RESUMO

De Fukuyama a Furukawa ou o Fim dos Fios? A importância estratégica do cabeamento estruturado para a segurança e a defesa cibernéticas no Brasil

Em um mundo cada vez mais sem fio, será que, realmente, fios e cabos – metálicos e ópticos – ainda possuem relevância? Em outras palavras, pode-se afirmar, em termos fukuyiâmicos, que a tecnologia sem fio (wireless) decreta 'o fim da história' para o cabeamento estruturado? O presente trabalho defende a hipótese que não, e, especificamente para os Estudos de Defesa, assevera que o surgimento da chamada guerra cibernética torna o cabeamento estruturado elemento impulsionador para se pensar estrategicamente o desenvolvimento do Brasil. Assim, o objetivo geral deste trabalho é apresentar o cabeamento estruturado como um nicho a ser melhor pensado pela base industrial de defesa (BID) brasileira.

Palavras-chave: Cabeamento estruturado. Estudos de Defesa. Segurança Cibernética.

ABSTRACT

Do is truethat, inan increasingly wireless world, wires and cables - metallic and optical one - are still relevant? In other words, can one say in, Fukuyama's terms, that wireless technology decrees 'the end of history' for structured cabling? This paper defends an opposite hypothesis, and specifically for the Defense Studies, asserts that the emergence of the so-called cyberwarfare makes structured cabling a driving force for strategic thinking about Brazil's development. Thus, the general objective of this paper is to present structured cabling as a niche to be better thought by the Brazilian industrial defense base (IDB).

Keywords: Strutucturecabling. DefenseStudies. Cyber security.

De Fukuyama a Furukawa ou o Fim dos Fios? A importância estratégica do cabeamento estruturado para a segurança e a defesa cibernéticas no Brasil

Gills Vilar Lopes[1]

INTRODUÇÃO

A proliferação das redes sem fio ou wireless/Wi-Fi[2], realidade cada vez mais latente no século XXI, não representa, em termos fukuyiâmicos, "o fim dos fios" e dos cabos de redes de computadores. Essa tese pode ser vislumbrada sob diversos ângulos, mas, aqui, escolhem-se os Estudos de Defesa, por meio dos quais se pretende lançar luz sobre os aspectos estratégico-militares do cabeamento estruturado, tema assaz negligenciado pela Base Industrial de Defesa (BID) brasileira.

Antemão, informa-se que o título deste trabalho faz uma dupla alusão, com fins marcadamente estilísticos, a dois importantes elementos para o desenvolvimento, nos anos 1990, dos debates sobre democracia, de um lado, e da expansão da Internet, do outro. O primeiro deles remete à ideia central contida no famoso livro "O fim da história e o último homem", de Francis Fukuyama, em que o autor estadunidense defende, "grosso modo", que, com o fim da União das Repúblicas Socialistas Soviéticas (URSS), o mundo testemunharia o último e mais avançado sistema político, baseado no tripé democracia-liberalismo-capitalismo (FUKUYAMA, 1992). Já o segundo elemento diz respeito à maior fabricante de equipamentos físicos de redes de computadores do mundo, qual seja: a japonesa Furukawa Eletric. Tratam-se, pois, de dois elementos-chave, que, quando juntadas suas principais ideias e objetivos, parecem, à primeira vista, ser confluentes, mas que, como se defende

1 Gills Vilar Lopes. Doutor em Ciência Política pela UFPE e Especialista em Cybersecurity pela National Defense University (NDU). Professor Adjunto de Ciência Política na Universidade Federal de Rondônia (UNIR).

2 Chama-se popularmente de Wi-Fi "a família de protocolos de transmissão por rádio (802.11a, 802.11b e 802.11g)" (WNDW, 2008, p. 3).

aqui, não o são, sobretudo do ponto de vista estratégico-militar.

Assim como a ocorre com a interpretação feita por Fukuyama (1992), a premissa do "fim dos fios" é falaciosa. Outrossim, advoga-se em favor de se pensar a segurança e a defesa cibernéticas não apenas a partir do software, mas também do hardware, isto é, desde a proteção – física – de cabos submarinos, servidores com cadeados, travas biométricas e no-breaks, passando pela indicação, via software, das potenciais fontes de interferência na transmissão da informação em uma rede de computadores. Nesse sentido, assume-se que a informação é um dos principais ativos estratégicos do século atual, e, como tal, seus meios de propagação – seja o sem fio, seja o cabeado – e de proteção devem ser melhor tratados pela BID.

Para corroborar essa hipótese de que a tecnologia sem fio não decreta o fim do uso estratégico dos fios nas segurança e defesa cibernéticas, utiliza-se metodologicamente o estilo qualitativo de pesquisa. Suas fontes primárias provêm dos principais normalizadores sobre esse assunto tanto no Brasil quanto alhures, quais sejam: a American National Standards Institute (ANSI); a Associação Brasileira de Normas Técnicas (ABNT); a já extinta Electronic Industries Alliance (EIA); a International Electrotechnical Commission (IEC); e a International Organization for Standardization (ISO). A revisão de literatura pauta-se, basicamente, em um diálogo entre os subcampos de Segurança Internacional e de Redes de Computadores, em que pesem especificamente três de seus temas, a saber: o Cabeamento Estruturado, a Segurança Cibernética e a Defesa Cibernética.

O presente artigo divide-se em duas partes principais. Na primeira, contextualiza-se o lugar estratégico para o cabeamento estruturado, qual seja: o amálgama entre segurança e defesa cibernéticas. Na segunda parte, discute-se o cabeamento estruturado em si, bem como o fato de que o século XXI não atesta o fim dos fios, mas, sim, o seu crescimento, criando-se, assim, um nicho a ser explorado pela BID brasileira.

SEGURANÇA CIBERNÉTICA E DEFESA CIBERNÉTICA NO BRASIL

Grosso modo, lida-se aqui, de forma precípua, com o espaço cibernético ou, simplesmente, ciberespaço. Mas cuidar de um tema tão abrangente como esse pode fazer com que erros incorram na análise e, por conseguinte, em suas conclusões político-estratégicas. Para evitá-los, esta subseção busca situar metodologicamente suas unidades e níveis de análise. Ademais, a filiação epistemológica deste trabalho se situa em uma zona cinzenta que flutua entre duas áreas científicas aparentemente distantes, quais sejam: a Ciência Política e a Ciência da Computação. Portanto, visa-se aproximar e manter um diálogo entre essas descendentes das Ciências Sociais e das Ciências Exatas, respectivamente.

Conforme apregoam os dois principais autores sobre guerra cibernética, Clarke e Knake (2012, p. xii), gerações diferentes de analistas pensam o ciberespaço também de forma diferente. Assim, vislumbra-se que, no período compreendido entre os últimos 10 anos do século XX e os 10 primeiros do XXI, vários autores versaram sobre o ciberespaço sob os mais diversos prismas. Por exemplo, Castells (1996) afirma que o uso compartilhado das tecnologias de informação e comunicação (TIC) fazem emergir uma nova Era ancorada em uma sociedade em rede (network society). Já Lévy (2001) foca a emergência de uma nova cultura baseada em relações sociais intermediadas por computadores. No âmbito das

relações internacionais, emerge o conceito de poder cibernético (cyber power), de Nye Jr (2011), segundo o qual os países estariam se defrontando com uma nova roupagem do poder no século XXI, amparada não apenas na luta por poder em termos bélicos, econômicos ou culturais, mas também informacionais. Em todos esses casos, o ciberespaço é descrito e/ou entendido como um meio em si mesmo.

Mas é à luz dos Estudos de Defesa que se observa a emergência de uma literatura especializada que atrela questões de segurança internacional e de defesa nacional com o uso estratégico do ciberespaço, ou seja, emergem-se os estudos de segurança e de defesa cibernéticas. Arquilla e Ronfeldt (1993) são praticamente os inauguradores de tal literatura, quando proclamam que a guerra cibernética (cyber war) está chegando aos Estados cujos sistemas de comando, controle e comunicação (C3) militares estão fortemente baseados e amparados em redes de computadores. Todavia, quase duas décadas foram necessárias para que essa afirmação pudesse ecoar no mundo real.

Em meio à busca por novas fontes de insegurança à soberania dos Estados Unidos da América (EUA), aponta-se para o fato de que as novas ameaças provenientes do ciberespaço (cyber threats) constituem desafios imperiosos àquele Estado (OBAMA, 2009) e que podem ser respondidas até mesmo com o uso convencional de ataques bélicos (GORMAN; BARNES, 2011). Enviesados nessa assertiva, Clarke e Knake (2012) lançam pilares para se repensar a proteção das estruturas estratégicas – antigamente chamadas de infraestruturas críticas – baseadas em redes de computadores, pois, de acordo com eles, são justamente esses tipos de infraestruturas – como hidroelétricas, gasodutos, sistemas gerenciadores de trânsito aeroportuário, usinas nucleares etc. – os principais alvos para um ataque terrorista ou, mesmo, em um contexto de conflito bélico interestatal (CLARKE; KNAKE, 2012).

Diferentemente, pois, do que ocorre nas searas da Antropologia, Ciência da Informação ou Sociologia, o ciberespaço não é mais visto, pelos estrategistas e analistas internacionais, apenas como um meio, mas igualmente como um fim em si mesmo. Não é por menos que, por exemplo, o setor militar[3] dos EUA o compreende como sendo um domínio – ao lado do ar, da terra, do mar e do espaço sideral – e o do Brasil o aloca como um setor estratégico (BRASIL, 2012b).

Aqui, cabe uma brevíssima diferenciação entre segurança e defesa cibernética.

No que concerne à segurança cibernética, tem-se que a esfera civil da administração pública federal (APF) brasileira também possui suas próprias diretrizes, políticas, ações e órgãos específicos para implementar e salvaguardar o ambiente cibernético. Por exemplo, no âmbito da extinta Secretaria de Assuntos Estratégicos (SAE) e do atual Gabinete de Segurança Institucional (GSI)[4] da Presidência da República, é possível perceber que análises prospectivas e situacionais são arroladas, no sentido de se criar uma cultura de segurança cibernética entre os servidores públicos federais, bem como um nicho para se pensar estrategicamente a proteção de estruturas estratégicas baseadas em redes de computadores.

3 Na acepção de Buzan, Wæver e Wilde (1998, p. 1-2, 27), "setores" são pontos de vista inseparáveis do todo – que, neste caso, é o sistema internacional –, os quais selecionam e separam certas interações, distinguindo-as entre militar, político, societal, econômico e ambiental. Descendentes dos pensadores da Escola de Copenhague, como Hansen e Nissenbaum (2009), já defendem a tese de que o setor cibernético pode ser considerado o sexto desses setores.

4 O GSI tem uma relação com a seara militar assaz estreita, fazendo com que a capilaridade entre segurança e defesa cibernéticas se ramifique ainda mais.

Sobre a defesa cibernética no Brasil, pode-se iniciar dizendo que a Estratégia Nacional de Defesa (END) elenca três setores como estratégicos tanto para a defesa nacional quanto para o desenvolvimento nacional, a saber: o nuclear, o espacial e o cibernético (BRASIL, 2012b), sendo este último levado a cabo pelo Exército Brasileiro. Nesse viés, o "braço forte e a mão amiga"[5] das Forças Armadas brasileiras é o encarregado por buscar a autonomia do País, no que tange às tecnologias cibernéticas, fulcrais para resguardar e implementar os sistemas de comunicação e informação estratégicos brasileiros. Esta é, portanto, a seara da Defesa Cibernética, que, no Brasil, é regulamentada por seu próprio documento, a Política Cibernética de Defesa (PCD), a qual é centrada no Sistema Militar de Defesa Cibernética (SMDC), cujo carro-chefe é o Centro de Defesa Cibernética do Exército (CDCiber), a ser transformado em Comando de Defesa Cibernética das Forças Armadas.

Não obstante essas diferenciações – que envolvem, sobretudo, quem deve atuar e como – segurança cibernética e defesa cibernética são espécies do mesmo gênero – Segurança da Informação –, a qual é levada a cabo tanto por agentes militares quanto civis, na esmagadora maioria dos países, quando pensadas como uma política pública.

Em âmbito internacional, a ISO e a IEC são referências para as boas práticas de Segurança da Informação, por meio de normas que versam, de maneira precípua, sobre a confidencialidade, a integridade e a disponibilidade da informação (ISO/IEC, 2005). Nessa busca por normatização em matéria de Segurança da Informação, o Brasil é um dos países – ao contrário de EUA e Canadá, por exemplo – que recepcionaram uma norma internacional por meio de uma nacional, qual seja: a ABNT NBR ISO/IEC 27002:2013 (ABNT, 2013). Além disso, o próprio GSI busca disciplinar a gestão de Segurança da Informação e Comunicações (SIC) na APF direta e indireta (BRASIL, 2008).

Assim, no que tange especificamente à Segurança da Informação na esfera pública federal brasileira, utiliza-se o conceito de SIC, ou seja, "ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações" (BRASIL, 2008, p. 6). Além disso, o diálogo entre a Segurança e a Defesa Cibernética se mostra latente, uma vez que a SIC "[...]é a base da Defesa Cibernética [no Brasil] e depende diretamente das ações individuais; não há Defesa Cibernética [portanto] sem ações de SIC" (BRASIL, 2012, p. 11).

Nesse sentido, embora os setores militar e político – civil – atuem em suas próprias esferas de competência, observam-se algumas áreas/situações em que a atuação pode ocorrer de forma conjunta, compartilhada ou, até mesmo, isolada, mas que cujas tecnologias não dizem respeito exclusividade a um ou a outro campo. Um desses exemplos é justamente o uso estratégico do cabeamento estruturado, que, como se vê abaixo, é regulado por normas internacionais e que, portanto, possui reserva de mercado não apenas para as indústrias que provêm material estratégico para os órgãos de Segurança Pública como também de Defesa no Brasil e também no exterior.

O CABEAMENTO ESTRUTURADO E O FIM DOS FIOS

Como salienta Marin (2013, p. 19), "nenhuma outra área de tecnologia cresceu tanto nos últimos anos como a de redes [computacionais] locais[...]". Em 30 anos, tanto a largura de

5 Slogan do Exército Brasileiro.

banda – do inglês, bandwidth, que é medida em mega-hertz (MHz) – quanto a velocidade de transmissão, medida em gigabit por segundo (GB/s), aumentaram vertiginosamente. Em uma era cada vez mais interconectada e interdependente, não é raro observar que o polo do espectro que ruma à dependência das TICs se volta para uma posição mais extrema. Pegue-se, por exemplo, os dois últimos conflitos bélicos em que a Rússia esteve envolvida – contra a Geórgia em 2008 e contra a Ucrânia em 2014 – e perceber-se-á que, no século XXI, quanto mais dependente da Internet, mais passível a danos causados por uma guerra cibernética um Estado está[6]. Diante desse cenário, preocupar-se com os ativos de redes de computadores que envolvem, principalmente, estruturas estratégicas que lidam com segurança e defesa cibernética tem se tornado uma constância mundial, ainda mais para o Brasil, que teve, dentre outros, seu Chefe de Estado alvo da espionagem cibernética internacional, delatada por Edward Snowden. Mais crítico, ainda, é perceber que padronizar e normalizar projetos de cabeamento estruturado prediais e não prediais também tem se constituído praticamente um hábito mundial[7].

Este artigo não questiona a importância de se normalizar tais equipamentos e suportes, porém lança luz sobre o fato de que essas normas estão sendo seguidas não apenas por profissionais civis, mas também militares. O que abre duas opções antagonistas para as forças armadas brasileiras, quais sejam: ou deixar de seguir o padrão internacional e investir em um modelo próprio e, portanto, difícil – mas não impossível – de ser sabotado; ou, então, não se acomodar como mero importador de equipamentos e tecnologias – desde os mais simples como os conectores dos cabos aos mais complexos como servidores data center – e investir em sua produção nacional, o que, por si só, ensejará mais pesquisa e desenvolvimento (P&D) em ciência e tecnologia (C&T) no País. É aqui que entra a importância qualitativa e quantitativa do cabeamento estruturado para o fomento às empresas e órgãos que alimentam a cadeia da BID brasileira.

Cabeamento Estruturado pode ser visto como uma subárea acadêmica e profissional de Redes de Computadores, bem como "[...]um ramo específico de telecomunicações e infraestrutura de TI" (MARIN, 2013, p. 20). Seu objetivo é prover, com o máximo de tempo e o mínimo de infraestrutura possíveis, soluções de compartilhamento de serviços relacionados a dados, voz e imagem, sem necessariamente depender de um determinado fabricante.

Embora seu nome seja "cabeamento", a infraestrutura física em torno dessa subárea não diz respeito apenas aos cabos e fios, embora estes sejam imprescindíveis para a mesma. Nesse sentido, há basicamente duas grandes famílias de cabos, quais sejam: os metálicos de pares traçados[8] e os de fibra óptica. Pelo fato intrínseco de um cabo metálico possuir extremidades, é necessário que haja comunicação entre suas duas pontas, o que é feito, geralmente, por um conector RJ-45 "macho", o qual se acopla à entrada "fêmea" de uma placa de rede Ethernet.

Há, ainda, vários outros aspectos técnicos que são levados em conta na hora de se estruturar um cabeamento, tais como: impedância, tipo do cabo (metálico ou óptico), ambiente

6 Sobre esse assunto, ver Clarke e Knake (2012).

7 Por exemplo, embora a Categoria 5e (100MHz) seja a mais popular no cabeamento estruturado, e a Categoria 7 (600MHz) tenha sido recém-lançada com pouquíssima implementação, já se discute a de Categoria 8 (~2000MHz), sem se esquecer de que tudo começou com meros 16MHz (MARIN, 2013, p. 15).

8 Que, por sua vez, podem ser sem blindagem – os chamados Unshielded Twisted Pair (UTP) – e os com blindagem ou ShieldedTwistedPair (STP).

(temperatura, pressão, animais "roedores" que vão desde ratos a tubarões), cobertura da área etc. Enfim, inúmeras são as variáveis a serem projetadas. Nos últimos anos, tem-se preferido as fibras ópticas aos cabos metálicos, pois aquelas permitem largura de banda e segmentos maiores, não possuindo interferência eletromagnética, já que seu princípio fundamental é a propagação da luz. Todavia, pelo custo ainda elevado dos periféricos relacionados ao cabeamento óptico – hubs, aparelhos de testes, certificações e conexão etc. –, a utilização de cabos metálicos ainda se mostra assaz compensadora.

Não é objetivo deste trabalho esmiuçar os detalhes técnicos por trás do cabeamento estruturado. Apenas com essas informações pode-se perceber a existência de outros aparelhos[9] que não apenas os cabos em si; isso sem contar a parte lógica de sistemas e software e as ferramentas auxiliares que dão vida ao cabeamento estruturado.

O Wireless, como já frisado, está cada vez mais popular em todo o globo. Porém, não há como se criar uma rede totalmente sem fio, haja vista que ela necessitaria, de uma forma ou de outra, de alguma conexão física, com fio. Por exemplo, apesar de ser possível navegar na Internet com apenas um celular, o cabeamento físico pode ser evidenciado nos data centers da operadora de telefonia móvel a que o chip do celular está atrelado. Essa é também a explicação por trás do próprio conceito de Internet, ou seja, a existência de uma rede mundial de computadores atrela-se à existência de infraestrutura física que faça com que as redes de computadores se interconectem. No caso específico das redes sem fio, a informação trafega por meio de ondas eletromagnéticas moduladas, pelo ar, mas, mesmo assim, ela precisa ser recebida ou enviada por um transmissor físico. Em ideia parecida, WNDW (2008, p. 3) atribui à rede sem fio o caráter de meio, e não de fim em si mesmo: "Wireless pode ser utilizado de muitas maneiras, como uma simples extensão (como um cabo Ethernet de vários quilômetros) até um ponto de distribuição (como um grande hub)". Ademais, em locais cujo ambiente apresente clima, temperatura, topologia e pressão extremos, a transmissão por fio ou cabeada (wire) é sempre preferida, como ocorre com os cabos submarinos.

Além disso, as normas nacionais e internacionais recomendam que, ao final de um projeto de cabeamento estruturado, deve haver um teste de certificação para, dentre outros, poder: evidenciar e corrigir eventuais conexões cruzadas[10] – nos pares – e conexões malfeitas; assegurar-se de que a transmissão da informação – seja dado, seja voz, seja imagem – está ativa e sem ruídos/interferências; e certificar-se de que as normas internacionais da EIA/TIA foram seguidas. De acordo com Marin (2013, p. 20), "[...]o cabeamento é uma das questões mais críticas para a implementação de uma rede[...]. Por isso, [...]deve ser feito [...] com base em normas e diretrizes de projeto".

O Quadro 1 relaciona as principais normas e seus objetos, no que se refere ao cabeamento estruturado.

9 Tais quais: conectores, amplificadores de sinal, placas e servidores.

10 As linhas cruzadas – crosstalk ou diafonias – mais comuns são as seguintes: Next e Fext. A primeira envolve um transmissor local em um receptor local, e a segunda, um transmissor local em um receptor remoto. Os principais testes e medidores para elas são os seguintes: Attenuation-to-Cross talk Ratio (ACR) e Skew Delay e Return Loss (RL).

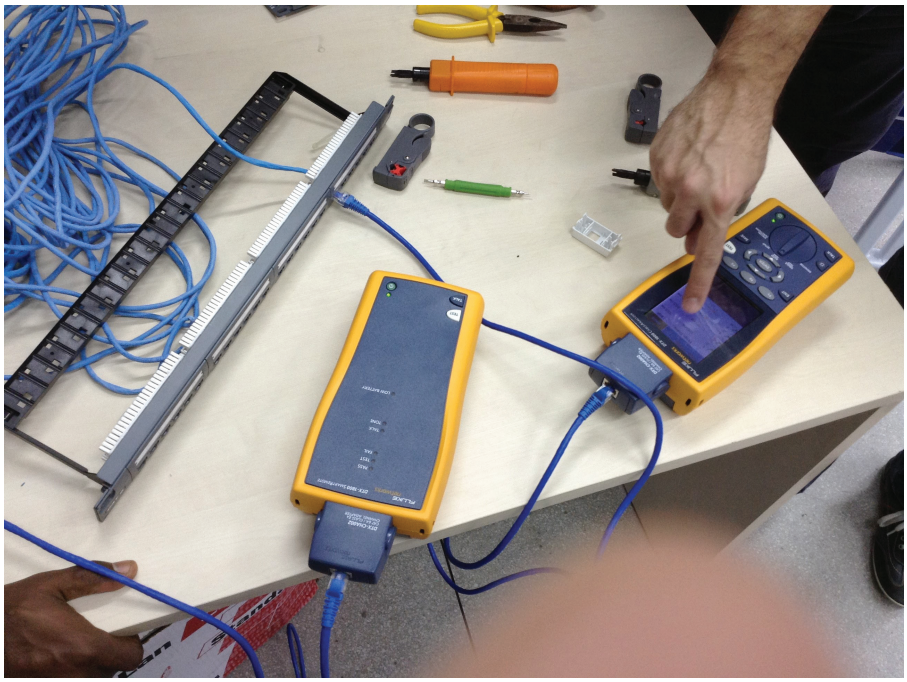
Quadro 1 – Normas sobre cabeamento estruturado

TIPO	NOME	CONTEÚDO
Geral	ANSI/TIA-568-C.0	cabeamento estruturado para as dependências do cliente
	ANSI/TIA-569-C	infraestrutura predial para cabeamento
	ANSI/TIA-606-B	gerenciamento do cabeamento estruturado
	TIA-607-B	aterramento para cabeamento de telecomunicações
	ANSI/TIA-862-A	automação predial (BAS)
Específico	ANSI/TIA-568-C.1	cabeamento estruturado para edifícios comerciais
	ANSI/TIA-570-C	cabeamento residencial
	ANSI/TIA-758-B	cabeamento de planta externa
	ANSI/TIA-942-A	infraestrutura de telecomunicações para data centers
	TIA-1005-1	cabeamento industrial
	ABNT NBR 14565:2013	cabeamento estruturado para edifícios comerciais e data centers
para componentes e teste de cabeamento balanceado	TIA-1158	teste de campo de cabeamento balanceado
	ANSI/TIA-568-C.2	cabeamento e componentes metálicos
	ABNT NBR 6814:1986 Versão Corrigida:2001	
	ANSI/TIA-568-C.3	cabeamento e componentes ópticos
	ANSI/TIA-568-C.4	cabeamento coaxial para banda larga e componentes
	ABNT NBR 13989:1997	cabo óptico
	ABNT NBR 13990:1997	
	ABNT NBR 14159:1998	
	ABNT NBR 14161:1998	
	ABNT NBR 14584:2000	
	ABNT NBR 14589:2000	
	ABNT NBR 14566:2004	
	ABNT NBR 15108:2004	
	ABNT NBR 15110:2004	
	ABNT NBR 14103:2005	
	ABNT NBR 14160:2005	
	ABNT NBR 14772:2006	
	ABNT NBR 14771:2007	
	ABNT NBR 14773:2009	
	ABNT NBR 14774:2009	

Fonte: Elaboração própria (com adaptações da Figura 1.4 de MARIN, 2013, p. 27).

Já a Figura 1 apresenta equipamentos e aparelhos medidores/certificadores para cabeamento metálico, todos aprovados internacionalmente. Note-se que tais equipamentos de teste são excessivamente caros. O que, à primeira vista, parece ser um problema é, na realidade, uma oportunidade para a inserção desse aparato no amplo rol do cabeamento estruturado. A isso as empresas da BID devem se atinar.

Figura 1 – Equipamentos auxiliares do cabeamento metálico



Fonte: do autor.

É justamente em atenção a essa parte – padronização do projeto – que reside o contexto do presente texto. Ora, se um projeto foi elaborado, implementado e certificado, seguindo-se determinadas normas e dentro de certos padrões aceitos e projetados por terceiros, então o grau de previsibilidade do estado de coisas dentro da rede se torna também alto. Previsibilidade e estratégia são antagônicas, e a padronização leva necessariamente à homogeneização e à previsibilidade.

Nesse sentido, o perigo reside justamente quando, ao estruturar e certificar um projeto de cabeamento metálico e/ou óptico com base em padrões internacionais, a infraestrutura física – lembrando que no Brasil, diga-se de passagem, é quase toda importada – fica à mercê de ameaças que podem estar embutidas nos próprios equipamentos, como os chamados backdoors.

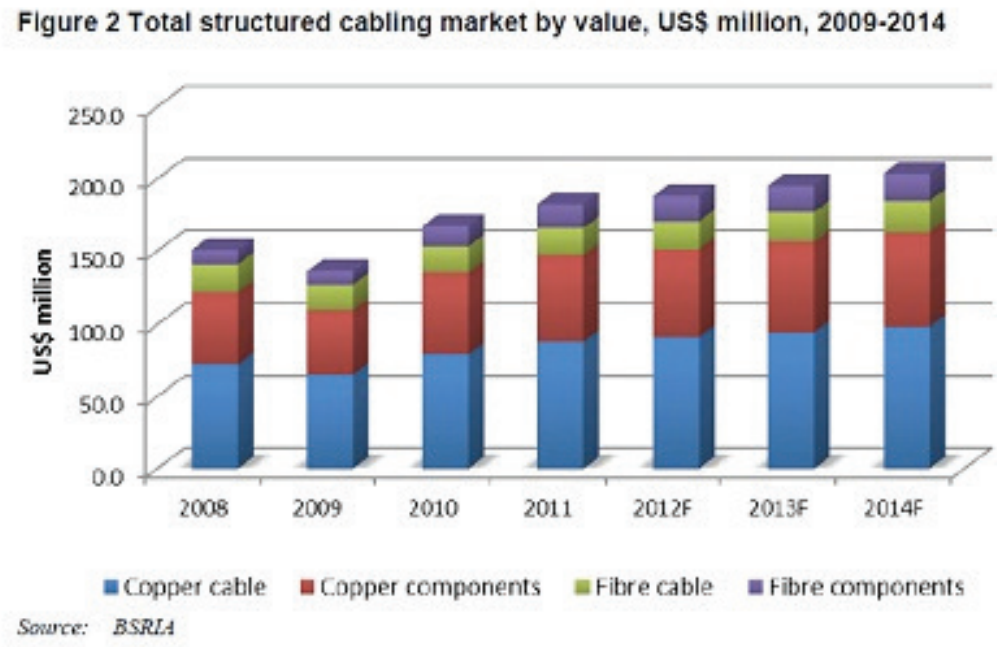
No que tange à segurança e à defesa cibernéticas, não se pode, hoje, falar em ataques cibernéticos sem mencionar possíveis danos físicos ou no hardware. Isso já é realidade. Os danos físicos provocados tanto pelo worm Stuxnet a uma usina nuclear iraniana em 2010 quanto pelo trojan Korhigh a computadores sul-coreanos em 2013 provam essa tese[11].

Como se vê, a inserção de produtos duais que envolvam o cabeamento estruturado é um

11 Para uma análise do Stuxnet, à luz dos Estudos de Defesa, vide Gama Neto e Vilar Lopes (2014) e Portela (2016, p. 94). Quanto ao trojan Korhigh, ver Goodin (2013).

nicho e a ser explorado pela indústria nacional, especialmente a de defesa. A Figura 2 apresenta um quadro geral da evolução, em milhões de dólares, do mercado de cabeamento estruturado no Brasil.

Figura 2 – Mercado de cabeamento estruturado no Brasil (2009-2014, em milhões de dólares)



Fonte: http://datacenterdynamics.com.br/sites/default/files/BSRIA_2_1.jpg.

Como se vê na Figura 2, apenas em 2009 que o mercado de cabeamento estruturado brasileiro não obteve crescimento, devido à crise financeira internacional de 2008. Nos demais anos, houve aumento significativo, sobretudo com os cabos metálicos (coopercable), cuja produção ainda é incipiente no País, embora encontre alternativas nacionais à Furukawa, como a Cablena Brasil.

Certamente, o principal incentivo para que a BID absorva parte da produção nacional de cabeamento estruturado advém da construção do Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), levado a cabo por empresas privadas e órgãos públicos do Executivo Federal, tais como o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) e o Ministério da Defesa. Possuir um satélite geoestacionário é mais do que um luxo para uma nação, é, hoje, uma necessidade, pois todos os satélites para comunicações estratégicas no Brasil são atualmente estrangeiros. Essa analogia com o cabeamento estruturado para a segurança e, principalmente, para a defesa cibernética torna-se deveras pertinente, ao se saber que as empresas da BID gastaram só para importar cabos coaxiais e outros condutores elétricos coaxiais aproximadamente US$ 3,8 milhões em 2012 e US$ 6 milhões em 2013 (VIANELLO, 2016, p. 156-157). Como se vê, é um nicho que a BID não pode menosprezar, pois, em um mundo cada vez mais interconectado, as questões afeitas à segurança cibernética estão na ordem do dia não só de empresas privadas, mas também de órgãos governamentais.

CONSIDERAÇÕES FINAIS

Este trabalho buscou apresentar o contexto em que se situa a produção de produtos e serviços de cabeamento estruturado que possam vir a impactar a segurança e a defesa cibernéticas do Estado brasileiro. A produção de tecnologia de ponta, a partir do solo brasileiro, quase sempre foi algo buscado pelos grandes estadistas, ao longo da história do Brasil. Porém, quase sempre, também, ela foi abandonada por falta de investimento ou por sabotagem industrial.

Possuir o domínio sobre as tecnologias – sobretudo as de informação e comunicação – é fator sine qua non para se alcançar o desenvolvimento do País (BRASIL, 2012b). Não se deve apenas querer tomar para si o conhecimento sobre os dados e informações, mas também sobre os meios sobre os quais eles trafegam. Aí reside o cerne e a imprescindibilidade do cabeamento estruturado para a segurança e a defesa cibernética no Brasil, país carente de uma efetiva base industrial de defesa que não esteja à mercê efêmera de governos e crises nacionais e internacionais.

Viu-se que, ao contrário do que se pode pensar, o uso maciço de redes sem fio não pode decretar o fim dos fios e cabos, haja vista o crescente mercado de fios – sobretudo metálicos- no País. Mais que isso, vive-se um momento em que a demanda só tende a aumentar, pois a necessidade de interconectar estruturas e infraestruturas não é apenas nacional, senão de âmbito internacional.

A padronização e a normalização de boas práticas de cabeamento estruturados são seguidas por órgãos civis e militares. Isso, se levado ao nível estratégico, pode tornar-se um problema, uma vez que é possível, por exemplo, saber exatamente a distância entre uma tomada e um cabo, e, a partir dessa informação, direcionar ruídos ou fazer emendas nos fios ou seus conectores[12]. Todavia, não se discutem, aqui, recomendações específicas para se lidar com essas externalidades negativas de se seguir as normas internacionais de Segurança da Informação. O que se faz, sim, é apontar para uma maior participação da indústria de defesa brasileira para que tenha sensibilidade mercadológica e apoio político – por meio, por exemplo, de incentivos fiscais – para que esse tipo de tecnologia seja não só consumido, mas também produzido em território nacional.

12 Tais recomendações poderiam girar em torno de temas, como: engenharia social, para se evitar que espiões se infiltrem na rede; equipe de certificação interna, que diz respeito à necessidade de se capacitar recursos humanos nas mais diversas certificações internacionais, como as CISCO, Microsoft, Linux, IBM etc.; atestar que não existem backdoors nos equipamentos já em uso nas redes da APF, como a que foi proposta pelo Exército Brasileiro, em resposta ao caso Snowden.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. (2013),ABNT NBR ISO/IEC 27002:2013: Tecnologia da informação – Técnicas de segurança – Código de pratica para a gestão da segurança da informação. Rio de Janeiro: ABNT.

ARQUILLA, John; RONFELDT, David. (1993),"Cyberwar is coming!",Comparative Strategy, vol. 12, no. 2: 141-165.

BRASIL.(2008), "Instrução Normativa GSI n. 1, de 13 de junho de 2008: disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências". Brasília: Gabinete de Segurança Institucional da Presidência da República.

_____. (2012a), Política Cibernética de Defesa. Brasília: Ministério da Defesa.

_____. (2012b), Política Nacional de Defesa (PND) e Estratégia Nacional de Defesa (END). Brasília: Ministério da Defesa.

BUZAN, Barry; WÆVER, Ole; WILDE, Jaap de. (1998), Security: a new framework for analysis. Boulder: Lynne Rienner.

CARR, Jeffrey. (2012),Inside cyber warfare: mapping the cyber underworld. 2. ed. Cambridge: O'Reilly.

CASTELLS, Manuel. (1996),The rise of the Network Society. Cambridge, MA: Blackwell. (The Information Age, Vol. 1).

CLARKE, Richard A.; KNAKE, Robert K. (2012),Cyber war: the next threat to national security and what to do about it. 2. ed. New York: HarperCollins.

ESPÍNDULA, Victor M.; GUERREIRO, Tirajú M.; LOPES, Gills. "Análise da Política Cibernética de Defesa brasileira à luz dos Estudos Estratégicos", in: Seminário Brasileiro de Estudos Estratégicos Internacionais. Porto Alegre: Universidade Federal do Rio Grande do Sul.

FUKUYAMA, Francis.(1992),The end of history and the last man. New York: The Free Press.

GAMA NETO, Ricardo B.; VILAR LOPES, Gills. (2014), "Armas cibernéticas e segurança internacional", in: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo B.; GONZALES, Selma L. de M. (Org.). Segurança e defesa cibernética: das fronteiras físicas aos muros virtuais. Recife: Ed. UFPE. (ColeçãoDefesa&FronteirasVirtuais, Vol. 1). cap. 1, p. 23-45.

GOODIN, Dan. "Hard drive-wiping malware part of new wave of threats targeting South Korea", in: ARS Technica, 28 jun. 2013. Disponível em: <http://arstechnica.com/security/2013/06/hard-drive-wiping-malware-part-of-new-wave-of-threats-targeting-south-korea/>. Acesso em: 26 nov. 2016.

GORMAN, Siobhan; BARNES, Julian E. (2011), "Cyber combat: act of war – Pentagon sets stage for U.S. to respond to computer sabotage with military force", in: The Wall Street Journal, New York, 30 maio 2011. Disponível em: <http://online.wsj.com/article/SB100014

240527023045631045763556231357827l8.html>. Acessoem: 20 out. 2016.

HANSEN, L.; NISSENBAUM, H. (2009), "Digital disaster, cyber security and the Copenhagen School",InternationalStudiesQuarterly, N. 53, p. 1555-1575.

ISO/IEC. (2005),ISO/IEC 27002: Information technology - Security techniques - Code of practice for information security management. Suíça: International Organization for Standardization / International Electrotechnical Commission.

LÉVY, Pierre. (2001),Cyberculture. Minneapolis: University of Minnesota Press.

LOPES, Gills. (2013), Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá. Recife: Universidade Federal de Pernambuco. Dissertação (Mestrado em Ciência Política).

MARIN, Paulo S. (2013),Cabeamento estruturado: desvendando cada passo – do projeto à instalação. 4. ed. rev. atual. São Paulo: Érica.

NYE Jr, Joseph S. (2011),The future of power. New York: PublicAffairs.

OBAMA, Barack. (2009), Remarks by the President on securing our nation's cyber infrastructure. Washington, DC: The White House. Disponívelem: <http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure>. Acesso em: 21 out. 2016.

PORTELA, Lucas S. (2016), "Agenda de pesquisa sobre o espaço cibernético nas Relações Internacionais", Revista Brasileira de Estudos de Defesa, Vol. 3, N. 1, p. 91-113. Disponível em: <http://seer.ufrgs.br/index.php/rbed/article/view/62071>. Acesso em: 24 nov. 2016.

TIA – TelecommunicationsIndustryAssociation. Disponível em: <http://www.tiaonline.org>. Acessoem: 22 out.2016.

VIANELLO, Juliano Melquiades. (2016), "Sistemas eletrônicos e sistemas de comando e controle", in: Mapeamento da Base Industrial de Defesa. Brasília:IPEA. Disponível em: <http://www.ipea.gov.br/portal/index.php?option=com_content&view=article&id=28101>. Acesso em: 25 nov. 2016.

WNDW – WIRELESS NETWORKING IN THE DEVELOPING WORLD.(2008),Redes sem fio no mundo em desenvolvimento: um guia prático para o planejamento e a construção de uma infra-estrutura de telecomunicações. [S.l.]: Hacker Friendly LLC.

UNIVERSIDADE
FEDERAL
DE PERNAMBUCO

CFCH

CENTRO DE FILOSOFIA E
CIÊNCIAS HUMANAS

Departamento de
Ciência Política

Programa de Pós-Graduação
em Ciência Política