

# VULNERABILIDADES DA LIDERANÇA MILITAR RUSSA

*Inteligência estratégica além das fronteiras: como GRU, SVR, FSB e MI6 operam em operações de sabotagem, contrainteligência e guerra moderna, revelando vulnerabilidades que definem os conflitos contemporâneos.*

**Carlos A. Klomfahs\***



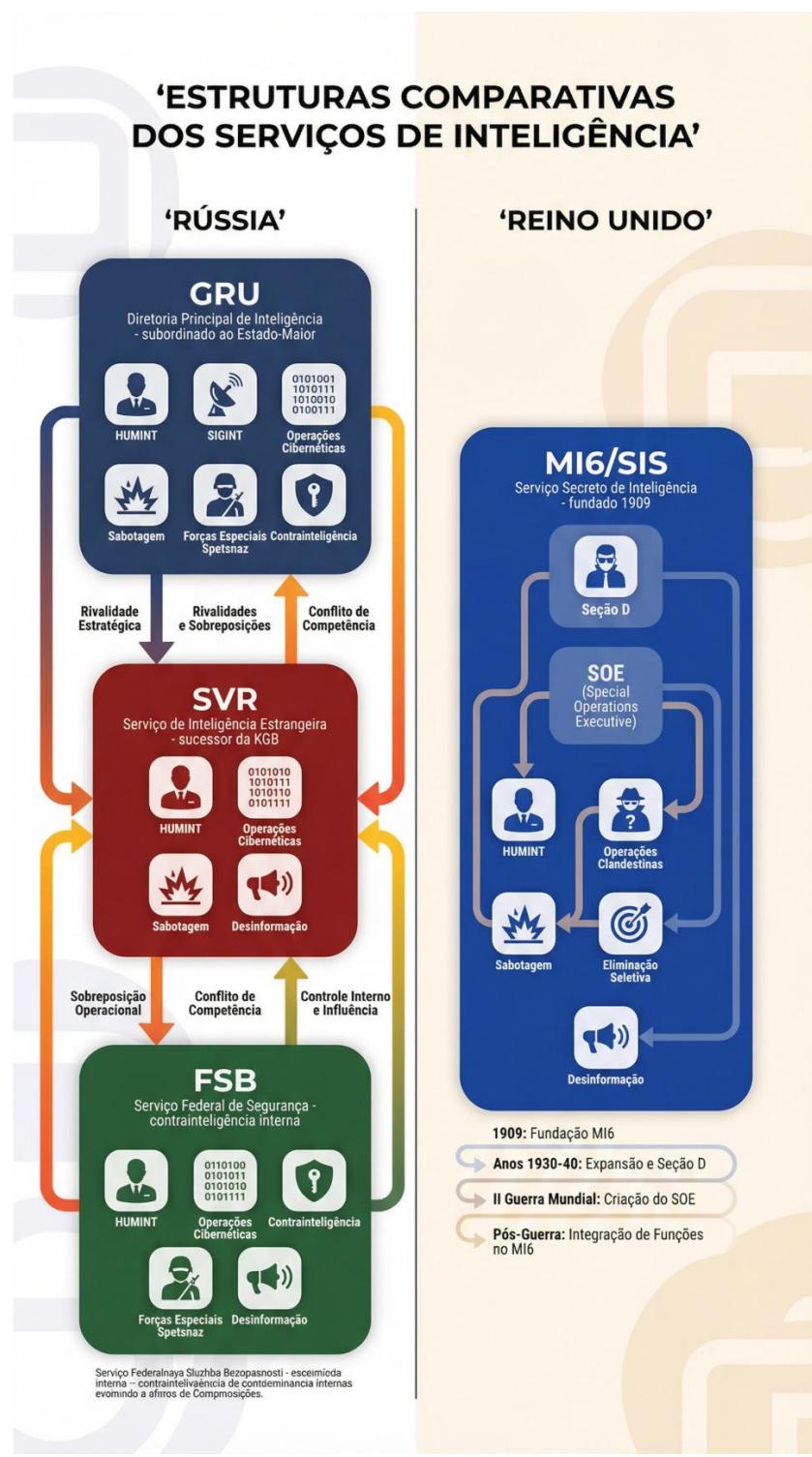
*Imagem meramente ilustrativa, gerada por inteligência artificial.*

Este breve artigo apresenta um resumo histórico e operacional dos principais serviços de inteligência da Federação Russa (GRU, SVR e FSB) e do Reino Unido (MI6), com foco em suas origens, evolução e *modus operandi* em operações de sabotagem e ações clandestinas no exterior, com objetivo de entender onde o governo russo tem errado em matéria de comunicação estratégica e nos protocolos de contrainteligência e contrasabotagem.

## SERVIÇOS DE INTELIGÊNCIA RUSSOS: GRU, SVR E FSB

Os serviços de inteligência da Federação Russa, herdeiros da vasta e complexa estrutura da era soviética, desempenham um papel central na projeção de poder e na defesa dos interesses nacionais russos no cenário global. Embora muitas vezes atuem de forma coordenada, o GRU (Diretoria Principal de Inteligência), o SVR (Serviço de Inteligência Estrangeira) e o FSB (Serviço Federal de Segurança) possuem mandatos distintos e *modus operandi* que se complementam e, por vezes, competem.

Não se sabe se os russos aprenderam as lições que os americanos, *in thesi*, aprenderam após o 11 de setembro sobre a importância da coordenação e integração entre as comunidades de inteligência, mitigando o princípio da compartimentação na área de inteligência do Estado.



*Infográfico 1: Comparativo dos serviços de inteligência britânicos e russos.*

## **GRU (DIRETORIA PRINCIPAL DE INTELIGÊNCIA)**

O GRU é o serviço de inteligência militar da Rússia, subordinado ao Estado-Maior Geral das Forças Armadas. Fundado em 1918, é conhecido por sua natureza agressiva e operações clandestinas em zonas de conflito e no exterior. Diferentemente de outras agências, o GRU possui suas próprias forças especiais (*Spetsnaz*), o que lhe confere uma capacidade única de executar operações paramilitares, sabotagem e assassinatos seletivos.

Historicamente, o GRU esteve envolvido em atividades de inteligência humana (HUMINT), inteligência de sinais (SIGINT) e guerra cibernética. Nos últimos anos, ganhou notoriedade por ataques cibernéticos de alto perfil, como o *hack* do Comitê Nacional Democrata dos EUA em 2016 e o ataque NotPetya em 2017, além de tentativas de assassinato, como o envenenamento de Sergei Skripal no Reino Unido em 2018. Seu *modus operandi* é caracterizado pela audácia, pela utilização de táticas de guerra híbrida e pela negação plausível, buscando desestabilizar adversários e influenciar eventos geopolíticos.

## **SVR (SERVIÇO DE INTELIGÊNCIA ESTRANGEIRA)**

O SVR é o principal serviço de inteligência civil da Rússia para operações no exterior, sucessor da Primeira Diretoria Principal da KGB. Sua missão é coletar informações políticas, econômicas, científicas e tecnológicas através de espionagem, análise e operações clandestinas. O SVR é o equivalente russo da CIA americana, focando em inteligência humana de longo prazo e na influência de políticas externas.

Embora menos associado a operações de sabotagem física direta do que o GRU, o SVR tem sido implicado em campanhas de desinformação, influência política e operações cibernéticas sofisticadas, como o ataque de 2020, que comprometeu redes governamentais e corporativas em todo o mundo. Seu *modus operandi* é mais sutil e focado na infiltração e na manipulação de informações para moldar o ambiente estratégico a favor da Rússia.

## **FSB (SERVIÇO FEDERAL DE SEGURANÇA)**

O FSB se assemelha ao FBI com funções extras, e é o principal serviço de segurança interna da Rússia, responsável pela contrainteligência, segurança de fronteiras, combate ao terrorismo e crime organizado. É o sucessor direto da KGB dentro das fronteiras russas.

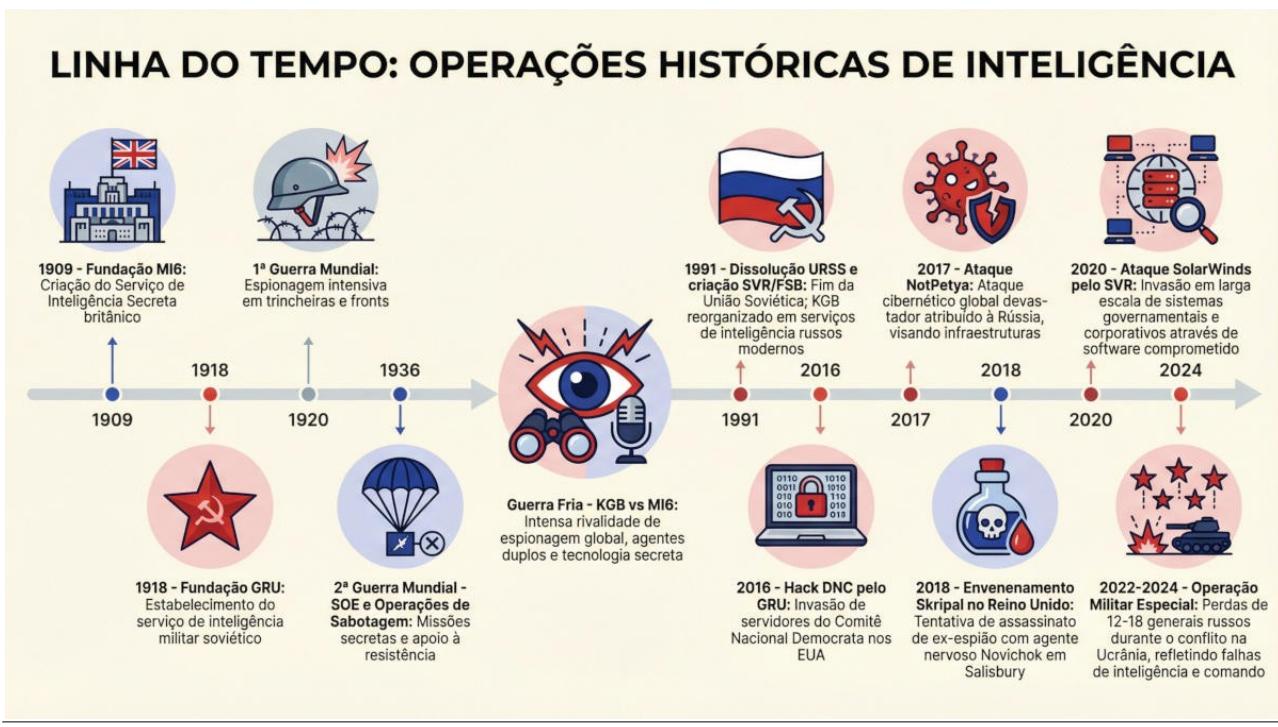
Em que pese seu foco principal ser doméstico, o FSB possui um braço de operações no exterior, especialmente em países da antiga União Soviética, onde atua para proteger os interesses russos e suprimir ameaças percebidas.

O FSB tem sua atuação caracterizada pela contenção interna, pela vigilância extensiva e pela capacidade de neutralizar ameaças à segurança do Estado, utilizando métodos que podem incluir a eliminação de alvos considerados perigosos para a estabilidade do regime, e quando possível, ao não reagir, os suspeitos são levados ao Poder Judiciário Russo.

# MI6 (SERVIÇO SECRETO DE INTELIGÊNCIA BRITÂNICO)

O Serviço Secreto de Inteligência (SIS), mais conhecido como MI6, é a agência de inteligência estrangeira do Reino Unido, responsável pela coleta de inteligência humana (HUMINT) no exterior em apoio aos interesses de segurança nacional britânicos. Fundado em 1909 como a Seção Estrangeira do Bureau do Serviço Secreto, o MI6 desenvolveu uma longa história de operações clandestinas, espionagem e sabotagem em território estrangeiro.

Desde suas possessões ultramarinas até suas ações contra os impérios Espanhol, Francês, Holandês e Alemão durante a Primeira Guerra Mundial, o Reino Unido investiu significativamente em capacidades de inteligência e sabotagem. Esse investimento doutrinário e financeiro deixou uma assinatura operacional característica nas ações britânicas, que pode ser identificada através de análise forense avançada de contrasabotagem, comprometendo potencialmente futuras operações em territórios onde o Reino Unido possua interesses estratégicos.



Infográfico 2: Linha do tempo histórica.

## ORIGENS E EVOLUÇÃO

As raízes do MI6 remontam ao início do século XX, com sua estrutura formalizada durante a Primeira Guerra Mundial. No período entre guerras e, especialmente, durante a Segunda Guerra Mundial, o MI6 desempenhou um papel crucial na coleta de inteligência, na desinformação e no apoio a movimentos de resistência em territórios ocupados.

A Seção D (para “Destruição”) e, posteriormente, a Executiva de Operações Especiais (SOE, *Special Operations Executive*), embora tecnicamente separadas, colaboraram estreitamente com o MI6 em

operações de sabotagem e guerra irregular, visando infraestruturas inimigas e desestabilizando regimes considerados hostis. Durante a Guerra Fria, o MI6 esteve na linha de frente da confrontação com a União Soviética, conduzindo operações de espionagem de alto risco e contrainteligência.

Sabe-se, por pesquisas, que a agência também se envolveu em ações secretas para influenciar governos e desestabilizar regimes considerados hostis aos interesses britânicos, particularmente em regiões como o Oriente Médio e a África.

## MODUS OPERANDI EM OPERAÇÕES DE SABOTAGEM NO EXTERIOR

O *modus operandi* do MI6 em operações de sabotagem no exterior é caracterizado por uma combinação de discrição, precisão e, quando necessário, brutalidade calculada. As operações de sabotagem visam geralmente:

**Infraestrutura Crítica:** Alvos incluem instalações militares, redes de transporte, comunicações e infraestruturas energéticas, com o objetivo de interromper as capacidades operacionais do adversário.

**Desestabilização Política:** Apoio a grupos de oposição, fomento de revoltas ou desinformação para minar a autoridade de regimes hostis.

**Eliminação Seletiva:** Embora o MI6 evite publicamente confirmar tais operações, há acusações e evidências históricas de envolvimento em assassinatos seletivos de indivíduos considerados ameaças diretas à segurança nacional desde o império espanhol até o governo de Adolf Hitler, utilizando métodos que variam de envenenamento a acidentes e suicídios simulados, com um “menu” bastante diversificado.

As táticas empregadas pelo MI6 em sabotagem incluem o uso de agentes infiltrados, recrutamento de fontes locais, guerra cibernética para desabilitar sistemas e, em casos extremos, o emprego de explosivos ou outros meios destrutivos.

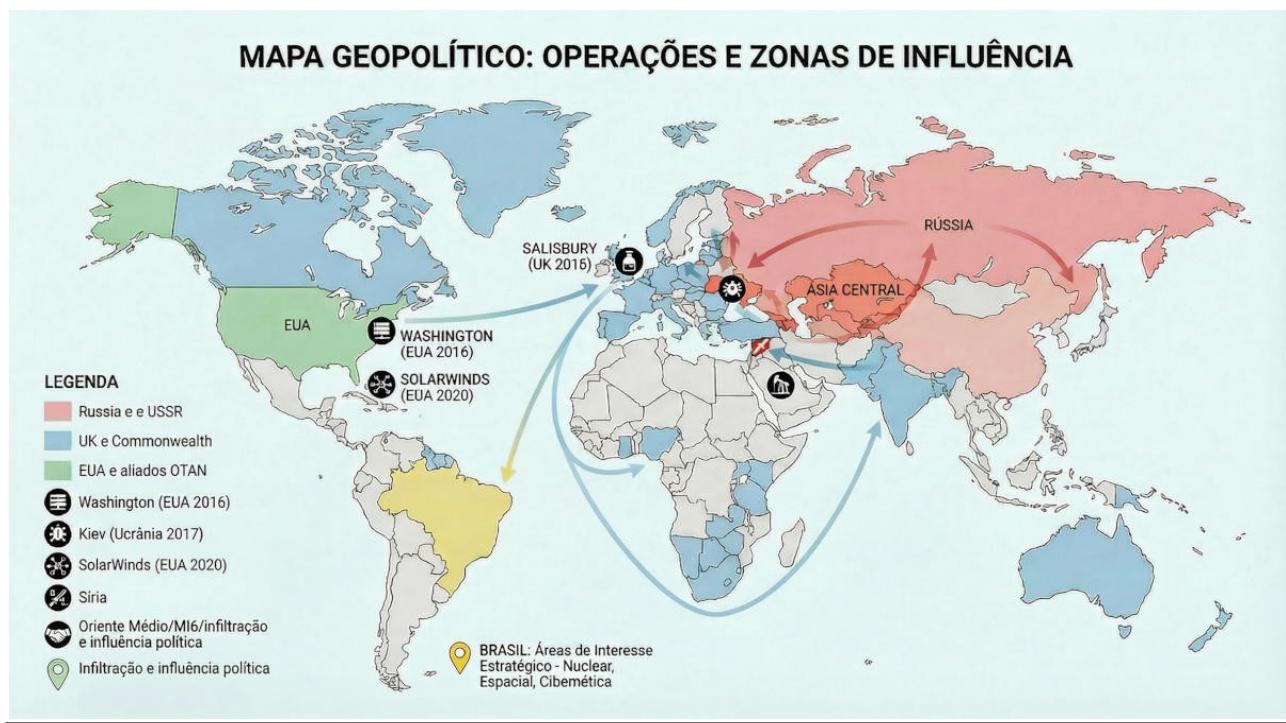
É público e notório que a agência opera sob um véu de sigilo, buscando sempre a negação plausível para evitar a atribuição direta de suas ações ao governo britânico. Logo, depreende-se que a sofisticação de suas operações e a capacidade de operar em ambientes hostis com um alto grau de discrição consolidaram a reputação do MI6 como um dos serviços de inteligência mais eficazes e, por vezes, implacáveis do mundo.

## EXPOSIÇÃO DA LIDERANÇA E A DESESTABILIZAÇÃO DO COMANDO E CONTROLE

Desde o início da Operação Militar Especial (SME, *Special Military Operation*) na Ucrânia, a Federação Russa tem enfrentado uma taxa de perdas de oficiais de alta patente sem precedentes em conflitos modernos, que vem conseguindo o êxito de baixar a moral da tropa desde o alto

escalão aos conscritos, na medida em que, mesmo que muita coisa tenha sido feita, a recusa em informar detalhes operacionais como estratégia de comunicação do Kremlin tem causado alguns inconvenientes interna e externamente.

Estimativas divulgadas por Anatoly Shariy apontam para a perda de 12 a 18 generais russos, incluindo o major-general Andrei Sukhovetsky, o major-general Vladimir Frolov, o tenente-general Oleg Tsokov, o tenente-general Igor Kirillov, o tenente-general Yaroslav Moskalik, o tenente-general Fanil Sarvarov, o capitão de primeira classe Valery Trankovsky e o tenente-general Vladimir Alexeyev. Esses postos correspondem aos escalões superiores do generalato russo, equivalentes aos postos brasileiros de general-de-brigada, general-de-divisão e general-de-exército (uma, duas, três e quatro estrelas, respectivamente; em caso de guerra declarada, marechal, com cinco estrelas).



Infográfico 3: Zonas de influência.

Essas perdas não são acidentais. O adversário ocidental tem deliberadamente visado os centros de comando do Exército russo, buscando desestabilizar o sistema de comando e controle (C2) e desmoralizar as tropas.

A diferença reside no modo como os serviços de inteligência russos operam. Quando atuam – seja através de prisões ou de interrogatórios coercitivos – na Rússia ou em qualquer país europeu, suas ações raramente vêm à tona na imprensa. Enquanto os atos de terrorismo de Estado ocidentais são amplamente divulgados e espetacularizados, a resposta russa permanece obscura. Nesse contexto, cada pessoa detida não será necessariamente morta, mas sofrerá punições proporcionais aos danos que causou. Essa é a lógica subjacente às operações russas.

A propósito, um dos desafios mais difíceis enfrentados durante a formação, treinamento e operações de campo das Forças Especiais e de Operações de Inteligência é a captura pelo inimigo,

seguida de tortura e “interrogatórios especiais” executados por profissionais altamente treinados. Esses procedimentos variam em objetivo e intensidade: alguns visam extrair informações, outros funcionam como punição. Enquanto alguns interrogatórios produzem resultados em poucas horas, outros se prolongam por meses, com médicos presentes para garantir a sobrevida do interrogado.

Os sobreviventes de “interrogatórios especiais” intensos enfrentam sequelas psicológicas permanentes: transtorno de estresse pós-traumático, traumas crônicos e distúrbios psiquiátricos. Esses traumas podem ser ativados por estímulos aparentemente triviais – um grito, barulhos altos, buzinas, portas batendo, “bombinhas” juninas, cadeados sendo fechados, espaços fechados e úmidos, privação de água, alimento ou luz solar.

Retornando à questão da vulnerabilidade da liderança militar russa, constata-se que ela reflete falhas estruturais na proteção de seus ativos mais valiosos. A doutrina militar russa, que historicamente privilegia a centralização do comando, exige que oficiais de alta patente se desloquem até a linha de frente para resolver problemas táticos, expondo-os a riscos desnecessários. Além disso, outras vulnerabilidades estruturais contribuem para essas perdas.

A RAND Corporation, em suas análises, tem apontado para as vulnerabilidades russas em logística e, crucialmente, em comando e controle, onde ataques ucranianos contra postos de comando têm sido eficazes em desorganizar operações e criar caos no seio do oficialato.

Isto porque, a perda de um general não é apenas a perda de uma patente, mas a eliminação de um especialista cuja formação e experiência são insubstituíveis a curto prazo, impactando a capacidade de planejamento e execução de operações complexas.

Além das operações de combate direto, é preciso considerar a possibilidade de operações de contrainteligência destinadas à eliminação de desertores ou traidores. Em cenários de alta tensão, as autoridades podem simular um ataque externo para eliminar oficiais de alta patente suspeitos de traição, utilizando essa cobertura para alcançar objetivos políticos ou militares. Essas operações podem ser executadas de forma espetacular, visando enviar uma mensagem clara, ou de forma encoberta, utilizando métodos que simulem morte natural – como envenenamento por agentes radioativos, quedas de grandes alturas, injeção de substâncias tóxicas ou contaminação de alimentos e água.

Esse *modus operandi* remete a operações históricas de serviços de inteligência como o MI6 britânico, que buscavam provocar terror psicológico e minar a moral do exército e dos serviços de inteligência internos, como fizeram contra o Exército Alemão.

## DESAFIOS DA INTELIGÊNCIA RUSSA E LIÇÕES PARA A CONTRAINTELIGÊNCIA

As falhas na proteção da liderança militar russa expõem desafios significativos para seus serviços de inteligência – o GRU, o FSB e o SVR. Em pesquisas no *think tank* americano RAND Corporation e outros estudos acadêmicos, encontram-se indicações de que a coordenação entre essas agências é

frequentemente prejudicada por rivalidades internas e falta de uma abordagem unificada, criando brechas de segurança que podem ser exploradas por adversários.

A capacidade de penetração de serviços de inteligência estrangeiros em território russo, facilitada pelas extensas fronteiras e pela possibilidade de cooptar minorias, russos insatisfeitos, criminosos ou cidadãos de países vizinhos como Ucrânia e Geórgia, representa uma ameaça constante. Essa facilidade em direcionar investigações para longe do verdadeiro agressor permite que operações de sabotagem e espionagem atinjam seus objetivos com menor risco de atribuição.

## LIÇÕES DO INCIDENTE PARA O BRASIL

Para o Brasil, que insiste e amarga uma dependência tecnológica, doutrinária e de armas de sistemas ocidentais, sem diversificar suas parcerias estratégicas, sofre cerceamento tecnológico em áreas estratégicas como nuclear, espacial e cibernética, como ensinado enfaticamente há décadas pelo ilustre professor William de Sousa Moreira da Escola de Guerra Naval, o que é um fato consumado, e a experiência russa pode oferecer lições elementares no fortalecimento de nossa cultura de constrainteligência, contrassabotagem e contraespionagem.

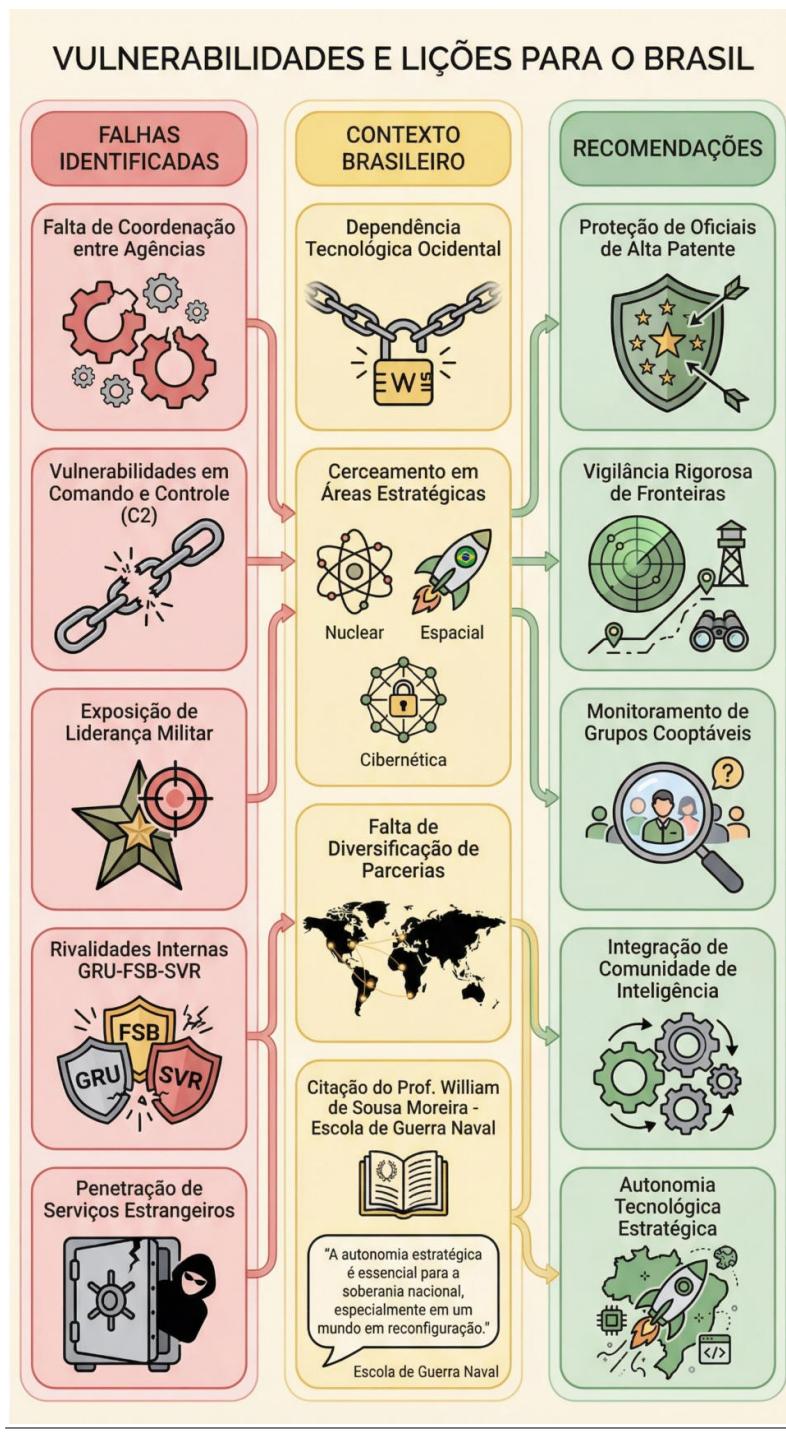
O Brasil, ao amargar e insistir em dependência tecnológica, doutrinária e de armamentos dos sistemas ocidentais sem diversificar suas parcerias estratégicas, sofre cerceamento tecnológico em áreas críticas como energia nuclear, exploração espacial e cibernética. Essa vulnerabilidade estrutural, conforme enfatizado pelo professor William de Sousa Moreira da Escola de Guerra Naval, representa um fato consumado que compromete a autonomia nacional. A experiência russa, nesse contexto, oferece lições valiosas para o fortalecimento das capacidades brasileiras em constrainteligência, contrassabotagem e contraespionagem.

Uma das lições é que a proteção de oficiais de alta patente e especialistas, a vigilância rigorosa das fronteiras e o monitoramento de grupos internos potencialmente cooptáveis, são imperativos estratégicos. Em síntese: a guerra moderna não se limita ao campo de batalha físico; ela se estende ao domínio da informação e da subversão, onde a capacidade de proteger ativos humanos e tecnológicos é tão vital quanto a superioridade militar.

Outra diferença observada reside na visibilidade das ações: enquanto operações de terrorismo de Estados ocidentais podem ser espetacularizadas, a resposta russa, quando ocorre, é frequentemente velada, com “interrogatórios especiais” e punições que visam garantir que o sofrimento seja proporcional ao prejuízo causado, servindo como um lembrete sombrio dos riscos envolvidos na espionagem e na traição.

Em conclusão, depreende-se que as vulnerabilidades russas no conflito atual resultam de aspectos multifatoriais, tanto intrínsecos quanto extrínsecos. Entre os fatores internos, destacam-se: a vasta extensão territorial do país, que dificulta a coordenação e vigilância; vulnerabilidades decorrentes da diversidade étnica; questões financeiras dos países envolvidos, ao prometer vultosas somas; suscetibilidade a chantagem e corrupção; infiltração de agentes criminosos; facilidade de recrutamento de imigrantes ucranianos; e falhas de coordenação e integração entre os serviços de inteligência doméstica, externa e militar russos. Os fatores externos incluem as capacidades

operacionais avançadas dos serviços de inteligência estrangeiros, que possuem longa experiência em operações de eliminação seletiva de autoridades militares.



Infográfico 4: Lições para o Brasil.

\***Carlos A. Klomfahs** é advogado, especialista em Direito Internacional dos Conflitos Armados e operador de Inteligência. Egresso curso de geopolítica da ECUME e estratégia marítima da Escola de Guerra Naval. É mestrado no Programa de Pós-Graduação em Segurança Internacional e Defesa (PPGSID) da Escola Superior de Guerra.