# Por que o Brasil deveria adotar uma *distro* Linux própria?

## Why should Brazil adopt its own Linux distro?

Rev. Bras. Est. Def. v. 7, nº 2, jul./dez. 2020, p. 161-183
DOI: 10.26792/RBED.v7n2.2020.75248
ISSN 2358-3932

**MARCELO ANTONIO OSLLER MALAGUTTI**
**RICARDO BORGES GAMA NETO**

## INTRODUÇÃO

Este trabalho analisa o uso de software de código aberto, em particular distribuições Linux, por motivação de segurança e defesa. É utilizado o método descritivo, do tipo *associations* (Gerring 2012, 721–46). Primeiro descrevemos as características do objeto de estudo, concentrando nas condições prevalentes e subjacentes as unidades de análise. A pesquisa é associada a estudos de caso de nações comumente apontadas como superpotências cibernéticas (EUA, China, Rússia e Coreia do Norte) e também de potências regionais relevantes (Índia, Turquia e Coreia do Sul). O argumento é que a maior parte dos casos aponta que a adoção do Linux ocorre por questões de segurança e defesa. A introdução de sistemas operacionais (SO[1]) de código aberto se dá pelo receio de imposição de restrições ao acesso a tecnologias e/ou uso de *backdoors* ou exploração de falhas do tipo *zero-day*. Por esta razão defendemos que o Brasil deve adotar a mesma estratégia, selecionar uma *distro* Linux para emprego em sistemas associados à defesa. Dessa forma pode-se reduzir os riscos de dependência tecnológica em cibernética e tecnologia da informação (TI).

O trabalho foi dividido da seguinte forma: esta introdução, depois uma brevíssima conceituação sobre software aberto e um pequeno histórico do Linux, seguido do contexto histórico do desenvolvimento da TI, riscos postos pela dependência tecnológica externa, exemplos de adoção do uso do Linux por forças armadas e governos de diferentes países, recomendações e argumentos exortando o Ministério da Defesa a adotar uma me-

**Marcelo Antonio Osller Malagutti** — Doutor em Ciências Militares pela Escola de Comando e Estado-Maior do Exército; Mestre em War Studies pelo King's College London.
**Ricardo Borges Gama Neto** — Professor Doutor do Departamento de Ciência Política da Universidade Federal de Pernambuco.

ta-distribuição para o desenvolvimento de um Linux nacional. Por fim, a conclusão e as referências bibliográficas.

## SOFTWARE ABERTO

Historicamente, a contratação de softwares era realizada de duas maneiras distintas: pela contratação do desenvolvimento sob especificação do cliente, ajustada às suas necessidades; e pela aquisição de licenças e serviços associados. Com o passar dos anos, novas formas de uso de software foram criadas por *novos entrantes* na busca pela abertura de mercados entre fornecedores já consolidados. Alguns softwares passaram a ter seus executáveis distribuídos gratuitamente (*freeware*) ou licenciados a preços irrisórios (*shareware*).

No início dos anos 1980, a ARPANET, precursora da Internet, ainda engatinhava, com menos de 1.000 servidores conectados, e restrita a militares e pesquisadores de universidades e centros de pesquisa (Rid 2016, 190). Não obstante, o usuário comum já podia *discar* (utilizando um modem) para uma Bulletin Board Service (BBS) e *baixar* softwares. Em alguns casos até mesmo software *pirata* (o mercado negro sempre existiu). Posteriormente evoluiu-se para iniciativas denominadas de software aberto (*Open Source Software*, OSS), cujo código-fonte, e não apenas seus executáveis, eram disponibilizados para usuários licenciados. OSS também é conhecido como software livre (*free*), mas não no sentido de que não tenha custo. O *livre* do nome advém da liberdade do usuário de não depender do fornecedor, e não necessariamente da *gratuidade* do uso (U.S. DoD n.d.).

O conceito de OSS é frequentemente confundido pelo grande público com aquele de software grátis (U.S. DoD n.d.). Em grande medida, pelo fato de que boa parte do OSS é, de fato, disponibilizada sem a cobrança de taxas de licenciamento e, portanto, sem custos. Mas OSS não é necessariamente *freeware*, que embora gratuito, não precisa ser aberto. De fato, dezenas de *freewares* são distribuídos apenas na forma de seus executáveis, verdadeiras *caixas-pretas* que podem implicar riscos à segurança dos dados e dispositivos de seus usuários. OSS, embora aberto, não necessariamente significa gratuito. É perfeitamente possível que o software OSS seja licenciado ao usuário por meio da cobrança de serviços associados (tipicamente treinamento e suporte).

Para fins legais e de aquisição, o governo dos EUA define OSS como "software para o qual o código fonte legível por humanos está disponível para uso, estudo, reutilização, modificação, aprimoramento e redistribuição pelos usuários desse software" (Wennergren 2009)the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing

requirements. The use of Open Source Software (OSS. Seja o software comercial (licenciamento pago) ou não (U.S. DoD n.d.).

Cada um desses tipos de software possui um modelo de negócios distinto. *Freewares* em geral são patrocinados por anúncios publicitários (*advertisements* ou *ads*) apresentados durante a utilização do software, e geralmente associados à *invasão de privacidade* dos usuários. Por vezes, alternativamente ou complementarmente, cobram seu preço por meio da captura e revenda de informações privilegiadas dos usuários, para uso em ações frequentemente não éticas ou legais. Já o OSS, em geral tem diferentes formas de rentabilização. Software comercial é remunerado pela venda de licenças, bem como dos serviços associados. Mas seu código aberto aufere transparência ao fornecedor, e ao cliente a percepção de liberdade e independência daquele fornecedor (o *livre* acima mencionado). Quando o OSS é licenciado sem custos, a remuneração pode se dar por meio da prestação dos serviços associados. Uma terceira forma de remuneração pode ser o licenciamento de *add-ins* ou *versões profissionais*: em sua versão básica é gratuito, mas incrementos de funcionalidades são licenciados comercialmente[2].

Dentre os muitos Softwares Abertos disponíveis no mercado, destaca-se o Linux, SO concorrente do Microsoft Windows e do Mac OS X, que além de aberto é também de licenciamento gratuito.

## UMA (MUITO BREVE) HISTÓRIA DO LINUX

A origem do Linux está associada ao Unix. Em fins dos anos 1960, o Bell Labs, que fazia parte da AT & T, iniciou o desenvolvimento de um SO para uso em minicomputadores PDP-7 da Digital Equipment Corporation. Sua migração, em fins dos anos 1970, para o modelo PDP-11, confirmou o que viria a ser um dos pontos-fortes do Unix: a portabilidade para diferentes tipos de equipamentos (Hosch 2008b).

Em meados dos anos 1970 um dos projetistas temporariamente se afastou do projeto para lecionar na Universidade da Califórnia em Berkeley. Professores e alunos passaram a realizar incrementos ao sistema original, desenvolvendo uma nova versão que se tornou também popular, o Berkeley Software Distribution (BSD). Paralelamente o trabalho continuava no Bell Labs, e em 1983 foi finalizada a versão Unix System V (Hosch 2008b). Posteriormente essas *distros* foram unificadas em diferentes versões produzidas por diversas companhias para seus minicomputadores: Solaris da Sun Microsystems; IRIX da Silicon Graphics; HP-UX da HP; AIX da IBM, dentre outras.

As características do Unix interessaram também ao mercado de microcomputadores. Em fins dos anos 1970 a Microsoft licenciou junto à AT&T

a comercialização do sistema, e por anos foi a maior distribuidora do Unix, fosse seu próprio Xenix, ou outras denominações (*distros*) da Siemens, Santa Cruz Operation (SCO) e "dúzias e dúzias de sublicenciados" (Gates 1996). Dificuldades comerciais com a AT&T levaram a Microsoft a vender o Xenix para a SCO, que o comercializou até 2007 sob o nome SCO Unix, e a focar no desenvolvimento do Windows NT, com arquitetura muito influenciada pelas características do Unix (Gates 1996). Do Unix FreeBSD derivou o Rhapsody DR2, base do Mac OS X da Apple, do qual descende o iOS que opera nos iPhones e iPads (Singh 2007, 32).

A guinada do Unix para OSS se deu com o advento do Linux, um k*ernel* (núcleo) Unix inteiramente reescrito, cuja primeira versão data de 1994. No mesmo período a Free Software Foundation (FSF) desenvolvia esforços para o desenvolvimento do GNU, um sistema baseado no Unix, mas de código aberto. Conquanto o Linux tivesse iniciado pelo núcleo do sistema, o GNU iniciou-se pela criação de utilitários do sistema. Esses utilitários foram então incorporados ao Linux criando o GNU/Linux, popularizado apenas pelo nome do núcleo (Hosch 2008a). Inicialmente, por ter uma interface gráfica menos amigável que a do Microsoft Windows ou do Mac OS, embora sendo mais confiável e robusto a falhas, o uso do Linux ficou mais restrito a servidores corporativos e da Internet. No entanto, sendo de código aberto, o sistema foi sendo adaptado por diferentes fabricantes, criando novas *distros*, como no caso da SUSE (antes Novell Linux), Red Hat, Debian e Slackware (Hosch 2008a). A incorporação de interfaces mais amigáveis (Gnome, KDE, WindowMaker), de servidores web e de aplicações foi tornando o sistema mais popular. O Android, da Google, que hoje equipa a maior parte dos smartphones, derivou de modificações no *kernel* original do Linux.

## A IMPORTÂNCIA DA INFORMÁTICA PARA A DEFESA E SEGURANÇA NACIONAIS

A inteligência de comunicações sempre desempenhou papel relevante em questões de segurança e defesa. *Signals Intelligence* (SIGINT) tornou-se cada vez mais relevante com a popularização das telecomunicações, e ainda mais importante para os militares. Em Bletchley Park, em 1941, Alan Turing e sua equipe criaram a *Bombe*, o primeiro computador da história, ainda que eletromecânico, que ajudou a decifrar o código Enigma, utilizado pelas forças armadas nazistas. No mesmo local, a equipe de Tommy Flowers criou o Colossus Mark I, o primeiro computador eletrônico, de 1943, que decifrou o ultrassecreto código Lorenz. Ambas foram ativos importantes para a vitória na Segunda Guerra Mundial (GCHQ 2016).

Não apenas para SIGINT o uso de processamento automatizado de informações foi relevante para os militares. Em 1943 o exército americano encomendou à Universidade da Pensilvânia o desenvolvimento de uma máquina capaz de computar alvos balísticos, resultando no desenvolvimento do ENIAC, o primeiro computador eletrônico programável, entregue em 1946. O medo da repetição da *blitz* (bombardeio de Londres durante a WWII) em território norte-americano levou à criação do Semi-Automatic Ground Environment (SAGE), integrando centenas de estações de radar com processamento em 23 supercomputadores distribuídos pelos EUA, cujo protótipo foi demonstrado já em 1951 (Rid 2016, 76–7). O sistema foi contratado à IBM, que utilizava linhas de comunicação comerciais da AT&T para integrar toda a rede, que em 1958 foi centralizada no mítico North-American Air Defense Command (NORAD) no Colorado, ao custo total (em 15 anos) de mais de 500 bilhões de dólares em valores atuais (Rid 2016, 76–7). Similarmente, por meio da Advanced Research Projects Agency (ARPA), o Pentágono custeou o desenvolvimento da ARPANET, a "famosa precursora da Internet" (Rid 2016, 111). O objetivo era melhorar sistemas de comando e controle militares e prover redundância de rotas em casos de falhas de algum nó da rede (Rid 2016, 147).

No Brasil o desenvolvimento da informática também esteve ligado a interesses militares. Foi por influência das ideias do Capitão de Corveta Geraldo Maia, que retornara dos EUA, que o Conselho de Desenvolvimento Nacional do Governo Juscelino Kubitscheck propôs a criação de um grupo para avaliar o uso de computadores (Moreira 1995, 24). No ano seguinte, a equipe tornou-se o Grupo Executivo para Aplicação de Computadores Eletrônicos (GEACE), e autorizou a importação dos três primeiros computadores brasileiros: um para a Pontifícia Universidade Católica do Rio de Janeiro; um para o Instituto Brasileiro de Geografia e Estatística; e um para a Listas Telefônicas Brasileiras (Moreira 1995, 23).

Em 1972 criou-se a Coordenação das Atividades para o Processamento Eletrônico de Dados (CAPRE), vinculada ao Ministério do Planejamento (Moreira 1995, 24; Figueiredo 1986, 288; Tonooka 1992, 274–6). À CAPRE foi atribuída a responsabilidade pelo desenvolvimento de uma política nacional de informática, e uma de suas primeiras determinações foi a restrição à importação de hardware estrangeiro por instituições governamentais (Moreira 1995; Figueiredo 1986; Tonooka 1992, 274–78). Iniciava-se uma Reserva de Mercado que duraria 20 anos. Em 1979 a CAPRE foi substituída pela Secretaria Especial e Informática (SEI), vinculada então ao Conselho de Segurança Nacional, e fortemente influenciada pelo Serviço Nacional de Informações (SNI) (Moreira 1995, 28–9; Tonooka 1992).

Em 1984, implementou-se a Lei de Informática[3]. Esta estabeleceu a Política Nacional de Informática, pela qual somente produtos *Made in Brazil* (ou estrangeiros autorizados) poderiam ser comercializados. A ideia era a de se criar um mercado visando o desenvolvimento de uma indústria nacional que pudesse ser competitiva internacionalmente. O modelo adotado baseava-se em três pilares: capacitação de pessoal; estímulo ao investimento privado; e numa empresa estatal, a Computadores Brasileiros (COBRA). Contudo, tais esforços foram infrutíferos, e até mesmo contraproducentes, dado que submeteram o país a um considerável atraso na adoção de novas tecnologias que rapidamente emergiam no mercado externo, mas que não entravam no Brasil e dos elevados valores que os usuários nacionais pagavam pelos produtos nacionais comparados aos preços internacionais (Moreira 1995; Tonooka 1992). Em 1993, com o fim da reserva de mercado, as empresas brasileiras optaram pelo licenciamento de produtos estrangeiros.

## RISCOS DA DEPENDÊNCIA TECNOLÓGICA EM TI

### *Backdoors*

Uma das maiores preocupações com a utilização de ativos importados é a existência de *backdoors* (portas dos fundos) desconhecidas que possam ser utilizadas contrariamente aos interesses dos clientes. Já em 2001, autoridades de inteligência dos EUA acreditavam que "certos equipamentos importados" estavam infectados com dispositivos capazes de "ler dados ou destruir sistemas" (Adams 2001). Posteriormente, hardware falsificado foi identificado em sistemas adquiridos pelo Departamento de Defesa dos EUA (Lynn 2010). Um relatório do Comitê Permanente de Inteligência da Câmara dos EUA, em 2012, recomendou restrições à aquisição de equipamentos de rede das empresas chinesas Huawei e ZTE por órgãos do governo americano e seus contratados, devido à possibilidade de vazamento de informações sigilosas por meio de *backdoors* (Banach 2012).

No Caso Snowden revelou-se que a empresa norte-americana Cisco, maior fabricante mundial de ativos de rede, tinha seus roteadores e servidores interceptados e manipulados pela National Security Agency (NSA), sem no entanto haver evidências de que a empresa estivesse envolvida (Greenwald 2014, 142). Em dezembro de 2015, a Juniper Networks, segunda maior fabricante de ativos de rede do mundo, anunciou a descoberta de uma *backdoor* secreta em seus *firewalls* (Zetter 2015). Posteriormente, a Cisco confirmou que uma vulnerabilidade *zero-day*[4] fora explorada por software ligado à NSA durante anos (Goodin 2016). Ao menos outras

oito *backdoors* foram encontradas pela Cisco em 2017 e 2018 (Cisco n.d.; Cimpanu 2018).

Nem mesmo empresas de países tradicionalmente neutros são insuspeitas. A suíça Crypto AG, fabricante de criptógrafos utilizados em mais de 120 países pertenceu, entre 1970 e 2018, a uma parceria altamente secreta da CIA com o serviço de inteligência alemão BND, e que os equipamentos vendidos pela companhia eram sabotados para que aquelas agências tivessem acesso às informações neles criptografadas AG (Miller 2020).

O governo norte-americano acusa a Huawei, líder mundial em telefonia 5G, de possuir ligações obscuras com a inteligência chinesa. Os EUA também pressionaram seus aliados a vetarem o uso de tecnologia chinesa de 5G. Em maio o Reino Unido anunciou a proibição da empresa atuar. Os EUA argumentam preferir o uso de equipamentos da sueca Ericsson e da finlandesa Nokia, mesmo que mais caros, e personalidades do governo dos EUA até sugeriram a aquisição do controle acionário dessas empresas (Kharpal 2020).

### Classificação de Itens como *Tecnologias Sensíveis*

Desde 2015 a Intel foi impedida pelo governo dos EUA de revender para a China seus processadores mais modernos, sob o argumento de que os mesmos seriam utilizados para testes nucleares (Clark 2015). Em 2018 os EUA reassumiram a liderança da lista de supercomputadores, pertencente anteriormente a China, e nela permaneceram com os dois maiores equipamentos até fins de 2020, quando foram superados pelos Japoneses (TOP500.org n.d.). A diferença dos processadores americanos e chineses se reflete nos números. Enquanto o Sierra, dos EUA, atinge 200 PFLOPS[5] com 2,4 milhões de núcleos (*cores*) e consome 10MW de energia, o chinês TaihuLight, duas posições atrás, utilizando processadores chineses, atinge 125 PFLOPS com 10,6 milhões de núcleos e consome 15MW (TOP500.org n.d.).

Após a proibição de uso de componentes norte-americanos pela Huawei em 2019, a gigante chinesa passou a trabalhar pela substituição desses componentes por versões chinesas (Strumpf 2020). Mas mesmo essa estratégia ficou ameaçada quando o Departamento de Comércio dos EUA subiu o tom em maio de 2020 e proibiu que fabricantes de componentes de todo o mundo, que utilizem tecnologia norte-americana, vendam produtos à Huawei (U.S. Dept. of Commerce 2020). Essa nova dificuldade pode mesmo tirar a empresa da posição dominante na corrida pelo 5G, e mesmo prejudicar a manutenção de redes de telefonia de outras gerações fornecidas pela empresa e já em uso em diversos países (Strumpf 2020).

Os EUA ainda consideram bloquear o fornecimento de tecnologia norte-americana para cinco empresas chinesas de vigilância por vídeo (Shidong 2019).

O Brasil também enfrenta dificuldades na importação de computadores e outros materiais *sensíveis*, e até na compra de computadores *Made in Brazil* por empresas americanas beneficiadas por encargos fiscais do governo brasileiro (Angelo 2007). O maior supercomputador brasileiro está ranqueado na posição 192 da lista, com 1,9 PFLOPS (TOP500.org n.d.).

Restrições ao uso não se referem apenas a hardware, mas também a software. O banimento imposto pelo governo dos EUA à Huawei impede que a Google licencie o uso do SO Android em aparelhos telefônicos da empresa (Moon 2019). Ainda que o núcleo do mesmo seja de código aberto, e assim possa continuar a ser usado pela empresa chinesa, diversos serviços associados são fornecidos pela Google e deixariam de estar disponíveis, limitando a utilidade dos smartphones (Moon 2019).

Em meio ao embargo dos EUA a fornecimento de tecnologia para a China, Pequim ordenou a todos os escritórios governamentais e instituições públicas que removam equipamentos e softwares estrangeiros até 2022 (Yang and Liu 2019). A medida faz parte de uma campanha para reduzir a dependência chinesa de tecnologias estrangeiras, provavelmente terá um efeito de *desacoplamento* das cadeias de fornecimento dos EUA e China, e pode representar um duro golpe para empresas estadunidenses (Yang and Liu 2019). As novas sanções impostas acrescentaram urgência ao projeto, diferentemente dos esforços anteriores por autossuficiência em tecnologia, e seu objetivo é que no futuro próximo as empresas e o governo estejam livres de ameaças (Yang and Liu 2019).

Mas a substituição de hardware e software norte-americano por equivalentes chineses também apresenta problemas. A chinesa Lenovo utiliza processadores fabricados pela Intel e discos rígidos produzidos pela sul-coreana Samsung (Yang and Liu 2019). A China fica atrás dos EUA em algumas das tecnologias mais avançadas, incluindo design e fabricação de chips. Os principais componentes usados por algumas das maiores empresas de tecnologia do país são fabricados pela Intel ou pela Qualcomm. Os SO mais usados em dispositivos produzidos na China são Google Android, em smartphones e tablets, ou Microsoft Windows, em computadores (Shidong 2019).

## EXEMPLOS DE ADOÇÃO DO LINUX

Em princípios dos anos 2000, governos e empresas pelo mundo se preocupavam com a possibilidade de que o uso de OSS os abrisse para *bugs*, brechas de segurança e, consequentemente, ações judiciais. Mas, apesar

desses medos iniciais, o código aberto passou a dominar o cenário digital (Finley 2016). Hoje, praticamente todas as principais tecnologias com as quais interagimos diariamente - da *Web* ao telefone e ao carro - foram construídas usando pelo menos alguma forma de OSS, muitos deles gratuitos (Finley 2016).

## Estados Unidos

Em 2003 o Departamento de Defesa dos EUA (DoD) encomendou uma pesquisa à MITRE Corporation[6] sobre o uso de OSS em sistemas de defesa (MITRE 2003). Essa pesquisa mostrou que diversos OSS já eram utilizados, e apontou sugestões para sua institucionalização. Em 2009, o DoD emitiu uma diretiva sobre o uso de OSS, dando preferência ao mesmo dentro de regras bem estabelecidas (Wennergren 2009)the Department of Defense must develop and update its software-based capabilities faster than ever, to anticipate new threats and respond to continuously changing requirements. The use of Open Source Software (OSS. Em 2016 a Casa Branca lançou sua primeira política oficial de código fonte, detalhando um programa que exige que as agências governamentais liberem como software de código aberto 20% de qualquer novo código que encomendarem, o que significa que o mesmo estará disponível para qualquer um examinar, modificar e reutilizar em seus próprios projetos (Scott and Rung 2016). As agências governamentais também compartilharão códigos entre si, adotando essencialmente práticas de OSS em seu próprio universo governamental (Scott and Rung 2016). Agências como a NASA e o serviço postal (USPS) estão entre os grandes usuários.

Embora tendo sido precursor no uso de OSS, o Pentágono não atendeu ao estipulado pela política governamental (Eversden 2019). Ainda assim, o uso de OSS pelos militares dos EUA se intensifica, e aqui destacamos exemplos emblemáticos.

A novíssima classe de destroieres USS Zumwalt incorporou Linux Red Hat em seus sistemas de navegação, manutenção, armamentos e monitoração (Gallagher 2013). Sistemas originalmente não construídos para serem conectados a uma rede IP são integrados por meio de processadores de adaptação distribuídos (DAPs). Tais adaptadores são computadores de placa única usando o Lynx RTOS (Real Time Operating System), uma *distro* de Linux para dispositivos e sensores em tempo real, que conectam à rede dispositivos da embarcação, como sistemas de engenharia e de combate a incêndio, lançadores de mísseis e equipamentos de comunicação de rádio e satélite, para que possam ser controlados por aplicativos na rede (Gallagher 2013; Lynx.com n.d.). Dessa forma, os aplicativos não precisam

estar instalados em computadores localizados em pontos determinados do navio, mas podem ser utilizados a partir de qualquer estação de trabalho do navio, provendo mais resiliência (Gallagher 2013). Cada estação de trabalho pode executar várias máquinas virtuais Linux particionadas por nível e finalidade de segurança (Gallagher 2013).

Noutra iniciativa, uma arquitetura de segurança Linux foi customizada pela NSA. O Security-Enhanced Linux, ou SELinux, incorpora controles de segurança aprimorados. Ele impõe políticas de controle de acesso mandatórias que limitam os programas de usuários e os servidores do sistema à quantidade mínima de privilégios necessários para realizar suas tarefas. Dessa forma, a capacidade de programas de usuário e do sistema causarem danos quando comprometidos é reduzida ou eliminada.

A Iniciativa de Proteção de Software (SPI), sob a direção do Laboratório de Pesquisa da Força Aérea e do Departamento de Defesa dos EUA, criou o Lightweight Portable Security (LPS). Trata-se de uma distribuição Linux que, como o nome indica, é pequena e pode ser usada a partir de um dispositivo removível, em qualquer computador, sem, no entanto, armazenar ou registrar qualquer informação nesse computador (Vaughan-Nichols 2011).

A Marinha dos EUA contratou a Raytheon para instalar o software de controle em sua frota de drones de decolagem e aterrissagem vertical (VTOL) em plataforma Linux (Thomson 2012). Possivelmente, em decorrência da revelação de um ataque de malware ao sistema de controle de drones baseado em Windows da Força Aérea dos EUA (Thomson 2012). Comentando sobre o incidente, Mikko Hypponen, respeitado pesquisador de segurança cibernética, teria declarado: "Se eu precisasse escolher entre o Windows XP e um sistema baseado em Linux durante a construção de um sistema militar, não duvidaria nem um segundo de qual seria" (Thomson 2012).

## China

Em meio às restrições impostas pelos EUA, a China estimula o crescimento da oferta de produtos nacionais; fabricantes de semicondutores e empresas de software têm isenção total de impostos por dois anos e de 50% nos três anos seguintes, à medida que a guerra comercial migra para "um ataque à tecnologia chinesa" (Shidong 2019).

Mesmo com a Microsoft tendo produzido uma "Edição do Governo Chinês" do Windows 10 em 2017, em conjunto com sua joint venture chinesa, empresas chinesas de cibersegurança informam que o governo deve migrar para SO *nacionais* (Yang and Liu 2019). Existem ao menos dois SO caseiros da China derivados do Linux: o Kylin OS e o Red-Flag Linux.

O Kylin OS é desenvolvido desde 2001 pela National University of Defense Technology in China (Kirin Software n.d.). Suas versões iniciais eram baseadas no FreeBSD, mas a partir de 2010 ele tornou-se baseado em Linux. Um projeto separado, denominado Ubuntu Kylin, foi anunciado em 2013. Por mais de uma década o Kylin tem sido amplamente utilizado pelos setores de defesa, governo, energia, transporte e aeroespacial da China, entre outros (Li, Liao, and Ma 2017, 66). Oferece compatibilidade com diversos processadores chineses independentes ou compatíveis com o Intel x86. Para reduzir a carência de aplicativos para ambiente Linux, o Kylin oferece compatibilidade para a execução de mais de 2.000 aplicativos Android. Possui também um sistema de segurança com proteção integrada dentro e fora do núcleo, gerenciamento e controle compatíveis com controle de acesso forte de código aberto e incorpora software que pode identificar e impedir automaticamente violações ilegais e evitar que dados privados sejam indevidamente acessados. Suporta métodos de autenticação biométrica como impressões digitais, veias, íris e impressões de voz.

O Red-Flag iniciou-se em 2000 sob os auspícios do Software Research Institute da Chinese Academy of Sciences (Zhongke Hongqi n.d.). Foi desenvolvido a partir do Red Hat Linux. O projeto, uma iniciativa governamental, tinha três motivações: baixo custo, fomento à indústria nacional, e desconfiança do "imperialismo americano", com possíveis *backdoors* no Windows (Pan and Bonk 2007, 2–3). Dentre suas funcionalidades de segurança destacam-se: adequação a padrões internacionais, separação de privilégios, reforço à autenticação de identidade, isolamento do domínio da operação, controle de acesso obrigatório, controle de acesso autônomo, sistema de arquivos criptografado, auditoria de segurança no nível do *kernel*, gerenciamento centralizado de segurança e auditoria, monitoramento e alarme de segurança, controle de sessão e recursos, assistente automatizado de políticas de segurança de aplicativos, e "boa compatibilidade" de hardware e software.

### Rússia

Os russos possuem sua própria versão de Linux, denominada Astra Linux (Astra Linux n.d.), e derivada do Debian. O sistema tem uma versão Edição Especial, com melhorias no tocante à segurança. Esta versão é certificada em conformidade com os requisitos de segurança do Ministério da Defesa Russo desde 1996, e pelo FSB, o Serviço Federal Russo de Segurança, sucessor da antiga KGB. Dentre suas funções de segurança destacam-se: controle de acesso obrigatório, isolamento do núcleo, limpeza da memória interna e externa, exclusão garantida de arqui-

vos, marcação de documentos, registro (*logging*) de eventos, mecanismos de segurança da informação no subsistema gráfico, modo de restrição de ação do usuário, proteção do espaço de endereço dos processos (acesso dos programas à memória), controle de integridade, ferramentas de organização de domínio, gerenciador de banco de dados relacional seguro e servidor de e-mail seguro.

Visando escapar do monopólio de Android e iOS em dispositivos móveis, os russos estão desenvolvendo seu próprio SO móvel como alternativa. De acordo com o ministro Nikolai Nikiforov, do Ministério da Comunicação da Rússia, o novo SO móvel será construído a partir do Sailfish OS, desenvolvido pela empresa finlandesa Jolla, formada por antigos engenheiros da Nokia e registrada em Hong Kong (Hanson 2015; Mohit Kumar 2016).

### Índia

Desde 2007 a Índia possui o Bharat Operating System Solution, (BOSS), apresentado como um SO alternativo ao Windows (Ganguli 2017; CDAC n.d.). Derivado do Debian, foi desenvolvido pelo National Resource Centre for Free and Open Source Software (NRCFOSS), órgão do Centre for Development of Advanced Computing (CDAC). Foi inicialmente anunciado como uma proposta para reduzir a desigualdade digital (*digital divide*) na Índia, por ser gratuito e suportar diversas línguas daquele país. Após o Caso Snowden, mostrando a Índia como objeto de grande interesse da NSA, e diante dos contínuos incidentes de ciberataques chineses à Índia, o governo daquele país decidiu adotar o BOSS como o SO nacional (Manan Kumar 2015). O sistema implementa diferentes opções de segurança. Uma versão Secured Operating System (algo como Sistema Operacional Seguro) foi criada com foco nos "clientes do setor de defesa", que exigem um SO livre de invasões e ataques cibernéticos. Implementa medidas específicas usadas para proteger o sistema contra ameaças, vírus, *worms*, malware e ataques cibernéticos, e técnicas de controle preventivo que protegem os dados no computador de serem editados ou excluídos. Inclui controle de acesso mandatório e atualizações regulares de segurança e do banco de dados antivírus. O BOSS oferece ainda um servidor de e-mail seguro, mecanismos de comando e controle para *smart-cities* (integração de componentes IoT — Internet das Coisas — para gestão urbana), armazenamento em "nuvem segura", integração com dispositivos móveis para coleta de dados distribuída, um "cofre eletrônico seguro" (*secured electronic vault*) para o armazenamento de documentos digitais e um scanner de reconhecimento facial que pode identificar pessoas num vídeo e gerar relatórios.

### Coreia do Norte

Red Star OS é um SO baseado em Linux, derivado do Fedora (portanto Red Hat) desenvolvido pelo Korean Computer Center (Schiess 2017, 1–2). Além de evitar eventuais *backdoors* em SO norte-americanos, o Red Star visa monitorar o comportamento digital dos cidadãos norte-coreanos (Hoffman 2014). Embora a maior parte de sua funcionalidade seja igual aos SO padrão, o Red Star contém recursos úteis à segurança do Regime vigente. Por exemplo, insere uma marca d'água digital rastreável em todos os documentos que o percorrem, visando combater a distribuição da mídia sul-coreana e dificultar o compartilhamento de informações (Pauli 2015; Schiess 2017, 2). O Red Star possui também um mecanismo para evitar violações, retornando uma mensagem de erro ou encerrando a execução se alguma violação dos arquivos do sistema for detectada (Wagstaff and Pearson 2015; Schiess 2017). Por fim, o Red Flag também não pode ser conectado à Internet, mas possui um navegador interno, baseado no FireFox, que funciona apenas na intranet norte-coreana, destinado a monitorar a atividade *online* (Hoffman 2014).

### Turquia

O Pardus é uma distribuição Linux turca, que desde 2013 é baseada no Debian GNU/Linux (Pardus n.d.). É desenvolvido desde 2004 pelo Instituto Nacional de Pesquisa em Eletrônica e Criptologia (UEKAE) daquele país, com o apoio do Conselho de Pesquisa Tecnológica da Turquia (TUBITAK), Ministério da Defesa e do Gabinete do Primeiro Ministro. O objetivo foi o de pesquisar a viabilidade de uma *distro* de um SO nacional para independência de países estrangeiros e para garantir a segurança de informações militares (Karakoç and Varol 2016, 26). Não foram encontradas informações sobre implementações específicas de segurança do Pardus.

### Coreia do Sul

Com o suporte ao Windows 7 vivendo seus momentos derradeiros, o governo sul-coreano estuda desistir do Windows. Em maio de 2019, o Ministério do Interior do país anunciou planos de migrar aproximadamente 3,3 milhões de computadores de Windows para Linux (Vaughan-Nichols 2020). Os motivos seriam os custos de licenciamento de software e a dependência do governo no tocante ao Windows. O custo da atualização do Windows 7 para o Windows 10 foi estimado em cerca de US$ 655 milhões (Vaughan-Nichols 2020).

O Ministério da Defesa Nacional e o Ministério da Administração Pública e Segurança já utilizam o SO coreano Gooroom Cloud, baseado no Linux Debian (Vaughan-Nichols 2020). Este sistema implementa algumas extensões de segurança (Gooroom n.d.). O Trust Boot assegura que o carregador de inicialização ou o próprio SO não sejam infectados antes de carregados os módulos de segurança, verificando a integridade do sistema e garantindo sua inicialização sem infecções. O núcleo também é protegido com um mecanismo de verificação baseado em virtualização para monitorar a falsificação ou adulteração de elementos chave do sistema, impedindo a operação de malware com acesso privilegiado ao sistema. Um sistema de proteção de integridade verifica *assinaturas de código* antes de ativar os principais arquivos executáveis, como serviços do sistema e bibliotecas, evitando instalações não autorizadas ou a execução de programas forjados ou alterados ilegalmente. O navegador incluído no sistema aplica diferentes políticas de segurança para limitar possíveis ações (reprodução de mídia, download, etc.) ao acessar sites não confiáveis.

O Ministério da Defesa Nacional e a Agência Nacional de Polícia usam também o Harmonica OS 3.0, baseado no Ubuntu, mas com muitas características da *distro* Mint (HarmoniKR n.d.). O Harmonica também inclui o navegador Naver Whale, criado em coreano (Vaughan-Nichols 2020).

## RECOMENDAÇÕES PARA O BRASIL

O aumento da segurança cibernética demanda que o Brasil siga os exemplos dos países citados e internalize softwares de código aberto em suas estruturas governamentais, especialmente na defesa. Esse processo naturalmente seria gradual, mas os casos estudados demonstram que já em dois anos é possível colher os primeiros resultados. Propõe-se, aqui, a Criação de um Núcleo de Software Básico da Defesa (NSBD). Mas não apenas a segurança e defesa do Estado são determinantes. A economia na aquisição de licenças também é motivo relevante, assim como a ampliação da inclusão digital. Observe-se que não se pretende aqui uma reserva de mercado, mas a simples oferta de uma alternativa viável, com ganhos de segurança, não mensuráveis, mas também econômicos e sociais, facilmente mensuráveis.

A criação desse NSBD é consoante com o eixo estratégico cibernético da Estratégia Nacional de Defesa (END), e permitiria que o país desenvolvesse tecnologia própria para proteger-se de certas classes de problemas. Ainda que, nos primeiros anos, não se desenvolva tecnologia genuinamente nacional, a internalização de plataformas OSS e o controle de acesso aos códigos fonte já reduziria significativamente a possibilidade de existência de *backdoors*.

Esse núcleo deveria ser vinculado ao Comando de Defesa Cibernética, no Ministério da Defesa (MD), responsável pela ciberdefesa e mais bem estruturado que o Gabinete de Segurança Institucional (GSI), responsável pela cibersegurança. O NSBD seria composto por militares e civis, necessariamente contendo representantes da iniciativa privada (componentes da Base Industrial de Defesa) e da academia. Essa necessidade advém do fato de que a dinâmica da carreira militar leva a constantes movimentações e transferências, dificultando o processo de retenção e transferência de conhecimento. A participação da iniciativa privada e da academia assegurariam essa retenção e repasse. Ressalte-se que todos os componentes propostos aqui têm emprego dual, tanto militar quanto civil, e assim atendem ao disposto na END.

O NSBD selecionaria uma versão do SO de código livre Linux a ser definida como padrão oficial brasileiro. Baseado nos exemplos dos países citados, as *distros* Debian ou Red Hat/Fedora seriam boas opções, embora o Ubuntu também pudesse sê-lo. Os códigos-fonte desse sistema seriam *internalizados* pela equipe, que os estudaria e providenciaria eventuais modificações necessárias. Seriam geradas versões periódicas desse sistema, distribuídas livremente. Esse procedimento levaria ao domínio completo do sistema, reduzindo a possibilidade de existência de códigos indesejados ou secretos, ou *backdoors* desconhecidas potencialmente exploráveis em situações de crise ou conflito. Além disso, em caso de ataques cibernéticos ou violações, a comunidade teria facilidade em identificar e corrigir os problemas.

Numa segunda fase, plataformas como servidores de e-mail e gerenciadores de banco de dados, navegadores web, e mesmo de automação de escritório, de código aberto, poderiam ser internalizadas e incorporadas à distribuição, com configurações padrão que atendam aos interesses de segurança e defesa do país.

A partir da *nacionalização* de cada plataforma, melhorias de segurança poderiam ser incorporadas, tornando-as mais robustas e incorporando tecnologias desenvolvidas nacionalmente.

## CONCLUSÃO

Diversos países, com regimes políticos e culturas distintos, optaram, por motivos de segurança, econômicos ou sociais, pela utilização de Software de Código Aberto para utilização em seus sistemas de missão crítica, relacionados à defesa, segurança, inteligência e governo, ou ainda para sua população. Claramente, razões de segurança nacional prevalecem sobre outros interesses nessa opção. A possibilidade de dispor de independência tecnológica, mesmo que limitada ao software, onde as barreiras de entrada

são consideravelmente menores que aquelas de hardware, tem um grande peso. E oferece alternativas viáveis quando se observa a imposição de restrições de acesso a tecnologias, presentes nas sanções à China, Rússia, Irã e Coreia do Norte, por exemplo. Além dessa, há também a questão da espionagem política e comercial, da qual o Brasil é obviamente um alvo de grande interesse, seja dos EUA, como ficou patente no Caso Snowden, ou de outros.

Mas não apenas questões de segurança justificam a adoção de uma *distro* Linux nacional. Interesses econômicos também são significativos, com a redução da exportação de divisas às empresas multinacionais de software, bem como de redução do déficit fiscal, dados os valores dispendidos pelos governos, em todas as suas instâncias, no licenciamento de SO comerciais estrangeiros. Não menos relevantes, interesses sociais também estão atrelados a essa decisão, posto que a disponibilização de um sistema nacional gratuito permitiria que a população não precisasse gastar recursos limitados na aquisição de produtos importados de elevado custo, ou que, na impossibilidade de fazer esse desembolso, fique sujeita ao *digital divide* ou compelida ao uso de software pirata, sem suporte e sujeita a vulnerabilidades potencialmente exploradas por criminosos.

Outrossim, são muitos os benefícios, e significativamente baixos os custos, para a adoção gradual de OSS, em particular o aqui proposto, num projeto coordenado pelo MD no Brasil.

## REFERENCIAS

Adams, James. 2001. "Virtual Defense". *Foreign Affairs* 80, no. 3: 98. https://doi.org/10.2307/20050154.

Angelo, Cláudio. 2007. "'Eixo Do Mal' Científico: Ministério Pede Explicações à Dell Sobre Exigências a Físicos". *Folha de São Paulo* (September). http://www1.folha.uol.com.br/fsp/ciencia/fe1409200703.htm.

Astra Linux. n.d. "Astra Linux - Универсальная Операционная Система". Astra Linux Website. http://www.astralinux.ru/en/.

Banach, William. 2012. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE". https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE Investigative Report (FINAL).pdf.

CDAC. n.d. "BOSS Linux". BOSS Linux Website. Accessed June 25, 2020. https://bosslinux.in/.

Cimpanu, Catalin. 2018. "Cisco Removed Its Seventh Backdoor Account This Year, and That's a Good Thing". *ZDNet* (November). https://www.zdnet.com/article/cisco-removed-its-seventh-backdoor-account-this-year-and-thats-a-good-thing/.

Cisco. n.d. "Cisco Prime Home Authentication Bypass Vulnerability - Cisco". https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20170201-prime-home.html.

Clark, Don. 2015. "U.S. Agencies Block Technology Exports for Supercomputer in China". *The Wall Street Journal*. http://www.wsj.com/articles/u-s-agencies--block-technology-exports-for-supercomputer-in-china-1428561987.

Eversden, Andrew. 2019. "Why Can't the Pentagon Use More Open Source Code?" *Wired* (September). https://www.fifthdomain.com/civilian/omb/2019/09/11/why-cant-the-pentagon-use-more-open-source-code/.

Figueiredo, Nice. 1986. "Legislação de Informática No Brasil". *Revista de Biblioteconomia de Brasília* 34, no. 81.

Finley, Klint. 2016. "Open Source Won. So, Now What?" *Wired* (November). https://www.wired.com/2016/08/open-source-won-now/.

Gallagher, Sean. 2013. "The Navy's Newest Warship Is Powered by Linux". *Ars Technica* (October).

Ganguli, Subrata. 2017. "Computer Operating Systems: From Every Palm to the Entire Cosmos in the 21st Century Lifestyle". *CSI Communications*: 5–8.

Gates, Bill. 1996. "Unix Expo Remarks by Bill Gates, October 9, 1996". Wayback Machine (October). https://web.archive.org/web/20010818203946/http://www.microsoft.com/billgates/speeches/industry&tech/uexpo.asp.

GCHQ. 2016. "GCHQ History". http://www.gchq.gov.uk/history/Pages/index.aspx.

Gerring, John. 2012. "Mere Description". *British Journal of Political Science* 42: 721–46. https://doi.org/10.1017/S0007123412000130.

Goodin, Dan. 2016. "Cisco Confirms NSA-Linked Zeroday Targeted Its Firewalls for Years". *Ars Technica*. https://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/.

Gooroom. n.d. "Cloud Platform Forum". Gooroom Website. https://www.gooroom.kr/.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. Penguin Books.

Hanson, Matt. 2015. "Russia's Making Its Own Mobile OS to Boot out Apple and Google | TechRadar". *TechRadar* (May). https://www.techradar.com/uk/news/phone-and-communications/mobile-phones/russia-s-making-its-own-new-mobile-os-to-boot-out-apple-and-google-1294258.

HarmoniKR. n.d. "Linux Community HarmoniKR". HarmoniKR Website. https://hamonikr.org/.

Hoffman, Chris. 2014. "Meet Red Star OS, the North Korean Linux Distro That Apes Apple's OS X | PCWorld". *PCWorld* (December). https://www.pcworld.com/article/2862737/meet-red-star-os-the-north-korean-linux-distro-that-apes-apples-os-x.html.

Hosch, William. 2008a. "Linux | Operating System | Britannica". *Encyclopaedia Britannica* (November). https://www.britannica.com/technology/Linux.

_____. 2008b. "UNIX | Operating System | Britannica". *Encyclopaedia Britannica* (December). https://www.britannica.com/technology/UNIX.

Karakoç, Mehmet, and Asaf Varol. 2016. "National Distribution Project and Pardus Operating System". *Turkish Journal of Science and Technology* 11, no. 2: 25–34.

Kharpal, Arjun. 2020. "US Should Take Stake in Nokia, Ericsson to Counter Huawei in 5G: Barr". *CNBC* (February). https://www.cnbc.com/2020/02/07/us-should-take-stake-in-nokia-ericsson-to-counter-huawei-in-5g-barr.html.

Kirin Software. n.d. "Kirin Software". KylinOS Website. http://www.kylinos.cn/.

Kumar, Manan. 2015. "Make In India: Now Government to Have Its Own Operating System, May Replace Microsoft Windows in Future". *DNA* (September). https://www.dnaindia.com/india/report-make-in-india-now-government-to-have-its-own-operating-system-may-replace-microsoft-windows-in-future-2125014.

Kumar, Mohit. 2016. "Russia to Get Rid of Android and IOS by Launching Its Own Mobile Operating System". *The Hacker News* (June). https://thehackernews.com/2016/06/russian-mobile-os.html.

Li, Jia-Qi, Xiang-Ke Liao, and Jun Ma. 2017. "A Typical Commercial Application for Kylin Operating System". In *2017 3rd International Conference on Computer Science and Mechanical Automation*: 66–70. Wuhan. https://doi.org/10.12783/dtcse/csma2017/17323.

Lynn, William. 2010. "Defending a New Domain: The Pentagon's Cyberstrategy". *Foreign Affairs* 89 (5).

Lynx.com. n.d. "LynxOS | POSIX Real Time Operating System | Lynx Software Technologies". Lynx.Com Website. https://www.lynx.com/products/lynxos-posix-real-time-operating-system-rtos.

Miller, Greg. 2020. "How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades – Washington Post". *The Washington Post* (February) https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/?fbclid=IwAR1ydM24snbzKUpHz1fsNny7LkLVScUwmUNAuiQMDWtsB4LUYTVopqyWOxg.

MITRE. 2003. "Use of Fre and Open-Source Software (FOSS) in the U.S. Department of Defense".

Moon, Angela. 2019. "Exclusive: Google Suspends Some Business with Huawei after Trump Blacklist - Source - Reuters". *Reuters* (May). https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB.

Moreira, José de Albuquerque. 1995. "Informática: O Mito Política Nacional de Informática". *Revista de Biblioteconomia de Brasília* 19, no. 1: 23–50.

Pan, Guohua, and Curtis J. Bonk. 2007. "The Emergence of Open-Source Software in North America". *International Review of Research in Open and Distance Learning* 8, no. 3: 1–18. https://doi.org/10.19173/irrodl.v8i3.496.

Pardus. n.d. "Pardus – TÜBİTAK ULAKBİM". Pardus Website. https://www.pardus.org.tr/.

Pauli, Darren. 2015. "North Korea's Red Star Linux Inserts Sneaky Serial Content Tracker". *The Register* (July). https://www.theregister.com/2015/07/20/north_korea_red_star_linux_inserts_sneaky_serial_content_tracker/.

Rid, Thomas. 2016. *Rise of the Machines*. London: Scribe Publications.

Schiess, Niklaus. 2017. "Governmental Control of Digital Media Distribution in North Korea: Surveillance and Censorship on Modern Consumer Devices". https://dprktech.info/media/governmental_control_of_digital_media_distribution_in_north_korea-nschiess.pdf.

Scott, Tony, and Anne Rung. 2016. "Federal Source Code Policy". Federal Source Code Policy (August). https://sourcecode.cio.gov/.

Shidong, Zhang. 2019. "China Offers Five-Year Tax Breaks to Chip Makers, Software Developers to Bolster Industry as Trade War Stretches to Tech | South China Morning Post". *South China Morning Post* (May). https://www.scmp.com/business/article/3011377/china-offers-five-year-tax-breaks-chip-makers-software-developers-bolster.

Singh, Amit. 2007. *Mac OS X Internals: A Systems Approach*. Boston: Pearson Education.

Strumpf, Dan. 2020. "Huawei's 5G Dominance Threatened by U.S. Policy on Chips – WSJ". *The Wall Street Journal* (June). https://www.wsj.com/articles/huawei-struggles-to-escape-u-s-grasp-on-chips-11592740800.

Thomson, Iain. 2012. "US Navy Buys Linux to Guide Drone Fleet". *The Register* (June). https://www.theregister.co.uk/2012/06/08/us_navy_linux_drones/.

Tonooka, Eduardo. 1992. "Política Nacional de Informática: Vinte Anos de Intervenção Governamental". *Estudos Econômicos* 22, no. 2: 273–97.

TOP500.org. n.d. "Top500". TOP500.Org. https://www.top500.org/lists/.

U.S. Dept. of Commerce. 2020. "Department of Commerce Announces the Addition of Huawei Technologies Co. Ltd. to the Entity List | U.S. Department of Commerce". Dept. of Commerce Press Releases (May). https://www.commerce.gov/news/press-releases/2019/05/department-commerce-announces-addition-huawei-technologies-co-ltd.

U.S. DoD. n.d. "DoD Open Source Software (OSS) FAQ". DOD CIO Web Site. https://dodcio.defense.gov/Open-Source-Software-FAQ/#Q:_Under_what_conditions_can_GPL-licensed_software_be_mixed_with_proprietary.2Fclassified_software.3F.

Vaughan-Nichols, Steven. 2011. "The Air Force's Secure Linux Distribution". *ZDNet* (September). https://www.zdnet.com/article/the-air-forces-secure-linux-distribution/.

_____. 2020. "South Korea's Government Explores Move from Windows to Linux Desktop". *ZDNet* (February). https://www.zdnet.com/article/south-koreas-government-explores-move-from-windows-to-linux-desktop/.

Wagstaff, Jeremy, and James Pearson. 2015. "Paranoid: North Korea's Computer Operating System Mirrors Its Political One – Reuters". *Reuters* (December). https://www.reuters.com/article/northkorea-computers-idUSKBN0UA0GF20151227.

Wennergren, David. 2009. "Clarifying Guidance Regarding Open Source Software (OSS)". http://www.defenselink.mil/cio-nii/cio/oss/.

Yang, Yuan, and Nian Liu. 2019. "Beijing Orders State Offices to Replace Foreign PCs and Software | Financial Times". *Financial Times* (December). https://www.ft.com/content/b55fc6ee-1787-11ea-8d73-6303645ac406.

Zetter, Kim. 2015. "Suite of Sophisticated NationState Attack Tools Found With Connection to Stuxnet". *Wired*. https://www.wired.com/2015/02/kapersky-discovers-equation-group/.

Zhongke Hongqi. n.d. "Zhongke Hongqi Website and Application". Zhongke Hongqi Website. http://www.chinaredflag.cn/.

NOTAS

1. Ou OS, acrônimo de Operating System.
2. Exemplos desses métodos de remuneração podem ser encontradas nos antivírus e serviços de Virtual Private Network (VPN) gratuitos, que ou fazem publicidade ou oferecem uma versão inicial limitada, com a versão profissional, mais completa, sendo paga.
3. Lei nº 7.232/1984.
4. Zero-day ou 0-day são vulnerabilidades decorrentes de falhas existentes na codificação do , desconhecidas do público e do fabricante do produto, demandando a publicação e instalação de correções do programa ou biblioteca de (*patches*).
5. PetaFLOPS, or $10^{15}$ FLoating-point Operations Per Second.
6. Um instituto privado de pesquisas com histórico de atuação em pesquisas militares e sociais.

POR QUE O BRASIL DEVERIA ADOTAR UMA *DISTRO* LINUX PRÓPRIA?

## RESUMO

Na tentativa de se escapar da dependência tecnológica externa em sistemas relacionados à defesa, por conseguinte de missão-crítica, bem como de elevados custos de licenciamento, alguns países evitam o uso de softwares comerciais desenvolvidos fora de suas fronteiras, utilizando sistemas abertos ou versões compatíveis desenvolvidas autonomamente. Este artigo argumenta que o Brasil deveria buscar tal autonomia, adotando uma versão própria de sistema operacional, a partir de uma distribuição Linux. É empregada uma metodologia descritiva, baseada em estudos de casos, para análise das opções feitas por diferentes nações. A adoção dessa opção permitiria que o país superasse a desconfiança existente quanto à existência de *backdoors* criadas por parte de serviços de inteligência estrangeiros nos softwares produzidos em seus países de origem. Adicionalmente, alinha-se à Estratégia Nacional de Defesa, permitindo a aquisição de tecnologia de uso dual pela indústria nacional.

Palavras-chave: Autonomia Tecnológica; Distribuições Linux; Software de Código Aberto.

## ABSTRACT

In an attempt to escape external technological dependence on defense-related systems, therefore mission-critical, as well as high licensing costs, some countries avoid using commercial software developed outside their borders, using open systems or compatible versions developed autonomously. This article argues that Brazil should seek such autonomy, adopting its own version of the operating system, based on a Linux distribution. A descriptive methodology, based on case studies, is used to analyze the options made by different nations. The adoption of this option would allow the country to overcome the existing mistrust regarding the existence of backdoors created by foreign intelligence services in the software produced in their countries of origin. Additionally, it is in line with the National Strategy of Defense, allowing the acquisition of dual-use technology by the national industry.

Keywords: Technological Autonomy; Linux Distributions; Open Source Software.

**Recebido em 03/05/2021. Aceito para publicação em 03/05/2021.**