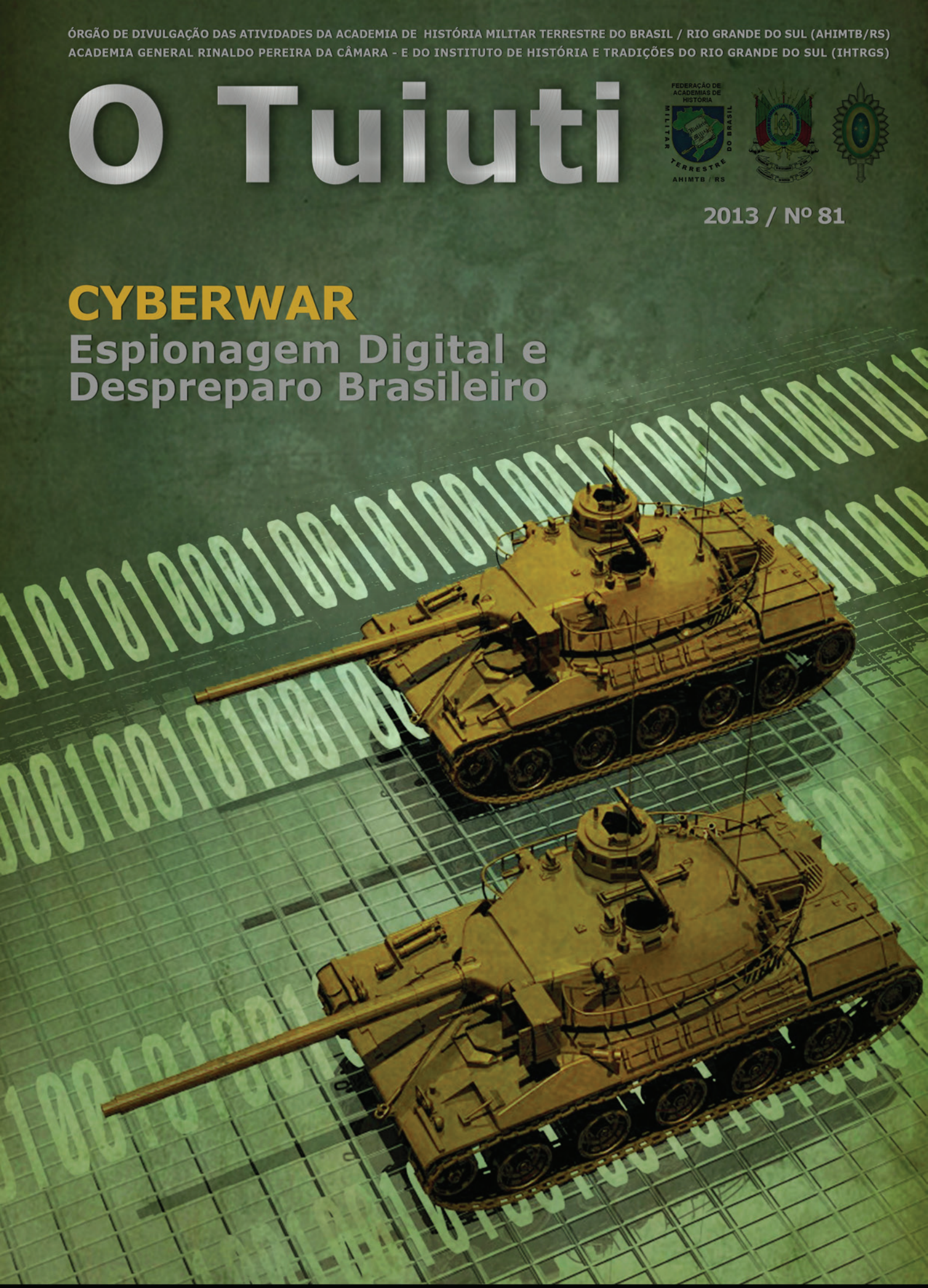
ÓRGÃO DE DIVULGAÇÃO DAS ATIVIDADES DA ACADEMIA DE HISTÓRIA MILITAR TERRESTRE DO BRASIL / RIO GRANDE DO SUL (AHIMTB/RS)
ACADEMIA GENERAL RINALDO PEREIRA DA CÂMARA - E DO INSTITUTO DE HISTÓRIA E TRADIÇÕES DO RIO GRANDE DO SUL (IHTRGS)

O Tuiuti

2013 / Nº 81

CYBERWAR
Espionagem Digital e Despreparo Brasileiro



O Tuiuti

ÓRGÃO DE DIVULGAÇÃO DAS ATIVIDADES DA ACADEMIA DE HISTÓRIA MILITAR TERRESTRE DO BRASIL/RIO GRANDE DO SUL (AHIMTB/RS) - ACADEMIA GENERAL RINALDO PEREIRA DA CÂMARA - E DO INSTITUTO DE HISTÓRIA E TRADIÇÕES DO RIO GRANDE DO SUL (IHTRGS)

210 ANOS DO NASCIMENTO DE CAXIAS – 70 ANOS DA CRIAÇÃO DA FEB

Editor:
Luiz Ernani Caminha Giorgis, Cel – Presidente daAHIMTB/RS e Vice do IHTRGS
lecaminha@gmail.com

Projeto Gráfico:
Fabricio Gustavo Dillenburg - Núcleo de Estudos de História Militar Vae Victis
nucleomilitar@gmail.com

Capa:
Montagem sobre imagem modificada, de autor não identificado.

NÚCLEO DE ESTUDOS DE HISTÓRIA MILITAR VAE VICTIS

Mais de duas décadas de trabalho voltado para a divulgação da História Militar

O Núcleo de Estudos de História Militar Vae Victis tem grande orgulho em participar da elaboração do informativo **O Tuiuti**, marco da formação histórica militar brasileira. Com o objetivo de divulgar a História, sobretudo em seu viés militar, o Núcleo de Estudos de História Militar Vae Victis trabalha tendo em vista a clareza de informação, a amplitude das análises, a relevância do material audiovisual, a atualização das hipóteses e a consistência na argumentação.

Nossa Missão: é levar ao máximo possível de pessoas o conhecimento da História Militar, divulgando sua importância, resgatando os seus valores e as suas memórias, preservando documentos e fornecendo subsídios para uma educação integral e de qualidade.

Nossa Postura: é independente, livre de qualquer posição política ou religiosa, voltada unicamente para a preservação e divulgação do conhecimento histórico, sem qualquer conexão com entidades que não tenham cunho explicitamente cultural, visando fornecer informação e compreensão com acessibilidade.

Para saber mais sobre nosso trabalho visite:

www.nucleomilitar.com / www.nucleomilitarblog.com

CYBERWAR
NA TERRA DE ALICE

A Fantástica, Estonteante, Inacreditável "Descoberta" De Que Estamos Sendo Espionados Pelos EUA

Fabricio Gustavo Dillenburg
Núcleo de Estudos de História Militar Vae Victis

Então, eis que, de repente, não mais que de repente, cai a bomba de que o Brasil está sendo espionado pelos EUA. Correria, gritaria, reuniões de emergência, cabelos arrancados, dedos em riste, bodes expiatórios envolvidos em desabaladas explicações, discursos de indignação. O governo, a ABIN, em polvorosa; justificativas, conversa fiada, e a população, como sempre, indignada, por quase cinco minutos, ou fazendo as já tradicionais e esperadas piadinhas, a propósito.

A arte da guerra estendeu-se, há muito, além das fronteiras físicas, geográficas. Há mais de vinte anos, o conceito de dominação de informações do mundo virtual rende investimentos de bilhões de dólares em estrutura e treinamento, voltados para gerar dados capazes de condicionar – senão determinar – decisões capazes de afetar, significativamente, a constituição geopolítica , em todos os continentes.

Por isso mesmo, a internet representa, hoje, um paradoxo. Enquanto permite a fluência gigantesca de conhecimento, como nunca antes na História, ela serve como plataforma de observação e controle. Há uma ilusão, generalizada, de liberdade em seu uso, que não corresponde, em absoluto, à realidade. A censura existe, e é pesada, mas habilmente dissimulada; o controle é contínuo, permanente, e não há um entendimento de como o sistema realmente funciona. Por isso, ficamos à mercê de quem sabe.

Não sejamos cínicos. Muito menos, estúpidos, ao dizer que "não sabíamos". O domínio das informações de um país, em suas estruturas de comunicação mais básicas – internet, telefones – representa vantagens inimagináveis, consideravelmente no plano político-econômico. Saber de antemão quem está negociando o quê, com quem e a que preço, fornece subsídios para a obtenção de lucros no mercado – ou, mesmo, seu próprio controle.

Passaram-se os tempos dos pesadelos de Orwell. No contexto atual, eles são a mais concreta realidade, acreditemos ou não. A militarização do ciberespaço é um fato, cada vez mais premente. E todas as nações, conscientes do papel que esse novo campo de batalha representa, estão investindo pesadamente para tentar obter vantagens, antes que a guerra tome proporções demasiadas.

Países com pretensões à superpotência, como a China, desde logo partiram para uma política que concentra a aplicação de recursos, em hardware e software, simultaneamente à preparação de mão-de-obra especializada, altamente técnica. Isso derivou em uma força-tarefa de grande capacidade, que se transformou em fonte de preocupações e de gastos imensos no Ocidente, para impedir que informações vazassem ou que sistemas críticos pudessem ser alvos de ataques. Não adiantou. Notícias recentes, de invasões e roubos virtuais de projetos e de muitos dados técnicos, na Austrália e nos EUA, parecem demonstrar que os chineses tiveram mais sucesso em seus planos de ataque, que suas vítimas, em suas estratégias de defesa.

Todas as informações que trafegam pela América Latina – principalmente pela internet – são alvo de monitoramento permanente dos EUA. Assim foi, assim é e assim será. Estamos, como todos os países de relevância estratégica, sob arguta vigilância, vinte e quatro horas por dia, sete dias por semana. Cada página acessada, cada e-mail trocado, cada ligação, fica registrada. Há equipamento para isso, há gente para isso. De fato, as agências são capazes de dizer mais sobre nós do que jamais seríamos capazes de suspeitar. Afinal,

nenhum país se torna o maior poder militar da Terra por ser condescendente com seus vizinhos. Eventualmente, a realidade – aquela, que vem com o velho e surrado livro de História, debaixo do braço, e parece que ninguém quer ver – tem que bater à nossa porta.

Do ponto de vista da interceptação e controle da informação pelos EUA, fundamentalmente, a coleta e análise dos dados podem ser classificadas como tática ou estratégica. Tática, quando a concentração dá-se sobre um alvo específico, buscando obter informações objetivas e pontuais. Estratégica – o caso da espionagem sobre o Brasil, e sobre a maioria dos países, não apenas latino-americanos – quando as informações são coletadas indiscriminadamente, para serem, posteriormente, analisadas, através de algoritmos sofisticados de busca e seleção. Neste caso, tudo fica armazenado, acessível a qualquer momento, material passível de ser complementado com informações mais recentes e cruzadas com minúcia, gerando relatórios abrangentes.

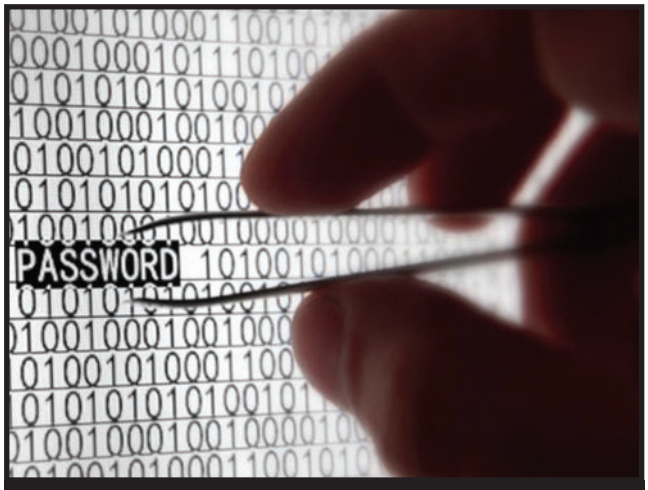
Pode-se pensar que há empecilhos para que isso aconteça e o primeiro, talvez, esteja relacionado aos custos e ao espaço de armazenamento necessário para tantos dados. Na verdade, não há. Como exemplo, cálculos realizados em 2012 demonstram que, para se armazenar todas as ligações telefônicas feitas de aparelhos fixos durante um ano – ressalto, *absolutamente* todas, públicas e privadas – em um país do tamanho e da complexidade da Alemanha, com boa qualidade de voz, basta um investimento de, aproximadamente, trinta milhões de euros, incluindo todas as despesas para administrar servidores e dados (valor que tende a cair). Objetivamente, sem os custos de administração, levando-se em conta apenas a armazenagem, o valor fica em torno de oito milhões de euros. Com o tamanho cada vez mais reduzido dos discos e computadores, o espaço físico necessário é irrisório: até um pequeno prédio, ou área subterrânea equivalente, pode servir (principalmente, porque é necessário um estacionamento, para o pessoal...). Em relação às questões legais, de livre acesso, as operadoras de comunicação, em sua maioria de capital estrangeiro, são absolutamente coniventes com o processo, na quase totalidade dos

Nossos dados são rastreados, metodicamente, em tempo integral

casos, como pode ser comprovado pela atuação da AT&T, no próprio território norte-americano. Pressão política – e dinheiro – derrubam quaisquer "inconvenientes" problemas éticos.

Por isso tudo, devemos nos espantar, justamente, com o espanto, em relação à constatação da espionagem. Alguns "especialistas", que comentaram

o caso da espionagem ao Brasil, parecem ter esquecido de que a própria Internet foi desenvolvida, originalmente, como um instrumento de comunicação militar. Ela seria uma alternativa, capaz de prover alguma troca de dados, entre o comando e as tropas, no caso de um ataque nuclear, bem como uma forma de compartilhar informações sigilosas, descentralizando-as, e tornando mais difíceis (ironicamente...), o roubo e a perda de dados. Com o tempo, e sua difusão gradual, primeiramente, como fonte de troca de informações científicas, a rede tornou-se de âmbito majoritariamente civil, até que uma parte considerável de sua estrutura se tornou aberta. Mas, isso, não eliminou o caráter de importância da espionagem sobre seu tráfego de dados; pelo contrário, abriu perspectivas para a obtenção de informações, até então, jamais sonhadas. Mesmo, porque, a internet foi adaptada, cada vez mais, para abarcar muitas funcionalidades que nunca foram previstas, oportunizando o aparecimento de vulnerabilidades.



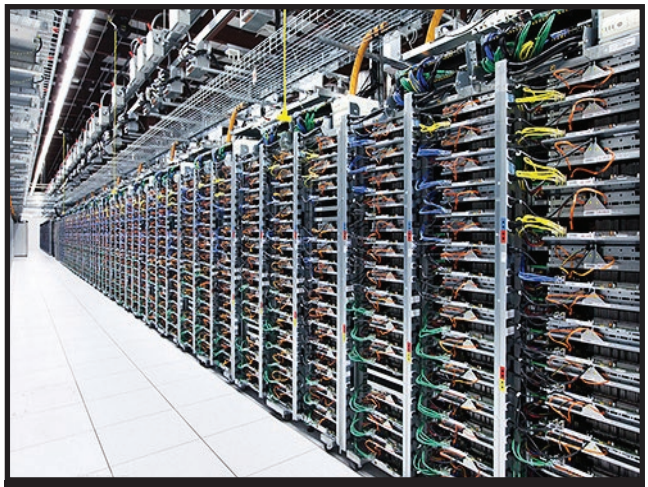
A questão não é ***se*** nossas informações serão roubadas, mas ***quando*** acontecerá

Não existem sistemas de informação cem por cento seguros. Isso é utopia. Mesmo no âmbito particular, obter segurança é uma tarefa infernal, que só quem tem algum conhecimento técnico, pode testemunhar com propriedade. *Sniffers*[1] vasculham a rede, tentando encontrar portas vulneráveis. *Trojans*[2] e *keyloggers*[3] tentam, constantemente, ser instalados e roubar informações. A maioria dos usuários sequer percebe isso, por pura ignorância do mundo digital em que navegam. Uma parcela se dá conta, pelo menos, de que, eventualmente, vírus podem representar uma ameaça aos arquivos. Não é o suficiente, é certo. Conforme estudos de segurança em tecnologia frequentemente demonstram, boa parte dos usuários colabora, sem querer, para que programas intrusos sejam acomodados em suas máquinas. A ignorância geral sobre o mínimo necessário para garantir a segurança dos dados armazenados, em um dispositivo qualquer, representa, sob tais aspectos, um grande risco, em larga escala. Proporcionalmente, o gerenciamento da segurança em redes do governo ou empresariais é um pesadelo descomunal para os administradores. Ainda mais, quando em situações de negligência.

A praticidade e a demanda permitiram, ainda, outras formas de exploração de informações, menos visíveis. A tecnologia GSM, usada em aparelhos portáteis de comunicação, é uma porta escancarada para reconhecimento e localização. Os celulares identificam a posição de um indivíduo com precisão, o que pode ser regularmente comprovado através da leitura de inúmeras acusações e processos contra

empresas de telefonia e fabricantes de aparelhos, incluindo a badalada e icônica Apple. Modelos da Blackberry possuem sistema interno de criptografia de rede, mas a chave permanece nas mãos da empresa e as ligações podem ser decodificadas por ela. A qualquer momento, qualquer pessoa que possua um telefone móvel ligado, pode ser encontrada com exatidão (e servir, por conseguinte, como alvo). Aplicativos, jogos, instalados com facilidade no dia-a-dia, também colaboram no processo. Da mesma forma, cartões de crédito, tablets e outros computadores, caracteristicamente com certas configurações, indicam seus locais de uso com certeza absoluta. Não apenas os IPs[4] de acesso são rastreados, como, também, alguns processadores possuem recursos que indicam exatamente sua origem, e sua movimentação. Como uma impressão digital, deixam rastros, que podem ser usados com clareza para definir toda uma trajetória, um histórico, até que aconteça uma eventual – e definitiva – ação de coleta ou repressão.

Estamos falando da possibilidade real de localização e de interceptação pontual de informações ou pessoas, sejam elas quem forem, ou do registro maciço de dados – *todos os dados* – através de equipamentos portáteis. Com alguns poucos aparelhos e conexões, graças à miniaturização, atualmente é possível varrer uma cidade inteira, apreendendo tudo que nela se comunica, com baixo custo e com equipes reduzidas. Basta ter os contatos certos, com os meios certos. Dependendo do equipamento utilizado, nem seres humanos são necessários, exceto para plugar o equipamento: o processo, como um todo, é automatizado. Imagine-se,



A concentração local de servidores facilita a instalação de dispositivos de espionagem

então, o que não pode ser feito através de estruturas complexas, com recursos imensos, projetadas especificamente para a função. Contando-se, ainda, com o fato de que os satélites, que formam as matrizes da transmissão de dados, não são, comumente, nacionalizados, nos países tecnologicamente dependentes ou atrasados, fica fácil entender como não é absurdo capturar um volume incrível de informações, com relativa prontidão e esforço.

Se restar, ainda, alguma dúvida sobre a extensão e o alcance da espionagem digital, cabe lembrar que muitos ataques fulminantes a membros de grupos terroristas – efetuados por drones, em sua maioria – só foram possíveis, devido à utilização de aparelhos celulares. Eles forneceram não apenas o conjunto de informes que permitiram a identificação positiva dos indivíduos, mas, também, seus sinais foram fonte de referência para o lançamento preciso de mísseis e a consequente destruição dos alvos. Da mesma forma, por meios semelhantes, ocorreram a varredura, a interferência e a anulação de contas bancárias,

cartões de crédito e a obtenção de informações pessoais, que foram feitas sob os auspícios do *Patriot Act*[5], nos EUA. Essas ações permitiram, virtualmente, a anulação da condição de existência civil de muitas pessoas, suspendendo seus direitos – às vezes, sem qualquer acusação clara.

Outra situação relevante é a do Irã. Como foi visto, há pouco tempo, na guerra não declarada dos EUA contra seu antigo aliado, a coleta de informações e a espionagem recorrente levaram à descoberta de fragilidades nos sistemas persas e, como resultado, à utilização de armas digitais. Vírus de grande poder destrutivo foram empregados, como o *Stuxnet* (provavelmente com o apoio de Israel), o *Duqu*, o *Flame*, sem que medidas eficientes pudessem ser tomadas, nem em tempo hábil, nem na escala necessária, para impedir grandes prejuízos. O *Stuxnet*, por exemplo, provocou um "acidente" que varreu do mapa boa parte das pesquisas realizadas nas instalações iranianas de enriquecimento de urânio.

Por todos esses fatores, e outros mais, a espionagem cibernética é um excelente negócio. Por um custo (e risco) ínfimo, quando comparado a outros métodos, é possível obter uma abrangência impressionante de acesso a informações estratégicas. Neste contexto, um caso que merece atenção é, mais uma vez, o da China, país que vem investindo pesadamente em infraestrutura digital, na África, praticamente "presenteando" alguns países com servidores, linhas de acesso, software, assessoria. Os chineses estão interligando escolas, ministérios, empresas públicas e privadas, disponibilizando às nações interessadas as benesses da "sua" internet. Trata-se, obviamente, de puro espírito democrático, do desejo de prestar serviços humanitários, sem quaisquer interesses ou fins lucrativos...

A vigilância, compreensivelmente, tornou-se excepcional ferramenta para a exploração econômica, política e militar. Agora, mais do que nunca, e há um forte lobby para isso, porque montantes gigantescos estão envolvidos no processo. A economia de mercado moderna, transnacional, está toda baseada em sistemas informatizados, e aí reside uma fonte inesgotável de exploração de lucros. Por isso, no caso do Brasil, em especial, com suas riquezas naturais e sua importância no continente, não é possível sequer imaginar que alguém duvidasse que a espionagem – em todos os níveis – vinha acontecendo. A coleta, o armazenamento e a análise de dados, sobre o país, são comuns há anos, promovidas por agências como a NSA (*National Security Agency*), em conluio com empresas de abrangência multinacional – gigantes com lucros maiores do que o PIB de muitos países – como a Microsoft e o Google.

Não que elas precisassem, de fato, empregar tantos esforços. O ex-ministro Nelson Jobim entregou, de mão-beijada, para os norte-americanos, uma série de informações, incluindo dados sobre decisões nacionais estratégicas (como as do infinito jogo de interesses do FX-2, por exemplo). Não por acaso, o governo Bush manteve-se próximo a Jobim

para obter, inclusive, informes regulares sobre conexões brasileiras com os países da América Latina, parceiros europeus e asiáticos. Na miséria que conforma nosso sistema de Inteligência, e na corrupção que é nosso governo, sabe-se lá o que mais não escapa, todos os dias, e por quais vias, em troca de alguns dólares.

E, claro, há o onipresente Facebook. Seu papel, como instrumento de articulação – política, inclusive – e de compartilhamento de informações, é inegável. Mas, como costumo afirmar, "não existe almoço grátis". Como no Google, tudo que ocorre no Facebook é armazenado, consistentemente, a cada interação. Absolutamente tudo. Curiosamente, na construção da estrutura do banco de dados que constitui o Facebook, não há "usuários"; eles (nós...) são identificados como targets, literalmente, "alvos". É algo para se pensar, mesmo, porque, os usuários (diferente do que a maioria pensa) não são os verdadeiros clientes do Facebook. Seus clientes são as grandes empresas e, especialmente, o governo norte-americano, que adquirem as informações, vasculham-nas, dissecam as vidas – já quase que completamente expostas – e tomam decisões sobre elas. Com a ajuda da falta de cuidado generalizada, tudo fica mais acessível. Faz-se necessária uma política de segurança de informação, consistente e permanente, para que se mantenha o sigilo.

O fato mais preocupante, em tudo isso, é que dependemos, profundamente, de tecnologia externa. Israelense, alemã, francesa, norte-

americana, tanto faz: continua sendo externa e, como tal, sujeita às necessidades e interesses de seus governos, e não do nosso. Por isso, privacidade e segurança tornaram-se devaneios, sujeitas à boa vontade – invariavelmente, inexistente, – de potências estrangeiras.

No caso do Brasil, é inconcebível que o governo e nossas forças militares dependam, ainda que em parte, de sistemas desenvolvidos externamente, em setores críticos. Utilizar softwares fechados e proprietários, é suicídio, em potencial. Falhas, desinformação, políticas de preços abusivos – além da óbvia impossibilidade de se possuir o código-fonte – são motivos mais do que suficientes para não utilizar programas desse tipo. A vulnerabilidade, nesse caso, é uma decorrência absolutamente esperada, uma tragédia claramente anunciada. Usuários de sistemas como Microsoft Windows, que o digam.

Mesmo os softwares de criptografia, adquiridos comercialmente e usados, justamente, para proteção de dados, representam perigo. Os detentores de seus direitos possuem informações sobre o acesso ao que foi criptografado, inclusive, infiltrando no código – propositalmente – falhas de

segurança. Somente um indivíduo por demais ingênuo e desinformado acreditaria que isso é mera ficção científica. As empresas que fabricam os softwares visam, logicamente, lucro, e mantêm relações estreitas com seus governos; via de regra, seus engenheiros e proprietários são fiéis depositários das agências de segurança, direta ou indiretamente.

A solução, adequada à nossa realidade, é o desenvolvimento de software nacional, de alta qualidade (quero crer que não nos faltam profissionais, qualificados, para tanto), baseado em sistemas abertos, tais como Linux. Trata-se de investimento em educação e em *know-how*, capaz de gerar soluções relativamente baratas, eficientes, e que podem ser controladas até o mais ínfimo ponto de código, desde que, claro, haja pessoal adequado para a tarefa. Com inteligência, é possível desenvolver excepcionais alternativas, incluindo sistemas de segurança baseados em encriptação avançada; eles existem, até mesmo em versões livres, disponibilizando todo o código para ser vasculhado, a fim de que vulnerabilidades sejam verificadas, e anuladas, já que se configurariam como armadilhas para os dados. Não partiríamos do zero: o que já temos, de bom, deve ser ampliado, repensado, reforçado. E, como bônus, estaríamos formando uma excepcional reserva de competências para o futuro do país.

Solução local, sim. Mas, não, por terceirização. As soluções têm que partir de ações internas. De nada adianta entregar a base para manter o sigilo nas mãos de alguém de fora da estrutura, sujeita a mudanças de governo, de política, de interesses, de humores. A terceirização, nos EUA, demonstrou, em alguns casos, como pode ser crítica, essa postura, no que diz respeito ao vazamento de informações. Os sistemas como um todo e, principalmente, os que dizem respeito à segurança, devem ser produzidos internamente. O fator político tem que ser deixado de lado, em favor da continuidade, lógica e racional, e do investimento a longo prazo.

De certa forma, as invasões digitais estabelecem um estado de guerra permanente que, em muitas nações, passa completamente desapercebido

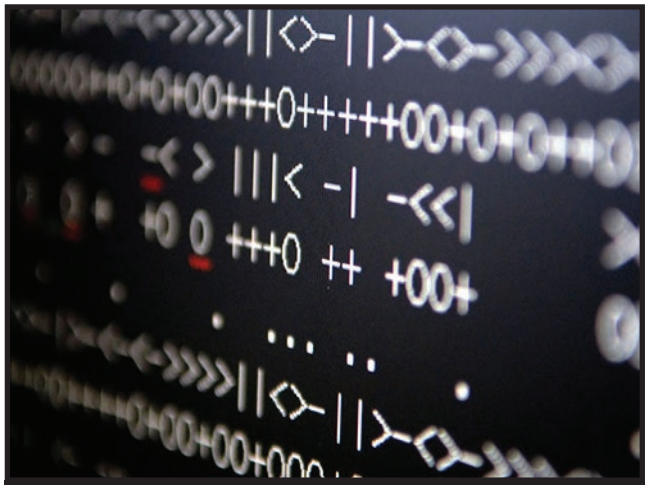
Da mesma forma, o Brasil – como a maior parte do mundo – depende de hardware externo, essencialmente de projeto norte-americano (e, quase sempre, fabricado na China...). Empresas como a Intel Corporation são verdadeiras hidras tecnológicas, senhoras do mercado, que tendem a engolir empresas menores, absorvendo sua tecnologia e devastando sua capacidade criativa, ao incorporar em suas linhas profissionais que, de outra forma, poderiam estra envolvidos em projetos concorrentes. Se, por um lado, isso amplia as possibilidades de termos produtos melhores, por

outro, é uma destruição da variedade, da multiplicidade de escolhas. Trata-se de um risco que não vale a pena correr. Contudo, não temos qualquer alternativa, em caráter nacional. Somos dependentes, ao extremo, da tecnologia que nos é permitida acessar.

Em hardware, pesa, ainda, o singelo fato de que bugs (erros) sérios, nos processadores da Intel (assim como em outras marcas), já foram descobertos, e a empresa só os admitiu, com muita relutância, depois de considerável pressão e sérias repercussões negativas.

Enfim, a questão toda é que somos vítimas, quase que absolutamente passivas, de uma guerra cibernética, perpetrada pelos "grandes". Ficamos no fogo cruzado, porque fomos incompetentes para perceber o grau da ameaça, e ineptos, no que diz respeito aos investimentos necessários, seja em equipamento, seja em pessoal. Por isso mesmo, não há porque, como sugeriram alguns, desvincular acessos a servidores externos e promover uma internet "nacionalizada". Trata-se de uma incompreensão generalizada da situação, o que não seria de se estranhar entre os nobres representantes da nação. Aliás, quem optou por esse caminho foram a China, o Irã, a Coreia do Norte. Não precisamos "fechar" a internet, ou os sistemas abertos de informação. O que precisamos é investir, nacionalmente, em mecanismos decentes de proteção e contra-ataque. Temos que estar prontos para agir, com uma política de prevenção e – com muita ênfase, – de amedrontamento: os golpes continuariam a vir, mas a resposta seria imediata e fulminante, fazendo com que qualquer invasor pensasse duas vezes, antes de tentar novamente.

O fato, é que tantos discursos ocos servem, absolutamente, para nada. Está na hora de começarmos a fazer. Precisamos de gente capacitada – e de dinheiro, bem utilizado – porque já perdemos mais do que podíamos. É impressionante – e perigoso – que tenhamos tantas falhas técnicas e um palavrório tão demagogo sobre algo tão essencial. Faz-se necessária, já, mais ação e menos propaganda. Para que acabe essa impressão de que, na Terra de Alice, não existem quaisquer *experts* em criptografia ou segurança digital; de que não existem especialistas na preservação de informação estratégica. Ou então, vamos admitir, de uma vez por todas,



A criptografia é fundamental para prover algum nível de proteção aos dados

que somos realmente um país mágico, no qual todas as informações são abertas, não têm importância, ou não podem ser consideradas como dignas de serem chamadas de "segredos". Longe disso. No país das Maravilhas,

a democracia é plena, tão grande que chega a ser absurda, cedendo, a tudo e a todos, quaisquer dados, sejam quais forem. Uma festa, uma alegria. A legítima "Casa da Mãe Joana".

Com a aplicação de recursos em soluções nacionais e, de fato, independentes, estaríamos nadando contra a maré, gastando mais, tendo mais trabalho e, principalmente, indo contra o inegável e irreversível processo de globalização, e até perdendo a chance de adquirirmos parceiros valiosos, diriam alguns. Pode ser. Mas, quando se fala sobre segurança nacional, sobretudo militar, a independência é a chave. Até porque, no âmbito bélico, como há a preocupação constante sobre o bem maior, que é a própria nação e seu povo, os projetos tendem a se concluir – não ficam apenas em discursos e presságios. Por exemplo, no Exército, se PAKs[6] forem necessários, certo é que poderão ser projetados e desenvolvidos nacionalmente, e funcionarão. Diferentes de outros PAKs, não virão sem munição, sem cano, ou ficarão, apenas, como esboços no papel. E, principalmente, não serão contados como existentes em inventário, quando são apenas promessas vazias. Não se pode defender um país com quimeras.

Estaremos, então, livres dos riscos? Não, claro que não. Há o fator humano envolvido. E, na maior parte dos casos, é ele o responsável pelos vazamentos de informações críticas. Quase sempre, em busca de vantagens pessoais, mormente financeiras. Até porque, ninguém, em sã consciência, pode acreditar em fidelidade e confiança, num país onde a corrupção é a norma – sobretudo, nos escusos corredores governamentais – e no qual almejam-se fantásticas soluções, pagando salários ridículos a profissionais de alto padrão (e os brasileiros estão entre os melhores do mundo), desviando, ao invés de investir, enquanto o dinheiro escoa, para satisfazer interesses de alguns punguistas engravatados. Sobre isso, convém pensar se, na Terra de Alice, a falta de visão e comprometimento não resultariam – de novo – em catástrofe.

Da invasão, da espionagem, do roubo de dados, a verdade é que fomos pegos "com as calças na mão". Enquanto olhávamos, deslumbrados, o coelho branco passar, com seu relógio *high-tech*, a Rainha de Copas vasculhava nossa maleta. Fizemos besteira, e penso que só há duas explicações para isso: 1) ignorância, o que pressupõe uma demissão imediata dos (ir)responsáveis, por incompetência, ou 2) conivência e muita cara de pau.

Aposto na segunda.

•

Notas:

1 O *sniffer* é um software ou hardware, invasor, e é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores. Conforme o fluxo de dados trafega na rede, o *sniffer* captura cada pacote (os dados, na rede, são transmitidos em "pacotes") e, eventualmente, decodifica e analisa o seu conteúdo, de acordo com protocolos pré-definidos.

2 Também chamado de "cavalo de Tróia", o *trojan* (ou *trojan horse*) é um programa de caráter malicioso, que, normalmente, se oculta em outro programa. Sua função é roubar, e transmitir, informações sobre o computador invadido, permitindo que mais falhas de segurança sejam descobertas e usadas como novos pontos de invasão. Muitos outros tipos de dados também podem ser passados, para quem designou o *trojan*.

3 Tecnicamente, o *Keylogger* é um tipo de cavalo de Tróia. São usados, comumente, para roubar senhas e dados pessoais, associados a crimes financeiros.

4 O endereço IP, de forma genérica, é uma identificação de um dispositivo (computador, impressora, etc) em uma rede local ou pública. Cada computador na internet possui um IP (*Internet Protocol* ou Protocolo de Internet) único, que é o meio que as máquinas usam para se comunicarem na rede.

5 *USA PATRIOT Act* (acrônimo de "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001", em tradução livre: "Lei de 2001 para unir e fortalecer a América, fornecendo instrumentos apropriados requeridos para interceptar e obstruir o terrorismo"), comumente referido como *Patriot Act*, é um controverso ato do Congresso dos Estados Unidos que o presidente George W. Bush assinou, tornando-o lei, em 26 de outubro de 2001. Entre as ações permitidas pelo *Patriot Act* estão a invasão de lares, a espionagem de cidadãos, interrogatórios e torturas de possíveis suspeitos de espionagem ou terrorismo, sem direito a defesa ou julgamento. Na prática, o ato suprime as liberdades civis. Muitos juristas consideram que essa lei facilita a instituição de lei marcial, na eventualidade de qualquer ameaça de terrorismo - real ou imaginária.

6 PAK (*Panzerabwehrkanone*) é a sigla alemã que designa canhões antitanques. Para o bom brasileiro, faz-se desnecessário explicar a que, na verdade, me refiro...

•

F. G. Dillenburg

Sobre o Autor: Fabricio Gustavo Dillenburg tem formação em História e é fundador e responsável pelo Núcleo de Estudos de História Militar Vae Victis. É autor de "Kamikaze: as Invasões Mongóis e as Origens do Vento Divino". Possui certificações Microsoft, bem como experiência em programação e projetos de hardware e software. (*Agradecimentos a Mateus Costa pela discussão técnica*).

AHIMTB/RS

ACADEMIA DE HISTÓRIA MILITAR TERRESTRE DO BRASIL / RS