

[25] J. Uchill, "Go deeper: Bloomberg's fraying 'secret chips' story" [Online]. Relatório no portal Axios, 9 de outrubro de 2018. Disponível: https://www.axios.com/bloombergs-fraying-secret-chips-story-70016e9b-313a-40a6-afb7-9682e5f220e3.html. Acessado 6 março 2019.

[26] Market Watch, "SuperMicro Computer Inc." [Online]. Histórico de preços das ações. Disponível: https://www.marketwatch.com/investing/stock/smci.

[27] S. Gallager, "Apple deleted server supplier after finding infected firmware in servers" [Online]. Artigo no portal Ars Technica, 24 de fevereiro de 2017. Disponível: https://arstechnica.com/information-technology/2017/02/apple-axed-supermicro-servers-from-datacenters-because-of-bad-firmware-update/. Acessado 6 março 2019.

[28] Z. Miller, "Pence accuses China of interfering in US policies, politics" [Online]. Artigo com vídeo distribuído pela Associated Press, em 4 de outubro de 2018, portal Yahoo. Disponível: https://www.yahoo.com/news/pence-accuses-china-interfering-us-policies-politics-040632578—politics.html. Acessado 6 março 2019.

[29] Reuters, "Pentagon identifies China as 'growing risk' to supply of materials vital to U.S. defense industry" [Online]. Artigo não assinado no jornal The Japan Times, 5 de outubro de 2018. Disponível: https://www.japantimes.co.jp/news/2018/10/05/asia-pacific/pentagon-identifies-china-growing-risk-supply-materials-vital-u-s-defense-industry/#.XIBys1Vv_eQ. Acessado 6 março 2019.

[30] A. Russell, "CIA plot led to huge blast in Siberian gas pipeline" [Online]. Artigo no jornal The Telegraph, 28 de fevereiro de 2004. Disponível: https://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html. Acessado 6 março 2019.

[31] Wikileaks, "Filter results by Leak: Valt 7" [Online]. Pesquisa simples por "supply chain". Disponível: https://search.wikileaks.org/?query=%22supply+chain%22&exact_phrase=&any_of=&exclude_words=&document_date_start=&document_date_end=&released_date_start=&released_date_end=&publication_type%5B%5D=51&new_search=False&order_by=most_relevant#results. Acessado 6 março 2019.

[32] Snowden Docs Search, "Supply Chain" [Online]. Diponível: .https://search.edwardsnowden.com/search?utf8=%E2%9C%93&q=%22supply+chain%22 Acessado 6 março 2019.

[33] U.S. Department of the Treasury, " Sanctions Programs and Country Information" [Online]. Repositório das medidas administrativas que impõem sanções econcômicas contra países, entidades e indivíduos. Disponível: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx. Acessado 6 março 2019.

[34] L. F. Shauren, "Segurança no Sistema Brasileiro de Votação Eletrônica" [Online]. Trabalho final de Graduação, Curso de Ciência da Computação, Universidade Federal do Rio Grande do Sul. Disponível: https://www.lume.ufrgs.br/bitstream/handle/10183/151030/001009822.pdf. Acessado 6 março 2019.

[35] P. A. D. Rezende (2012, jun), "Reforma Eleitoral e Informatização do Voto" [Online]. Apresentação no Seminário Internacional *Implementación del voto electrónico en perspectiva comparada*, Lima, Peru. Disponível: http://www.cic.unb.br/%7Erezende/trabs/Voto-eLima2012.html. Acessado 6 março 2019.

[36] Wikipedia, "DRE voting machine" [Online]. Artigo de edição colaborativa. Disponível: https://en.wikipedia.org/wiki/DRE_voting_machine. Acessado 6 de março de 2019.

[37] P. A. D. Rezende (2010, jul), "Votação Eletrônica, 3ª Geração" Apresentado em Audiência Pública no TSE, Brasília, [Online]. Disponível: https://cic.unb.br/~rezende/trabs/TSE3G.pdf. Acessado 6 março 2019.

[38] P. A. D. Rezende, "Podemos Classificar Sistemas de Votação?" [Online]. Artigo publicado no Portal Observatório da Imprensa. Disponível: http://observatoriodaimprensa.com.br/interesse-publico/ed708-podemos-classificar-sistemas-de-votacao/. Acessado 6 março 2019.

[39] Wikipedia, "Binary Blob" [Online]. Artigo de edição colaborativa. Disponível: https://en.wikipedia.org/wiki/Binary_blob. Acessado 6 de março de 2019.

[40] Informação Classificada – Comunicação Pessoal, 2018. (Nota do Editor/Revisor: informação sem possibilidade de confirmação)

[41] P. Festa, "California votes against Diebold" [Online]. Artigo no portal C|Net, 33 de abril de 2004. Disponível: https://www.cnet.com/news/california-votes-against-diebold/. Acessado 6 março 2019.

[42] P. Z. Giestas, Comunicação Pessoal, 2018 [Online]. Disponível: https://cic.unb.br/~rezende/trabs/prep2018_files/MONITORAMENTO DE DADOS DIEBOLD.pdf. Acessado 6 março 2019.

[43] M. A. Coritz, "Relatório sobre participação da Smartmatic nas Eleições Brasileiras de 2012 e 2014" [Online]. Publicado no portal do autor, fevereiro de 2015. Disponível: https://cic.unb.br/~rezende/trabs/relatorio-smart.html. Acessado 6 março 2019.

[44] P. A. D. Rezende, "Alerta sobre os Preparativos para a Eleição de 2018" [Online]. Publicado no portal de notícias da Universidade de Brasília, 25 de setembro de 2018. Disponível: https://noticias.unb.br//artigos-main/2518-alerta-sobre-os-preparativos-para-a-eleicao-de-2018. Acessado 6 março 2019.

[45] M. A. R. Cortiz, (video) [Online]. Apresentação em Audiência Pública na Comissão de Ciência, Tecnologia e Inforrmática da Câmara dos Deputados em Brasília, sobre vulnerabilidades no sistema de votação do TSE, 16 de dezembro de 2014. Disponível: https://www.youtube.com/watch?v=XcOe5Mn9ZKA. Acessado 6 março 2019.

[46] V. O. Silveira, "Presidente da Huawei cita Snowden como contradição às acusações dos EUA" [Online]. Artigo publicado no portal Money Times, 27 de fevereiro de 2019. Disponível: https://moneytimes.com.br/fast/presidente-da-huawei-cita-snowden-como-contradicao-as-acusacoes-dos-eua/. Acessado 6 março 2019.

Pedro Antonio Dourado de Rezende Matemático e Professor Adjunto no Departamento de Ciência da Computação da Universidade de Brasília, onde obteve grau de Mestre em Matemática em 1977. No Vale do Silício, trabalhou com controle de qualidade na Apple Computer, e com as primeiras aplicações em hipertexto (hypercards) em 1988. Publicou no Brasil, no exterior e na web, centenas de artigos e ensaios sobre a revolução digital, software livre, criptografia, segurança na

informática, evolução de programas maléficos, paradigmas computacionais e epistemologia da ciência. Assinou a coluna "Segurança, Bits & Cia" no Jornal do Commercio de 2002 a 2003. Consultor para criptografia e segurança na informática para empresas, órgãos públicos, legisladores, operadores do Direito e agências de fomento à pesquisa científica e à produção cultural. Coordenador do Programa de Extensão em Criptografia e Segurança Computacional da UnB, onde montou e ministrou o primeiro curso de programação para Infraestrutura de Chaves Públicas (ICP) no Brasil. Conselheiro do Instituto Brasileiro de Política e Direito na Informática, ex-conselheiro da Free Software Foundation Latin America (2006-2008), e ex-representante da sociedade civil no Comitê Gestor da Infraestrutura de Chaves Públicas Brasileira, ICP-BR, por nomeação do presidente da República (2003-2006).