

# **Segurança de Ativos Espaciais na Era da Competição Estratégica: Um Guia Abrangente sobre Vulnerabilidades, Identificação e Mitigação**

# Autor: Cristian Fortuna

## **Sumário Executivo**

Este relatório apresenta uma análise exaustiva das vulnerabilidades que afetam os ativos espaciais, juntamente com um guia operacional detalhado para a sua identificação e mitigação. O domínio espacial, outrora um santuário para a exploração científica, transformou-se num ambiente operacional congestionado e contestado, onde a dependência global de serviços baseados em satélites para comunicação, navegação e observação tornou estes ativos alvos de alto valor. Uma mudança de paradigma fundamental está em curso: a "normalização" das ameaças contraespaciais, onde atos hostis como a interferência intencional (jamming) e a falsificação de sinais (spoofing) se tornaram ocorrências comuns em zonas de conflito e competição estratégica.

As vulnerabilidades são categorizadas em quatro domínios principais: (1) ameaças cibernéticas e de guerra eletrônica (soft-kill), que incluem jamming, spoofing e hacking; (2) ameaças físicas (hard-kill), como armas cinéticas antissatélite (ASAT) e armas de energia dirigida (DEW); (3) vulnerabilidades do segmento terrestre e da cadeia de suprimentos, que representam pontos de entrada críticos para ataques; e (4) riscos orbitais e ambientais, como detritos espaciais e radiação.

Para a identificação destas vulnerabilidades, este relatório advoga por uma abordagem estruturada de gestão de riscos, fundamentada em frameworks como o Cybersecurity Framework do National Institute of Standards and Technology (NIST), especificamente o NIST IR 8401 para o segmento terrestre. Contudo, enfatiza-se a necessidade crítica de adaptar (tailoring) estes controles ao ambiente de missão espacial único, uma vez que uma abordagem genérica é insuficiente. A identificação é complementada por técnicas de avaliação técnica, como testes de penetração e análise de sinais, e pela integração de inteligência de ameaças e Consciência do Domínio Espacial (SDA).

As estratégias de mitigação são centradas na construção de resiliência através de uma defesa em profundidade. As contramedidas incluem criptografia robusta, técnicas anti-jamming como antenas adaptativas, blindagem contra radiação e EMP, redundância de subsistemas críticos, capacidade de manobra orbital evasiva e a adoção de arquiteturas de constelações desagregadas. Uma atenção especial é dada à segurança da cadeia de suprimentos de software, integrando práticas de DevSecOps ao longo de todo o ciclo de vida do desenvolvimento.

Finalmente, a análise examina as tendências futuras, destacando a natureza de duplo uso da inteligência artificial (IA) — tanto como uma ferramenta poderosa para a defesa autônoma quanto como um vetor para ataques mais sofisticados. Os desafios impostos pelas megaconstelações, que trocam a vulnerabilidade de ativos individuais por um risco sistêmico massivo, são explorados em detalhe. As recomendações estratégicas são dirigidas a operadores, governos e à indústria, sublinhando que, na era atual, a segurança robusta não é apenas um custo, mas um habilitador de negócios e um diferencial competitivo essencial para a sustentabilidade e viabilidade das operações espaciais.

## Seção 1: O Cenário de Ameaças em Evolução para Ativos Espaciais

### Análise Introdutória

O domínio espacial deixou de ser um santuário benigno, dedicado exclusivamente à exploração científica e à cooperação internacional. Hoje, representa um ambiente operacional cada vez mais congestionado, contestado e competitivo. A infraestrutura espacial é a espinha dorsal da sociedade moderna, sustentando uma vasta gama de serviços essenciais, desde comunicações globais e transações financeiras até navegação precisa, previsão do tempo e segurança nacional.1 Esta dependência crítica transformou os satélites e a sua infraestrutura de suporte em alvos de alto valor para uma gama crescente de atores estatais e não estatais que procuram obter vantagens estratégicas ou perturbar adversários.

A proliferação de tecnologia espacial, impulsionada pela redução dos custos de lançamento e pela miniaturização de componentes, democratizou o acesso ao espaço. No entanto, esta mesma tendência reduziu as barreiras de entrada para o desenvolvimento e emprego de capacidades contraespaciais. O resultado é um ambiente de segurança complexo e volátil, onde as ameaças não são mais teóricas, mas uma realidade operacional diária.

### A Normalização da Agressão Espacial

Uma das mudanças mais significativas no cenário de segurança espacial é a normalização de comportamentos hostis. Conforme observado por analistas do Center for Strategic and International Studies (CSIS), "atividades que antes eram vistas como desviantes ou fora da norma, estão simplesmente se tornando comuns agora".2 Esta tendência é corroborada pelo relatório

*Space Threat Assessment 2025* do CSIS, que aponta para a continuação de "tendências preocupantes", como o uso generalizado de jamming e spoofing de sinais de Sistemas Globais de Navegação por Satélite (GNSS) em e ao redor de zonas de conflito, como a Ucrânia e o Oriente Médio.3

Esta normalização reflete uma mudança fundamental na doutrina e na aceitação de riscos por parte dos atores globais. Atos de interferência eletrônica, que podem ter consequências significativas para a aviação civil e o transporte marítimo, ocorrem com uma frequência alarmante e raramente são atribuídos de forma conclusiva.4 Este padrão de comportamento sugere a emergência de um estado de conflito de baixa intensidade no domínio espacial. Em vez de ataques cinéticos destrutivos, que cruzariam um limiar claro de guerra e provocariam uma retaliação severa, os adversários estão a empregar ataques eletrônicos e cibernéticos como uma forma de coerção, perturbação e teste de defesas de forma contínua e, muitas vezes, denegável. Esta "zona cinzenta" estratégica corrói a estabilidade e a confiança nos sistemas espaciais globais sem provocar uma guerra aberta, afetando a confiança nos sistemas de satélites.2

### Proliferação e Atores

A capacidade de ameaçar ativos espaciais já não é exclusiva das superpotências tradicionais. Nações como a China, Rússia, Índia, Irã e Coreia do Norte estão a desenvolver e a demonstrar ativamente uma gama de capacidades contraespaciais.6 A Índia, por exemplo, juntou-se ao clube exclusivo de nações com capacidade de armas antissatélite (ASAT) de ascensão direta com o seu teste "Mission Shakti" em 2019.10

A barreira de entrada para ataques cibernéticos e de guerra eletrônica é particularmente baixa. Equipamentos de jamming podem ser adquiridos ou construídos com relativa facilidade, e o conhecimento para executar ataques cibernéticos está amplamente disponível. Relatórios indicam que o acesso a controles de satélites pode ser oferecido no mercado negro por valores tão baixos quanto 15.000 USD.11 Esta realidade expande o leque de potenciais adversários para além dos Estados-nação, incluindo organizações terroristas, crime organizado e hackers individuais, cada um com as suas próprias motivações para perturbar ou explorar os serviços de satélite.

## Seção 2: Taxonomia Detalhada das Vulnerabilidades de Satélites

Para desenvolver estratégias de defesa eficazes, é imperativo compreender a gama completa de ameaças que os ativos espaciais enfrentam. Estas vulnerabilidades podem ser classificadas em quatro categorias principais: ameaças cibernéticas e de guerra eletrónica, ameaças físicas, vulnerabilidades do segmento terrestre e da cadeia de suprimentos, e riscos orbitais e ambientais. A análise destas categorias revela que a segurança de satélites deve ser abordada de forma holística, pois as ameaças estão interligadas e um comprometimento num domínio pode criar vulnerabilidades noutro.

### 2.1 Ameaças Cibernéticas e de Guerra Eletrônica (Soft-Kill)

Estas ameaças não destrutivas visam a funcionalidade dos sistemas de satélite através do espectro eletromagnético ou de redes digitais.

#### Jamming (Interferência Intencional)

O jamming é o ato de sobrecarregar os receptores de satélite com ruído de radiofrequência, impedindo a recepção de sinais legítimos. É uma das ameaças mais comuns e difundidas, em grande parte devido à relativa simplicidade e baixo custo da tecnologia necessária.2 Os alvos mais frequentes são os sinais de GNSS, como o GPS, que são fracos por natureza e, portanto, fáceis de sobrepujar. A interrupção dos serviços de GNSS tem implicações graves para a segurança da navegação aérea e marítima, operações humanitárias e a sincronização de tempo essencial para redes de telecomunicações e financeiras.4 Incidentes de jamming são rotineiramente reportados em múltiplas zonas de conflito e áreas de tensão geopolítica, incluindo a Ucrânia, o Mar Báltico, o Mar da China Meridional e o Oriente Médio.5

#### Spoofing (Falsificação de Sinais)

O spoofing é uma forma de ataque mais sofisticada, que envolve a transmissão de sinais falsos, mas estruturalmente idênticos aos sinais de satélite, para enganar um receptor.11 Em vez de simplesmente negar o serviço, o spoofing fornece informações perigosamente incorretas. Por exemplo, um sistema de navegação de um navio ou avião pode ser levado a calcular uma posição ou tempo errados, resultando em desvios de rota, potenciais colisões ou incursões em território hostil.11 O Joint Maritime Information Center (JMIC) tem emitido avisos sobre interferência eletrônica persistente no Estreito de Ormuz e uma intensidade crescente de eventos no Mar Vermelho, onde os navios reportam comportamentos anómalos nos seus sistemas de GPS.12

#### Hacking (Invasão Cibernética)

O hacking refere-se ao acesso não autorizado e à manipulação dos sistemas de computador que controlam os satélites, processam os seus dados ou gerem as suas redes. As vulnerabilidades podem existir no próprio satélite (software embarcado), nos links de comunicação ou, mais comumente, no segmento terrestre. Pesquisas de empresas de cibersegurança como a Kaspersky Labs e a IOActive revelaram, há anos, falhas críticas de software que deixam a infraestrutura marítima global e os seus sistemas de rastreamento por satélite vulneráveis a ataques.11

A crescente tendência de construir microssatélites que são "completamente impulsionados por software e completamente em rede" e que se conectam à internet pública para reduzir custos, expande drasticamente a superfície de ataque.13 O ciberataque de 2022 contra a rede de satélites KA-Sat da Viasat, que desativou a internet de banda larga para milhares de utilizadores na Europa no início da invasão da Ucrânia, é um exemplo proeminente desta ameaça.2 Este ataque não visou os satélites em órbita, mas sim os modems dos utilizadores no solo, demonstrando a vulnerabilidade de todo o ecossistema.

### 2.2 Ameaças Físicas (Hard-Kill)

Estas ameaças envolvem a destruição física ou o dano permanente de um satélite.

#### Armas Cinéticas Antissatélite (ASAT)

As armas cinéticas utilizam a energia do impacto para destruir os seus alvos.

* **Mísseis de Ascensão Direta (DA-ASAT):** São mísseis lançados da superfície terrestre, do ar ou do mar que viajam numa trajetória suborbital para colidir com um satélite em órbita baixa.10 Os Estados Unidos, a Rússia, a China e a Índia demonstraram esta capacidade em testes que, embora bem-sucedidos, criaram nuvens massivas de detritos espaciais perigosos e de longa duração.9 O teste russo de 2021 que destruiu o satélite extinto Cosmos 1408 gerou mais de 1.500 fragmentos rastreáveis, ameaçando a Estação Espacial Internacional.9
* **Sistemas Co-orbitais:** Estes são satélites "inspetores" ou "assassinos" que são colocados em órbita e podem manobrar para se aproximar de outros satélites. Podem ser usados para espionagem, mas também podem ter a capacidade de atacar um alvo através de colisão, de uma carga explosiva, ou de um braço robótico.10 A Rússia e a China têm demonstrado capacidades de manobra orbital cada vez mais avançadas com satélites como o Luch e o Shijian 17, que realizaram aproximações a satélites ocidentais, um comportamento descrito por oficiais dos EUA como ameaçador.3

#### Armas de Energia Dirigida (DEW)

As DEW utilizam energia focada, como lasers ou micro-ondas, para danificar ou desativar os sistemas de um satélite à distância.17

* **Lasers de Alta Energia:** Podem ser usados a partir do solo ou de plataformas aéreas para "cegar" temporariamente ou danificar permanentemente os sensores óticos sensíveis de satélites de imagem e reconhecimento.10
* **Micro-ondas de Alta Potência:** Podem gerar campos eletromagnéticos intensos capazes de perturbar ou "fritar" os circuitos eletrônicos a bordo de um satélite, causando danos permanentes.17

#### Pulso Eletromagnético (EMP)

Um EMP é uma explosão breve e intensa de energia eletromagnética que pode incapacitar sistemas eletrônicos numa vasta área.

* **EMP Nuclear (NEMP):** Gerado pela detonação de uma arma nuclear em alta altitude (acima de 30 km), um NEMP é a ameaça mais devastadora. A interação dos raios gama da explosão com a atmosfera terrestre cria um pulso eletromagnético de alta intensidade com três componentes (E1, E2, E3) que podem induzir correntes e tensões destrutivas em condutores, como linhas de energia e circuitos eletrônicos.23 Os circuitos integrados modernos, especialmente os de tecnologia MOS, são extremamente vulneráveis a estes picos de tensão.25 Um único NEMP de alta altitude poderia paralisar a rede elétrica e os sistemas de comunicação de um continente inteiro.
* **EMP Não Nuclear (NNEMP):** São armas que utilizam fontes de energia convencionais para gerar um pulso eletromagnético poderoso, embora mais localizado, sem uma detonação nuclear.23

### 2.3 Vulnerabilidades do Segmento Terrestre e da Cadeia de Suprimentos

A segurança de um sistema de satélites é tão forte quanto o seu elo mais fraco, e muitas vezes esse elo está na Terra.

* **Ataques a Estações de Controle:** As estações terrestres, que incluem os centros de operações de missão (MOCs) e os centros de controle de carga útil (PCCs), são pontos de estrangulamento críticos.19 Um ataque físico ou cibernético a uma destas instalações pode permitir que um adversário assuma o controle de um satélite, intercepte ou manipule os dados transmitidos, ou negue completamente o serviço.13
* **Vulnerabilidades da Cadeia de Suprimentos:** Estes são ataques insidiosos que exploram a confiança entre uma organização e os seus fornecedores externos de hardware e software.27 O ataque à SolarWinds em 2020 serve como um exemplo paradigmático: hackers comprometeram o processo de atualização de software da empresa para distribuir malware aos seus clientes, que incluíam agências governamentais dos EUA.27 No contexto espacial, um ataque à cadeia de suprimentos poderia envolver a inserção de um backdoor num chip de computador, o comprometimento do software de controle de solo de um fornecedor, ou a manipulação do firmware de uma antena antes da sua entrega.13

### 2.4 Riscos Orbitais e Ambientais

Mesmo na ausência de um ator malicioso, o ambiente espacial apresenta perigos significativos.

* **Detritos Espaciais:** Esta é talvez a ameaça mais persistente e indiscriminada para todos os operadores de satélites. Mais de um milhão de objetos de detritos estão em órbita, desde satélites extintos a pequenos fragmentos de colisões e testes ASAT anteriores. Devido às velocidades orbitais extremas (até 28.000 km/h em LEO), uma colisão com um objeto de apenas 1 cm pode ser catastrófica.30 A proliferação de megaconstelações em LEO está a aumentar drasticamente a densidade de objetos, elevando o risco de colisões e a possibilidade de uma cascata de colisões autossustentada (conhecida como Síndrome de Kessler) que poderia tornar certas altitudes orbitais inutilizáveis por gerações.31
* **Radiação Espacial:** O ambiente espacial está repleto de radiação ionizante proveniente dos cinturões de Van Allen, raios cósmicos galácticos e eventos solares (como erupções solares). A exposição prolongada a esta radiação degrada os componentes eletrônicos através de um efeito cumulativo conhecido como Dose Total de Ionização (TID), que pode encurtar a vida útil de um satélite ou causar falhas prematuras.35 A proteção contra a radiação requer blindagem, o que adiciona massa e custo significativos a uma missão.35

A análise destas categorias distintas revela uma interconexão profunda. Um ataque cibernético à cadeia de suprimentos de um fornecedor de software 27 pode introduzir uma vulnerabilidade no subsistema de controle de atitude de um satélite.36 Um adversário poderia, então, explorar remotamente essa vulnerabilidade para comandar o satélite a realizar uma manobra não planeada, colocando-o numa trajetória de colisão com outro ativo espacial — transformando um ataque

*soft-kill* num efeito *hard-kill*. Da mesma forma, o ataque à Viasat demonstrou como um ataque ao segmento terrestre pode ter efeitos operacionais massivos sem nunca tocar no ativo em órbita.14 Portanto, a segurança dos satélites já não pode ser tratada em silos de "segurança física" versus "cibersegurança". É necessário adotar um modelo de

**segurança holística da missão**, compreendendo que a superfície de ataque se estende desde a estação de trabalho do programador que escreve o código-fonte 37, passando pelo fabricante de um componente eletrónico 13, até à estação de controle terrestre 19, o link de comunicação, o próprio satélite e, finalmente, o terminal do utilizador final. A mitigação eficaz exige a proteção de toda esta cadeia de valor.

## Seção 3: Metodologias para Identificação de Vulnerabilidades

A identificação proativa de vulnerabilidades é a pedra angular de qualquer estratégia de segurança robusta. Para sistemas espaciais, onde a correção pós-lançamento é extremamente difícil ou impossível, este processo assume uma importância ainda maior. A metodologia de identificação deve ser multifacetada, combinando frameworks de gestão de risco de alto nível com técnicas de avaliação técnica e inteligência de ameaças.

### 3.1 Fundamentos da Gestão de Riscos de Cibersegurança

A base para a identificação de vulnerabilidades é um processo de gestão de riscos estruturado e contínuo. Esta abordagem envolve a identificação sistemática de ativos, a avaliação de fraquezas, a análise do impacto potencial e a implementação de controles para mitigar os riscos a um nível aceitável.38 Os conceitos fundamentais, conforme definidos por agências como o Centro Nacional de Cibersegurança de Portugal, são:

* **Ameaça:** Uma causa potencial de um incidente indesejado (ex: um hacker, uma erupção solar).
* **Vulnerabilidade:** Uma fraqueza de um ativo ou controle que pode ser explorada por uma ameaça (ex: software desatualizado, falta de blindagem).
* **Impacto:** As consequências de um evento de segurança (ex: perda de serviço, perda de dados).
* **Risco:** A combinação da probabilidade de um evento ocorrer e o seu impacto.39

O **NIST Cybersecurity Framework (CSF)** oferece uma estrutura padrão-ouro para organizar e melhorar os esforços de cibersegurança. As suas cinco funções principais — **Identificar, Proteger, Detectar, Responder e Recuperar** — fornecem um roteiro abrangente para a gestão de riscos. De particular relevância é o **NIST Interagency Report (IR) 8401**, que aplica especificamente o CSF ao **segmento terrestre de satélites**, com foco em garantir o comando e controle.40 Este perfil ajuda as organizações a classificar os seus sistemas de solo, definir um estado de cibersegurança desejado e gerir os riscos residuais de forma sistemática.

No entanto, um documento crítico da NASA adverte contra a aplicação cega e "tamanho único" dos controles do NIST a sistemas de missão espacial.45 O documento argumenta que ser "compatível" não é sinónimo de ser "seguro". Os sistemas de controle de solo e o software de voo são ambientes altamente especializados, e os controles de segurança devem ser cuidadosamente

**adaptados (tailored)** para serem eficazes sem perturbar as operações da missão. Por exemplo, uma política de bloqueio de conta após três tentativas de login falhadas, padrão em TI empresarial, poderia causar uma negação de serviço catastrófica num centro de controle de missão. Esta necessidade de adaptação sublinha a complexidade única da cibersegurança espacial.

### 3.2 Técnicas de Avaliação Técnica

Para além dos frameworks de gestão, são necessárias técnicas práticas para descobrir vulnerabilidades específicas.

* **Análise de Sinais e Monitoramento do Espectro:** Esta é a principal ferramenta para a detecção em tempo real de guerra eletrónica. Operadores utilizam analisadores de espectro para monitorizar as frequências de rádio usadas para comunicação com satélites. Picos de energia anómalos, perda de sinal ou distorções podem indicar a presença de jamming. A análise da estrutura do sinal pode revelar tentativas de spoofing.46
* **Avaliação de Vulnerabilidades (Scanning):** Este processo, frequentemente automatizado, utiliza ferramentas de software para verificar redes, sistemas e aplicações em busca de vulnerabilidades conhecidas, como software desatualizado, portas abertas ou configurações incorretas.47 É uma forma eficaz de manter a higiene cibernética básica e identificar "frutos mais baixos" para os atacantes. A avaliação pode ser feita com scanners ativos, que sondam ativamente a rede, ou scanners passivos, que monitoram o tráfego de forma não intrusiva.47
* **Teste de Penetração (Pentesting):** Enquanto a avaliação de vulnerabilidades identifica fraquezas potenciais, o pentesting vai um passo além. É uma simulação de ataque controlada, realizada por especialistas em segurança ("hackers éticos"), que tentam ativamente explorar as vulnerabilidades identificadas para determinar o seu impacto real.47 O objetivo é responder à pergunta: "O que um atacante real poderia fazer com esta vulnerabilidade?". Esta abordagem é mais profunda, muitas vezes manual, e fornece uma avaliação realista da postura de segurança de um sistema. Ferramentas como o Nessus da Tenable são frequentemente utilizadas como ponto de partida para estas avaliações.49

### 3.3 Inteligência e Consciência Situacional

A identificação de vulnerabilidades não ocorre no vácuo; deve ser informada por uma compreensão do ambiente de ameaças.

* **Inteligência de Ameaças (Threat Intelligence):** É o processo de recolher, processar e analisar informações sobre atores de ameaças, às suas motivações, táticas, técnicas e procedimentos (TTPs). A inteligência de ameaças permite que uma organização passe de uma postura de segurança reativa para uma proativa, antecipando ataques em vez de apenas reagir a eles.50 Saber que um grupo específico está a visar o setor aeroespacial com um novo tipo de malware permite que os defensores ajustem as suas defesas em conformidade.
* **Consciência do Domínio Espacial (Space Domain Awareness - SDA):** O equivalente à inteligência de ameaças para o domínio físico do espaço. O SDA envolve o uso de uma rede global de radares terrestres, telescópios óticos e sensores espaciais para rastrear e catalogar todos os objetos em órbita — satélites ativos, satélites desativados e detritos.21 Um SDA robusto é essencial para prever conjunções de alto risco (potenciais colisões) que exigem manobras evasivas e para detetar comportamentos orbitais anómalos, como um satélite "inspetor" a aproximar-se de um ativo de alto valor.

A aplicação destas metodologias ao domínio espacial revela uma lacuna fundamental entre a identificação teórica de vulnerabilidades e a sua validação prática. Em ambientes de TI terrestres, é prática comum realizar testes de penetração em sistemas de produção (ou em cópias exatas). No entanto, realizar um "pentest" ao vivo num satélite em órbita é uma proposta de altíssimo risco. Um comando malformado ou uma exploração com consequências imprevistas poderia resultar na perda de controle, dano ou destruição de um ativo que custou centenas de milhões de dólares e é fisicamente inacessível. A investigação do IEEE destaca a dificuldade que os próprios investigadores de segurança têm em obter acesso a hardware e software de satélites para análise, dependendo frequentemente da cooperação de agências espaciais como a ESA.51 Esta incapacidade de testar exaustivamente no ambiente operacional real força uma dependência muito maior de

**simulação de alta fidelidade, emulação de sistemas e, crucialmente, segurança na fase de projeto (security-by-design)**. A confiança na robustez do projeto inicial e na integridade da cadeia de suprimentos torna-se exponencialmente mais crítica do que em sistemas terrestres, onde a aplicação de patches e a correção pós-implantação são processos rotineiros.

## Seção 4: Estratégias de Mitigação e Resiliência

Uma vez que as vulnerabilidades são identificadas, é necessário implementar uma estratégia de mitigação multifacetada. Para sistemas espaciais, o objetivo não é apenas a prevenção, mas a **resiliência** — a capacidade de um sistema resistir a um ataque, continuar a operar de forma degradada, se necessário, e recuperar rapidamente a sua funcionalidade total. Isto é alcançado através de uma combinação de contramedidas técnicas, resiliência arquitetural e processos de segurança rigorosos.

### 4.1 Contramedidas Técnicas Defensivas

Estas são as tecnologias e técnicas específicas implementadas para derrotar ou mitigar ameaças diretas.

* **Criptografia e Autenticação Forte:** A base da cibersegurança é proteger a confidencialidade e a integridade dos dados e comandos. Todos os links de comunicação, especialmente os de Telemetria, Rastreamento e Comando (TT&C), devem ser protegidos com criptografia forte e protocolos de autenticação que garantam que apenas entidades autorizadas possam comunicar com o satélite.52 A falta de criptografia e autenticação robustas foi identificada como uma falha de segurança primária em alguns satélites analisados por investigadores, deixando-os vulneráveis à interceção e ao sequestro de comandos.51
* **Técnicas Anti-Jamming:** Para combater a ameaça onipresente de interferência, são utilizadas várias técnicas avançadas:
  + **Salto de Frequência (Frequency-Hopping Spread Spectrum - FHSS):** Esta técnica muda a frequência de transmissão centenas de vezes por segundo, de acordo com uma sequência pseudo-aleatória conhecida tanto pelo transmissor como pelo receptor. Para um jammer, é extremamente difícil seguir esses saltos e concentrar a sua energia de interferência numa única frequência.53
  + **Antenas Adaptativas (CRPA):** As Controlled Reception Pattern Antennas são sistemas de antenas inteligentes, compostas por múltiplos elementos. Estas antenas podem analisar o ambiente de radiofrequência, detectar a direção de chegada de um sinal de interferência e, em seguida, ajustar eletronicamente o seu padrão de receção para criar um "nulo" (uma área de sensibilidade mínima) nessa direção específica. Isto permite que a antena "ignore" o jammer enquanto continua a receber o sinal desejado do satélite.54
* **Blindagem (Shielding):** A proteção física do satélite contra o ambiente hostil do espaço e ataques de energia dirigida é crucial.
  + **Contra Radiação:** Para mitigar os efeitos da Dose Total de Ionização (TID), os componentes eletrônicos sensíveis são protegidos por blindagem. Isto pode envolver o uso de materiais de alta densidade, como o tântalo, ou estruturas em sanduíche (por exemplo, Tântalo + ligas de Alumínio-Lítio) que são otimizadas para abrandar e absorver partículas de alta energia, como protões e eletrões, antes que possam danificar os semicondutores.35
  + **Contra EMP/DEW:** Para proteger contra pulsos eletromagnéticos e armas de energia dirigida, os componentes eletrônicos são alojados dentro de uma "gaiola de Faraday" — um invólucro condutor que bloqueia campos eletromagnéticos externos. A blindagem e o endurecimento dos circuitos são essenciais para sobreviver a tais ataques.25

### 4.2 Resiliência Operacional e Arquitetural

A resiliência não vem apenas de componentes individuais, mas da arquitetura geral do sistema e das suas capacidades operacionais.

* **Redundância de Sistemas:** Este é um princípio fundamental da engenharia de sistemas espaciais. Componentes críticos, como computadores de bordo, processadores, fontes de alimentação e elementos do subsistema de controle de atitude (AOCS), são duplicados ou mesmo triplicados.58 Se um componente primário falhar (devido a radiação, falha de hardware ou ataque), um sistema secundário pode ser ativado para assumir as suas funções, garantindo a continuidade da missão. O caso do satélite CBERS-1, onde um problema no AOCS causava reinicializações contínuas do computador de bordo, ilustra vividamente a importância da redundância para evitar a perda da missão.36
* **Manobras Orbitais Evasivas:** A capacidade de um satélite usar os seus propulsores para alterar a sua órbita é uma defesa ativa crucial contra ameaças físicas. Quando a Consciência do Domínio Espacial (SDA) prevê uma conjunção de alto risco com um pedaço de detrito ou detecta a aproximação de um satélite hostil, o operador pode comandar uma manobra evasiva.30 Esta é uma prática comum, mas tem um custo: consome propelente, o que encurta a vida útil operacional do satélite. Para satélites em órbitas mais altas, o custo em propelente pode ser proibitivo.32 Para megaconstelações, estima-se que possam ser necessárias milhares de manobras de evasão por ano, representando um desafio de gestão e um custo operacional massivo.33
* **Arquiteturas Desagregadas e Proliferadas:** A mudança estratégica de satélites monolíticos, grandes e caros em órbita geoestacionária (GEO) para grandes constelações de satélites mais pequenos e baratos em órbita terrestre baixa (LEO) é, em si mesma, uma poderosa estratégia de resiliência.21 Numa arquitetura desagregada, a perda de um ou mesmo de vários satélites devido a um ataque ou falha tem um impacto mínimo na capacidade geral da rede, que pode continuar a fornecer serviço. Além disso, a abundância de sinais de comunicação de constelações LEO pode ser aproveitada para fornecer serviços de navegação, criando uma camada de redundância para os sistemas GNSS tradicionais.64

### 4.3 Segurança da Cadeia de Suprimentos de Software (DevSecOps)

Dado que o software controla todos os aspetos de um satélite moderno, proteger a sua cadeia de suprimentos é de suma importância.

* **Segurança Integrada (Security-by-Design):** A segurança não pode ser um pensamento tardio. Deve ser integrada em todas as fases do Ciclo de Vida de Desenvolvimento de Software (SDLC), uma prática conhecida como DevSecOps. Isto inclui monitorização contínua, controle de acesso rigoroso e verificações de segurança automatizadas.65
* **Proteção do Ambiente de Desenvolvimento:** Os ambientes onde os programadores escrevem e testam o código devem ser seguros e geridos centralmente para evitar a introdução de código malicioso ou vulnerabilidades. O uso de estações de trabalho virtuais e seguras é uma prática recomendada.37
* **Verificação de Componentes e SBOM:** O software moderno é construído a partir de inúmeros componentes de código aberto e de terceiros. É essencial utilizar ferramentas de análise de composição de software (SCA) para verificar estes componentes em busca de vulnerabilidades conhecidas.66 A criação de uma Lista de Materiais de Software (SBOM — Software Bill of Materials) fornece um inventário transparente de todos os componentes, permitindo uma gestão de vulnerabilidades rápida e eficaz.65
* **Pipeline de CI/CD Seguro:** O pipeline de Integração Contínua/Entrega Contínua (CI/CD), que automatiza a construção, teste e implantação de software, deve ser ele próprio protegido. Isto inclui proteger os sistemas de controle de versão (como o Git), usar ambientes de construção isolados e efémeros, e assinar digitalmente os artefactos de software para garantir a sua integridade.66

A ascensão das megaconstelações LEO introduz um paradoxo de resiliência. Por um lado, a sua natureza proliferada e desagregada torna-as inerentemente resilientes a ataques *hard-kill* que visam satélites individuais.21 A perda de alguns nós da rede é tolerável. Por outro lado, esta mesma arquitetura cria uma vulnerabilidade sistêmica massiva a outras ameaças. A superfície de ataque cibernético expande-se por milhares de satélites e milhões de terminais de utilizador, tornando a defesa da rede um problema de escala sem precedentes.68 O modelo de negócio de baixo custo pode levar a um menor investimento em endurecimento ("hardening") para cada satélite individual em comparação com um ativo GEO de alto valor.13 Além disso, a enorme quantidade de satélites agrava exponencialmente o problema dos detritos espaciais e a complexidade da gestão do tráfego espacial.33 Assim, as megaconstelações resolvem o problema da resiliência arquitetural à custa de uma complexidade de segurança cibernética e de gestão ambiental muito maior. O foco da segurança desloca-se da proteção do

*ativo individual* para a proteção da *rede como um todo* e do *ambiente orbital partilhado*.

## Seção 5: Análise Estratégica e Estudos de Caso

A aplicação dos conceitos teóricos de vulnerabilidade e mitigação a cenários do mundo real fornece insights valiosos sobre a natureza da segurança espacial contemporânea. A Guerra na Ucrânia serve como o mais proeminente estudo de caso, enquanto uma análise comparativa dos regimes orbitais revela os compromissos estratégicos inerentes ao projeto de missões espaciais.

### 5.1 Estudo de Caso Aprofundado: A Guerra na Ucrânia e o Domínio Espacial

O conflito na Ucrânia tornou-se o primeiro grande conflito terrestre onde as capacidades espaciais, tanto militares como comerciais, desempenharam um papel central e visível, oferecendo lições críticas para a guerra moderna.7

* **O Ataque à Viasat:** Horas antes da invasão em fevereiro de 2022, um sofisticado ciberataque foi lançado contra a rede de satélites KA-SAT da Viasat. O ataque não visou os satélites em órbita, mas sim o seu segmento terrestre, explorando uma vulnerabilidade no mecanismo de gestão da rede para enviar comandos maliciosos que inutilizaram dezenas de milhares de modems de utilizadores em toda a Europa.2 O objetivo principal era perturbar o comando e controle militar ucraniano, mas o ataque teve consequências em cascata, afetando serviços de internet e até mesmo o controle remoto de turbinas eólicas na Alemanha.69 Este evento sublinhou dramaticamente a vulnerabilidade do segmento terrestre e demonstrou que obter a superioridade ciberespacial é um objetivo inicial chave em campanhas militares modernas.69
* **Guerra Eletrônica Generalizada:** Desde o início do conflito, a Rússia tem empregado extensivamente o jamming e, em menor grau, o spoofing de sinais GNSS. Esta interferência tem como objetivo degradar a eficácia de munições guiadas com precisão, perturbar as operações de veículos aéreos não tripulados (drones) que dependem do GPS para navegação, e criar confusão para a aviação civil na região.3 A persistência e a escala desta guerra eletrónica confirmam a sua normalização como uma tática de campo de batalha padrão.
* **O Papel Transformador dos Satélites Comerciais:** Uma das lições mais importantes da guerra foi o papel decisivo da indústria espacial comercial. Empresas como a Starlink da SpaceX forneceram comunicações de banda larga resilientes às forças ucranianas e ao governo, contornando os esforços russos para destruir a infraestrutura terrestre. Empresas de observação da Terra, como a Maxar e a Planet, forneceram imagens de satélite de alta resolução que foram cruciais para a inteligência de código aberto, permitindo ao mundo acompanhar os movimentos das tropas russas e documentar crimes de guerra. Este fenómeno, apelidado de "o olho comercial que não pisca", demonstrou que a surpresa estratégica para grandes concentrações de forças convencionais é agora praticamente impossível.7
* **Lições Aprendidas Estratégicas:** De acordo com análises do CSIS, a guerra demonstrou que a superioridade espacial é fundamental para a guerra moderna, permitindo a operação de forças convencionais menores, mas mais letais.7 A Rússia, apesar do seu poderio militar, falhou em alcançar a superioridade espacial, em grande parte devido à sua incapacidade de neutralizar a vasta e resiliente rede de ativos espaciais comerciais que apoiavam a Ucrânia. Isto destaca a importância crescente das parcerias público-privadas na segurança nacional.7

### 5.2 Análise Comparativa de Segurança por Regime Orbital (LEO, MEO, GEO)

A escolha de uma órbita — Órbita Terrestre Baixa (LEO), Órbita Terrestre Média (MEO) ou Órbita Geoestacionária (GEO) — é uma das decisões de projeto mais fundamentais para uma missão de satélite, com profundas e distintas implicações de segurança.68 Cada regime orbital apresenta um perfil único de vulnerabilidades e vantagens defensivas. A tabela abaixo sintetiza estes compromissos estratégicos, fornecendo um guia para a tomada de decisão informada por riscos.

| Fator de Segurança | Órbita Terrestre Baixa (LEO) | Órbita Terrestre Média (MEO) | Órbita Geoestacionária (GEO) |
| --- | --- | --- | --- |
| **Vulnerabilidade a Ataques Cinéticos (DA-ASAT)** | Baixa. É difícil visar e atingir um satélite específico numa constelação de milhares de objetos em movimento rápido. A rede é resiliente à perda de alguns nós. | Média. Menos satélites do que em LEO, com órbitas mais altas e previsíveis, tornando-os alvos mais viáveis. Os satélites de GNSS em MEO são alvos críticos. | Alta. Os satélites são ativos de alto valor, grandes e aparecem estacionários a partir do solo, tornando-os os alvos mais fáceis de rastrear e atingir. |
| **Vulnerabilidade a Jamming/Spoofing (Uplink)** | Alta. A arquitetura depende de um grande número de estações terrestres e gateways distribuídos, criando uma superfície de ataque muito ampla para interferência no uplink. | Média. Menos estações terrestres do que as constelações LEO, mas ainda assim uma rede distribuída que apresenta múltiplos pontos de vulnerabilidade. | Baixa. Geralmente depende de poucos gateways de uplink, que são grandes, centralizados e podem ser fisicamente protegidos com altos níveis de segurança. |
| **Resiliência Arquitetural (Perda Individual)** | Muito Alta. A perda de vários satélites tem um impacto mínimo ou nulo na capacidade geral da rede, que se auto-reconfigura. | Média. A perda de um satélite de navegação (ex: GPS) pode degradar a precisão do serviço numa vasta região até que um substituto seja ativado. | Muito Baixa. A perda de um único satélite de comunicações ou de alerta de mísseis resulta na perda total de cobertura para aproximadamente um terço da superfície terrestre. |
| **Exposição a Detritos Espaciais** | Muito Alta. LEO é a região orbital mais congestionada, com a maior densidade de detritos. O risco de colisão é uma preocupação operacional constante. | Média. Passa pelos cinturões de radiação de Van Allen, o que representa um risco ambiental, mas o ambiente de detritos é menos denso do que em LEO. | Baixa. É uma órbita menos congestionada, mas qualquer detrito gerado aqui permanecerá em órbita quase indefinidamente, representando uma ameaça a longo prazo. |
| **Complexidade e Vulnerabilidade do Segmento Terrestre** | Muito Alta. Milhares ou milhões de terminais de utilizador, cada um sendo um potencial ponto de entrada para um ataque cibernético. A gestão da segurança desta rede é um desafio massivo. | Média. Redes de gateways regionais e terminais de utilizador mais especializados, mas ainda assim uma superfície de ataque considerável. | Baixa. O segmento terrestre consiste em poucos gateways centralizados e terminais de utilizador profissionais, que são mais fáceis de proteger e monitorizar. |
| **Custo e Viabilidade de "Hardening" por Satélite** | Baixo. O modelo de negócio das megaconstelações depende de satélites de baixo custo, produzidos em massa e facilmente substituíveis. O investimento em blindagem pesada ou redundância extensiva por satélite é economicamente inviável. | Médio. Satélites mais caros e com maior tempo de vida do que os de LEO, como os de GNSS, justificam um nível moderado de endurecimento e redundância. | Alto. São ativos estratégicos de alto valor e longa duração. O investimento máximo em blindagem, redundância e proteção é justificado e esperado. |

## Seção 6: O Futuro da Segurança de Satélites: Tendências e Recomendações

O domínio espacial está a evoluir a um ritmo vertiginoso, impulsionado por tecnologias disruptivas e novas arquiteturas de sistemas. Estas tendências apresentam tanto oportunidades sem precedentes para a defesa e resiliência dos ativos espaciais como novos e complexos desafios de segurança. Compreender estas dinâmicas é essencial para formular estratégias e recomendações que garantam a segurança e a sustentabilidade das operações espaciais no futuro.

### 6.1 Inteligência Artificial: A Faca de Dois Gumes da Segurança Espacial

A Inteligência Artificial (IA) está a emergir como a tecnologia mais transformadora no domínio espacial, funcionando simultaneamente como uma poderosa ferramenta de defesa e uma arma ofensiva sofisticada.

* **IA para Defesa (IA Defensiva):** A IA está a revolucionar a capacidade de proteger e utilizar satélites. Algoritmos de IA e machine learning podem analisar vastos volumes de dados de sensores em tempo real para detetar anomalias e prever ameaças.75 Satélites equipados com processamento de IA a bordo, como o Φsat-2 da Agência Espacial Europeia (ESA) e o CogniSAT-6 da NASA/Ubotica, podem analisar imagens autonomamente para detetar eventos como incêndios florestais, derrames de petróleo ou atividade marítima ilegal, e tomar decisões em tempo real, como reorientar os seus sensores para uma observação mais detalhada, sem necessidade de intervenção humana.78 Esta capacidade de "edge computing" no espaço reduz drasticamente a latência entre a observação e a ação, o que é crítico para a resposta a desastres e a monitorização de segurança. Além disso, a IA está a ser desenvolvida para sistemas de navegação resilientes que podem funcionar mesmo na ausência de sinais GNSS, utilizando outros sensores e dados de mapas.82
* **IA para Ataque (IA Ofensiva):** Inevitavelmente, os adversários também estão a aproveitar o poder da IA. Os ciberataques baseados em IA estão a tornar-se cada vez mais sofisticados. Isto inclui o desenvolvimento de malware que pode adaptar-se e evoluir para evitar a detecção por sistemas de segurança tradicionais, a criação de campanhas de phishing altamente personalizadas e convincentes, e a orquestração de ataques de negação de serviço (DoS) em larga escala.48 No contexto espacial, a IA poderia ser usada para otimizar ataques de jamming, tornando-os mais eficazes e difíceis de mitigar, ou para permitir o controle autônomo de enxames de satélites de ataque que poderiam coordenar-se para sobrecarregar as defesas de um alvo.

### 6.2 Os Desafios das Megaconstelações

A proliferação de megaconstelações em LEO, lideradas por empresas como a Starlink, OneWeb e o Projeto Kuiper da Amazon, está a redefinir a economia e a arquitetura do espaço, mas também a introduzir desafios de segurança de uma escala sem precedentes.34

* **Aumento Exponencial da Superfície de Ataque:** Uma constelação com dezenas de milhares de satélites e milhões de terminais de utilizador em todo o mundo cria uma superfície de ataque cibernético vasta e distribuída, muito mais difícil de defender do que um sistema centralizado tradicional.68 Cada satélite e cada terminal é um potencial ponto de entrada para um atacante.
* **Gestão de Tráfego e Sustentabilidade Orbital:** O congestionamento extremo em LEO aumenta dramaticamente o risco de colisões, tanto acidentais como intencionais. A gestão do tráfego espacial (STM) e a mitigação de detritos tornam-se desafios críticos não apenas para operadores individuais, mas para a sustentabilidade a longo prazo do ambiente espacial.31 A NASA expressou publicamente sérias preocupações sobre os planos de expansão da Starlink, citando o aumento do risco de colisão para as suas próprias missões científicas e tripuladas.87

### 6.3 Recomendações Estratégicas Finais

Face a este cenário complexo, é necessária uma ação coordenada por parte de todos os stakeholders do ecossistema espacial.

* **Para Operadores de Satélites:** É fundamental adotar uma filosofia de **"segurança desde o projeto" (security-by-design)**. A segurança deve ser uma consideração central em todas as fases do ciclo de vida de uma missão, desde o conceito inicial até ao descarte do satélite. Isto implica a implementação de uma **defesa em profundidade** que abranja todos os segmentos da missão: o software, o hardware, o segmento terrestre, os links de comunicação e o segmento do utilizador. O investimento deve ser direcionado para arquiteturas resilientes (redundância, diversidade de fornecedores, constelações desagregadas) e para a integração de contramedidas técnicas avançadas, como sistemas anti-jamming adaptativos e a transição para criptografia resistente a computadores quânticos (criptografia pós-quântica).
* **Para Governos e Agências Reguladoras:** Há uma necessidade urgente de desenvolver, adotar e aplicar **normas internacionais de comportamento responsável no espaço**. Isto inclui regras claras e vinculativas para a partilha de dados de SDA, coordenação de manobras, mitigação de detritos e transparência operacional. A cooperação internacional em Consciência do Domínio Espacial (SDA) e Gestão do Tráfego Espacial (STM) deve ser fortalecida para criar um sistema global que possa gerir com segurança o crescente número de satélites.88
* **Para a Comunidade de Defesa e Inteligência:** É imperativo acelerar o investimento em investigação e desenvolvimento de capacidades de defesa espacial de próxima geração. Isto inclui o desenvolvimento de sistemas de IA defensiva, sensores de SDA mais precisos e distribuídos, e o aprofundamento da transição para arquiteturas espaciais mais resilientes e proliferadas. As **parcerias público-privadas** são cruciais; a comunidade de defesa deve alavancar a inovação e a escala do setor comercial, ao mesmo tempo que trabalha com a indústria para garantir a segurança de sistemas de duplo uso que são vitais para a segurança nacional.1

Em última análise, a percepção da segurança no domínio espacial deve evoluir. Tradicionalmente, medidas de segurança como blindagem, redundância e combustível extra para manobras eram vistas como um custo, uma sobrecarga que aumentava a massa e o orçamento de uma missão. No entanto, no ambiente espacial contestado e economicamente vital do século XXI, esta visão está obsoleta. A normalização das ameaças 2 e a crescente dependência económica e social dos serviços espaciais 1 alteraram fundamentalmente a equação de risco. Uma falha de segurança, seja por um ataque bem-sucedido ou por uma colisão com detritos, pode resultar na perda de serviços críticos, com impactos financeiros, de reputação e de segurança nacional devastadores. O mercado de seguros espaciais já está a adaptar-se a esta nova realidade de risco acrescido.34

Neste novo paradigma, a segurança robusta e a resiliência demonstrável já não são apenas um requisito técnico ou um centro de custo. Tornaram-se um **diferencial competitivo e um habilitador de negócios fundamental**. Os operadores que conseguem garantir aos seus clientes a disponibilidade, a integridade e a continuidade dos seus serviços, mesmo num ambiente hostil, possuirão uma vantagem de mercado decisiva. O investimento em resiliência é, portanto, um investimento direto na continuidade e na viabilidade a longo prazo do próprio negócio espacial. A segurança tornou-se um componente intrínseco e inseparável da proposta de valor.

#### Referências citadas

1. Secure Our Satellites - Aerospace Industries Association, acessado em julho 5, 2025, <https://www.aia-aerospace.org/publications/secure-our-satellites/>
2. Jamming, Spoofing, Hacking: Today's Most Pervasive Counterspace ..., acessado em julho 5, 2025, <https://spacepolicyonline.com/news/jamming-spoofing-hacking-todays-most-pervasive-counterspace-threats/>
3. Space Threat Assessment 2025 - CSIS, acessado em julho 5, 2025, <https://www.csis.org/analysis/space-threat-assessment-2025>
4. ICAO, ITU, IMO sound alarm over rising satellite navigation jamming ..., acessado em julho 5, 2025, <https://industrialcyber.co/critical-infrastructure/icao-itu-imo-sound-alarm-over-rising-satellite-navigation-jamming-and-spoofing-attacks-call-for-urgent-safeguards/>
5. What are the Impacts of GPS Jamming and Spoofing on Civilians? - YouTube, acessado em julho 5, 2025, <https://www.youtube.com/watch?v=zXdPJcbbe5Y>
6. Space Threat Assessment 2024 - CSIS Aerospace Security, acessado em julho 5, 2025, <https://aerospace.csis.org/space-threat-assessment-2024/>
7. Space Threat Assessment 2023 - CSIS, acessado em julho 5, 2025, <https://www.csis.org/analysis/space-threat-assessment-2023>
8. Space Threat Assessment 2024 - CSIS, acessado em julho 5, 2025, <https://www.csis.org/analysis/space-threat-assessment-2024>
9. Armas contraespaciales - Air University, acessado em julho 5, 2025, [https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-5\_Issue-2/04-Martini\_s-w.pdf?ver=f-8aSPMS6WSZDJ3W5tSYyw%3D%3D×tamp=1694881367327](https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-5_Issue-2/04-Martini_s-w.pdf?ver=f-8aSPMS6WSZDJ3W5tSYyw%3D%3D&timestamp=1694881367327)
10. ¿Qué son las armas antisatélite o ASAT? - Segurilatam, acessado em julho 5, 2025, <https://www.segurilatam.com/actualidad/que-son-las-armas-antisatelite-o-asat_20250319.html>
11. Satellite Navigation Systems Facing Rising Jamming and Spoofing ..., acessado em julho 5, 2025, <https://hackread.com/satellite-navigation-systems-jamming-spoofing-attacks/>
12. GPS Jamming, Spoofing and Hacking | NorthStandard | Marine ..., acessado em julho 5, 2025, <https://north-standard.com/insights-and-resources/resources/articles/gps-jamming-spoofing-and-hacking>
13. Small satellites, big weakness - Aerospace America, acessado em julho 5, 2025, <https://aerospaceamerica.aiaa.org/features/small-satellites-big-weakness/>
14. Hackers no espaço: a crescente ameaça de ataques cibernéticos ..., acessado em julho 5, 2025, <https://www.tecmundo.com.br/ciencia/286674-hackers-espaco-crescente-ameaca-ataques-ciberneticos-satelites-espaciais.htm>
15. ¿Qué son las armas antisatélite? - EFE, acessado em julho 5, 2025, <https://efe.com/mundo/2024-02-16/armas-antisatelite-claves/>
16. Destruyendo satélites: los sistemas ASAT de las potencias ..., acessado em julho 5, 2025, <https://danielmarin.naukas.com/2020/04/21/destruyendo-satelites-los-sistemas-asat-de-las-potencias-espaciales/>
17. PORTARIA Nº 042-EME, DE 20 DE MARÇO DE 2018. - Secretaria-Geral do Exército, acessado em julho 5, 2025, <http://www.sgex.eb.mil.br/sg8/006_outras_publicacoes/07_publicacoes_diversas/04_estado_maior_do_exercito/port_n_042_eme_20mar2018.html>
18. UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL, acessado em julho 5, 2025, <https://www.lume.ufrgs.br/bitstream/handle/10183/71933/000879936.pdf?sequence=1&isAllowed=y>
19. 1 IntroduÃ…Â§Ã…Â£o - Marinha do Brasil, acessado em julho 5, 2025, <https://repositorio.mar.mil.br/bitstream/ripcmb/846885/1/TCC%20CApA_Phelipe%20Barbosa.pdf>
20. ACADEMIA MILITAR O paradigma do Carro de Combate no futuro, acessado em julho 5, 2025, <https://comum.rcaap.pt/server/api/core/bitstreams/c0f7fba1-c7e3-4960-9220-40ccecde9fa0/content>
21. Cibersegurança, Inteligência Artificial e Novas ... - Portal Gov.br, acessado em julho 5, 2025, <https://www.gov.br/esg/pt-br/composicao/editora/ciberseguranca-inteligencia-artificial-e-novas-tecnologias-na-area-de-defesa.pdf>
22. Portaria n.º 439/94 | DR - Diário da República, acessado em julho 5, 2025, <https://diariodarepublica.pt/dr/detalhe/portaria/439-183848>
23. Compreender os impulsos eletromagnéticos: um guia simples para ..., acessado em julho 5, 2025, <https://wraycastle.com/pt/blogs/knowledge-base/what-is-an-electromagnetic-pulse>
24. Pulso eletromagnético – Wikipédia, a enciclopédia livre, acessado em julho 5, 2025, <https://pt.wikipedia.org/wiki/Pulso_eletromagn%C3%A9tico>
25. EMP – A arma capaz de destruir computadores – Defesa Aérea ..., acessado em julho 5, 2025, <https://www.defesaaereanaval.com.br/ciencia-e-tecnologia/emp-a-arma-capaz-de-destruir-computadores>
26. Comunicações por satélite são novo alvo de ataques cibernéticos ..., acessado em julho 5, 2025, <https://transformacaodigital.com/seguranca/tecnologia/comunicacoes-por-satelite-sao-novo-alvo-de-ataques-ciberneticos/>
27. O que é um ataque à cadeia de suprimentos? | Zscaler, acessado em julho 5, 2025, <https://www.zscaler.com/br/resources/security-terms-glossary/what-is-a-supply-chain-attack>
28. O que é um ataque à cadeia de suprimentos? | Cloudflare, acessado em julho 5, 2025, <https://www.cloudflare.com/pt-br/learning/security/what-is-a-supply-chain-attack/>
29. Os 5 principais riscos digitais da cadeia de suprimentos | Avetta, acessado em julho 5, 2025, <https://www.avetta.com/pt-br/blog/top-5-supply-chain-cyber-risks>
30. Detritos espaciais: avaliar o risco - ESA, acessado em julho 5, 2025, <https://www.esa.int/Space_in_Member_States/Portugal/Detritos_espaciais_avaliar_o_risco>
31. Mais de 1 milhão de satélites podem ser lançados na órbita da ..., acessado em julho 5, 2025, <https://www.tecmundo.com.br/ciencia/272768-1-milhao-satelites-lancados-orbita-terra.htm>
32. DETRITOS ESPACIAIS EM ÓRBITA TERRESTRE BAIXA ... - TEDE, acessado em julho 5, 2025, <https://tede.unisantos.br/bitstream/tede/6665/1/Francisco%20Campos%20da%20Costa.pdf>
33. Soluções para a redução do lixo espacial - MAPFRE Global Risks, acessado em julho 5, 2025, <https://www.mapfreglobalrisks.com/pt-br/gerencia-riscos-seguros/estudos/solucoes-para-a-reducao-do-lixo-espacial/>
34. Satélite Mega Constelações Tamanho do Mercado, Compartilhar ..., acessado em julho 5, 2025, <https://www.fortunebusinessinsights.com/pt/satellite-mega-constellations-market-112989>
35. SIMULAÇÃO DE BLINDAGEM CONTRA RADIAÇÃO IONIZANTE EM SATÉLITES DE ÓRBITA BAIXA (LEO) - SIGE, acessado em julho 5, 2025, <https://www.sige.ita.br/edicoes-anteriores/2024/st/242567_1.pdf>
36. Rastreio e controle de satélites do INPE, acessado em julho 5, 2025, <http://200.144.244.96/cda/oba/aeb/a-conquista-do-espaco/Capitulo-6.pdf>
37. Ameaças de cadeia de suprimentos de software | Software supply ..., acessado em julho 5, 2025, <https://cloud.google.com/software-supply-chain-security/docs/attack-vectors?hl=pt-br>
38. SUMÁRIO - TCE-AL, acessado em julho 5, 2025, <https://www.tceal.tc.br/view/documentos/doc2511202410362000000067447d5491ede.pdf>
39. Guia para Gestão de Riscos em matérias de Segurança da ..., acessado em julho 5, 2025, <https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos.pdf>
40. NIST rolls out cybersecurity profile that focuses on command and ..., acessado em julho 5, 2025, <https://industrialcyber.co/nist/nist-rolls-out-cybersecurity-profile-that-focuses-on-command-and-control-of-satellite-buses-payloads/>
41. Satellite Ground Segment: Applying the Cybersecurity Framework to ..., acessado em julho 5, 2025, <https://www.nist.gov/publications/satellite-ground-segment-applying-cybersecurity-framework-satellite-command-and-control>
42. NIST works on applying cybersecurity framework for satellite ..., acessado em julho 5, 2025, <https://industrialcyber.co/threats-attacks/nist-works-on-applying-cybersecurity-framework-for-satellite-command-and-control-seeks-feedback/>
43. NIST.IR.8401.pdf - NIST Technical Series Publications - National ..., acessado em julho 5, 2025, <https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.pdf>
44. IR 8401, Satellite Ground Segment: Applying the Cybersecurity ..., acessado em julho 5, 2025, <https://csrc.nist.gov/pubs/ir/8401/final>
45. Tailoring NIST Security Controls for the Ground System: Selection ..., acessado em julho 5, 2025, <https://ntrs.nasa.gov/api/citations/20160011256/downloads/20160011256.pdf>
46. Interferência em Satélite Adjacente (ASI) em Comunicações Via ..., acessado em julho 5, 2025, <https://www.whcengenharia.com.br/post/interfer%C3%AAncia-em-sat%C3%A9lite-adjacente-asi-em-comunica%C3%A7%C3%B5es-via-sat%C3%A9lite>
47. Avaliação de vulnerabilidades e teste de penetração: como escolher?, acessado em julho 5, 2025, <https://www.tempest.com.br/blog/avaliacao-de-vulnerabilidades-e-teste-de-penetracao>
48. Pentest vs Análise de Vulnerabilidades: qual a melhor estratégia de ..., acessado em julho 5, 2025, <https://esr.rnp.br/seguranca/pentest-analise-de-vulnerabilidade/>
49. Soluções para avaliação de vulnerabilidades | Tenable®, acessado em julho 5, 2025, <https://pt-br.tenable.com/source/vulnerability-assessment>
50. Guia de Análise de Ameaças em Cibersegurança: Proteção Proativa, acessado em julho 5, 2025, <https://bravotecnologia.com.br/analise-de-ameacas-em-ciberseguranca/>
51. Satellite security lags decades behind the state of the art | EurekAlert!, acessado em julho 5, 2025, <https://www.eurekalert.org/news-releases/995157>
52. COMANDO DA AERONÁUTICA - ITA, acessado em julho 5, 2025, <https://www.pgfis.ita.br/post/download/5e32049b9a124f6d5d3cc6a4>
53. (Actos cuja publicação é uma condição da sua aplicabilidade, acessado em julho 5, 2025, <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:281:0001:0225:PT:PDF>
54. Antena Anti-bloqueio Personalizada Do Jammer Do Sinal Para ..., acessado em julho 5, 2025, <https://www.shinewave-tech.com/list_75/2351.html>
55. Anti-Jam GPS DACU (8-Channel) | Chelton, acessado em julho 5, 2025, <https://www.chelton.com/product/anti-jam-gps-dacu-8-channel/>
56. Anti-Jamming Antennas for GPS & GNSS Protection - Kosminis Vytis, acessado em julho 5, 2025, <https://kosminis-vytis.lt/products/anti-jamming-solutions/anti-jamming-antennas/>
57. Uma ideia nova que eu tive sobre blindagem de naves. É boa? : r, acessado em julho 5, 2025, <https://www.reddit.com/r/scifiwriting/comments/1jivrh8/a_new_idea_i_have_on_the_subject_of_armoring/?tl=pt-br>
58. Resiliência Operacional: Estratégias para Enfrentar ... - MICROHARD, acessado em julho 5, 2025, <https://microhard.com.br/resiliencia-operacional-estrategias-para-enfrentar-desafios-ciberneticos/>
59. Redundância em TI: entenda sua relevância no ambiente operacional, acessado em julho 5, 2025, <https://noventiq.com.br/sobre-a-empresa/blog/redundancia-em-ti-entenda-sua-relevancia-num-ambiente-operacional>
60. controle de atitude de um satélite aplicando a união dos métodos ..., acessado em julho 5, 2025, <http://mtc-m21c.sid.inpe.br/col/sid.inpe.br/mtc-m21c/2020/03.09.12.26/doc/publicacao.pdf>
61. Paper Title (use style: paper title) - UFSM, acessado em julho 5, 2025, <https://www.ufsm.br/app/uploads/sites/553/2020/07/90656-field_submission_abstract_file2.pdf>
62. Subsistema de Controle de Atitude, acessado em julho 5, 2025, <http://mtc-m21c.sid.inpe.br/col/sid.inpe.br/mtc-m21c/2019/08.22.14.06/doc/170_Subsistema%20de%20Controle%20de%20Atitude_P2.2_v1_2002.pdf>
63. Maneuvers to avoid space debris will become a constant for the ISS ..., acessado em julho 5, 2025, <https://www.youtube.com/watch?v=1uCm3atWEfw>
64. AVANÇOS EM SISTEMAS DE SATÉLITES EM BAIXA ÓRBITA ..., acessado em julho 5, 2025, <https://revistaft.com.br/avancos-em-sistemas-de-satelites-em-baixa-orbita-protocolos-de-comunicacao-navegacao-e-aprendizado-federado/>
65. Segurança da cadeia de suprimentos de software: as 7 melhores ..., acessado em julho 5, 2025, <https://scribesecurity.com/pt/blog/enhancing-software-supply-chain-security/>
66. Lista de verificação de segurança da cadeia de suprimentos de ..., acessado em julho 5, 2025, <https://www.paloaltonetworks.com.br/resources/datasheets/software-supply-chain-security-checklist>
67. Segurança da cadeia de suprimentos de software | Software supply ..., acessado em julho 5, 2025, <https://cloud.google.com/software-supply-chain-security/docs/overview?hl=pt-br>
68. Picking the Right SatCom Path: LEO, MEO or GEO? | Milexia Group, acessado em julho 5, 2025, <https://milexia.com/in-the-media/picking-the-right-satcom-path-leo-meo-or-geo>
69. Conflict in Focus: Lessons from Russia-Ukraine - CSIS, acessado em julho 5, 2025, <https://www.csis.org/analysis/conflict-focus-lessons-russia-ukraine>
70. Popular Orbits 101 - Aerospace Security, acessado em julho 5, 2025, <https://aerospace.csis.org/aerospace101/earth-orbit-101/>
71. LEO vs. MEO vs. GEO Satellites: What's the Difference? - Anywaves, acessado em julho 5, 2025, <https://anywaves.com/resources/blog/leo-meo-geo-satellites-definition-difference/>
72. Understanding LEO, MEO, and GEO Satellite Orbit Systems, acessado em julho 5, 2025, <https://ast-networks.com/insights/blog/guide-to-leo-meo-geo-orbit-systems/>
73. A guide: GEO, LEO and MEO Satellites - OceanWeb Ltd, acessado em julho 5, 2025, <https://www.oceanweb.com/a-guide-geo-leo-and-meo-satellites/>
74. LEO vs. MEO vs. GEO Satellites: What's the Difference? | Symmetry ..., acessado em julho 5, 2025, <https://www.symmetryelectronics.com/blog/leo-vs-meo-vs-geo-satellites-what-s-the-difference-symmetry-blog/>
75. O Potencial Da Tecnologia De Satélite: Tendências Para 2025 ..., acessado em julho 5, 2025, <https://bpmoney.com.br/noticias/o-potencial-da-tecnologia-de-satelite-tendencias-para-2025/>
76. Tendências em tecnologia de segurança para 2025 - Avigilon, acessado em julho 5, 2025, <https://www.avigilon.com/br/blog/security-technology>
77. Como a IA pode ajudar na análise de imagens de satélite? - Blog da ..., acessado em julho 5, 2025, <https://www.geoambiente.com.br/blog/ia_imagens_satelite/>
78. Satélite com IA vai monitorar a Terra - Próximo Nível - Embratel, acessado em julho 5, 2025, <https://proximonivel.embratel.com.br/satelite-com-ia-vai-monitorar-a-terra/>
79. Satélites equipados com IA podem revolucionar a resposta a ..., acessado em julho 5, 2025, <https://fastcompanybrasil.com/impacto/satelites-equipados-com-ia-resposta-a-desastres-naturais/>
80. Satélite com inteligência artificial será lançado para monitorar a ..., acessado em julho 5, 2025, <https://www.cnnbrasil.com.br/tecnologia/satelite-com-inteligencia-artificial-sera-lancado-para-monitorar-a-terra/>
81. Smart satellites for fast action - Aerospace America, acessado em julho 5, 2025, <https://aerospaceamerica.aiaa.org/departments/smart-satellites-for-fast-action/>
82. Alternativa de GPS com IA funciona sem sinal de satélite | Exame, acessado em julho 5, 2025, <https://exame.com/inteligencia-artificial/alternativa-de-gps-com-ia-funciona-sem-sinal-de-satelite/>
83. 5 tendências em segurança digital e cibersegurança para 2025, acessado em julho 5, 2025, <https://cloudtarget.com.br/5-tendencias-em-seguranca-digital-e-ciberseguranca-para-2025/>
84. Fenômeno das Mega Constelações de Satélites ... - Conteúdo Jurídico, acessado em julho 5, 2025, <https://conteudojuridico.com.br/consulta/artigos/68088/fenmeno-das-mega-constelaes-de-satlites-e-inteligncia-artificial-as-startups-na-concorrncia-comercial-espacial-planetria-do-setor-telecom-e-o-comrcio-eletrnico-global-na-internet>
85. O crescimento da oferta de satélites LEO para conectividade, acessado em julho 5, 2025, <https://digital.futurecom.com.br/artigos/o-crescimento-da-oferta-de-satelites-leo-para-conectividade/>
86. Astrônomos querem impedir megaconstelações de satélites - YouTube, acessado em julho 5, 2025, <https://m.youtube.com/watch?v=4pSkLqmvA4M>
87. Expansão de constelação da Starlink preocupa Nasa e operadoras ..., acessado em julho 5, 2025, <https://teletime.com.br/11/02/2022/expansao-de-constelacao-da-starlink-preocupa-nasa-e-operadoras-de-satelite/>
88. Act now, before we're trapped on Earth - Aerospace America, acessado em julho 5, 2025, <https://aerospaceamerica.aiaa.org/departments/act-now-before-were-trapped-on-earth/>
89. Report Archives - CSIS Aerospace Security, acessado em julho 5, 2025, <https://aerospace.csis.org/post_types/report/>