

# Os Satélites e o Espaço na Transformação da Atividade Militar

Tenente-coronel  
Pedro Marquês de Sousa



## Introdução

As novas tecnologias transformaram o “Espaço” numa nova dimensão da atividade militar, dependente de satélites para as comunicações, para orientação de mísseis, drones, navios e aviões, através do sistema global de navegação por satélite e para o funcionamento dos sistemas de armas. As principais potências militares têm dado grande importância a esta nova dimensão, onde se verifica a ascensão da China, o declínio da Rússia e o grande poder dos Estados Unidos da América e de Israel.

Devido à guerra na Ucrânia, a Agência Espacial Europeia abandonou os projetos que tinha com a Rússia e em alternativa estabeleceu parcerias com empresas dos EUA.

Israel realizou recentemente a primeira ação de combate no espaço<sup>1</sup> que, apesar de ter passado despercebida, ficará na história como o primeiro caso em que um sistema de armas destruiu um alvo fora da atmosfera<sup>2</sup>, mostrando como um sistema anti-míssil pode funcionar como arma anti-satélite (ASAT)<sup>3</sup> o que alimenta a polémica sobre o escudo anti-míssil que os EUA instalaram na Europa e que a Rússia considera uma ameaça, também ao seu poder espacial. A utilização de satélites comerciais em missões militares, na Ucrânia, também levanta novas questões, sobre a legitimidade das empresas de satélites, para realizarem missões de combate.

Além da atividade militar, os satélites são fundamentais no funcionamento de muitos serviços civis, especialmente nas telecomunicações e Internet, e por isso o domínio do espaço e do espectro eletromagnético, são fundamentais para as grandes potências. Além das missões de vigilância que localizam pessoas e equipamentos com precisão, os satélites fazem a interceção de comunicações e de sinais de radar, o bloqueio e falsificação de dados, a deteção de alvos aéreos e ações ofensivas. Enquanto a vigilância feita por radares e meios aéreos, fornece apenas uma “visão” limitada, os satélites têm

uma visão global e permitem o funcionamento de um sistema “integrado” em que as diversas componentes militares (terrestre, aérea e naval) e civis, partilham informações em tempo real, coordenando a sua atuação com base num conhecimento da situação muito completo, como nunca antes foi possível.

As grandes potências estão a desenvolver capacidades no espaço, onde se observa a ascensão da China, o atraso da Rússia e o poder superior dos EUA. A China criou em 2015 um novo ramo militar (Força de Apoio Estratégica) que foi recentemente transformado na “Força de Apoio à Informação”, para desenvolver um sistema de informação em rede, através da integração das capacidades espaciais, cibernéticas e de guerra eletrónica. Nas Forças Armadas dos EUA, foi também criada em 2019 a Força Espacial<sup>4</sup> que, em 2025, irá realizar um exercício militar sem precedentes, que poderá significar uma revolução na atividade militar, confirmando que os EUA são a potência com maior potencial, também no espaço, enquanto a Rússia sofre as sanções e o isolamento que a impede de ter acesso à tecnologia, a chips e microprocessadores. A qualidade dos chips da Rússia é muito inferior ao padrão da indústria do ocidente, pelo que as suas armas, comunicações e os sistemas de guerra eletrónica são altamente dependentes de microchips fabricados no ocidente. Em relação aos sistemas de posicionamento via satélite, o russo GLONASS também é inferior ao GPS (EUA), que é mais preciso e tem mais cobertura global do que o sistema russo, pois o GLONASS perde sinal em algumas partes do planeta e o seu erro de precisão é 1 a 2 metros superior ao do GPS.

## Os Sistemas Militares no Espaço

O espaço é a nova fronteira da guerra, de onde se pode controlar a Terra de uma posição superior, com grande vantagem, através de diversos tipos de satélites: de vigilância, de comunicação, de navegação e de ações ofensivas. Os satélites de Inteligência, Vigilância e Reconhecimento (ISR) equipados com câmaras de alta resolução e outros sensores (infravermelhos, rádio frequências, etc.) são usados para recolher imagens e outras informações, localizar armas e equipamentos dos adversários<sup>5</sup>. Os satélites de comunicação garantem as ligações entre as forças militares, a transmissão de dados e Internet enquanto os satélites de navegação são usados para guiar os drones e mísseis, aviões e navios, além de fornecer às tropas, informações precisas sobre as suas posições em tempo real<sup>6</sup>. Os Sistemas Globais de Navegação por Satélite (GNSS) fornecem serviços espaciais de posição, navegação e tempo (PNT) e os mais conhecidos são o sistema GPS dos EUA, a rede Galileo da UE, a BeiDou da China e a Glonass da Rússia.

Os primeiros satélites de vigilância recolhiam imagens através de equipamentos ópticos usando a luz visível ou infravermelha, mas as limitações deste sistema, de noite e em condições meteorológicas adversas levaram ao desenvolvimento da tecnologia de satélite radar SAR (Synthetic Aperture Radar). A guerra na Ucrânia mostrou as capacidades destes satélites dos EUA, com sensores radar, de radiofrequência e hiperespectral, dando grande vantagem aos ucranianos sobre os russos, que não possuem satélites deste tipo. A

deteção por [radiofrequência \(RF\)](#) localiza emissões através de um sensor remoto (em satélites de baixa órbita) para detectar navios, viaturas e outros equipamentos que emitam sinais de radiofrequência. Os sensores hiperspectrais recolhem dados em diversas bandas espectrais para a recolha de informações mais detalhadas, como a composição material dos alvos, o tipo de vegetação, equipamentos camuflados/simulados e materiais perigosos. Uma das inovações neste campo são os satélites de vigilância, vocacionados para o apoio direto a operações de nível tático, como é o caso do sistema israelita LITESAT7 com capacidades HR2C (Very High Resolution & High Revisit Constellation) que pode cumprir missões táticas, com muito alta resolução (30 cm) combinando o sensor eletro-óptico com o radar (SAR).



Figura 1 - Ilustração do sistema israelita LITESAT

(RAFAEL Advanced Defense Systems)

Outra missão dos satélites é na defesa anti-míssil, para seguirem a trajetória dos mísseis e de outras ameaças em voo, fornecerem o alerta antecipado e os dados necessários, para que os interceptores destruam os mísseis em voo, antes de atingirem os alvos. Só os satélites conseguem detectar e seguir os mísseis de cruzeiro e a nova ameaça dos veículos supersônicos, como os HGV (Hypersonic Glide Vehicle) cuja trajetória a baixa altitude e em velocidade supersônica, os torna invisíveis para os radares na Terra.

Estão a surgir novas capacidades espaciais ofensivas, sob a forma de ataques cinéticos e não-cinéticos, ações eletrônicas e operações cibernéticas: os ataques “cinéticos” danificam ou destroem satélites, com meios que podem ser lançados da terra ou de um satélite em órbita, para outro. O modelo comum das armas anti-satélite de ascensão direta (ASAT) usa um “veículo de ataque” que é montado num míssil balístico e após o míssil deixar a atmosfera, abandona o míssil e navega até ao alvo, usando a energia

cinética no ataque. Existem novas formas de ataques cinéticos através de satélites de “grappling” orbital<sup>8</sup> que fazem o ataque com um veículo espacial para “sequestrar” um equipamento inimigo. Os ataques não cinéticos usam energia laser, micro-ondas, ou através de detonações nucleares ou de impulso eletromagnético. Os sistemas laser de alta potência, tal como os sistemas de micro-ondas de alta potência, estão incluídos nesta categoria, assim como os “dazzlers” que servem para cegar temporariamente um satélite óptico.



Figura 2 - Lançador laser Iron Beam de Israel.

As armas de raio laser são discretas (não produzem luz nem som) têm grande alcance, à velocidade da luz e não exigem munições, nem a logística associada. Os projetos em desenvolvimento estão focados essencialmente nas ameaças aéreas e perseguem o objetivo de usar os sistemas anti-míssil como armas anti-satélite (ASAT) e os EUA, tal como Israel, têm investido muito no desenvolvimento destas armas, como o sistema Iron Beam<sup>9</sup>, que usa um laser de alta energia, em conjunto com as baterias de mísseis Iron Dome.

Um feixe de energia laser pode fornecer luz (iluminar) o alvo, aquecer, derreter e queimar o alvo, consoante a potência do laser, a distância entre o laser e o alvo e a capacidade de focar o feixe no alvo e o deslumbramento (dazzler) consiste em saturar os sensores dos satélites ópticos com luz, para impedi-los de funcionar.

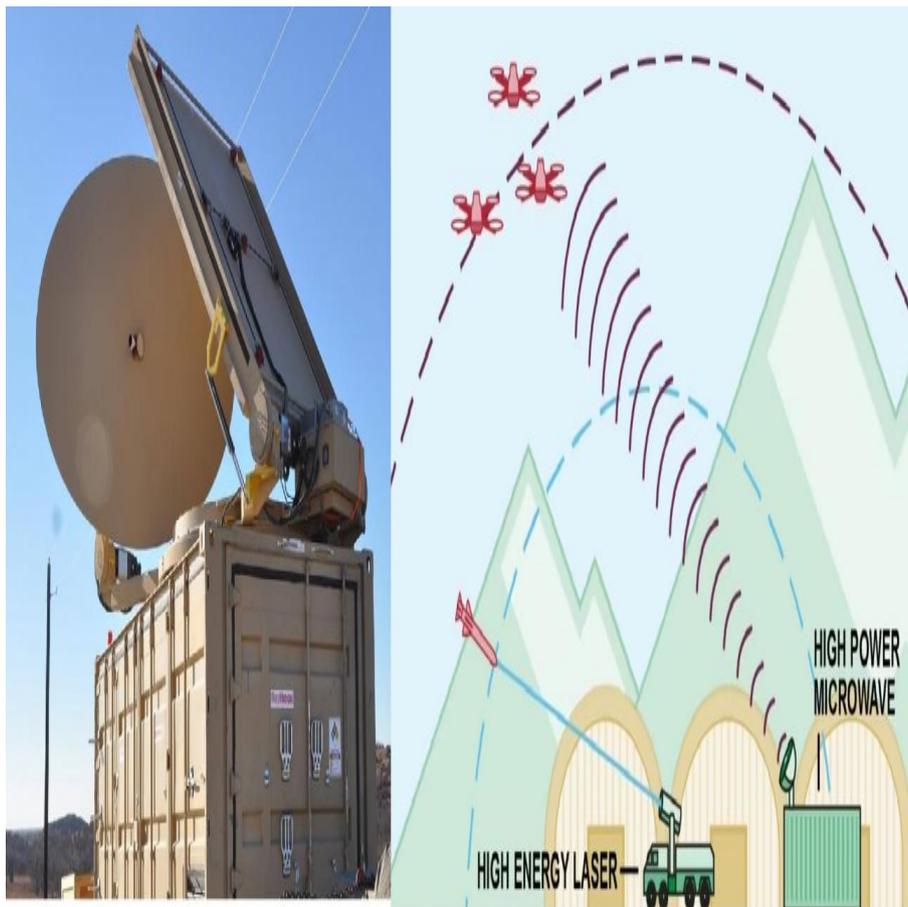


Figura 3 - Ilustração de armas laser e de micro-ondas em terra.

As armas eletrônicas fazem a “falsificação” e o “bloqueio” de sinais do sistema global de navegação por satélite (GNSS) e das comunicações por satélite. A falsificação “spoofing” é a forma de ataque eletrônico em que um invasor engana o receptor, através de um sinal falso para afetar os sinais dos sistemas GPS (Global Positioning System) e dos “downlinks” de satélite<sup>10</sup>. Também estão incluídos nesta categoria os ataques eletrônicos para bloquear radares espaciais e a recepção de sinais de radiofrequência (RF) pelos utilizadores dos serviços de satélites em terra, além do próprio satélite e da estação terrestre. A falsificação pode ser realizada por um “spoofing” terrestre atuando sobre um “uplink” de satélite, que transmite um sinal falso ao satélite, obrigando o satélite a realizar uma manobra contrária à sua missão ou mesmo a neutralizar a sua carga útil. Estas novas ameaças (bloqueio e falsificação de sinais) tornaram-se frequentes e têm sido sentidas em aviões comerciais, pois existem dois tipos de sinais GPS: os sinais GPS militares criptografados, designados por código P(Y) e os sinais GPS civis, chamados de código C/A. Como os dados civis de código C/A são publicados abertamente no espaço público, podem ser usados por um adversário para gerar uma versão “falsificada” do sinal GPS e enganar um receptor GPS. Os sinais GPS criptografados de código P(Y) são mais resistentes a ataques, porque a chave para a descryptografia só pode ser usada por utilizadores especiais ([Selective Availability Anti-Spoofing Modules](#)) autorizados pelo

Departamento de Defesa dos Estados Unidos, que controla a venda e distribuição dos códigos.

As operações cibernéticas constituem a atividade ofensiva no ciberespaço sobre sistemas espaciais, incluindo infraestruturas terrestres e terminais de satélites, e pode desativar os satélites e as suas bases terrestres. Além da espionagem de dados, as ameaças cibernéticas visam os sistemas espaciais que suportam capacidades críticas, como as telecomunicações e a Internet, e a maioria dos ataques cibernéticos são dirigidos aos utilizadores e não contra os próprios satélites, como foi o ataque cibernético da Rússia contra os utilizadores do serviço comercial de banda larga da Viasat, no dia em que as forças russas invadiram a Ucrânia (2022).

Os EUA referem que os satélites russos e chineses fazem aproximações aos seus satélites, para ações cibernéticas, referindo o exemplo do satélite Luch/Olymp da Rússia, lançado em 2023, que se posicionou perto de satélites dos EUA em órbita geostacionária (GEO).

Os sistemas militares espaciais incluem três segmentos que asseguram as missões dos satélites, mas também são vulneráveis a determinadas ameaças: o segmento terrestre é constituído pelos sistemas localizados em terra, que asseguram o comando e controle dos satélites e a gestão dos dados que enviam e recebem do espaço, destinados aos diversos utilizadores. O segmento espacial é constituído pelos próprios satélites e o segmento de ligação assegura a transmissão de sinal entre o satélite e a estação terrestre, e entre satélites. A ameaça mais comum é o bloqueio de GPS, pois os sistemas GPS dependem de sinais de rádio enviados do satélite para determinar a localização dos utilizadores e, por isso, os bloqueadores GPS enviam sinais na mesma frequência que o dispositivo GPS, para substituir ou distorcer os sinais de satélite GPS<sup>11</sup>. Outra modalidade de ataque é o “spoofing” baseado na falsificação de sinais de GPS e que pode ser muito mais perigoso, porque os sistemas atacados podem não saber que estão a ser atingidos<sup>12</sup>. As ameaças de “bloqueio” e de “falsificação” envolvem a interrupção ou adulteração de sinais de frequências, mas podem ainda fazer a interceção de dados de satélite não criptografados e enquanto o bloqueio impede o utilizador de receber sinais GNSS, o “spoofing” é mais sofisticado, influenciando a tomada de decisões com falsos dados, que podem ser fatais, se um recetor GPS for anulado ou levado a processar a sua localização de forma errada. Na guerra da Síria e no leste da Ucrânia (2014) foram usados bloqueadores de alta potência para afetar os sistemas de navegação das aeronaves e das redes de comunicações.

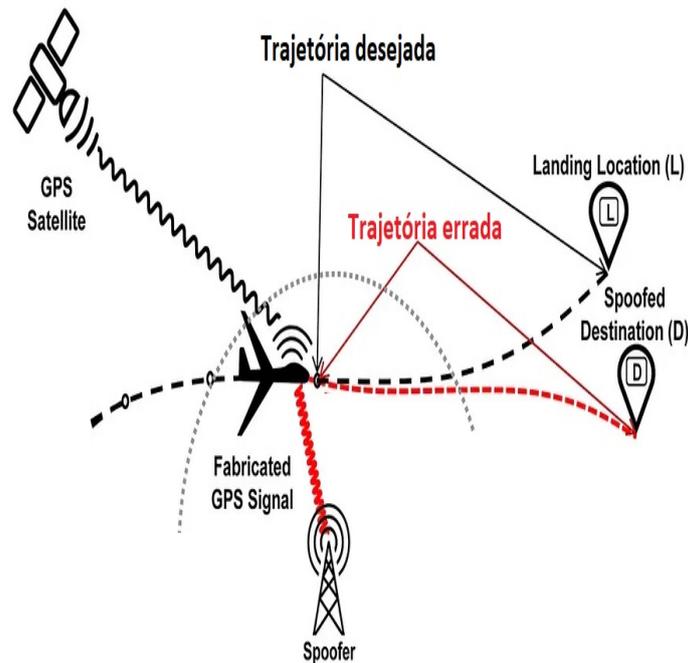


Figura 4 - Representação de GPS falsificado, afetando uma aeronave.

As técnicas de defesa para a falsificação de GPS têm sido muito estudadas, mas a maioria é baseada na detecção de ataques de spoofing, mas não na sua mitigação e na recuperação dos sinais corretos e existem poucos utilizadores com recursos anti-spoofing. Além dos meios militares do inimigo (mísseis, drones, aviões e navios), estas novas ameaças podem afetar também os aviões comerciais, sobretudo quando a ameaça actua na modalidade<sup>13</sup> Aircraft Target Ghost Injection, com a injeção de sinais falsos num avião, em que as falsas mensagens aparecem no painel de comando no cockpit. Estas ações provocam a perda de sinal GNSS (GLONASS e GPS) e podem levar os pilotos das aeronaves inimigas a “voar às cegas”, sem saber a sua posição, levar o avião a entrar noutro espaço aéreo, perder a capacidade de medir adequadamente a distância ao solo (o que pode desencadear comandos de alerta) e originar falhas noutros sistemas. A transmissão de sinais GPS falsificados pode ser muito eficaz, pois um recetor GPS que seja anulado ou levado a processar a sua localização de forma errada pode fazer abortar a missão de um míssil ou ser fatal para um drone, uma aeronave ou um navio.

Os EUA têm o bloqueador de comunicações (L3 Harris Counter Communications System) da Força Espacial, um sistema que tem sido atualizado nos últimos anos e é a principal plataforma de controle espacial terrestre da Força Espacial dos EUA, com capacidades de guerra eletrónica ofensiva no espaço, que pode desligar as ligações de satélite dos adversários.



Figura 5 - Bloqueador de comunicações L3 Harris dos EUA.

## **A competição militar no espaço**

As principais potências mundiais têm dado grande importância ao espaço, mas os desenvolvimentos decorrem com dinâmicas muito diferentes, observando-se o grande poder dos EUA, o aumento das capacidades da China e o declínio da Rússia. A China tem desenvolvido diversas capacidades, ao nível dos sistemas de interferência e de energia dirigida, dispondo de capacidades ASAT, cibernéticas e armas eletrónicas, que podem interferir com links de comunicação via satélite, sinais GNSS e satélites de recolha de informações SAR. Os EUA acusam os chineses de causarem interferências no GPS na região do Indo-Pacífico, sentida por aviões e navios comerciais: em março de 2023, a companhia aérea australiana Qantas e a Federação Internacional de Associações de Pilotos de Linha Aérea, emitiram alertas aos pilotos sobre navios de guerra chineses envolvidos em bloqueio de sinal de rádio e GPS sobre o mar da China Meridional, no mar das Filipinas, no leste do Oceano Índico e noroeste da Austrália. A falsificação de GPS também afetou o transporte marítimo nos últimos anos, como ocorreu no Mar Negro em 2017, no Porto de Xangai em 2019 e nos mares do Sul da China, quando os navios da marinha dos EUA (USS McCain e o USS Fitzgerald) colidiram com navios comerciais.

Relativamente a ações cibernéticas, a China esteve envolvida em várias ações cibernéticas contra satélites meteorológicos dos EUA e numa rede indiana de comunicações e tem procurado aceder a redes governamentais, e de empresas para realizar espionagem sobre tecnologia e implantar malwares, levando os EUA a emitir um

alerta para a indústria espacial dos EUA (em agosto de 2023). Uma dessas ações cibernéticas foi feita pelo grupo Volt Typhoon, em agosto de 2023, e teve como alvo infraestruturas críticas dos EUA na ilha de Guam e noutros lugares nos Estados Unidos. A Microsoft divulgou esta ameaça cibernética<sup>14</sup>, e afirmou que foi realizada para interromper as ligações entre os Estados Unidos e a Ásia, afetando os transportes logísticos (em portos e ferrovias), serviços públicos, telecomunicações e sistemas de comunicações via satélite. Em relação a armas não cinéticas, os serviços de Inteligência dos EUA, afirmam que a China tem diversas armas laser terrestres (capacidade ASAT) de diferentes níveis de potência e equipamentos móveis terrestres, equipados com armas de micro-ondas de alta potência (HPM).

Os EUA têm reforçado o seu poder espacial no Pacífico e a China considera isso uma ameaça: em janeiro de 2024, a China afirmou que os satélites Starlink da Space X têm objetivos militares, ameaçando a segurança da China, que anunciou que uma das formas de combater as constelações de satélites dos EUA, é através de detonações nucleares de alta altitude. No que diz respeito a armas cinéticas, apesar da China ter sistemas de mísseis ASAT baseados em terra, não tem realizado testes destrutivos contra satélites, mas admite-se que continuem a desenvolver testes não destrutivos para alcançar órbitas mais altas.

Depois da mudança política em 2014, a China abriu o setor espacial ao investimento privado e na atualidade existem sete empresas (algumas subsidiárias de empresas estatais) que realizam lançamentos. Em abril de 2023, ocorreu o primeiro lançamento bem sucedido de um satélite da China por uma empresa privada e, em julho de 2023, outra empresa lançou o primeiro satélite do mundo de oxigénio líquido de metano, tecnologia que prevê melhorar o desempenho dos foguetes. Recentemente, em janeiro de 2024, a startup espacial iSpace testou um SLV reutilizável e a Orienspace lançou o novo foguete Gravity-1 a partir de uma plataforma baseada no mar, colocando no espaço três satélites em órbita LEO, sendo este veículo de lançamento o mais poderoso desenvolvido pelo setor espacial privado da China. Além disso, a China desenvolveu o foguete “Longa Marcha 9”, um foguete reutilizável super pesado, rival do Starship da Space X, que irá dinamizar os planos de exploração do espaço da China<sup>15</sup>. Em 2023, a China desenvolveu a sua capacidade de vigilância remota espacial, para detetar ameaças no espaço Indo-Pacífico e nos últimos dois anos, lançou mais de 400 satélites, metade dos quais são satélites de sensores remotos. Segundo as recentes informações do Comando Espacial dos EUA (de janeiro de 2024), a China tem cerca de 360 satélites ISR em órbita e, em agosto de 2023, lançou o Ludi Tance-4, o primeiro satélite de radar (SAR) do mundo baseado em órbita GEO. Em dezembro de 2023, lançou o Yaogan-41, um satélite de imagens ópticas para o GEO e com estes novos sistemas, integrados com outros satélites ISR e com inteligência artificial, a China pode melhorar o “conhecimento da situação” quase em tempo real, na região do Indo-Pacífico. No início de 2023, os Estados Unidos sancionaram as empresas chinesas Spacety e China HEAD Aerospace, por fornecerem imagens da Ucrânia ao grupo Wagner da Rússia.

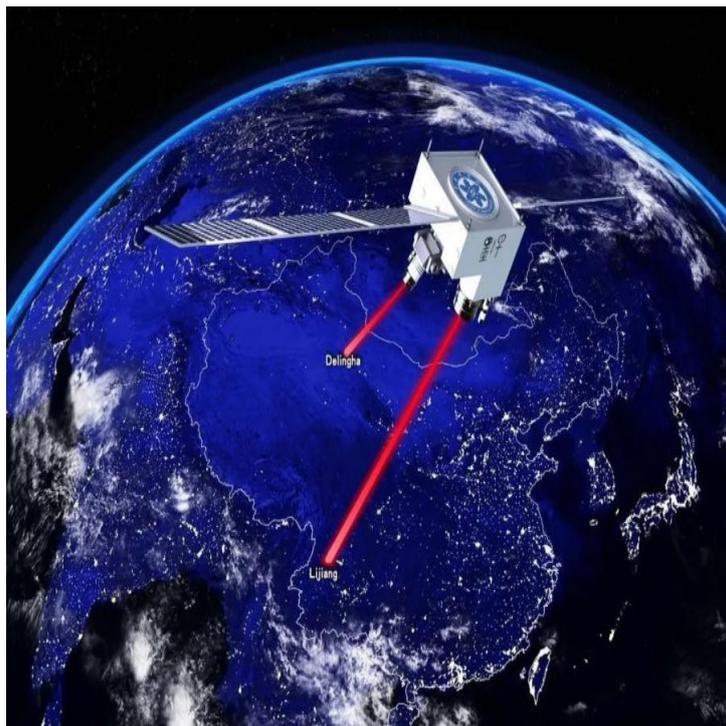


Figura 6 - Gravura representando um satélite chinês da série Yaogan.

Em novembro de 2023, a China lançou o primeiro lote de satélites para testar a conectividade à internet do espaço para ter uma constelação de banda larga LEO, com 13.000 satélites GuoWang. Outra constelação de 12 mil satélites, a G60 Starlink, viu os seus primeiros satélites saírem da linha de produção em dezembro de 2023 e ambas as constelações deverão começar a operar em 2024 para fornecerem um serviço de internet de banda larga, semelhante à Starlink dos EUA. A China tem capacidades para manter a ligação entre os seus meios de segurança em órbita, para atacar satélites e usar armas espaciais, capacidades instaladas em navios equipados com radares, em estações terrestres na China e noutros países, e tem equipamentos avançados de comunicação que apoiam o seguimento e os lançamentos de satélites e dos mísseis balísticos intercontinentais (ICBM).

Os EUA referem que os satélites chineses têm realizado exercícios de aproximação no GEO, destacando o caso do satélite Shijian-21 (SJ-21), um satélite experimental de mitigação de detritos espaciais, que se agarrou e moveu um satélite antigo GNSS. Outro satélite experimental, o SJ-23, foi lançado no GEO em janeiro de 2023, levando um equipamento (um motor), normalmente usado para ajudar a mover um satélite para o GEO antes de ser lançado. Durante o ano 2023 e no início de 2024, o SJ-23 e outros satélites chineses revelaram manobras de aproximação a satélites comerciais e governamentais dos EUA. A capacidade de acoplamento a outros equipamentos espaciais serve normalmente para a manutenção e remoção de detritos orbitais, mas também serve para obter dados (inteligência) para projetos de novas armas espaciais.

Os EUA começaram a desenvolver capacidades ASAT há mais de 60 anos, enquanto a China, só recentemente dispõe destas tecnologias, pois o primeiro teste ASAT da China ocorreu em 2007. Existem informações de que os russos desenvolveram uma arma laser, o Peresvet ASAT, mas não há evidências sobre isso, tal como a notícia sobre a criação de uma arma nuclear espacial e de um satélite de guerra eletrônica, movido a energia nuclear. A Rússia tentou sem sucesso, bloquear e impedir o acesso ao Starlink aos diversos utilizadores na Ucrânia, sendo acusada também de fazer interferências de GPS na Polónia, na Escandinávia, nos Estados Bálticos e na Ucrânia. As sanções continuam a bloquear o acesso à tecnologia ocidental e isso impede a modernização da força russa no espaço, que não evoluiu muito desde a era soviética. Depois do fim da União Soviética, a Rússia desenvolveu apenas um novo lançador, o foguete Angara, em 2014, e durante o ano 2023 realizou apenas 20 lançamentos espaciais, uma quantidade semelhante aos lançamentos realizados em 2021 e em 2022. A Rússia depende da tecnologia e de componentes ocidentais para construir satélites, e devido às sanções teve que interromper a produção de satélites de comunicação desde 2022. Os seus processos de produção estão lentos e enquanto os russos demoram 18 meses para construir um satélite, a SpaceX dos EUA, produz seis satélites por dia.

Apesar das dificuldades, a Rússia apresentou, em outubro de 2023, uma ambiciosa agenda espacial para ter uma nova estação espacial, um rebocador espacial nuclear e dois novos veículos de lançamento: o Amur-LNG e o Korona. Colocou em funcionamento o novo sistema SSA, Razvyazka, baseado em radar e anunciou a construção de 264 satélites para fornecer acesso de banda larga, mas alguns destes projetos, como a nova estação espacial e o foguete Amur, estão parados devido à falta de financiamento. O sistema Razvyazka, localizado perto de Moscovo, serve para detetar ameaças espaciais, substituindo uma antiga estação de radar de longo alcance, que estava operacional desde 1978.

Em 2023, os russos instalaram na África do Sul uma nova estação de vigilância ótico-eletrônica para identificar objetos espaciais, revelando a intenção de cooperar com a África do Sul e, em novembro de 2023, o satélite Sentinel-1 (SAR) da Agência Espacial Europeia sofreu interferências quando captava imagens de Sevastopol na Ucrânia, tal como já tinha sentido em 2021, quando recolhia imagens da região de Rostov, na Rússia, mas alguns especialistas admitem que as interferências sentidas pelo satélite europeu podem ter sido causadas pelos sistemas de guerra eletrônica usados pela Rússia para afetar drones. A quantidade de satélites russos no espaço vem diminuindo há anos e, como a Rússia não usou meios modernos na Ucrânia, isso é indicador do declínio do seu poder no espaço, embora os EUA exagerem na avaliação sobre as capacidades russas, certamente com algum objetivo estratégico, pois os russos não demonstram capacidades espaciais relevantes, além de ações cibernéticas e bloqueios.

A guerra eletrônica representa uma séria ameaça para os sistemas de navegação por satélite e neste contexto a utilização de sistemas como o israelita ADA (Anti-Jam GPS System) é um exemplo sobre como proteger a navegação GPS/GNSS de interferências, contra bloqueadores GNSS, uma componente essencial para qualquer sistema que use recetores GNSS/GPS. O sistema de guerra eletrônica israelita Scorpius [16](#) é um sistema

preparado para interromper as comunicações e os radares, de navios, mísseis etc., usando feixes contra os alvos, sem causar efeitos colaterais, sendo capaz de visar várias ameaças simultaneamente, com um alcance sem precedentes.

As atividades de bloqueio e falsificação procuram negar o acesso ao GNSS numa determinada área na Terra, e podem colocar em risco a segurança das atividades civis e comerciais nas proximidades das zonas de conflito. Não foram ainda impostas medidas reguladoras por parte dos países, relativamente aos bloqueios e falsificação do GNSS, mas estas ameaças são cada vez mais comuns. Israel reconheceu publicamente as suas ações para interferir no GNSS em Gaza, mas como os Estados Unidos também são acusados de causar interferências, não é de esperar a implementação de normas reguladoras internacionais, ainda mais quando a maioria dos casos registados de jamming e spoofing, acontecem fora do território dos EUA e sobre alvos que não pertencem aos EUA.

Com a guerra em Gaza, também o Irão dinamizou os ataques cibernéticos, que se tornaram cada vez mais sofisticados e agressivos, mas além das capacidades cibernéticas, os grupos de iranianos no Iraque e no Iémen podem fazer interferências e falsificações para afetar os seus adversários. O Irão anunciou que as suas ações de falsificação do GNSS já provocaram a queda de um drone dos EUA (em 2011) e, mais recentemente (entre setembro e novembro de 2023), dezenas de aviões civis registaram falsificações GPS, perto de Bagdad (Iraque), no Cairo (Egipto) e em TelAviv (Israel). Alguns especialistas que analisaram a origem da falsificação numa região a leste de Teerão (Irão), confirmam que Israel também produziu falsificações no médio Oriente, especialmente após os ataques do Hamas, em outubro de 2023.

## Os aliados dos EUA

Em dezembro de 2023, a Austrália, os Estados Unidos e o Reino Unido anunciaram uma parceria no programa Deep Space Advanced Radar Capability (DARC), com vista à implementação de um sistema capaz de fornecer vigilância de satélites no GEO. O Japão também reforçou a sua parceria com os EUA para o desenvolvimento de capacidades militares espaciais, tendo sido celebrado um acordo de segurança, em que os Estados Unidos defendem o Japão se o seu território for atacado, mas o Japão já tem capacidade ASAT, através do seu sistema de defesa anti míssil. Os EUA investiram muito num sistema de defesa contra mísseis hipersónicos, com um sistema de alerta e deteção de mísseis de última geração, que deverá entrar em funcionamento em 2025, contando com 28 satélites projetados para detetarem mísseis e veículos hipersónicos, para os quais os [EUA](#) não tinham capacidades de deteção. A finalidade é criar um sistema de alerta e deteção de ameaças no espaço, com um primeiro nível de proteção a uma altitude de cerca de 1.000 Km e um segundo nível a cerca de 20.000 Km da superfície<sup>17</sup>.

Israel continua a expandir as suas capacidades espaciais e, em março de 2023, lançou um novo satélite SAR e, juntamente com a NASA (EUA), a Agência Espacial de Israel vai

lançar a primeira missão de telescópio espacial de Israel, o Ultraviolet Transient Astronomy Satellite (ULTRASAT). Durante o conflito com o Hamas, o exército israelita utilizou capacidades de guerra eletrônica afetando os serviços de satélite: em outubro de 2023, quando iniciou as operações militares em Gaza, Israel afetou e falsificou sinais de GPS nas zonas de combate, afetando a população civil, justificando essa medida para evitar mísseis, drones e foguetes usados pelo Hezbollah. Estas ações para interromper e confundir os sinais de GPS também afetaram aeronaves civis, e foram vários os casos relatados por pilotos da aviação comercial que sentiram essas ações. Israel tem um inovador sistema de defesa aérea, de energia direcionada de curto alcance, que poderá ser usado contra satélites e anunciou que este sistema será implantado em breve, para melhorar as defesas durante o conflito com o Hamas. O empenhamento bem sucedido do sistema Arrow, no dia 31 de outubro de 2023, quando interceptou e destruiu um míssil lançado do Iémen, mostra como os sistemas de defesa anti-míssil, são capazes de funcionar como armas ASAT.

A anexação da Crimeia pela Rússia em 2014 e a invasão da Ucrânia em 2022 originou uma crise na cooperação espacial entre os EUA e a Rússia, o que criou uma oportunidade para o reforço de parcerias entre a Rússia e a China no domínio espacial, mas não existem evidências se as transferências de tecnologia espacial entre os dois países aumentou, pois as duas potências continuam com receios recíprocos e a Rússia até acusou a China de realizar ações cibernéticas de espionagem a alguns serviços russos. Entre 2017 e 2022, os dois países estabeleceram acordos de transferência de tecnologia de defesa espacial e para tornar compatíveis o GLONASS e o BeiDou. Foram instaladas estações terrestres GLONASS em seis cidades chinesas e estações terrestres BeiDou em seis cidades russas e a Rússia apoiou a China a desenvolver um sistema de alerta de mísseis baseado no espaço. A Rússia tem procurado parcerias estratégicas e clientes para a sua tecnologia espacial, ao mesmo tempo que precisa de armas para a guerra na Ucrânia e o Irã e Coreia do Norte têm apoiado a Rússia, recebendo em troca algum apoio para os seus programas espaciais.

## **A guerra na Ucrânia**

A guerra na Ucrânia também decorre no espaço e, apesar da escassez de informações sobre os meios militares, sabemos que os satélites comerciais de diversas empresas dos EUA fornecem aos ucranianos imagens e dados de rádio frequência sobre os russos. A avaliação do Centro de Estudos Estratégicos e Internacionais (CSIS) observou que os satélites de comunicação e de imagens aumentaram decisivamente o potencial militar dos ucranianos, pois os satélites de vigilância são capazes de penetrar nas nuvens e recolher fotos de noite, observando o movimento das forças russas e outros satélites podem detetar e localizar as fontes de interferência do GPS, permitindo que os veículos aéreos não tripulados (drones) ucranianos alterem o seu percurso para escaparem aos radares russos. Várias empresas como a Aurora Insight, HawkEye 360, Kleos Space, PredaSAR, Spire Global e Umbra Lab apoiam a Ucrânia e a NanoAvionics e a Aurora Insight começaram a trabalhar em conjunto, na Lituânia, dois anos antes do início da guerra.

É muito relevante o “satélite do povo” comprado pelo governo da Ucrânia à empresa norte americana ICEYE, que começou a operar em setembro de 2022, e com o qual as forças ucranianas passaram a receber dados sobre a localização das tropas russas, a aproximação de aviões e helicópteros, a localização dos mísseis balísticos de curto alcance Iskander, dos sistemas antiaéreos S-300, dos mísseis Pantsir S1 e das estações de radar dos russos. O “satélite do povo” está integrado na vasta rede de satélites SAR (Synthetic Aperture Radar) da empresa ICEYE que tem a maior rede de satélites SAR comerciais do mundo.

Os russos têm tido problemas com as comunicações através dos satélites militares e civis (Gonets e Express) e das comunicações por satélite da Gazprom e têm poucos satélites de inteligência (vigilância) apesar de, entre 2021-2022, terem feito sem sucesso [três tentativas para lançar](#) uma nova geração de satélites de vigilância, ainda de reconhecimento óptico e não da tecnologia radar (SAR) mais avançada. A Rússia tem feito grandes esforços para preservar o seu sistema GLONASS e, no ano 2022, foram lançados dois satélites de navegação: o GLONASS-K de uma nova geração e o GLONASS-M da geração anterior. A rede de satélites GLONASS está bastante desatualizada, tendo já ultrapassado o prazo de vida útil e a substituição dos meios está atrasada, pois, entre 2022 e 2030, devem ser lançados 15 satélites GLONASS-K, mas mesmo assim não resolvem o problema dos satélites obsoletos. Apesar da Rússia poder contar com o sistema chinês Beidou (equivalente ao GPS ocidental) não há garantias de que seja possível a transição do sistema russo GLONASS para pequenos satélites de navegação de baixa órbita, do Beidou da China.

A Rússia também procurou melhorar as suas capacidades de vigilância espacial, aumentando a quantidade de satélites de alerta de mísseis, com mais três satélites “Liana”, incluindo um Pion-NCS com radar ativo, um satélite de localização de radar Neutron e o satélite Condor, lançado em 2013, mas todos são bastante antiquados. A implementação de um novo sistema anti-míssil ainda não está concluída para conseguir ter uma cobertura global, pois este sistema [estava programado](#) para ficar operacional em 2022 e isso não aconteceu. Os russos têm um sistema anti-míssil com radares de detecção terrestres de longo alcance, para manter um sistema de defesa anti-míssil em torno de Moscovo, mas precisa de satélites para ter um sistema mais avançado de defesa anti-míssil.

Em abril de 2023, a Rússia anunciou que tinha um novo sistema de guerra eletrônica capaz de bloquear satélites a uma altitude de 36.000 Km, mas pelo que sabemos tem ainda o sistema Tobol 14Ts227, que foi usado em setembro de 2022 para afetar as comunicações via satélite na área de Bakhmut. Além de suprimir eletronicamente os sinais ascendentes, o Tobol poderá também captar os sinais enviados pelos satélites para os meios terrestres e fazer a interferência ou identificar uma interferência dos EUA num satélite russo e responder, enviando um sinal de “neutralização” para o satélite, anulando as duas interferências. Temos poucas informações sobre o 14Ts227 Tobol, mas sabemos que é um sistema antigo de guerra eletrônica, criado na década de 1980-90, para proteger os satélites russos de ataques eletrônicos.



Figura 7 - Estação móvel Tobol em viatura Fazan.

O bloqueio de satélites pode ser feito de duas formas: no espaço (uplink jamming) ou em terra (interferência downlink). A interferência no espaço (uplink) combina um sinal falso com a transmissão original, o que distorce as informações recebidas por todos os utilizadores daquele satélite (será o caso do Tobol russo). O método baseado em terra (downlink), transmite um sinal na mesma frequência do satélite, o que impede que os dispositivos ligados ao satélite recebam o sinal legítimo, mas nesta modalidade o sistema emissor falso tem que estar próximo do sistema que pretende interromper.

Os Estados Unidos são a potência militar mais desenvolvida tecnologicamente e o seu serviço de inteligência espacial que gere as plataformas orbitais secretas é o National Reconnaissance Office (NRO)[18](#) que, em 2022, colocou em órbita mais de uma dezena de satélites de observação (USA-326) a 500 km de altitude, capazes de captar imagens muito detalhadas (ler as placas de matrícula dos carros). O satélite russo Kosmos-2558, lançado em agosto de 2022, fez manobras de aproximação ao satélite militar USA-326 e isso levou os EUA a avisarem que tal atitude poderia acionar o Artigo 5.º (NATO) se os russos atacassem algum satélite dos EUA. Segundo informações dos EUA, o Kosmos-2558 é um satélite capaz de se aproximar de outros satélites para recolher dados e quando foi lançado, em agosto de 2022, foi colocado quase na mesma órbita do satélite de reconhecimento USA-326 dos EUA. Os satélites de radar (SAR) dos EUA conseguem ver pequenos detalhes, como o USA-281, em órbita desde 2018, cujo radar é capaz de obter imagens espectrais com uma resolução inferior a 50 cm, operando a uma altitude de cerca de 1.100 km. O NRO tem capacidade para escutar e decifrar comunicações e para isso usa diversos dispositivos de inteligência eletromagnéti-

ca, ELINT (ELectronic INTelligence), e dispositivos de sinais, SIGINT (SIGnals INTelligence), que examinam, bloqueiam ou decifram as comunicações. Os mais recentes satélites dedicados às missões SIGINT captam sinais eletromagnéticos, com sensores infravermelhos de alerta antecipado, altamente sensíveis como o SBIRS HEO-3 para detetar os disparos de mísseis balísticos, sendo o USA-278 o mais recente, colocado em órbita em 2017, a uma altitude de 36.000 km. As missões ELINT são realizadas pelos satélites Intruders, como os USA-274A e B, que operam numa altitude de 1.100 km com a finalidade de localizar navios de guerra e submarinos, através das suas transmissões de rádio. Durante os próximos anos, o NRO vai quadruplicar a quantidade de satélites em órbita<sup>19</sup>, para aumentar dez vezes mais a sua capacidade de recolha de informações, usando satélites menores em grande quantidade, para processar de forma mais rápida a “inteligência baseada no espaço”.

Num artigo de opinião publicado recentemente, um alto responsável dos EUA<sup>20</sup> diz que o conflito na Ucrânia ficará na história como a primeira guerra espacial, mas o poder espacial tem limites e as guerras ainda são decididas no terreno. Segundo o autor, a Ucrânia continua a ter o domínio do “espaço” mas as capacidades espaciais não decidem a guerra, pois, tal como outras capacidades assimétricas, o espaço pode criar vantagens temporárias, mas não decisivas.

## **Os satélites e o escudo anti-míssil na Europa**

O plano dos EUA para instalar na Europa o sistema integrado de Defesa contra Mísseis Balísticos (escudo anti-míssil), considera oficialmente a ameaça dos mísseis Shahab-3 do Irão (alcance de 2.000 Km), embora o objetivo seja também impedir a Rússia de responder a um ataque nuclear, reduzindo a sua capacidade de resposta nuclear e também a capacidade espacial da Rússia<sup>21</sup>. Este plano apresentado em 2002 pelo Presidente G. Bush e assumido pela NATO nas cimeiras de Lisboa (2010) e de Chicago (2012), possibilitou a instalação de um sofisticado sistema de defesa com capacidade para detectar alvos, através de satélites e radares e garantir o alerta antecipado e rápido (um ou dois minutos), após o lançamento de um míssil inimigo. As baterias de mísseis e os seus radares móveis estão instalados no sul da Roménia, na Polónia, na Alemanha, na Turquia e na Inglaterra, e o sistema envolve também navios dos EUA no mar mediterrâneo, baseados na base naval de Rota (sul de Espanha) e os meios navais de outros países. Embora projetado como um sistema anti-míssil, este sistema de armas (RIM 161 SM-3) também tem capacidade para atacar satélites<sup>22</sup> e isso foi mal recebido pelos russos. Os mísseis RIM-161 SM-3 e os novos modelos de mísseis Patriot (MIM-104) com elevados alcances e links com satélites, comprometem a capacidade russa de realizar um segundo ataque (resposta a um primeiro ataque) e ameaçam os satélites russos GLONASS, pois o alcance (500 km) e o teto máximo (160 km de altitude) do sistema RIM-161 (o melhor dos sistemas existentes) pode afetar a capacidade espacial da Rússia.



Figura 8 - O Sistema anti-míssil dos EUA na Europa.

Os Estados Unidos resolveram alargar este sistema também ao Pacífico, com o apoio do Japão e da Coreia do Sul, com meios instalados na ilha de Guam, o que é visto como uma ameaça para a China e para a Coreia do Norte. Devido às crescentes tensões militares no Pacífico, a Austrália também foi envolvida no programa Deep Space Advanced Radar Capability (DARC) em parceria com os EUA e o Reino Unido. Na Austrália foi instalada a primeira das três estações de radares, com capacidade para detetar satélites no espaço, enquanto as outras duas serão instaladas nos EUA e no Reino Unido<sup>23</sup>. Os satélites e os seus sensores no espaço complementam as capacidades estratégicas de alerta antecipado, baseadas em terra, que detetam os mísseis dentro e fora da atmosfera, mas a ameaça das novas armas hipersónicas exige novas capacidades. Inicialmente, eram usados apenas os satélites com o Sistema de Infravermelho Baseado no Espaço (SBIRS) para detetar os lançamentos de mísseis inimigos na fase inicial, mas com o aparecimento das novas ameaças de mísseis intercontinentais e hipersónicos (como o míssil balístico russo Kinzhal e o veículo hipersónico Avangard), de elevada velocidade (superior a Mach 5) e no caso dos HGV (hypersonic glide vehicle) a sua trajetória é ainda mais difícil de seguir pelo meios de deteção. Os mísseis de cruzeiro já apresentavam uma trajetória mais complexa de interceção dos que os mísseis balísticos, mas a ameaça dos HGV ou veículo supersónico, é um desafio ainda mais exigente, para as defesas anti-míssil. Os veículos HGV não seguem uma trajetória previsível e realizam manobras para os sistemas de deteção os perderem de vista, mas a vantagem de um HGV é ainda a sua trajetória de voo dentro da atmosfera<sup>24</sup> imune a um intercetor de primeira geração, que faz apenas o

empenhamento a altitude superior (fora da atmosfera) desde a fase intermédia até à fase terminal, antes da reentrada na atmosfera.

Tal como a figura 9 representa, a trajetória dos mísseis de cruzeiro e dos veículos hipersónicos decorre dentro da atmosfera (abaixo dos 100 km de altitude) ao contrário dos mísseis balísticos, cuja trajetória se dá no espaço. Assim, a forma de detetar um HGV é diferente da deteção de um míssil balístico, porque o HGV voa numa altitude que os sistemas de defesa anti-míssil não estavam preparados para vigiar. Estes novos sistemas voam mais baixo e podem manobrar ao longo de toda a trajetória, e isso é uma dificuldade para o sistema defensivo: numa altitude entre 20 e 60 km, as armas hipersónicas voam acima dos aviões, mas muito abaixo de satélites e por isso nem os sensores espaciais projetados para detetar mísseis balísticos nem os radares terrestres estavam preparados para enfrentar essa ameaça. Assim, para responder a este desafio, os EUA desenvolveram o programa HBTSS (Hypersonic and Ballistic Space Sensor) com satélites equipados com sensores capazes de fazer o seguimento contínuo de ameaças de mísseis (balísticos e hipersónicos) desde o lançamento até à reentrada e na fase terminal do voo, para fornecerem dados para o comando do sistema de defesa anti-míssil. Os satélites HBTSS vão trabalhar em conjunto com radares terrestres e marítimos, e com os restantes satélites da Força Espacial dos EUA.

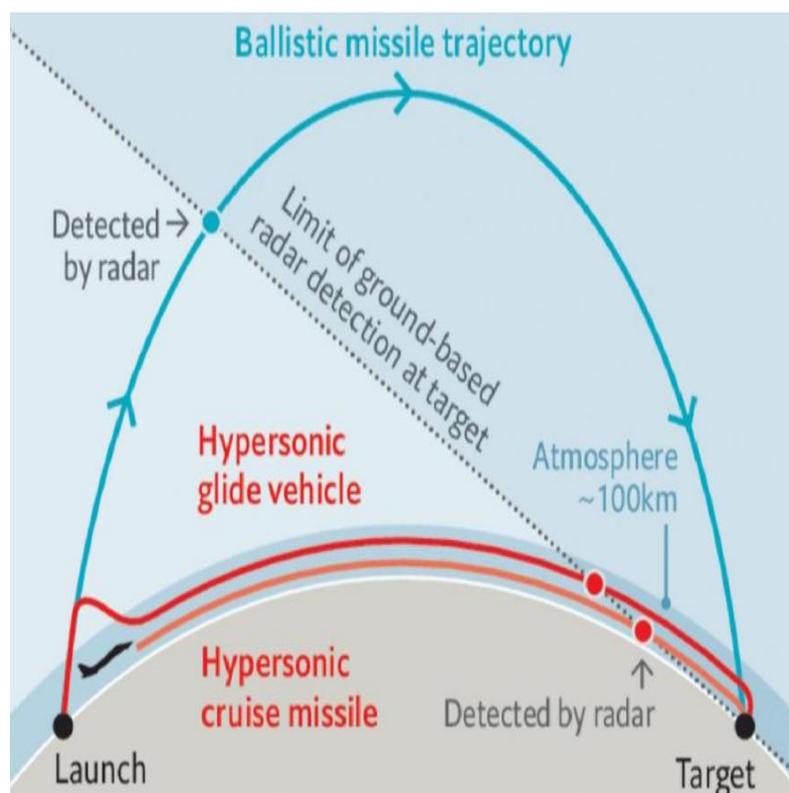


Figura 9 - Os três tipos de trajetórias das ameaças.

O sucessor dos sistemas SBIRS (sensores de Infravermelhos) será o OPIR (Overhead

Persistent Infrared Block), que fornecerá informações atualizadas sobre as ameaças de mísseis, num curto espaço de tempo. Os satélites com o sistema OPIR serão capazes de detectar as ameaças hipersônicas altamente manobráveis e farão a vigilância por infravermelhos de forma contínua no planeta, permitindo a resposta às ameaças de mísseis. Após os mísseis inimigos serem detetados pelos satélites OPIR, os satélites HBTSS, que operam em órbita terrestre baixa, fazem o seguimento dos mísseis e de veículos hipersônicos e entregam dados aos sistemas localizados na terra, para atacarem as ameaças. Assim, os satélites HBTSS serão alertados pelos satélites SBIRS, pelos satélites de apoio à defesa e pelo sistema de infravermelho persistente (OPIR) para conseguirem detetar e seguir as ameaças desde a fase inicial de lançamento até à sua interceção.

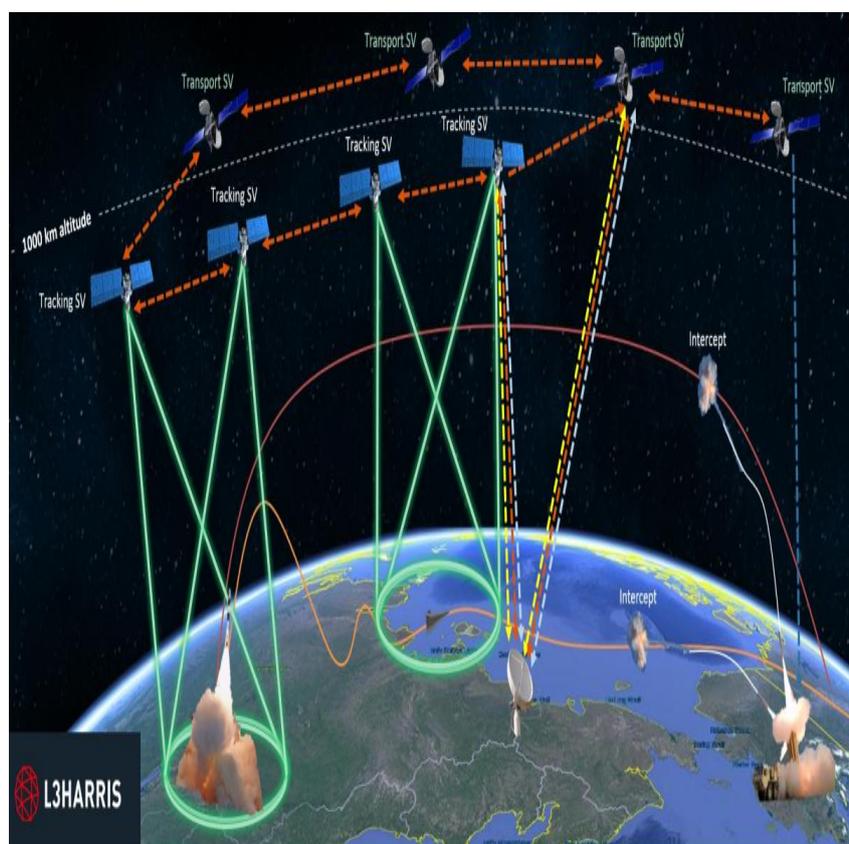


Figura 10 - A deteção de mísseis intercontinentais feita por satélites.

## Conclusões

As capacidades militares no Espaço mostram como a inovação tecnológica acentuará as diferenças de potencial entre os diversos atores do sistema internacional e promoverá a criação de poderes dominantes. As grandes potências estão envolvidas numa nova “corrida ao espaço” sem respeitar os princípios do Tratado do Espaço Exterior, que tem servido como Lei Espacial Internacional<sup>25</sup>.

As potências militares têm criado organismos para gerir o controlo do espaço e desenvolverem armas espaciais numa dinâmica sem regras internacionais, nem tratados, o que pode ser negativo para a segurança e a estabilidade mundial. O Tratado do Espaço Exterior de 1967 proíbe armas de destruição em massa no espaço, nos corpos celestes, como a Lua, e também proíbe “bases militares e instalações”, embora não proíba esses meios na órbita da Terra. As grandes potências espaciais ratificaram o Tratado, mas as suas ambições e a retórica cada vez mais agressiva mostram como a corrida ao espaço vai decorrendo sem regras.

As grandes mudanças na atividade militar são baseadas no Espaço, Inteligência Artificial, Robótica, Computação, Comunicações e Sensores, que dão forma ao novo conceito militar C5ISTAR (Comando, Controle, Comunicações, Computadores, Inteligência Cibernética, Vigilância, Aquisição de Alvos e Reconhecimento) através da utilização de dados, análise e conectividade, para a tomada de decisões mais rápidas e de melhor qualidade. A Inteligência Geoespacial afirma-se como uma nova e decisiva atividade, através da partilha de informações entre as componentes militar e civil (imagens de satélite, etc.) com o setor privado (satélites comerciais) no apoio às forças armadas.

As interferências nas comunicações por satélite e nos sinais GNSS tornaram-se muito frequentes e decisivas em combate, mas representam um risco para a aviação civil e para a segurança das pessoas, de modo geral. Existem diversos relatos de companhias aéreas e de navios mercantes que foram afetados por interferências nos sinais GNSS, através de “spoofing” de dados falsos<sup>26</sup>.

Além dos satélites estatais, verifica-se cada vez mais o envolvimento de satélites comerciais no desempenho de missões militares em combate, o que levanta questões sobre a legitimidade e a forma como as empresas prestam os seus serviços, enquanto não existem normas internacionais, para regular a atividade das empresas espaciais nos conflitos.

Relativamente à ameaça cibernética, verifica-se uma tendência para o aumento da intervenção de atores não estatais, com capacidades para afetar funcionalidades decisivas, como o Sistema Global de Navegação por Satélite (GNSS), as comunicações via satélite e outras.

A tecnologia da informação e a revolução digital nas forças militares da China [estão em andamento numa dinâmica](#) mais avançada do que na Rússia, que foi ultrapassada, devido à perda de especialistas e às sanções internacionais impostas desde a anexação da Crimeia em 2014. A Agência Espacial Europeia abandonou os projetos que tinha com a Rússia e irá usar foguetes SpaceX dos EUA para realizar as missões que estavam previstas com os foguetes Soyuz da Rússia, o que irá prejudicar bastante a agência espacial russa Roscosmos, que, além do financiamento do governo, depende da receita dos acordos comerciais, principalmente com lançamentos do seu foguete Soyuz.

As grandes potências desenvolvem projetos secretos e desviam as atenções, influenciando as notícias e o debate público, de acordo com os seus objetivos estratégicos

e os interesses das empresas ligadas ao setor militar. Num artigo publicado recentemente, sobre a evolução da guerra na Ucrânia, um alto responsável dos EUA<sup>27</sup> refere que o conflito foi a primeira guerra espacial, mas que o poder espacial tem limites e que as guerras ainda são decididas no terreno, com armas e munições. Inicialmente, a Ucrânia tirou vantagem do “espaço” perante o antiquado poder espacial russo, mas segundo o autor, parece que a situação se alterou: “as capacidades espaciais, comerciais ou estatais, podem apoiar as forças militares no terreno, mas, não decidem o resultado final da guerra, pois tal como outras capacidades assimétricas, o espaço pode criar vantagens temporárias, mas não decisivas.[...] atualmente a componente militar dos EUA gasta no espaço, anualmente, mais de 50 bilhões de dólares, mas as suas reservas de munições podem esgotar-se numa semana, num eventual conflito com a China e por isso, além dos satélites, é necessário ter armas e munições”<sup>28</sup>.

## Bibliografia

Barbara Opall, Arrow-3 Could Be Adapted for Anti-Satellite Role, November 9, <https://spacenews.com>, 2009.

Clayton Swope, Kari A. Bingen, Makena Young, Madeleine Chang, Stephanie Songer, and Jeremy Tammelleo, Space Threat Assessment 2024, Center for Strategic and International Studies (CSIS) April, 2024.

Deganit Paikowsky and Isaac Ben, Israel’s Perspectives on Space Security, Springer Science+Business Media, New York, 2015.

Joey Roulette and Marisa Taylor, Northrop Grumman working with Musk’s SpaceX on U.S. spy satellite system, 18april2024, [www.reuters.com](http://www.reuters.com).

Galamas, Francisco, A NATO e as Tensões Derivadas do Escudo Antimíssil. IDN Brief, Instituto da Defesa Nacional, 2015.

Grego, Laura, The AntiSatellite Capability of the Phased Adaptive Approach Missile Defense System. Federation of American Scientists, Public Report, Winter, 2011.

Hadley, Greg, Space Force Eyes Better EW Test and Training Ranges with New Contract Awards, Air & Space Forces Magazine, May 28, 2024.

National Geospatial Agency, Geospatial Intelligence Basic Doctrine, NGA, EUA, 2006.

Sousa, Pedro Marquês, A guerra da Ucrânia: o sucesso da artilharia e a guerra eletrónica, Revista Militar, Vol. 75, n.º 2/3 (fev.-mar. 2023), pp. 193-215.

Space Systems Command, DARC Technology Demonstrator test a success, Dec. 22, 2021, [www.ssc.spaceforce.mil](http://www.ssc.spaceforce.mil)

Stashevskiy, Oleksandr e Bajak, Frank, Como a guerra eletrônica molda o conflito Rússia-Ucrânia, Portal BIDS (7 de Junho de 2022), [portalbids.com.br](http://portalbids.com.br)

Swope, Clayton, Os limites do poder espacial, SpaceNews, 8 de março de 2024, <https://spacenews.com/>

Theodora Ogden, Anna Knack, Mélusine Lebret, James Black e Vasilios Mavroudis, The Role of the Space Domain in the Russia-Ukraine War and the Impact of Converging Space and AI Technologies, CETaS Expert Analysis (fevereiro de 2024).

## Créditos das imagens

Figura 1 - Ilustração comercial da empresa RAFAEL Advanced Defense Systems ([www.rafael.co.il](http://www.rafael.co.il))

Figura 2 - Foto divulgação do laser Iron Beam da empresa RAFAEL ([www.rafael.co.il](http://www.rafael.co.il))

Figura 3 - Imagens de armas laser e de micro-ondas da empresa Raytheon ([www.rtx.com/raytheon](http://www.rtx.com/raytheon))

Figura 4 - Representação de GPS jamming afetando uma aeronave (desenho do autor)

Figura 5 - Ilustração do Counter Communications L3 Harris ([www.l3harris.com](http://www.l3harris.com))

Figura 6 - Gravura de satélite chinês Yaogan (<https://asiatimes.com>)

Figura 7 - Ilustração da estação móvel Tobol (open source photo <https://en.defence-ua.com>)

Figura 8 - O Sistema anti-míssil dos EUA na Europa (<https://www.bbc.com>)

Figura 9 - Adaptação desenho trajetórias da ameaça ([www.arabnews.com](http://www.arabnews.com))

Figura 10 - A detecção feita por satélites de mísseis intercontinentais (L3 Harris [www.l3harris.com](http://www.l3harris.com))

---

<sup>1</sup> No dia 31 de outubro de 2023, o sistema de defesa aérea israelita Arrow, interceitou e destruiu um míssil lançado do Iémen, a 1600 km de distância do alvo que pretendia atingir em Israel (o porto de Eilat). O míssil que foi destruído em voo, no espaço (a 100 km de altitude) foi um míssil balístico Qadar (um modelo mais avançado do Shahab 3) produzido no Irão e que foi lançado pelos rebeldes Houthi do Iémen.

[2](#) A Linha de Karman é considerada o limite entre a atmosfera terrestre e o espaço exterior, a uma altitude de 100 km acima do nível do mar. Não é um limite oficial, pois em diversos países e entidades são considerados outros níveis de altitude, entre os 80 km e os 150 km.

[3](#) Alguns especialistas como o presidente da Agência Espacial de Israel, o general Yitzhak Ben Yisrael, admitem que o Arrow 3, desenvolvido numa parceria entre a Israel Aerospace Industries e a Boeing dos EUA, pode ser um eficaz sistema ASAT.

[4](#) A Força Espacial dos EUA assegura o funcionamento da Rede de Controle de Satélites, o sistema de comunicações por satélite de defesa, os aviões espaciais X-37B, o funcionamento do GPS, do Space Fence, do sistema de alerta de mísseis dos Estados Unidos e da Rede de Vigilância Espacial dos EUA.

[5](#) Esta tipologia de satélites também assegura missões civis relevantes, como é o caso do sistema FIRMS (Fire Information for Resource Management System) da NASA, que detecta incêndios em todo o mundo, fazendo pesquisas duas vezes por dia, através de sensores infravermelhos.

[6](#) Durante a primeira Guerra do Golfo, as aeronaves dos EUA já usaram dados de satélite com grande sucesso, através do Sistema de Posicionamento Global (GPS), que permitiu que as suas aeronaves atingissem alvos com grande precisão.

[7](#) O sistema de satélites táticos de Israel, foi produzido pela empresa RAFAEL Advanced Defense Systems que também desenvolveu os sistemas Iron Dome e C-DOME.

[8](#) Equipamento ou veículo robótico, capaz de se aproximar e agarrar satélites. Tecnologia já usada para fazer a manutenção e o reabastecimento de combustível no espaço (como o Restore-L, o projeto de manutenção através de satélite mais desenvolvido) e que no futuro será usada para ações hostis.

[9](#) Iron Beam é o primeiro caso já operacional, de um Sistema de Armas a Laser de Alta Energia (HELWS) de 100kW, desenvolvido pela empresa israelita Rafael Advanced Defense Systems.

[10](#) O “uplink” é o sentido percorrido pelas ondas eletromagnéticas até ao satélite e o inverso “downlink” são as ondas enviadas pelo satélite. O downlink e o uplink usam frequências diferentes para evitar interferências.

[11](#)A falsificação pode alterar o tempo (relógio) de um receptor GPS e como os utilizadores dependem da sincronização de tempo precisa e todos os componentes da rede devem estar sincronizados no mesmo tempo (horário) para fazerem a troca de dados, estas ações impedem as ligações.

[12](#)Um relatório de 2017 da Administração Marítima dos EUA revelou diversos casos de navios no mar negro que foram desviados pelas ações russas, através da falsificação de dados nos sistemas GPS.

[13](#)A ameaça (sinais falsos) pode ser introduzida na aeronave (Aircraft Target Ghost Injection) ou numa estação em terra (Ground Station Target Ghost Injection) em que os sinais falsos originam mensagens falsas apresentadas na consola do controlador (painel de radar).

[14](#)O grupo chinês Volt Typhoon foi sinalizado pela Microsoft e pelas autoridades dos EUA como uma ameaça persistente avançada (APT) que conseguiu assumir o controlo de centenas de routers antigos e desatualizados, que utilizaram para criar uma rede de transferência de dados, semelhante ao Tor para realizar operações maliciosas.

[15](#)O novo foguete, chinês “Longa Marcha 9”, terá capacidade de colocar em órbita até 130 toneladas de carga útil, uma capacidade indispensável para levar astronautas à Lua e cujo primeiro lançamento poderá acontecer em 2028.

[16](#)Produzido pela Israel Aerospace Industries (IAI), foi anunciado em novembro de 2021.

[17](#)Os mísseis hipersónicos são difíceis de detetar devido à sua velocidade e capacidade de manobra, dificultando a previsão de sua trajetória pelos radares em terra, algo que não acontecia no passado.

[18](#)National Reconnaissance Office (NRO), a organização responsável pelo desenvolvimento, lançamento e a operação das plataformas orbitais secretas dos Estados Unidos.

[19](#)Este projeto baseado em satélites em órbitas baixas é desenvolvido pelas empresas Northrop Grumman e a SpaceX. Joey Roulette and Marisa Taylor, 18april2024, [www.reuters.com](http://www.reuters.com).

[20](#)Clayton Swope, Os limites do poder espacial, SpaceNews, 8 de março de 2024. O autor é vice-diretor do Projeto de Segurança Aeroespacial e membro do Programa de

Segurança Internacional do Centro de Estudos Estratégicos e Internacionais, em Washington.

[21](#)Tal como o citado sistema anti-míssil israelita (Arrow 3) admite-se que o sofisticado sistema dos EUA instalado na Europa poderá funcionar como um sistema ASAT (anti-satélite).

[22](#)Laura Grego, The AntiSatellite Capability of the Phased Adaptive Approach Missile Defense System. Federation of American Scientists, Public Report, Winter 2011.

[23](#)Na Austrália foi instalado o radar espacial Deep Space Advanced Radar Capability (DARC) uma parceria com os EUA, a Austrália e o Reino Unido para localizar e seguir satélites no espaço, a mais de 35.000 km de altitude.

[24](#)A atmosfera é a camada até aos 100 km de altitude. As altitudes acima dos 100 km são consideradas no “espaço”.

[25](#)Em 1963, a Assembleia-Geral da ONU aprovou por unanimidade uma resolução proibindo a introdução de armas de destruição em massa no espaço e, na sequência desta resolução, foi assinado, em 1967, o Tratado do Espaço Exterior ou Tratado sobre os Princípios que Regem as Atividades dos Estados na Exploração e Uso do Espaço Exterior, incluindo a Lua e Outros Corpos Celestiais, assinado pelos Estados Unidos da América, União Soviética e Reino Unido.

[26](#)O “spoofing” é uma forma de ataque eletrónico, em que um emissor ilude o receptor, através de um sinal falso, que é recebido pelo destinatário como se fosse legítimo (verdadeiro).

[27](#)Clayton Swope é vice-diretor do Projeto de Segurança Aeroespacial e membro do Programa de Segurança Internacional do Centro de Estudos Estratégicos e Internacionais em Washington.

[28](#)Clayton Swope, Os limites do poder espacial, SpaceNews, 8 de março de 2024, <https://spacenews.com>