A AMEAÇA DOS KILL SWITCHES PARA A SOBERANIA NACIONAL

*Por Júlio Shidara**



Imagem meramente ilustrativa, gerada por inteligência artificial.

Kill switches e backdoors em tecnologias estrangeiras podem ameaçar a defesa e a infraestrutura do Brasil; precedentes históricos servem de alerta para a necessidade de autonomia tecnológica como condição para proteger a soberania nacional.

"Todo equipamento feito no exterior tem backdoor... eles podem ser desabilitados."

Com essa contundente afirmação de Alok Shankar Pandey, coronel veterano do Exército indiano e especialista em Telecomunicações e Tecnologia da Informação (TI), iniciei minha apresentação "Soberania Nacional x Ameaça de Kill Switches em Sistemas Estrangeiros", no XXVIII SIGE – Simpósio de Aplicações Operacionais em Áreas de Defesa, realizado no Instituto Tecnológico de Aeronáutica (ITA), de 29 de setembro a 1º de outubro deste ano.

Negação de uso e cerceamento de informações que afetam a Segurança Nacional não são acontecimentos incomuns nem recentes.

Quase 40 anos depois da Guerra das Malvinas, ocorrida em 1982, oficiais franceses admitiram que o míssil Exocet, utilizado pela Argentina contra embarcações britânicas, possuía *kill switch* para evitar que esse armamento fosse empregado contra embarcações francesas.

Em 1996, os Estados Unidos negaram à China o acesso ao Global Positioning System (GPS) durante a Terceira Crise do Estreito de Taiwan. O episódio, conhecido como o "dia da humilhação inesquecível", representou a gênese do Beidou, sistema global de navegação por satélite chinês, e da atual multibilionária indústria espacial daquele país.

Três anos depois, em 1999, foi a vez da Índia sofrer a negação de acesso ao GPS durante a Guerra de Kargil, contra o Paquistão. O episódio impulsionou os esforços para a implementação de seu próprio sistema de navegação regional, o NavIC. Mais recentemente, ocorrências envolvendo drones produzidos na Índia, mas com emprego de componentes críticos chineses, reforçaram a preocupação daquele governo com a dependência de equipamentos e componentes estrangeiros.

Muitos brasileiros ficam surpresos ao saber que o Brasil também já sofreu negação de acesso ao GPS. Aconteceu em 1997 e em 1999, no primeiro e no segundo lançamentos do Veículo Lançador de Satélites (VLS) do Centro de Lançamento de Alcântara (CLA), no Maranhão, conforme relatou o prof. Waldemar de Castro Leite Filho. Em 2024, também foram levantados questionamentos sobre a vulnerabilidade decorrente do emprego do Starlink pelas Forças Armadas Brasileiras em missões de segurança nacional.

Ainda que um equipamento estrangeiro possa funcionar por décadas em operações realizadas pelas Forças Armadas Brasileiras, sem qualquer evidência de interferência externa pelo emprego de mecanismos como *kill switches* ou *backdoors*, isso não representa garantia de que funcionará da mesma forma numa eventual guerra.

A ameaça não é apenas hipotética. Em 2012, pesquisadores da Universidade de Cambridge descobriram um *backdoor* gravado no próprio silício de um FPGA chinês de grau militar, que permitiria a terceiros acessar o controle de armas e plantas nucleares.

Em 2024, a *Bloomberg* reportou que a ASML, fabricante holandesa de máquinas EUV necessárias para produzir os chips mais modernos existentes, incorporou um *kill switch* em equipamento vendido à fabricante taiwanesa TSMC, para permitir sua desativação caso a China invadisse Taiwan.

Em tempos mais recentes, circularam notícias de que sistemas de defesa da Europa poderiam sofrer as consequências do acionamento de *kill switches* em equipamentos fornecidos pelos Estados Unidos.

Com relação a esse tema, um dos artigos mais contundentes sobre a ameaça de *kill switches* para a Europa foi publicado pelo fundador do *Global4Cast* em 2025. Nele, Ingo Piepers afirma que o sistema de mísseis HIMARS (*High Mobility Artillery Rocket System*) foi fornecido pelos Estados Unidos para a Ucrânia deliberadamente com desempenho degradado. O artigo cita ainda outros equipamentos críticos com mecanismos de controle incorporados e que poderiam ser desabilitados numa crise.

No artigo *The Programmable Diplomatic Kill Switch*, o professor da Universidade Americana da Armênia, David Davidian, afirma que: "Os principais fabricantes de armas estratégicas seriam negligentes se não acrescentassem tal capacidade de controlar o uso de seus armamentos", referindo-se a *kill switches* e *backdoors*.

Portanto, embora o Brasil possa não ter sofrido ainda as consequências do acionamento de *kill switches* ou *backdoors*, isso não significa que tais dispositivos não estejam presentes em equipamentos estrangeiros empregados pelas Forças Armadas e em infraestruturas nacionais críticas.

Nesse cenário, a pergunta óbvia é: como o Brasil poderia mitigar tal vulnerabilidade?

A resposta é simples: priorizando o desenvolvimento endógeno de tecnologias críticas de interesse nacional, para buscar a autonomia tecnológica em áreas estratégicas para o País.

Para que isso aconteça, primeiro é necessário que os tomadores de decisão não encarem a ameaça de *kill switches* como teoria da conspiração, mas tenham real consciência da vulnerabilidade decorrente da dependência de tecnologia estrangeira em áreas críticas para a soberania nacional.

Essa conscientização representa a fundação sobre a qual deve ser construída a vontade política para implementar uma política industrial de Estado que, em poucas décadas, possa alterar drasticamente o atual quadro de dependência de tecnologia estrangeira no Brasil, como faz a Índia com sua política *Aatmanirbharta*, ou política de autossuficiência.

O Brasil precisa seguir pelo mesmo caminho.

***Júlio Shidara** é coronel da reserva da Força Aérea Brasileira (FAB) e engenheiro formado pelo Instituto Tecnológico de Aeronáutica (ITA). Presidente da Associação das Indústrias Aeroespaciais do Brasil (AIAB), dedicou grande parte de sua carreira a projetos de modernização da FAB, muitos deles desenvolvidos em parceria com organizações internacionais. Atualmente, trabalha pelo fortalecimento da Base Industrial Aeroespacial Brasileira. No setor espacial, atua especialmente na conscientização da sociedade sobre a importância do Programa Espacial Brasileiro para o desenvolvimento socioeconômico do país.*