

GUERRA HÍBRIDA E LAWFARE: COMO DESESTABILIZAR UM PAÍS

Por Carlos Alexandre Klomfahs*



Imagem meramente ilustrativa, gerada por inteligência artificial.

Guerra híbrida, lawfare e dependência tecnológica desafiam a soberania brasileira. Proteger o país exige autonomia digital, instituições íntegras e controle democrático, sem reproduzir os abusos que se pretende combater.

INTRODUÇÃO

A evolução dos conflitos internacionais no último século mostra que a guerra deixou de ser travada prioritariamente no campo de batalha tradicional. O esgotamento do modelo de invasões militares diretas, devido ao alto custo político, econômico e humano, forçou as grandes potências a desenvolverem métodos dissimulados de intervenção e desestabilização política, empregando a fusão entre operações de inteligência e operações especiais, estas, às vezes, com uso de operações clandestinas, oficialmente negadas por governos caso os operadores falhem.

O presente artigo objetiva entender estas interferências/desestabilizações políticas e propor meios jurídicos para diminuir esta influência. É nesse contexto que emergem os

conceitos interdependentes de Guerra Híbrida e *Lawfare*, as principais ferramentas de desestabilização política e mudança de regime na geopolítica contemporânea que usa o controle da imprensa internacional nos países de interesse, dependência tecnológica e o poder das sanções financeiro-econômicas.

Cabe ressaltar que não se busca direcionar a crítica a um país específico, mas a um “padrão de ações em conjunto” que colocam em xeque não só a soberania nacional, mas sobretudo a liberdade e segurança física de brasileiros no exterior, como alertamos em nossas consultorias estratégicas para autoridades e empresários que viajam a trabalho ou turismo.

A ORIGEM TEÓRICA DA GUERRA HÍBRIDA

O termo Guerra Híbrida ganhou força na virada do século XXI, inicialmente cunhado pelo analista militar norte-americano Frank Hoffman¹ (hoje aposentado) em 2007. Hoffman descreveu um cenário onde um ator (estatal ou não) mescla simultaneamente armas convencionais, táticas irregulares, terrorismo e criminalidade no mesmo espaço de batalha para alcançar objetivos políticos.

No Brasil, no âmbito das Forças Armadas, conforme o Glossário de Termos e Expressões para uso no Exército² (2018, pág. 183):

GUERRA HÍBRIDA – Caracteriza-se quando as ações de combate convencional são aglutinadas, no tempo e no espaço, com operações de guerra irregular, de guerra cibernética e de operações de informação, dentre outras, com atores estatais e não estatais, no ambiente real e informacional, incluindo as redes sociais.

No âmbito da Inteligência Nacional, o relatório oficial mais recente da Agência Brasileira de Inteligência (ABIN), *Desafios de Inteligência: Edição 2026*, consolida a avaliação da agência sobre os riscos complexos enfrentados pelas instituições brasileiras. O documento aborda eixos centrais que constituem a guerra híbrida contemporânea:

- Ciberataques autônomos potencializados por Inteligência Artificial;
- Interferência externa vinculada à dependência tecnológica;
- Vulnerabilidades na segurança de processos institucionais e infraestruturas críticas.

¹ Ver a breve biografia de Hoffman em: <https://www.usf.edu/gnsi/about/fellows-bio-hoffman.aspx>.

² Ver o Glossário de Termos e Expressões Para Uso no Exército em: <https://bdex.eb.mil.br/jspui/bitstream/1/1148/1/Glossário%20EB%202018.pdf>.



Figura 1: Consolidação dos eixos da Guerra Híbrida segundo a Agência Brasileira de Inteligência (imagem gerada com apoio de inteligência artificial).

No entanto, o conceito foi ampliado e profundamente ressignificado pela ciência política e pela estratégia militar global (notadamente depois das formulações teóricas russas e chinesas sobre a “Guerra Irrestrita”):

Guerra Irrestrita (1999): Proposta pelos coronéis chineses Qiao Liang e Wang Xiangsui, defende que a guerra moderna não possui mais limites de campo de batalha. O sistema financeiro, as redes de computadores, a mídia e os tribunais tornaram-se frentes de combate tão letais quanto mísseis.

Guerra de Quinta Geração: A Guerra Híbrida contemporânea opera no espectro da informação e da cognição. O alvo principal não é o exército inimigo, mas a mente da população e das elites institucionais do país-alvo. O objetivo é destruir o Estado por dentro, gerando caos social, polarização extrema e paralisia política através da

manipulação de vulnerabilidades reais da nação (como crises econômicas ou escândalos de corrupção).

A GENEALOGIA DO *LAWFARE*: A LEI COMO ARMA DE DESTRUIÇÃO

O termo *Lawfare* resulta da fusão das palavras *Law* (Lei) e *Warfare* (Guerra). Embora tenha sido utilizado de forma embrionária na década de 1970, o conceito foi formalizado em 2001 pelo general da Força Aérea dos EUA, Charles Dunlap. Ele definiu *lawfare* como “o uso da lei como um meio para conseguir um objetivo militar”.

Originalmente pensado para descrever como nações mais fracas usavam o direito internacional para conter o poder de fogo norte-americano, o conceito foi invertido na prática geopolítica. Hoje, o *lawfare* é entendido como o uso estratégico, abusivo e ilegítimo do direito nacional e internacional para deslegitimar, paralisar ou destruir um inimigo político ou geopolítico.

A fundamentação do *lawfare* moderno assenta-se em três eixos essenciais:

a. Aparência de Legalidade: Diferente de um golpe militar tradicional (com tanques nas ruas), as rupturas promovidas pelo *lawfare* utilizam ritos constitucionais, processos judiciais e investigações oficiais. Isso confere legitimidade internacional e dificulta a reação da opinião pública.

b. “Diplomacia Judicial” e Cooptação: Conforme documentado em Manuais de Estratégia de Política Externa, potências globais promovem intensos programas de intercâmbio, cooperação jurídica internacional e treinamento de magistrados e procuradores em países em desenvolvimento. Esse alinhamento ideológico e procedimental cria uma elite jurídica local disposta a aplicar o direito de forma assimétrica contra lideranças soberanistas.

c. Sinergia Midiática: O *lawfare* não sobrevive sem a espetacularização. O vazamento seletivo de informações para grandes conglomerados de mídia serve para “assassinar” a reputação do alvo antes mesmo do julgamento, justificando medidas de exceção (prisões preventivas abusivas, bloqueio de bens, suspensão de direitos políticos) sob o pretexto do “combate à corrupção” ou da “defesa da democracia”.

A FUSÃO PRÁTICA DAS DUAS ESTRATÉGIAS

Na prática do século XXI, a Guerra Híbrida fornece o ambiente de caos e descontentamento popular, enquanto o *lawfare* desfere o golpe institucional “limpo”.

Historicamente, essa combinação substituiu as ditaduras militares explícitas das décadas de 1960 e 1970 por processos de deposição parlamentar, *impeachment* sem base jurídica

sólida, *lawfare* eleitoral (banimento de candidatos competitivos) e asfixia econômica internacional via sanções multilaterais, redefinindo as fronteiras da soberania nacional no mundo globalizado.

A cooptação do Poder Judiciário e o uso de mecanismos econômico-financeiros são pilares fundamentais da chamada Guerra Híbrida e do *Lawfare* (uso do sistema legal como arma política). Essas táticas complementam o controle político e midiático, fechando o cerco institucional sobre um país-alvo.



Figura 2: A Guerra Híbrida cria o ambiente de pressão; o *lawfare* converte essa pressão em ação institucional por meios jurídicos, midiáticos e burocráticos, provocando a erosão da soberania (imagem gerada com apoio de inteligência artificial).

A análise em conjunto desses fatores demonstra, indubitavelmente, como a soberania nacional pode ser erodida por vias “legais” e burocráticas, tais como:

COOPTAÇÃO DA CÚPULA DO JUDICIÁRIO E “DIPLOMACIA ACADÊMICA”

O alinhamento de magistrados, procuradores/promotores do Ministério Público e juízes/desembargadores e Ministros de Cortes Superiores ocorre frequentemente por meio do chamado *soft power* acadêmico e cultural, notadamente por meio de:

Eventos e palestras financiadas: Convites para palestras internacionais com passagens, hospedagens e honorários pagos por fundações, ONGs ou *think tanks* estrangeiros funcionam como ferramentas eficientes e eficazes de aproximação e criação de laços ideológicos de longo prazo.

Bolsas e prestígio acadêmico: Vagas de estudo exclusivas em universidades de prestígio global (especialmente nos EUA e Europa) para as autoridades e/ou seus familiares criam

um sentimento de dívida institucional e moldam a visão jurídica do magistrado de acordo com os interesses da potência estrangeira.

Cultura jurídica importada: Esse intercâmbio constante promove a importação de doutrinas jurídicas que fragilizam a segurança jurídica local ou legitimam ações excepcionais contra o próprio governo do país; grosso modo, um exemplo é o fortalecimento do direito inglês baseado nos juízes em detrimento do direito europeu baseado nas leis, conhecidos respectivamente como *Common Law* e *Civil Law*.

DEPENDÊNCIA FINANCEIRA E ARMAMENTIZAÇÃO DO DÓLAR (WEAPONIZATION OF FINANCE)

Quando um país depende de instituições financeiras internacionais (como o FMI e o Banco Mundial) ou do sistema bancário global controlado por potências ocidentais, sua autonomia política fica severamente limitada:

Condicionalidades econômicas: Empréstimos e refinanciamentos de dívidas exigem “reformas estruturais” (privatizações, austeridade e desregulamentação), que muitas vezes transferem o controle de setores estratégicos nacionais para o capital estrangeiro.

Controle do Sistema SWIFT: Os EUA possuem hegemonia sobre a rede global de transações financeiras (SWIFT), o que permite monitorar o fluxo de dinheiro do país-alvo e bloquear o acesso de bancos nacionais ao comércio global.

SANÇÕES UNILATERAIS E CONSTRANGIMENTO INTERNACIONAL

O alcance extraterritorial das leis americanas (como o uso do dólar como jurisdição universal) dá aos EUA o poder de punir indivíduos e instituições em qualquer lugar do mundo, por exemplo:

Bloqueio em paraísos fiscais: Agências como o OFAC (*Office of Foreign Assets Control*, em português, Escritório de Controle de Ativos Estrangeiros dos EUA) podem congelar contas bancárias e investimentos de autoridades nacionais em paraísos fiscais ou bancos estrangeiros, asfixiando financeiramente qualquer oposição aos seus interesses.

Suspensão de passaportes e vistos: O cancelamento de vistos de viagem para autoridades locais e seus familiares é utilizado como uma punição psicológica e de *status* social, sem contar nos riscos de sequestro e extorsão (incluindo a digital).

Extradição e constrangimento em países terceiros: Por meio de alertas da Interpol ou pressões diplomáticas bilaterais, os EUA (mas não somente eles) conseguem fazer com que autoridades ou empresários de um país sejam detidos, constrangidos ou extraditados durante viagens de turismo ou trabalho em nações aliadas de Washington (caso de executivos de tecnologia e diplomatas estrangeiros detidos em trânsito são exemplos históricos disso).



Figura 3: Representação gráfica do alcance das sanções econômicas e a dependência digital do país com softwares estrangeiros e computação em nuvem (imagem gerada com apoio de inteligência artificial).

DEPENDÊNCIA TECNOLÓGICA

O controle de empresas transnacionais sobre a infraestrutura de computação em nuvem (*cloud*) e *softwares* que exigem atualizações contínuas criou o que cientistas políticos chamam de interdependência armada (*weaponized interdependence*).

RISCO DO KILL SWITCH E PARALISIA OPERACIONAL

A maior parte dos governos e grandes empresas nacionais migrou seus bancos de dados e sistemas para os chamados *hyperscalers* americanos (como Amazon AWS, Microsoft Azure e Google Cloud), que concentram a vasta maioria do mercado global.

Bloqueio de contas e acesso: Em caso de conflito diplomático ou sanções econômicas, essas corporações privadas são obrigadas por leis federais americanas a interromper imediatamente a prestação de serviços a entidades sancionadas.

O precedente real: Esse risco deixou de ser teórico. Casos documentados mostram gigantes de tecnologia suspendendo contas e atualizações de agências governamentais, empresas de energia e até autoridades de tribunais internacionais sob as ordens de sanções de Washington.

BLOQUEIO DE ATUALIZAÇÕES (SOFTWARE UPDATE BLOCKADE)

Softwares modernos não são mais mercadorias estáticas compradas de forma definitiva; eles funcionam sob o modelo de SaaS (*Software as a Service*, em português, Software como Serviço) e exigem atualizações diárias de segurança e funcionalidade.

Vulnerabilidade programada: Se uma potência estrangeira proibir a exportação de tecnologia ou atualizações para um país-alvo (por meio de ferramentas como a *Entity List* do Departamento de Comércio dos EUA), os sistemas nacionais tornam-se obsoletos e vulneráveis a ataques cibernéticos em questão de semanas.

Sem atualizações, sistemas de arrecadação de impostos, tráfego aéreo, prontuários de saúde e redes de distribuição de energia de um país inteiro podem ser severamente comprometidos ou paralisados remotamente.

O ALCANCE EXTRATERRITORIAL: O U.S. CLOUD ACT

Além do risco de corte de serviço, existe o risco de espionagem e quebra de sigilo por vias legais. Aprovada nos EUA, a lei conhecida como “CLOUD Act” determina que qualquer empresa de tecnologia sediada em solo americano é obrigada a fornecer dados armazenados em seus servidores ao governo dos EUA, independentemente de onde os servidores estejam fisicamente localizados (mesmo que os dados estejam armazenados em *data centers* na Europa ou na América Latina).

A REAÇÃO GLOBAL: A BUSCA POR SOBERANIA DIGITAL



Figura 4: Governos buscam reduzir a dependência de infraestruturas digitais estrangeiras por meio de núvens soberanas, ecossistemas tecnológicos próprios e software livre, protegendo dados e infraestrutura crítica (imagem gerada com apoio de inteligência artificial).

Essa vulnerabilidade sistêmica acendeu um alerta global. Governos de todo o mundo estão tentando construir defesas contra essa dependência tecnológica:

Resposta europeia: A própria União Europeia avançou com pacotes de Soberania Tecnológica (*Tech Sovereignty Package*) e regras rígidas para nuvens soberanas, tentando proibir ou restringir o uso de nuvens americanas para armazenar dados confidenciais do governo, do judiciário, das forças de defesa e da saúde.

Reação de outras nações: Países como a China desenvolveram ecossistemas tecnológicos totalmente apartados do Ocidente. No Sul Global, governos debatem cada vez mais a criação de nuvens governamentais soberanas e o uso de soluções baseadas em *software* livre, justamente para evitar que a infraestrutura crítica do Estado seja mantida como refém de decisões políticas estrangeiras.

Portanto, a desestabilização de um país por meio de cooptação de militares, membros do congresso, autoridades policiais e controle global dos meios de comunicação descreve o que cientistas políticos e analistas de relações internacionais chamam de Guerra Híbrida ou Guerra de Quinta Geração.

Diferente dos conflitos tradicionais, como visto, essa estratégia foca na erosão interna das instituições de uma nação sem necessidade de uma invasão militar direta. O processo geralmente ocorre também pelos seguintes mecanismos:

Cooptação de forças de segurança (militares e policiais): Realizada por meio de programas de treinamento compartilhado, financiamento velado, intercâmbio de inteligência, dependência de insumos críticos de armas, sistemas de armas e manuais de equipamentos importados, bem como oferta de prestígio. O objetivo é garantir que, em momentos de crise política, essas forças adotem uma postura de omissão ou apoiem veladamente uma mudança de regime (como em golpes de Estado), em vez de defender o governo vigente.

Influência no poder legislativo (membros do congresso): Envolve convites para parlamentares recém-empossados visitarem países no estrangeiro sob argumentos duvidosos, bem como o financiamento de campanhas (direta ou indiretamente via ONGs e fundações), *lobby* e *lawfare*. Ao blindar ou impulsionar parlamentares alinhados aos seus interesses, constrói-se a base jurídica necessária para processos de *impeachment* ou paralisia institucional do país-alvo.

Controle e alinhamento da mídia e informação: A hegemonia sobre agências de notícias globais, plataformas digitais e o financiamento de redes locais do “jornalismo dito oficial”, bem como facilitar o investimento de emissoras nacionais no exterior para criar dependência financeira, permite controlar “o que” e “sobre quem” algo é publicado, moldando assim a opinião pública. Essa estrutura é utilizada para amplificar escândalos de corrupção do governo local, criminalizar movimentos sociais e criar uma narrativa

de “Estado falido”, legitimando intervenções policiais ou militares ou rupturas democráticas.

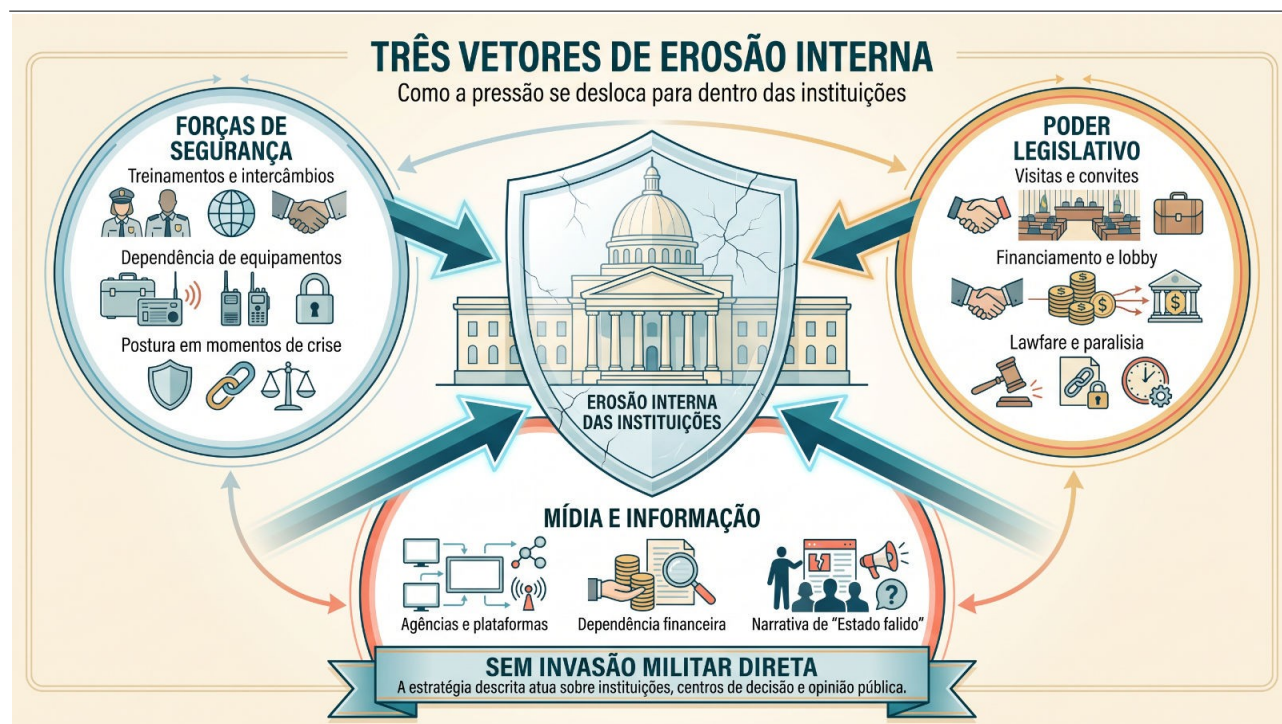


Figura 5: A erosão interna é descrita como resultado da interação entre forças de segurança, Poder Legislativo e mídia e informação, sem necessidade de invasão militar direta (imagem gerada com apoio de inteligência artificial).

PARA O BRASIL

À luz do exposto, este artigo teve por objetivo lançar alguma luz à interferência e desestabilização política, e propor meios jurídicos para diminuir esse efeito, é forçoso concluir que a fragilidade institucional e tecnológica de um país diante de estratégias modernas de desestabilização política demonstra que a soberania nacional no século XXI não se defende mais apenas com fronteiras físicas, mas com fiscalização pública, autonomia jurídica, digital e econômica. A integração profunda de mecanismos de guerra híbrida, *lawfare*, hegemonia financeira, melhoria das regras éticas, jurídicas e de responsabilização dos veículos tradicionais do chamado “jornalismo oficial”, e o controle de infraestruturas críticas em nuvem (*cloud*), transformou as vulnerabilidades internas de uma nação em armas geopolíticas silenciosas e altamente eficazes.

Desde o período colonial, passando pelo Império e pela República, o Brasil convive com pressões geopolíticas. Desde a redemocratização, o país tem vivenciado as consequências concretas de interferências em suas políticas internas e em suas relações com potências nucleares.

A compreensão desse cenário oferece duas lições fundamentais e aponta para medidas urgentes a serem adotadas pelas novas autoridades que assumirão o poder após as eleições presidenciais deste ano:

CONSTRUÇÃO DA SOBERANIA TECNOLÓGICA E DE DADOS (NUVEM SOBERANA)

O Brasil não pode depender de *softwares* que não sejam integralmente nacionais na administração pública, nas Forças Armadas, no Poder Judiciário, incluindo o Supremo Tribunal Federal e o Tribunal Superior Eleitoral, e em suas empresas estratégicas. Tampouco pode armazenar os dados sensíveis dessas instituições em infraestruturas sujeitas a legislações estrangeiras, como o U.S. CLOUD Act.

Medidas sugeridas: O país deve acelerar a implementação e o fortalecimento de uma Nuvem Governamental Soberana, apoiada em centros de dados localizados em território nacional e sob o controle de empresas públicas brasileiras, como a Dataprev e o Serpro. Paralelamente, deve priorizar um planejamento de longo prazo, com horizonte de 30 anos, para a produção nacional de semicondutores, incluindo a fabricação de *wafers* de silício. Nas áreas de segurança e defesa, é necessário priorizar o desenvolvimento e a adoção de sistemas baseados em software livre e de código aberto, com o objetivo de eliminar a dependência de pacotes proprietários estrangeiros sujeitos a atualizações obrigatórias e bloqueios arbitrários.

BLINDAGEM INSTITUCIONAL CONTRA O LAWFARE E A COOPTAÇÃO EXTERNA

A integridade das instituições democráticas, especialmente do Poder Judiciário, do Legislativo e das forças de segurança (militares e policiais), exige freios e controle da sociedade organizada contra a influência assimétrica de potências estrangeiras que utilizam o *soft power* acadêmico e financeiro.

Medidas sugeridas: É necessário estabelecer regras rigorosas de transparência e quarentena para a cooperação jurídica internacional e para o financiamento externo de palestras, seminários e bolsas de estudo destinados a servidores públicos de alto escalão, agentes políticos, ministros e outras autoridades. Deve-se também exigir autorização do Congresso Nacional para a participação de qualquer autoridade pública em cursos no exterior.

Além dessas medidas, propõe-se:

a. Tipificação penal e responsabilização: Criar tipos penais com penas mínimas de oito anos para servidores públicos, ministros, militares, policiais, membros do Ministério Público e agentes políticos que favoreçam interesses estrangeiros em detrimento dos interesses nacionais. Buscar também a responsabilização de seus congêneres estrangeiros que promovam essas interferências, recorrendo a instrumentos

equivalentes aos empregados contra o Brasil, como mecanismos de justiça internacional, pressões diplomáticas e medidas tarifárias, além da articulação com países-parceiros para a adoção de medidas recíprocas.

b. Medidas de reciprocidade econômica e tecnológica: Adotar medidas recíprocas que incidam sobre ativos e interesses econômicos dos países envolvidos, incluindo o bloqueio de dividendos e a quebra de patentes de tecnologias, fármacos e outros produtos de elevado valor estratégico para esses países.

c. Controle institucional e participação social: Criar mecanismos internos de controle e auditoria dessas agendas no Senado Federal, na Câmara dos Deputados, no Conselho Nacional de Justiça e no Conselho Nacional do Ministério Público, com participação da sociedade em audiências públicas. Esses mecanismos devem prevenir conflitos de interesse e assegurar que os agentes dos sistemas de justiça e de segurança nacional atuem estritamente em conformidade com a Constituição, o interesse público e a soberania nacional. Devem, ainda, impedir o uso do aparato estatal como instrumento de perseguição política, de viabilização de mudanças de regime ou de favorecimento de partidos na disputa pelo poder.



Figura 6: A soberania brasileira deve combinar autonomia tecnológica, blindagem institucional e controle democrático, sem isolamento internacional (imagem gerada com apoio de inteligência artificial).

CONCLUSÃO

Em síntese, a defesa da soberania brasileira deve constituir uma política de Estado, contínua e suprapartidária, capaz de integrar autonomia tecnológica, proteção de dados,

integridade institucional e participação efetiva da sociedade. Não se trata de isolar o Brasil do mundo, mas de assegurar que a cooperação internacional se realize em condições de reciprocidade, transparência e respeito à autodeterminação nacional.

Cabe às novas autoridades transformar essas diretrizes em ações concretas, submetidas à Constituição, ao devido processo legal e ao controle democrático, para que a proteção do país não reproduza os abusos que pretende combater.

A soberania não se sustenta apenas em declarações: exige capacidade própria, instituições íntegras e o compromisso permanente de preservar o direito do povo brasileiro de decidir, livremente, os rumos de seu futuro.

****Carlos Alexandre Klomfahs** é advogado, especialista em Direito Internacional dos Conflitos Armados e operador de inteligência egresso dos cursos de geopolítica da Escola de Comando e Estado-Maior do Exército (ECEME) e de estratégia marítima da Escola de Guerra Naval (EGN). É mestrando no Programa de Pós-Graduação em Segurança Internacional e Defesa (PPGSID) da Escola Superior de Guerra (ESG).*
