TRUMP E OS 800 GENERAIS: ENTRE O PALCO E OS BASTIDORES

*Por Carlos A. Klomfahs**

Imagem meramente ilustrativa, gerada por inteligência artificial.

Reuniões militares de alto escalão nos EUA funcionam como sinalização estratégica e veículo para comunicações secretas; com tensões geopolíticas e frente a vulnerabilidades tecnológicas, esses encontros transcendem a mera coordenação operacional.

Na história dos Estados Unidos, há precedentes de reuniões militares de alto escalão cujos propósitos públicos fogem de uma simples coordenação operacional — frequentemente, funcionam como sinalização estratégica tanto para audiências domésticas quanto estrangeiras. Este artigo pretende capturar essa ambiguidade: a reunião é, a um só tempo, espetáculo político e veículo para comunicações secretas.

Cumpre assinalar, outrossim, que a recente mudança de Departamento de Defesa para Departamento de Guerra, aliada *às* movimentações táticas e estratégicas de tropas, equipamentos e armamentos, *somada à* reunião incomum de oficiais-generais lotados nas bases americanas ao redor do mundo pelo governo americano[1], pode ser vista em conjunto *como* um possível sinal que antecede uma operação militar de larga escala.

Neste artigo, defende-se que eventos desse tipo frequentemente servem como pretexto para transmitir mensagens confidenciais — inclusive aquelas que não

[1] https://www.war.gov/News/News-Stories/Article/Article/4319081/unfit-undertrained-troops-no-longer-tolerated/

podem transitar por rádio, internet ou canais criptografados convencionais, por razões de segurança operacional — aproveitando a legitimidade institucional da reunião para encobrir comunicações veladas.

Para sustentar a argumentação, usamos literatura sobre o paradigma do segredo governamental nos EUA, bem como estudos técnicos sobre sistemas de mensagens militares que demonstram limitações reais em transmissões eletrônicas convencionais frente *a* novas tecnologias conhecidas e desconhecidas da Rússia e da China. Em particular, utiliza-se o relatório *Secrecy in U.S. National Security: Why a Paradigm Shift is Needed* (RAND) para discutir a lógica institucional do sigilo nos EUA, e o artigo clássico *A Security Model for Military Message Systems* (Landwehr *et al.*, 1984) para mostrar os desafios técnicos de comunicar *informações* classificadas por rotas digitais seguras.

Pari passu, delineiam-se dois eixos analíticos: (1) análise de uma reunião de generais como ato de comunicação política e simbólica; (2) explicação técnica e institucional de por que certas mensagens não transitam por canais convencionais. Por fim, concluem-se as implicações para a compreensão do uso estratégico do segredo militar em contextos de tensão.

REUNIÃO SIMBÓLICA E SUA FUNÇÃO DE SINALIZAÇÃO GEOPOLÍTICA

Neste primeiro eixo, investiga-se como reuniões militares de alto nível — especialmente envolvendo generais e almirantes — são usadas como instrumentos geopolíticos de imagem e de comunicação estratégica. Duas dimensões merecem destaque:

1. **A mensagem para público interno:** Ao reunir generais, o governo envia uma mensagem de "controle, preparação e unidade" para audiências domésticas: ao Congresso, à mídia e à opinião pública civil. A retórica oficial antecipa fortalecimento, prontidão e coerência das Forças Armadas, sobretudo em cenários de incerteza geopolítica, sob o verniz que, inclusive, pode realçar a presença e os aspectos físicos dos oficiais-generais.

2. **Mensagem para público externo:** Internamente abrigada sob pretenso caráter funcional, a reunião serve para projetar força ou intenção *para* adversários e aliados, sem necessariamente revelar os conteúdos concretos da comunicação. A própria convocação gera especulações estratégicas, com a notícia de que centenas de generais e almirantes americanos seriam reunidos em Quantico, Virgínia, sem clareza *sobre* o objetivo formal — o que alimenta interpretações de sinalização estratégica tanto para a comunidade internacional quanto para grupos internos nos EUA.

Com efeito, esse tipo de encontro oferece cobertura institucional e legitimidade para deslocamentos, troca de documentos e encontros paralelos discretos (bilaterais ou multilaterais entre participantes), mascarados como "agenda técnica". O caráter raro ou extravagante da reunião (número expressivo de generais, espaço militar reservado, sigilo sobre pauta) reforça seu efeito dramático de palco político.

Porém, indaga-se: qual é o valor prático dessa "mensagem simbólica"? Ele reside no duplo nível de comunicação: formal (o que é anunciado) e informal (o que se transmite nos bastidores). O caráter secreto é parte integrante do *design*: enquanto a agenda pública *distrai*, comunicações veladas circulam "abaixo do radar".

Seria isso?

CANAL ENCOBERTO: COMUNICAÇÃO CLANDESTINA ALÉM *DA* CRIPTOELETRÔNICA

No segundo eixo, passo à parte técnica e institucional: por que, historicamente, certos governos (e, particularmente, o americano) procuram meios de comunicação alternativos ao rádio, redes digitais ou mesmo canais criptografados, *ainda que* relativamente seguros? A hipótese provisória é de que o atual estado de inteligência e interceptação de sinais, capacidade cibernética, computação pós-quântica e de guerra eletrônica da Rússia e da China *é inconclusivo*, não se podendo correr riscos *diante do* caráter gravoso das comunicações, ordens ou preparações para operações militares em grande escala.

LIMITAÇÕES DE CANAIS ELETRÔNICOS E O PARADIGMA DO SIGILO INSTITUCIONAL

Apesar dos decantados avanços criptográficos, os Estados Unidos mantêm um paradigma robusto de sigilo institucional, que regula *a forma como* informações classificadas são criadas, protegidas, transmitidas e eventualmente desclassificadas, em tempos de insegurança cibernética e sobre o atual estado da inteligência de sinais da China e da Rússia. Em casos de comunicação emergencial, a presença pessoal de oficiais-generais em reunião com o secretário do Pentágono em Quantico, Virgínia, em 30 de setembro de 2025, é a forma mais antiga e relativamente segura de transmissão de ordens sigilosas e/ou comunicação de fatos e situações relevantes do ponto de vista militar e geopolítico. É possível, portanto, que a situação econômica, geopolítica e militar dos EUA tenha chegado a um nível em que a única opção é "criar" uma guerra.

Geralmente, o *script* do governo americano para ingressar em uma guerra declarada *sempre se posiciona* como vítima: "os EUA foram atacados por tropas mexicanas em 1846; *idem*, na Guerra Hispano-Americana em 1898; pelo Japão em 1941, precipitando o ingresso *dos EUA* na II Guerra Mundial; o incidente no Golfo de Tonquim, em 1964, na Guerra do Vietnã; no Iraque em 2003; e várias outras lições históricas de que todos os envolvimentos americanos em guerra *partiram* do pretexto de um 'Estado de Defesa'."

Seja diretamente, seja por seus interesses no estrangeiro, como observa o professor Guilherme Sandoval[2] da Escola Superior de Guerra (PPGSID) sobre as estratégias de segurança nacional dos Estados Unidos, que projetam mundialmente a economia americana, a qual *se encontra* acuada pela desdolarização, perda de competitividade internacional de sua indústria e das cadeias de abastecimento de terras raras e *de* segurança hídrica, bem como pelo clima internacional de contestação do

[2] *Revista da Escola Superior de Guerra, v. 39, n. 86, p. 34-61, maio-ago. 2024.*

imperialismo ocidental sobre os demais países, como apontado no relatório *Global Trends* (2030) do Conselho Nacional de Inteligência.

Já o relatório da RAND, *Secrecy in U.S. National Security: Why a Paradigm Shift is Needed*, de 2018, destacou que a vulnerabilidade nas comunicações militares dos EUA é uma realidade diante das capacidades cibernéticas, de guerra eletrônica e de criptografia quântica da China e da Rússia, bem como o ciclo do segredo (classificação, salvaguarda, divulgação) é institucionalizado por leis, decretos, regulamentos e cultura organizacional, não apenas por tecnologia.

Esse paradigma ressalta que, para certas camadas de informação, *não existe nenhum canal* totalmente confiável: o risco de interceptação, vazamentos ou falhas de chave é inescapável.

Logo, o aparato institucional muitas vezes recorre a "formas físicas ou híbridas de comunicação" (documentos fechados, mensageiros especializados, encontros presenciais sob cobertura oficial) para garantir integridade e sigilo.

ESTUDOS TÉCNICOS SOBRE SISTEMAS *DE* MENSAGENS MILITARES CLASSIFICADAS

O artigo clássico[3] *A Security Model For Military Message Systems* (Landwehr *et al.*, 1984) demonstra que sistemas de mensagens militares enfrentam problemas intrínsecos para operar sob segurança multinível (*multilevel security*), revelando-se *demasiadamente* limitador em casos práticos de comunicação militar, especialmente quando usuários precisam reclassificar mensagens ou extrair partes de diferentes níveis de classificação, causando *lacunas de* vulnerabilidades para oponentes e para sistemas de vigilância e monitoramento de tráfego de informações multiespectrais e multibandas.

Na edição atual da *Military Review*, há um artigo[4] de John R. Creel e James J. Torrance, ambos coronéis do U.S. Army, intitulado: *Beyond the Network: The Army Signal Corps and the Future of Warfare*, onde se descreve que "*O campo de batalha do futuro: transparente, saturado e contestado*" exigirá que as formações de combate lutem em ambientes saturados de sensores e definidos por vigilância persistente. O resultado é um campo de batalha onde, como observa John Antal, as forças "*devem se mascarar ou morrer*", e que a capacidade de gerenciar assinaturas — eletromagnéticas, físicas e digitais — tornou-se tão crítica quanto a própria manobra, *sendo* inclusive reforçado pelo Manual de Campo (FM) 3-0, Operações, ao observar que as formações operarão sob "*contato eletromagnético persistente*" e que o domínio do espectro é um requisito para a sobrevivência.

Essas limitações técnicas servem como precedentes para a hipótese de que, em contextos de crise ou preparação para conflito, as instituições militares recorrem a rotas de comunicação física ou semifísica — encontros, documentos transportados por mensageiros autorizados, trocas diretas durante reuniões — justamente para

[3] https://dl.acm.org/doi/pdf/10.1145/989.991.

[4] https://www.armyupress.army.mil/journals/military-review/online-exclusive/2025-ole/beyond-the-network/.

superar vulnerabilidades que permanecem mesmo em sistemas criptografados, dada a incerteza sobre a capacidade do inimigo.

PRECEDENTES HISTÓRICOS: "CODE TALKERS", MAGIC *E* VENONA

Como exemplos históricos, vale citar os "Code Talkers" da Marinha e do Corpo de Fuzileiros Navais dos EUA durante a Segunda Guerra Mundial, que usavam línguas indígenas (como o navajo) para transmitir mensagens táticas que não podiam ser decifradas por inimigos *convencionais*. Outro exemplo é o projeto MAGIC, de criptoanálise dos códigos japoneses, cujo manuseio era estritamente controlado: mesmo autoridades superiores recebiam apenas relatórios filtrados, sem acesso direto à fonte criptográfica. *Similarmente*, o projeto VENONA foi mantido restrito inclusive dentro de órgãos do governo dos Estados Unidos, com sua origem e operação parcialmente veladas para a própria alta administração.

Esses casos ilustram que, historicamente, os EUA já recorreram a formas híbridas de comunicação — onde parte do conteúdo permanece oculta, *sendo* distribuído apenas sob confiança e pessoalmente — quando a sensibilidade da informação excede o que pode ser entregue via rede criptografada *convencional*.

À GUISA DE CONCLUSÃO

Nestas mal traçadas linhas, pode-se concluir, *en passant*, que um dos maiores riscos que países e suas Forças Armadas adotam *consiste em* não "oxigenar" o topo político-estratégico com perspectivas disruptivas *provenientes da base* das novas gerações; o sucessivo e contraditório "choque de gerações iminente e atual" *expande-se* da sociedade para as instituições. O *modus operandi* do governo americano já foi "*mapeado*" pelas principais potências mundiais, assinalando que suas táticas estão ultrapassadas, *uma vez que* perderam muito tempo tentando ser a "polícia do mundo", imiscuindo-se em planos e mais planos imperialistas de suas empresas globais *e* na política de Estados que lhes interessam (Estados falidos e tampão) sob a vetusta "diplomacia do *big stick*" *e da* "cenoura ou porrete", e a estratégia de Nicolas Spykman de cerco ao Rimland, ou seja, a Ilha Mundo e o Heartland que, se conquistado, *poderia* dominar o mundo, exatamente *países que são* potências terrestres como Rússia e China.

O risco de uma guerra aberta e declarada entre o Ocidente e os países do Oriente reside na estafa que pode afetar o processo decisório, *no* erro de cálculo e *no* limite de tolerância daqueles países *em relação* às reiteradas ações lideradas pelos EUA de forma permanente, desde o fim da Segunda Guerra Mundial, para implantar uma política de cerco e contenção a todo momento, agindo, como se diz na Artilharia, *na forma de* "*tiro de inquietação*" (p. 268, MD35-G-01), desafiando a conhecida "paciência estratégica" das potências orientais e asiáticas, até que o ponto de não retorno se consubstancie.

Em suma, a reunião de generais americanos, como movimento simbólico e estratégico, deve ser compreendida não apenas como ato de coordenação militar, mas como momento de comunicação política multiforme: para consumo interno e externo e com funções ocultas de transmissão confidencial. A ambiguidade dessa reunião — sua convocação pública sem divulgação clara de pauta e *a* posterior divulgação oficial sobre questões físicas e ideológicas *dos* oficiais-generais — sugere que parte de seu

propósito real é permitir o trânsito de mensagens sensíveis sob cobertura institucional.

Tecnicamente, *observa-se* que o paradigma do sigilo nos EUA permanece profundamente arraigado: o uso de canais físicos, encontros presenciais e documentos controlados ainda figura como alternativa necessária quando a criptografia eletrônica não oferece segurança suficiente para as camadas mais sensíveis da informação.

O relato técnico de Landwehr *et al.* sobre sistemas de *mensagens* militares demonstra que, mesmo em ambientes potencialmente seguros, a reclassificação e controle de fluxos multigerenciados ainda é um desafio.

Além disso, precedentes históricos — dos "Code Talkers" aos projetos MAGIC e VENONA — confirmam que o uso de meios velados já faz parte da matriz institucional americana. Esses exemplos validam a hipótese provisória de que, em momentos de tensão ou preparação estratégica, o governo dos Estados Unidos pode deliberadamente orquestrar uma reunião de generais como fachada, simultaneamente para encenar poder, definir diretrizes presidenciais de uma iminente operação militar em grande escala e viabilizar comunicações discretas. Nenhum ato militar ou geopolítico *se centra* em apenas uma motivação: é essencial à doutrina militar o princípio da economia de forças!

Por fim, esse tipo de fato público de alta relevância, junto com a situação econômica e de contestação dos EUA, aliado *à* recente alteração de Departamento de Defesa para Departamento de Guerra — *incluindo a* reunião militar como canal híbrido de comunicação — merece atenção como objeto de análise nas Relações Internacionais. O conjunto dos fatos (*big picture*) revela como estratégias de poder operam também no domínio simbólico e comunicativo, em que o segredo e a visibilidade são dois lados de uma mesma moeda política, apontando o que pode ou não ser o começo de uma Terceira Grande Guerra Mundial.

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