

O PARADOXO DO USO DUAL DA TECNOLOGIA: O CASO DA STARLINK EM CONFLITOS RECENTES E NAS ATIVIDADES ILÍCITAS NA AMAZÔNIA LEGAL BRASILEIRA

Marcus Vinicius Gonçalves da Silva¹

1. Introdução

O uso da tecnologia na sociedade contemporânea desempenha um papel vital, impulsionando avanços em todos os setores da vida humana. O campo das comunicações, da medicina, da educação e da indústria, são apenas alguns, dos inúmeros setores onde a tecnologia vem realizando inovações e dando suas contribuições quase que diariamente.

No entanto, o uso ubíquo da tecnologia trouxe consigo uma série de desafios e considerações que não podem ser ignorados. A *internet*, em particular, abriu novos horizontes de comunicação, possibilitando o compartilhamento instantâneo de informações e conhecimento para todas as partes do globo. Porém, como tecnologia dual (civil e militar), a *internet* não está disponível somente para usuários civis, setores governamentais, órgãos de defesa e segurança. Pelo contrário, tal ferramenta também está disponibilizada para ser empregada em situações de guerra e pelo crime organizado em atividades ilícitas.

Em matéria publicada em 20 de outubro de 2023 na BBC News Brasil, tornou-se público que a *Starlink* instalou antenas em 90% dos municípios da Amazônia legal brasileira, a qual é formada pelos Estados do Acre, Amapá, Amazonas, Mato Grosso, Pará, Rondônia, Roraima, Tocantins e parte do Maranhão (SENRA; COSTA, 2023). Contudo, aquilo que tinha tudo para ser um meio para trazer o desenvolvimento e a prosperidade dessa região, acabou por se tornar também numa valiosa ferramenta que vem sendo utilizada em atividades ilícitas na Amazônia.

Do exposto, este ensaio objetiva descrever o domínio da empresa *Starlink* no fornecimento de serviços de *internet* no conflito russo-ucraniano, no conflito entre Israel e *Hamas*, na região amazônica, da mesma forma que procura descrever sumariamente como está estruturado o setor da defesa cibernética no Brasil, correlacionando essa temática com as questões relacionadas à segurança e soberania nacional.

2. *Starlink* e o conflito russo-ucraniano

Starlink é uma rede de satélites desenvolvida pela empresa privada *SpaceX* e que pertence ao

¹ 1º Tenente do Exército Brasileiro e Doutor em Administração pela PUC-PR.

O paradoxo do uso dual da tecnologia: o caso da Starlink em conflitos recentes e nas atividades ilícitas na Amazônia Legal brasileira - Panorâmico

fundador e diretor-executivo *Elon Musk*. A *SpaceX* tem como objetivo fornecer *internet* de baixo custo para locais remotos. Um satélite *Starlink* tem a vida útil de aproximadamente cinco anos. E a *SpaceX* espera desenvolver 42.000 satélites, formando a chamada mega constelação.

A versão atual do satélite *Starlink* tem aproximadamente 800 kg no lançamento. Ou seja, um peso quase três vezes maior do que os satélites da geração anterior, que pesavam 260 kg. Howell e Pultrarova (2023) revelam que em julho de 2023, a empresa *SpaceX* possuía 4.519 satélites *Starlink* em órbita, sendo que apenas 4.487 estavam em operação.

Em fevereiro de 2022, *Elon Musk* enviou terminais *Starlink* à Ucrânia, em resposta aos apelos públicos das autoridades ucranianas. A conectividade fornecida pelo satélite *Starlink* foi fundamental para que o exército ucraniano coordenasse os ataques e obtivesse dados com o uso de drones.

Figura 1 - Combatente ucraniano usando o sistema *Starlink*



Fonte: KIM, 2023.

Porém, em setembro de 2023, *Elon Musk* não autorizou que o governo da Ucrânia tivesse acesso à rede *Starlink*. Como justificativa para tal decisão, *Elon Musk* disse que estava receoso de que o conflito russo-ucraniano pudesse escalar para um conflito nuclear (KIM, 2023).

Mykhailo Podolyak, conselheiro sênior do presidente ucraniano *Volodymyr Zelensky*, classificou o ato de *Elon Musk* como *interferência*, pois permitiu que a frota naval russa continuasse a disparar mísseis de cruzeiro contra as cidades ucranianas com maior liberdade de ação. Em que pese os esforços realizados para verificar alternativas junto a outros provedores mundiais de *internet* via satélite, as autoridades ucranianas concluíram que não há outra empresa que ofereça um serviço que tenha o mesmo alcance e a mesma qualidade do que o serviço prestado pela *Starlink*. Em suma, a principal provedora da infraestrutura de comunicações na Ucrânia continua sendo a *Starlink* (KIM, 2023).

3. Starlink e o conflito entre Israel e Hamas

Mais recentemente, no dia 28 de outubro de 2023, em razão dos ataques israelenses à infraestrutura do *Hamas*, os quais causaram danos aos provedores de *internet*, *Elon Musk* prometeu prover conexão à *internet*, via satélite, às organizações humanitárias internacionais que operam em Gaza (ISRAEL NATIONAL NEWS, 2023).

Após as reações contrárias do ministro das comunicações de Israel, *Shlomo Karhi*, relacionadas ao fornecimento do serviço de *internet* em Gaza, *Elon Musk* revelou que nenhum terminal da *Starlink* irá se conectar a partir de Gaza. E, caso um único terminal da *Starlink* seja conectado, serão tomadas as medidas necessárias para confirmar que o uso seja somente para questões humanitárias e sob o chapéu dos protocolos de segurança, que estarão sendo verificados pelos governos dos Estados Unidos da América e de Israel.

A decisão de *Elon Musk* suscita questões relevantes sobre o uso de tecnologias monopolizadas, em específico, no fornecimento de serviços de *internet* de banda larga para os sistemas de comunicações bélicos. Considerando que o satélite *Starlink* é um produto comercial e a *SpaceX* não é uma fornecedora exclusiva de produto para a área de Defesa, as decisões tomadas por *Elon Musk* podem causar conflitos de interesses com o governo dos Estados Unidos da América.

4. Starlink e a Amazônia Legal

O uso do satélite *Starlink* na Amazônia Legal brasileira, como qualquer outra tecnologia, pode ter implicações positivas, como negativas, incluindo questões relacionadas à segurança e atividades criminosas. O uso é positivo na medida em que fornece acesso à *internet* para populações que vivem em locais remotos da Amazônia, onde a infraestrutura de comunicações é limitada ou inexistente, melhorando a qualidade de vida das pessoas residentes nesses locais. Para Senra e Costa (2023), os equipamentos da *Starlink* têm sido utilizados pelas comunidades indígenas *Yanomami*. Para o presidente da associação *Yanomami*:

“[...] o equipamento tem ajudado de forma excepcional, tanto para equipe de saúde, que diariamente repassa informações e solicitações de resgate, como para os yanomami, que nos comunicam sobre tudo que acontece na região em que está instalada a internet” (SENRA; COSTA, 2023, s.p.).

Em emergências relacionadas à saúde e a crises ambientais, a conectividade proporcionada pelos equipamentos da *Starlink* pode ser essencial, pois permite a comunicação e a coordenação de forma eficaz. Para o filósofo Feenberg (1991), a democratização da tecnologia se estrutura a partir dos interesses daqueles que geralmente são excluídos dos processos tecnológicos. Isso significa oportunizar tecnologia às populações mais vulneráveis, que confrontariam, por exemplo, com a lógica do lucro que orienta a tecnologia para os interesses do mercado.

O paradoxo do uso dual da tecnologia: o caso da Starlink em conflitos recentes e nas atividades ilícitas na Amazônia Legal brasileira - Panorâmico

Em operação realizada em janeiro de 2023 pelo Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis (IBAMA), os agentes do IBAMA apreenderam cinco antenas de internet de banda larga *Starlink* em terras *Yanomami*, conforme apresentado a seguir:

Figura 2 - Apreensão de antena *Starlink* em terra *Yanomami*



Fonte: ASSOCIATED PRESS, 2023.

Diante do crescente número de apreensões de equipamentos da *Starlink*, o IBAMA tem realizado estudos junto a outros órgãos federais brasileiros para bloquear o sinal do satélite da *Starlink* em áreas de mineração ilegal (ASSOCIATED PRESS, 2023). Isso se deve porque tais equipamentos têm sido empregados em atividades ilícitas pelos criminosos para coordenar as comunicações, receber avisos sobre a movimentação dos órgãos de segurança durante as operações e realizar pagamentos, via pix. Dados do IBAMA revelam que até o mês de agosto de 2023, trinta e duas antenas *Starlink* haviam sido apreendidas em operações de combate ao garimpo ilegal (SENRA; COSTA, 2023).

Figura 3 - Apreensão de antena *Starlink* em área de garimpo ilegal



Fonte: ASSOCIATED PRESS, 2023.

O acesso à *internet*, pelo provedor *Starlink*, tem facilitado o trabalho desenvolvido por garimpeiros ilegais, pela extração ilegal de madeira e pelos traficantes de drogas em locais isolados da região amazônica, inclusive com o uso do aplicativo *whatsapp*, implicando em novo *modus operandi* das organizações criminosas.

Figura 4 - Equipamento *Starlink* apreendido em área de garimpo ilegal



Fonte: GAVRAS, 2023.

Contudo, cabe salientar que o uso da *internet* pelos garimpeiros não é algo recente. Anteriormente à chegada da *Starlink* na Amazônia Legal brasileira, os garimpeiros costumavam contratar técnicos para fornecer as comunicações necessárias a atividade. Normalmente, os técnicos instalavam uma antena para possibilitar a realização dessas comunicações. Isso só não acontecia quando os locais de mineração eram alvos de operações dos órgãos de segurança ou quando era necessário realizar a mudança de local. Todavia, a conexão era lenta e instável, principalmente em dias chuvosos.

5. Defesa Cibernética no Brasil

No Brasil, a concepção estratégica de defesa entende que o desenvolvimento de tecnologias de uso dual é o elemento fundamental para alcançar o abastecimento de produtos de defesa visando à autonomia tecnológica do país (BRASIL, 2020). Com relação ao setor cibernético, percebe-se a preocupação da Estratégia Nacional de Defesa ao descrever que as capacitações cibernéticas destinar-se-ão ao mais amplo espectro de emprego dual (BRASIL, 2023).

As Estratégias Nacionais de Defesa elaboradas nos anos de 2008, 2012, 2016 e 2020, têm elencado os três setores considerados essenciais para a Defesa Nacional: o nuclear, o *cibernético* e o espacial. Esses setores possuem elevada complexidade, exigem liderança centralizada, estreita e

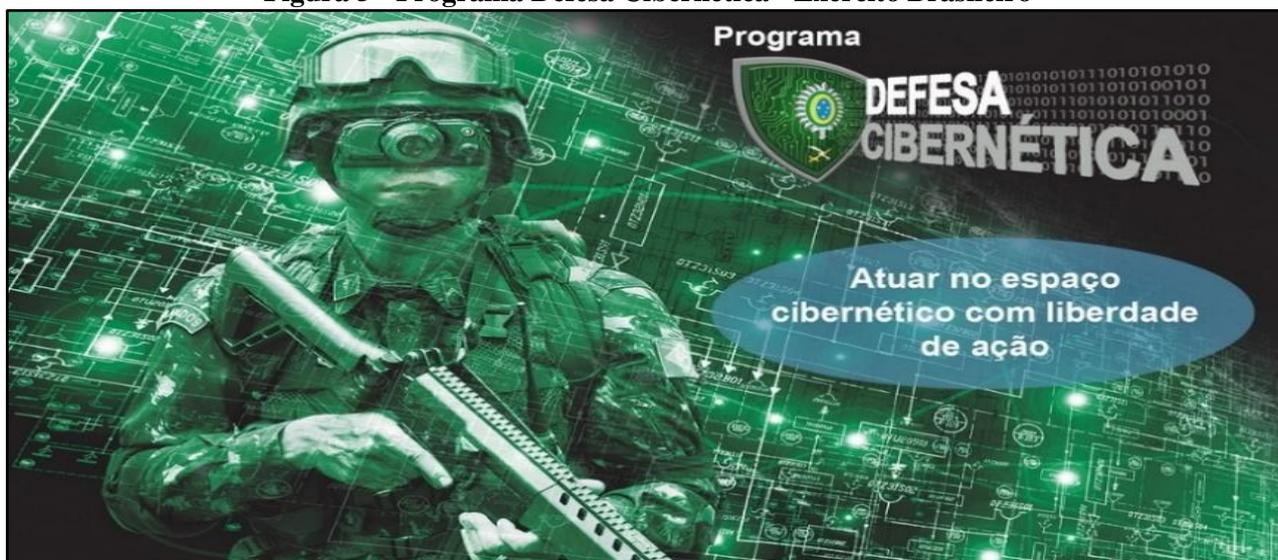
O paradoxo do uso dual da tecnologia: o caso da Starlink em conflitos recentes e nas atividades ilícitas na Amazônia Legal brasileira - Panorâmico

integrada coordenação com diversos atores e com várias áreas do conhecimento. Dessa forma, a Estratégia Nacional de Defesa atribui ao Exército Brasileiro a responsabilidade pelo setor **cibernético** e estabeleceu que os projetos estratégicos relacionados à segurança cibernética devem fortalecer a atuação colaborativa entre o setor de Defesa, a comunidade acadêmica nacional, o setor público, o setor privado e a Base Industrial de Defesa (BRASIL, 2020). Para o Escritório de Projetos do Exército:

“O Setor Cibernético abrange atualmente todos os aspectos da vida cotidiana, uma vez que atua através do emprego de modernos meios tecnológicos, redes de computadores e de comunicações destinadas ao trânsito de informações. Desta forma, seja no atendimento das necessidades individuais das pessoas, seja dando suporte para as organizações diversas, inclusive aquelas dedicadas a setores estratégicos do País, como a Defesa Nacional, a Cibernética é um campo de atuação vasto e complexo, e sua segurança implica na segurança das pessoas e da própria Nação” (BRASIL, 2023, s.p.).

No âmbito do Exército Brasileiro, compete ao Centro de Defesa Cibernética coordenar e integrar os esforços dos vetores vocacionados para essa área de atuação. Por meio do programa de defesa cibernética, o Escritório de Projetos do Exército adotou o seguinte *slogan*: "Atuar no espaço cibernético com liberdade de ação”:

Figura 5 - Programa Defesa Cibernética - Exército Brasileiro



Fonte: BRASIL, 2023.

Com base nesse *slogan* e para melhor compreender o que significa o espaço cibernético, torna-se necessário tecer detalhes adicionais acerca do conceito de ciberespaço. Para Lévy (1998), ciberespaço é o universo das redes digitais, consubstanciando numa nova fronteira econômica e cultural. Ou seja, o ciberespaço é uma plataforma de uma nova realidade humana, cuja acronia e atopia ampliam os limites de possibilidades do homem, tanto às informações e comunicações, quanto à sua criatividade (LÉVY, 1999).

No entendimento de Kissinger (2015), o ciberespaço abarca desde informações transmitidas via telefones celulares, até complexos sistemas autônomos de uso militar. No ciberespaço, devido às vulnerabilidades às quais os Estados são expostos, é produzido um estado de natureza, cujas fronteiras, governança, responsabilidade e autoria são indefinidas e indeterminadas.

Para Ribas e Ziviani (2008), no ciberespaço há um elemento denominado comunidade virtual, que, auxiliada pela tecnologia, organiza-se em torno de uma finalidade em comum, englobando um conjunto de pessoas que estabelecem vínculos sociais e de pertencimento, diferenciando-se dos grupos e equipes tradicionais, principalmente pelo modo que ocorre a interatividade.

No país, cabe ao Exército Brasileiro envidar esforços no sentido de propor alternativas que tenham como finalidade proteger as principais infraestruturas estratégicas do Brasil no ciberespaço.

6. Considerações Finais

Para mitigar os riscos associados ao uso da *Starlink* na Amazônia, é fundamental que sejam estabelecidos protocolos de segurança e regulamentações adequadas. Além disso, as agências de aplicação da lei devem estar preparadas para monitorar a atividade na rede e investigar possíveis atividades criminosas. Também é importante envolver as comunidades locais e organizações de conservação na promoção do uso responsável da tecnologia, ao mesmo tempo em que se aproveitam os benefícios da conectividade.

No caso da Amazônia brasileira, o combate ao garimpo ilegal é um desafio multifacetado que requer esforços contínuos de normatização, fiscalização e repressão. Além disso, a conscientização sobre os impactos negativos do garimpo ilegal é fundamental para mobilizar ações junto a sociedade com o fito de proteger a região e suas comunidades.

Em relação ao uso da tecnologia em atividades ilícitas, em consonância com a Estratégia Nacional de Defesa, cabe ao Exército Brasileiro, por meio de ações conjuntas com órgãos federais e estaduais, promover a defesa cibernética a fim de impedir que o ciberespaço seja utilizado para fins ilegais.

O domínio do provedor de *internet* de banda larga *Starlink* na Amazônia Legal, apresenta-se como uma oportunidade para novas discussões sobre regulação e fiscalização, principalmente quanto à natureza de tecnologias duais, produzidas e comercializadas por empresas estrangeiras.

Referências:

ASSOCIATED PRESS. **Antenas da Starlink são apreendidas em garimpo ilegal na Terra Yanomami.** Associated Press, 2023. Disponível em: <https://g1.globo.com/tecnologia/noticia/2023/0>

O paradoxo do uso dual da tecnologia: o caso da Starlink em conflitos recentes e nas atividades ilícitas na Amazônia Legal brasileira - Panorâmico

3/15/antenas-da-starlink-sao-apreendidas-com-garimpeiros-em-terra-yanomami.ghml. Acesso em: 26 de outubro de 2023.

BRASIL. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2020.

BRASIL. Exército Brasileiro. Estado-Maior do Exército. **Defesa Cibernética**. Brasil, 2023. Disponível em: <http://www.epex.eb.mil.br/index.php/defesa-cibernetica/defesa-cibernetica>. Acesso em: 29 de outubro de 2023.

FEENBERG, Andrew. **Critical theory of technology**. New York: Oxford University Press, 1991.

GAVRAS, Douglas. **Kits da Starlink, de Elon Musk, são apreendidos em garimpo ilegal na Amazônia**. Folha de São Paulo, 2023. Disponível em: <https://www1.folha.uol.com.br/tec/2023/06/kits-da-starlink-de-elon-musk-sao-apreendidos-em-garimpo-ilegal-na-amazonia.shtml>. Acesso em: 26 de outubro de 2023.

HOWELL, Elizabeth; PULTRAROVA, Tereza. **Starlink satellites: Everything you need to know about the controversial internet megaconstellation**. Space.com, 2023. Disponível em: <https://www.space.com/spacex-starlink-satellites.html>. Acesso em: 26 de outubro de 2023.

KIM, Victoria. **Elon Musk Acknowledges Withholding Satellite Service to Thwart Ukrainian Attack**. New York Times, 2023. Disponível em: <https://www.nytimes.com/2023/09/08/world/europe/elon-musk-starlink-ukraine.html>. Acesso em: 26 de outubro de 2023.

KISSINGER, Henry. **Tecnologia, equilíbrio e consciência humana**. São Paulo: Objetiva, 2015.

ISRAEL NATIONAL NEWS. **Elon Musk promises to connect Gaza to internet**. Israel National News, 2023. Disponível em: <https://www.israelnationalnews.com/news/379293>. Acesso em: 29 de outubro de 2023.

LÉVY, P. **A inteligência coletiva por uma antropologia do ciberespaço**. São Paulo: Loyola, 1998.

LÉVY, P. **Cibercultura**. São Paulo: Editora 34, 1999.

RIBAS, C. S. C.; ZIVIANI, P. **Redes de informação: novas relações sociais**. Revista de Economia Política de las Tecnologías de la información y Comunicación, Vol. 10, nº 1, p. 1-21, 2008.

SENRA, Ricardo; COSTA, Camilla. **Elon Musk domina internet por satélite na Amazônia com antenas em 90% das cidades**. BBC, 2023. Disponível em: <https://www.bbc.com/portuguese/articles/cv2edkw84zmo>. Acesso em: 26 de outubro de 2023.