A utilização da Internet sob domínio cibernético inimigo

Augusto da Silva Guimarães[1]

Introdução

Peter Drucker (1999) cunha o termo "sociedade do conhecimento" e afirma que esta é a grande transformação do século XX. O salto qualitativo que caracteriza a Era do Conhecimento é observado por Helena Lastres (1999) da seguinte forma:

> (...) à conjunção e à sinergia de uma série de inovações sociais, institucionais, tecnológicas, organizacionais, econômicas e políticas, a partir das quais a informação e o conhecimento passaram a desempenhar um novo e estratégico papel. (LASTRES, 1999, p. 8)

Parafraseando Lastres, entende-se que a gestão do conhecimento deixou de ser encarada como um mero processo de suporte para ser a finalidade em si.

A Era do Conhecimento não é uma cisão radical com a sua precedente, a Era Industrial. O salto qualitativo não se deu em um momento crucial em que toda a sociedade foi reorganizada a partir de uma nova base conceitual, não podendo assim, se citar uma revolução. E sim, sucessivas evoluções, que ocorreram de forma assíncrona nas diversas expressões do conhecimento.

Protagoniza essas evoluções o mais poderoso advento da Era do Conhecimento, a Internet — que talvez até seja a expressão máxima desta. Não se pode pensar em colocar a gestão das informações como um processo finalístico desconsiderando essa plataforma.

Francis Fukuyama (1989), em seu ensaio sobre o *Fim da História e o Último Homem*, promulgou que o término da Guerra Fria (GF) em 1989 reduziria os estímulos à Guerra, uma vez que a normalização das democracias liberais seria a panaceia da nova realidade das relações internacionais.

Contudo, a partir da década de 1990 — período em que a Internet se espraiou no meio civil com consequências transversais nas relações humanas —, observou-se uma profusão de conflitos armados de toda sorte de motivos beligerantes.

O **Quadro 1** apresenta um resumo esquemático dos conflitos que aconteceram no corte temporal deste artigo. O objetivo é identificar características recorrentes nestes episódios da política internacional, sobretudo quanto ao balanceamento do poder bélico entre os partidos contendores.

---

[1] Cap Com (AMAN/06), mestre em Ciências Militares (EsAO/15). Atualmente, é instrutor do Curso de Comunicações da EsAO.

Nome do Conflito	Partido A	Partido B	Assimetria
Guerra de Nagorno-Karabakh (1988-94)	República de Nagorno-Karabakh	República do Azerbaijão	Não
Guerra do Golfo (1990-91)	EUA, Arábia Saudita, Reino Unido, França e Egito	Iraque	Sim
Primeira Guerra da Chechênia (1994-97)	Rússia	Chechênia e *Mujahideen* Estrangeiros (a)	Sim
Guerra do Cenepa (1995)	Equador	Peru	Não
Primeira Guerra do Congo	AFDL (a), Uganda, Ruanda, Burundi e Angola	Zaire, ALIR (a) e UNITA (a)	Não
Guerra do Kosovo (1996-99)	Iugoslávia, Rússia e Grécia	Exército de Libertação do Kosovo (a), Albânia e OTAN (b)	Sim
Guerra Etíope-Eritreia (1998-2000)	Etiópia	Eritreia	Não
Segunda Guerra do Congo (1998-2003)	República Democrática do Congo, Zimbabwe, Namíbia, Angola, Chade e Forças *Hutus* (a)	Uganda, Ruanda, Burundi, Forças *Tutsis* (a) e UNITA (a)	Não
Guerra de Kargil (1999)	Índia	Paquistão	Não
Guerra do Kosovo (1999)	Iugoslávia	OTAN (b)	Sim
Segunda Guerra da Chechênia (1999-)	Rússia	República da Chechênia e *Mujahideen* Estrangeiros (a)	Sim
Guerra do Afeganistão (2001-14) e (2015-)	ISAF (a), OTAN (b) e Afeganistão	Talibã (a) e *Al-Qaeda* (a)	Sim
Segunda Guerra do Iraque (2003-11) e Insurgência Iraquiana (2011-)	EUA, Reino Unido, Espanha, Itália, Novo Exército Iraquiano, Curdistão e Polônia	Iraque, Partido *Baath* (a), *Al-Qaeda* (a), Estado Islâmico (a), Exército *Mahdi* (a)	Sim
Segunda Guerra no Líbano (2006)	Israel	Partido Comunista Libanês(a), Frente Popular de Libertação da Palestina (a)	Sim
Operação Chumbo Fundido (2008-09)	Israel	*Hamas* (a)	Sim
Operação Odisseia do Amanhecer (2011)	Conselho Nacional de Transição apoiado por: EUA, Canadá, Reino Unido, Itália, França, Dinamarca, Bélgica, Suécia, Qatar, Espanha, Noruega, Países Baixos e Emirados Árabes Unidos	Líbia dos leais a Gaddafi (a)	Sim
Guerra em Donbass (2014-)	Ucrânia e OTAN	Nova Rússia (a)	Não
Legenda: (a) Grupo ou entidade não-estatal com atividade paramilitar. (b) Organização supranacional.			

Quadro 1 – Resumo esquemático dos conflitos iniciados a partir de 1990
Fonte: www.sohistoria.com.br, www.wikipedia.com, adaptado pelo autor

O mundo cartesiano e linear típico da Era Industrial, em que a fonte de poder era constituída e sinônimo de Estado, já não existe mais. Talvez a bipolaridade da GF, quando se era forçoso o alinhamento ideológico a um dos blocos, mantivesse as aparências.

Contudo, a multipolaridade decorrente do fim da GF revelou a diminuição gradativa de importância que sofre a figura política do Estado. Observa-se no **Quadro 1** que, em onze dos dezessete conflitos listados, estava envolvido algum ator não estatal. As identidades nacionais elegem novos entes políticos em face dos seus anseios de preservação cultural. O reequilíbrio dessas fontes de poder tem sido obtido através de conflitos armados, as Guerras de Quarta Geração. Segundo Lind (2005),

> a Quarta Geração marca a mudança mais radical desde a Paz de Westphalia. Na guerra de Quarta Geração, o Estado perde o monopólio sobre a guerra. Em todo o mundo, os militares se encontram combatendo oponentes não estatais, tais como a al-Qaeda, o Hamas, a Hezbollah e as Forças Armadas Revolucionárias da Colômbia. (LIND, 2005, p. 3)

Diante das tendências apreciadas, percebe-se que o modelo de Guerra de Conquista é típico e mais representativo da Era Industrial; já na Era do Conhecimento, os conflitos são de identidade e representatividade.

Contudo, a despeito da menor probabilidade de que o Brasil tenha um enfrentamento bélico contra um oponente que possa plasmar sua superioridade militar como domínio do espaço cibernético, forças armadas profissionais e permanentes devem desenvolver doutrina, técnicas, táticas e procedimentos (TTP) e tecnologias que se mostrem eficientes no amplo espectro de conflitos e em qualquer gradiente de proporção dos poderes bélicos.

O prefácio do manual EB20–MC-10.205 (Comando e Controle) aborda os conflitos de Quarta Geração e a necessidade de maciços recursos de tecnologia da informação e comunicações (TIC) para alimentar os comandantes militares de informações necessárias para o exercício do comando e controle (C^2).

> Os conflitos armados ocorridos nas últimas décadas demonstram que o tradicional confronto entre atores estatais antagônicos vêm tomando configuração cada vez mais complexa, embora continuem sendo marcados pelo emprego da força.
> Os combates modernos têm se caracterizado pelo uso maciço de tecnologia, pela presença de civis e da mídia no ambiente operacional, pelo emprego de estruturas de combate com maior proteção coletiva, velocidade e letalidade seletiva, pela utilização de aeronaves remotamente pilotadas e pela capacidade de operar no espaço cibernético. (BRASIL, 2015 prefácio, grifo do autor)

Outra característica de dez dos dezessete conflitos listados é o drástico desbalanceamento do poder de combate entre os atores, configurando a assimetria.

Segundo o manual MD51-M-04, Doutrina Militar de Defesa, quanto ao poder de combate, este é assimétrico quando:

> (...) contrapõe dois poderes militares que guardam entre si marcantes diferenças de capacidades e possibilidades. Trata-se de enfrentamento entre um determinado partido e outro com esmagadora superioridade de poder militar sobre o primeiro. Nes-

> te caso, normalmente o partido mais fraco adota majoritariamente técnicas, táticas e procedimentos típicos da guerra irregular. (BRASIL, 2007, p. 25)

A assimetria pode inferir que o inimigo tenha a capacidade de impor o domínio do espaço cibernético e, nessa situação, indaga-se: seria possível estabelecer canais de comunicações de alta capacidade e resiliência prescindindo de explorar a Internet? Ou, o sistema de comunicações que seja estabelecido sem explorar a Internet permitiria produzir e gerir o conhecimento de forma eficiente para que se obtenha a consciência situacional em conflitos típicos de Quarta Geração?

Desenvolvimento

Da própria citação extrai-se a solução. O país em desvantagem deve explorar a Internet empregando majoritariamente TTP não ortodoxas ("típicas de guerra irregular"). Com isso, o potencial de transmissão de informações que a Internet propicia pode ser, em grande parte, utilizado pelo sistema de comunicações em uma guerra em que a assimetria pese ao Brasil.

Ainda de acordo com o do manual EB20 – MC 10.205:

> CAPACIDADE DE COMANDO E CONTROLE – Reflete o valor de uma força armada, em todos os seus escalões, e resulta de um adequado processo decisório, do gerenciamento eficiente das informações e comunicações e da primordial preparação de lideranças, de modo a assegurar o preparo adequado e o emprego operacional eficaz. (BRASIL, 2015, p. 1-2; grifo do autor)

Contrapondo essa citação com a de Helena Lastres, a capacidade de comando e controle é a vantagem estratégica a ser conquistada nos conflitos na Era do Conhecimento.

A Internet permite que o sistema de tecnologia da informação para C^2 ($STIC^2$) consiga prover um fluxo intenso de informações em tempo real — anulando os fatores tempo e distância como variáveis para o planejamento das ligações. Essa possibilidade, contudo, não garante a eficácia do C^2, porque se restringe a diminuir o tempo do recebimento dos substratos do processo decisório, a divulgação e o acompanhamento deste. O processo decisório em si, a arte da guerra, o que garante o acerto das decisões, ainda é competência do comando.

Ou seja, a Internet aumenta a eficiência do sistema de comunicações e não do comando e controle, diretamente, mas cria as condições favoráveis para tal.

O ponto de interrogação nessa situação reside no parâmetro segurança da comunicação. Por não existirem padrões rígidos que atestem um modelo de segurança, os critérios para concepção são subjetivos. Nunca se saberá, com precisão, as reais possibilidades de quem pretende atacar/devassar um $STIC^2$.

Propor um paradigma de segurança para a exploração da Internet em um ambiente de domínio do espaço cibernético imposto pelo inimigo é um desafio de difícil solução.

As características relevantes da Internet para $STIC^2$ são: sua alta capacidade de tráfego de informações, sua disponibilidade em tempo integral e real, sua difícil regulação (fruto dos inquantificáveis roteamentos), a atomicidade dos acessos e sua arquitetura baseada em protocolos.

Os modelos de segurança da informação são constituídos para atender a quatro requisitos fundamentais: disponibilidade, integridade, confidencialidade e autenticidade — constituindo o modelo DICA.

A disponibilidade consiste em haver a possibilidade de acesso à Internet. A integridade visa garantir que a mensagem recebida não foi alterada no seu caminho. A confidencialidade se relaciona com a negação de abertura do dado. A autenticação permite garantir que tanto o emissor quanto o receptor da mensagem sejam quem dizem que são e que não se omitam quanto à emissão ou recebimento da mensagem.

O modelo de segurança é eficaz se garante que a comunicação aconteça de forma idônea entre fonte e destino, ou seja, que negue a possibilidade de qualquer ataque passivo (análise de trafego ou cópias de dados que preservem o original) ou ataque ativo (interrupção, falsificação ou modificação dos dados).

Essa é uma situação assimétrica, pois o invasor conhece o sistema que deseja invadir, enquanto o defensor nunca poderá conhecer na totalidade a capacidade de ataque do invasor. Para diminuir esta assimetria, a próxima seção utiliza o caso Snowden para analisar o *modus operandi* do sistema de vigilância desenvolvido pela National Security Agency (NSA) dos EUA.

Uma releitura do caso Snowden

Os EUA criaram a NSA em 1952 para ser um órgão do sistema de defesa dedicado à inteligência do sinal, ou seja, interceptar e analisar dados oriundos de fontes eletromagnéticas, bem como proteger as comunicações oficiais. Os instrumentos de inteligência cresceram de importância diante do caráter difuso que as ameaças têm nos conflitos de Quarta Geração.

As informações reveladas por Edward Snowden, técnico a serviço da NSA, que analisava os dados obtidos pelos sistemas de monitoramento, permitem traçar, de forma mais ampla, a doutrina de monitoramento do espaço cibernético que um país, ou coalizão de países, com poder militar incontestavelmente superior ao brasileiro, tem para impor seu domínio no espaço cibernético.

O sistema montado e gerenciado pela NSA contava com a cooperação dos países signatários do Tratado de Segurança UK-USA, que foram denominados os cinco olhos (*the five eyes*), que são: EUA, Inglaterra, Canadá, Austrália e Nova Zelândia. Estes países compunham a rede Echelon. Por hipótese, o inimigo também usufrui desta rede.

A rede Echelon propicia uma imensa amostra de dados para que se apliquem as técnicas de mineração dos metadados. Consiste em identificar ligações que contém em seu conteúdo palavras-chave arbitradas pelo elemento que monitora a rede (análise de conteúdo) combinando com padrões de comunicações que fogem aos parâmetros estatísticos de normalidade (análise de tráfego).

Os principais programas de vigilância que os membros da rede Echelon compartilhavam eram: PRISM, Xkeyscore e Fairview.

O PRISM é um programa de vigilância que permite à rede Echelon obter dados estatísticos dos acessos às principais suítes de aplicações na Internet, como Google, Microsoft, Apple, Yahoo!, Facebook, YouTube, AOL, Paltalk e Skype.

Esse programa permitia aos seus usuários criar inferências estatísticas para análise de tráfego em relação aos horários de acesso, tempo de conexão, rede de conexões por *e-mail* (quais contas de *e-mail* costumam se comunicar) a partir dos dados brutos dos assuntos pesquisados nos motores de busca da Internet etc.

Outro programa disponibilizado para a rede Echelon foi o XKeyscore. Esse programa permite acessar qualquer conta de *e-mail* dos servidores cooptados e em tempo real as ações dos usuários destas suítes de serviços.

Completando o sistema, o programa Fairview permitia redirecionar as comunicações dos países estrangeiros para os bancos de dados da NSA. As gigantes das telecomunicações cooptadas firmam parcerias com as empresas dos países estrangeiros; dessa forma, esse acordo empresarial permitia o acesso indireto da NSA à infraestrutura informacional dos países estrangeiros.

Esses programas caracterizam o domínio da "nuvem", ou seja, os principais nós troncais das incalculáveis rotas lógicas existentes na Internet podiam ser perfeitamente acessados pela NSA.

Uma solução

Para a concepção deste artigo, uma rotina de acesso à Internet é tida como segura, se atender aos requisitos do modelo DICA ante as técnicas de mineração de dados aplicadas pela rede Echelon. Para tal, essa rotina deve garantir que:

a) as estações configurem um tráfego de acordo com os padrões estatisticamente comuns de acesso; na prática, que usem protocolos e serviços típicos para os usuários domésticos, como HTTP (porta :80 ou :8080), HTTPS (porta :443) e não tenha seu IP mascarado por *proxy* anônimo público; e

b) a informação produzida também se adapte aos padrões médios de formatos (extensões do tipo .jpg, .doc, .ppt, .mp3 etc.) em tamanhos relativamente comuns para a extensão considerada.

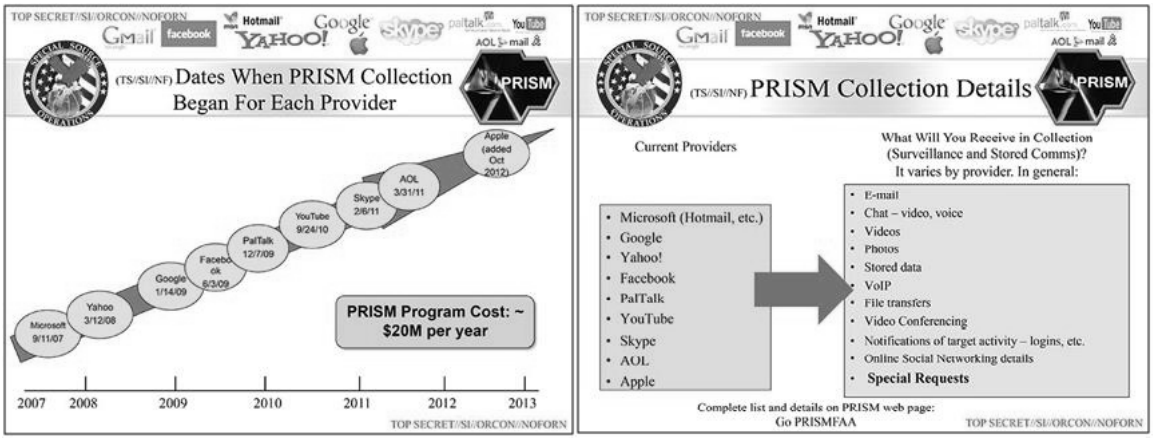

Figura 1 – Cronologia e serventia do PRISM

Fonte: www.br.wikipedia.com, a partir de dados da NSA vazados

Também caracteriza o problema a presunção de que o inimigo, na fase da consolidação da invasão militar, permita que as pessoas comuns gozem de aparente normalidade. Observa-se aqui que a opinião pública local também é um objetivo militar, portanto, não deverá haver a negação dos serviços públicos. Sendo assim, no espaço cibernético, a normalidade se traduziria na possibilidade de as pessoas acessarem seus *internet-banking*, realizarem cursos de ensino a distância etc.

Conclui-se que, para o inimigo implementar um sistema global de vigilância eletrônica, ele define como estratagema uma combinação de técnicas de mineração de dados. Primeiro, vasculha-se o conteúdo trafegado a partir de busca por palavras-chave. Identificando-se as estações que acessam ou hospedam conteúdo "alvo", analisa-se o tráfego, criando-se inferências estatísticas e, principalmente, rastreio de IP para identificar os operadores.

Para estabelecer uma rotina que atenda aos pressupostos acima configurados, aplicou-se um questionário aos militares voluntários do Centro de Defesa Cibernética (CD Ciber), do Centro de Instrução de Guerra Eletrônica (CIGE) e do 1º Batalhão de Guerra Eletrônica (1º BGE), possuidores do Curso de Guerra Cibernética ou atuadores dessa atividade, no período de 24 de junho a 10 de julho de 2015, o qual obteve vinte e uma respostas.

Estas respostas foram consolidadas e analisadas pelo autor em conjunto com o entrevistado, o investigador Marcelo Coimbra da Polícia Civil do Estado do Rio de Janeiro (PCERJ), que compõe o corpo técnico da Delegacia de Repressão aos Crimes de Informática (DRCI).

Ao final, a proposta de acesso que melhor configuraria o modelo DICA ante a Rede Echelon consiste em utilizar os citados serviços normais da Internet como cachês de mensagem.

Por serem serviços normais, ou seja, de comum acesso, não fugiriam aos padrões estatísticos de acesso diminuindo a relevância da análise de tráfego.

Com prerrogativas de *logins* (acesso com identificação de usuário e senha) especiais, os operadores acessam páginas que contém as mensagens operacionais. Esses serviços, normalmente, utilizam a aplicação HTTPS, ou seja, com um módulo Secure Socket Layer (SSL), que encripta a transmissão dos dados.

Para evitar suspeitas e a busca deliberada por palavras-chave das técnicas de vigilância de redes conhecidas, os módulos de encriptação devem ser certificados e distribuídos desde a paz estável e ter sua utilização ampla para não fugirem aos padrões de normalidade estatística.

Assume-se que os membros da Echelon têm condições de quebrar os códigos SSL; portanto, para aumentar a segurança, esses módulos devem ter seus algoritmos constantemente atualizados.

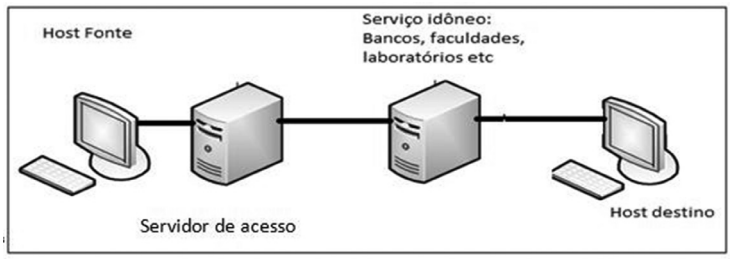

Figura 2 – Acesso a partir de terceiros idôneos
Fonte: o autor

Ainda conclui-se que a produção da informação deve contar com a sobreposição dos seguintes recursos: esteganografia com criptografia simétrica com chaves criptografadas assimetricamente.

Também se deve pensar em segurança física. Uma vez que a rastreabilidade do acesso poderá ser feita pelo gestor de tecnologia da informação (TI) do invasor, só haverá confirmação se forem encontradas provas que relacionem o conteúdo aos operadores. Uma forma em que isso poderia ocorrer seria com a apreensão do computador que gerou a conexão.

Dessa forma, medidas de segurança física devem ser adicionadas. Exemplifica este conceito o desenvolvimento de um *pen drive* que autoexecute todas as configurações necessárias para que o acesso se dê através de uma máquina virtual. Isso garante que não se deixariam rastros no terminal de acesso que, mediante perícia técnica, comprovariam a ligação do acesso com a exploração da Internet por parte do operador do Exército.

A solução do estado islâmico

A reportagem publicada pela Folha de São Paulo em 17 de setembro de 2015 apresenta uma possível solução encontrada pelo Estado Islâmico (EI) para explorar de forma não ortodoxa a rede mundial de computadores para se comunicar com suas células terroristas e planejar os atentados de 2015 em Paris.

Segundo a reportagem, o ministro do Interior belga, Jan Jabom, teria afirmado:

> A pior comunicação [para se monitorar] entre esses terroristas é via Playstation 4 (...) É muito difícil para os nossos serviços [de espionagem] — não apenas os belgas, mas serviços internacionais — decodificar a comunicação que é feita via Playstation 4. (FOLHA DE SÃO PAULO, 2015)

Os consoles Playstation 4 (PS4) permitem jogos *online* com diversos jogadores simultâneos (jogos *multiplayers*). Para tal, constituem uma rede segregada a Playstation Network (PSN), que permite aos jogadores estabelecer redes de comunicação gráficas e de voz.

Por ser uma tecnologia popular e segregada (com sistema de encriptação próprio) a PSN oferece um grande desafio para o estabelecimento de métricas para a análise de tráfego. Segundo a detentora, Sony, são mais de 29 milhões de contas ativas.

Por vezes, os jogos apresentam um contexto muito próximo ao da realidade de ataques terroristas; portanto, a análise de conteúdo não consegue perceber que a exploração de termos como "bombas", "explosão", "explosivos" como suspeita. Esses são os termos típicos da rede, ou seja, não se destacam estatisticamente para a análise de conteúdo.

Conclusão

O tema deste trabalho se relaciona com as Guerras Assimétricas, e adotou-se como referencial a posição desvantajosa, por criar os maiores desafios à resolução do problema científico. Porém, em outros tipos de Op, como as de apoio aos órgãos governamentais (Op AOG) e de pacificação (Op Pac), o Exército estaria em posição mais vantajosa, e os agentes perturbadores da ordem pública (APOP) poderiam se valer de TTP não ortodoxas para acessar a Internet e exercer seu C^2.

Sendo assim, ao mudar-se de perspectiva, este trabalho também gera conhecimento no campo da Inteligência Cibernética.

Referências

BRASIL. Exército. Estado-Maior. **EB20-MF-10.205**: Comando e Controle. 1ª Edição/2015.

_____. Ministério da defesa. **MD51-M-04:** Doutrina Militar de Defesa. 2ª Edição/2007.

COSTA, Celso José; FIGUEIREDO, Luiz Manoel Silva. **Introdução à criptografia**. Rio de Janeiro, UFF / CEP - EB, 2007.

DRUCKER, Peter. **Desafios Gerenciais para o Século XXI.** São Paulo, Thompson Learning, 1999.

FUKUYAMA, Francis**. The end of history.The national interest**, California 1989.

LIND, Wiliam S. **A quarta geração de conflitos.** Disponível em: <http://www.ecsbdefesa.com.br/fts/MR%20WSLind.pdf>. Acesso em: 2 de fevereiro de 2015.

LASTRES, Helena M. **Informação e globalização na era do conhecimento.** Rio de Janeiro, Campus, 1999.

EI dribla vigilância ao se comunicar por Playstation, diz especialista. **Folha de São Paulo**, SP, 2015. Disponível em: <http://www1.folha.uol.com.br/mundo/2015/11/1707486-ei-dribla-vigilancia-ao-se-comunicar-por-playstation-dizem-specialistas.shtml>. Acesso em 11 de abril de 2016.

SONY. Playstation Network. Disponível em: <http://br.playstation.com/psn/>. Acesso em 11 de abril de 2016.

NR: A adequação do texto e das referências às prescrições da Associação Brasileira de Normas Técnicas (ABNT) é de exclusiva responsabilidade dos articulistas.