デジタル時代の欺瞞：GPSスプーフィング、シームレス・テイクオーバー、およびPNTレジリエンスの未来に関する分析

エグゼクティブサマリー

本レポートは、全地球測位システム（GPS）に対するスプーフィング（なりすまし）攻撃、特に「シームレス・テイクオーバー」として知られる高度な技術の動向、具体的な実装例、およびそれに対する防御策について、専門的かつ包括的な分析を提供する。GPSは、そのユビキタスな性質と高い信頼性から、運輸、金融、通信、農業、国家安全保障といった重要インフラの根幹を成している。しかし、その民生用信号の根本的な脆弱性は、深刻な脅威にさらされている。

本レポートの主要な分析結果は以下の通りである。

1. 根本的脆弱性： 民生用GPS信号（L1 C/A）は、その構造が公開されており、暗号化も認証も行われていない。さらに、地上に到達する信号は極めて微弱であるため、比較的低出力の偽信号によって容易に無力化または乗っ取られる可能性がある。この脆弱性は、設計上の欠陥というよりも、普及を優先した意図的な設計思想に起因するものであり、現代の脅威環境下で深刻なリスクとなっている。
2. 脅威の民主化： かつては国家レベルのアクターや高度な研究機関のみが利用可能であった高価な専用シミュレータに代わり、安価なソフトウェア無線（SDR）とオープンソースソフトウェアの登場により、高度なスプーフィング攻撃の実行が技術的・経済的に容易になった。これにより、脅威は国家間の戦略的対立から、犯罪組織やテロリスト、個人による非対称な戦術的攻撃へと拡散している。
3. シームレス・テイクオーバーの技術的実現性： 最も危険な攻撃形態であるシームレス・テイクオーバーは、受信機にロック喪失を気づかせることなく制御を奪う技術である。この攻撃の成功は、送信電力の大きさよりも、ナノ秒単位の極めて精密なタイミング同期（コード位相およびキャリア位相の整合）と、ターゲットの位置・速度に関する正確なリアルタイムの状況認識能力に依存する。この攻撃の実行には、ターゲットの信号をまず受信・分析してから偽信号を送信する「レシーバー・スプーfer」アーキテクチャが不可欠であり、この特異な挙動自体が新たな探知の手がかりとなり得る。
4. 現実世界の脅威と多様な意図： 学術的な実証実験（テキサス大学によるUAVや大型ヨットの乗っ取り実験）から、国家レベルの電子戦（ロシア連邦による黒海やモスクワでの大規模スプーフィング）まで、スプーフィングは理論上の脅威ではなく、現実の兵器として使用されている。その意図は、特定のターゲットを欺瞞し乗っ取る「ハイジャック型」、ドローンのような単純なシステムを無力化する「拒否・抑止型」、そして広範囲の商業・軍事活動を妨害し混乱させる「混乱・摩擦型」に分類でき、それぞれ異なる技術的特徴と防御要件を持つ。
5. 多層防御戦略の現状と課題： 単一の万能な解決策は存在しない。防御は、受信機自律信頼性監視（RAIM）のような基本的な整合性チェックから、複数アンテナによる到来方向分析、信号フィンガープリンティング、SPREE受信機のような高度な相関処理、そして慣性計測装置（IMU）や他のセンサーとのフュージョンによるシステムレベルの冗長性確保まで、多層的に構築される必要がある。GalileoのOSNMAやGPSのChimeraといった信号レベルでの暗号認証は強力な防御策であるが、リプレイ攻撃や、暗号の信頼性の基点（トラストアンカー）自体のライフサイクル（製造、配布、更新）における脆弱性など、新たな攻撃対象を生み出している。

本レポートは、これらの分析に基づき、PNT（測位・航法・時刻）セキュリティの未来は、単一技術の

完成度を高めることではなく、多様な技術を組み合わせた「システム・オブ・システムズ」として、回復力（レジリエンス）を設計することにあると結論付ける。真のレジリエンスとは、攻撃を完全に防ぐことではなく、攻撃を受けてもその影響を限定し、システムの信頼性を維持し、優雅に失敗（fail gracefully）できる能力である。このためには、技術開発だけでなく、人間のオペレーターと機械の信頼関係を考慮したヒューマン・マシン・インターフェースの設計、認知バイアスを克服するための訓練、そして中央集権的な衛星システムを補完する分散型PNTインフラ（eLoranなど）への政策的投資を含む、包括的なアプローチが不可欠である。

第1章 民生用GPSの固有の脆弱性

1.1 序論：グローバル・ユーティリティのパラドックス

全地球測位システム（GPS）は、現代社会において不可欠なグローバル・ユーティリティとなっている。運輸、金融、通信、農業から緊急サービスに至るまで、数え切れないほどのセクターがその測位・航法・時刻（PNT）情報に依存している 。そのユビキタスな性質と高い信頼性は、我々の生活と経済活動に革命をもたらした。しかし、この広範な依存の裏には、しばしば見過ごされがちな深刻なパラドックスが潜んでいる。すなわち、GPSへの過度の信頼が、そのシステムに内在する脆弱性を覆い隠し、認識されていないリスクを生み出しているのである 。多くのシステムにおいてPNTの利用は隠されており、GPSが常に利用可能で正確であるという前提のもとに設計されているため、ひとたびその前提が崩れると、インフラは急速に機能不全に陥る可能性がある 。
この章では、民生用GPSがなぜスプーフィング（なりすまし）攻撃に対して本質的に脆弱であるのか、その技術的根源を解明する。この脆弱性は、単なる設計上の欠陥ではなく、普及を最優先した意図的な設計思想に根差している。この設計思想が、現代の脅威環境においていかにして深刻なリスクへと転化したのかを明らかにすることが、本レポート全体の理解の基礎となる。

1.2 民生用信号：公開された設計図

民生用GPSの脆弱性の核心は、最も広く利用されているレガシー信号であるL1 C/A信号の設計そのものにある 。この信号は、意図的に「オープン」にされており、その構造や仕様は誰でもアクセス可能な公開情報となっている。この透明性が、スプーフィング攻撃を可能にする根本的な土壌を提供している 。

1.2.1 信号構造と構成要素

民生用L1 C/A信号は、主に3つの要素で構成されている 。

- 搬送波（**Carrier Wave**）：信号は、1575.42 MHzという公開された周波数の搬送波に乗せて送信される 。この周波数は固定されており、攻撃者がターゲットとすべき周波数を特定することは極めて容易である。
- **C/A**コード（**Coarse/Acquisition Code**）：これは、測距の基準となる測位符号であり、各衛星に固有のPRN（疑似ランダム雑音）コードが割り当てられている。具体的には、1023チップ長のゴールド符号であり、毎ミリ秒繰り返される 。このC/Aコードの生成方法は公開されており、誰でも容易に特定の衛星のコードを複製できる。受信機はこのコードのレプリカを生成し、受信信号との相関をとることで衛星を識別し、信号の伝播時間を測定する。攻撃者は、この公開されたコードを生成することで、本物の衛星信号であるかのように見せかけることが可能となる 。
- 航法メッセージ（**Navigation Message, NAV**）：50 bpsという低速で送信されるデータストリームであり、衛星の正確な軌道情報（エフェメリス）、全衛星の概略軌道情報（アルマナック）、衛

星クロックの補正データなど、測位計算に必要な情報が含まれている 。この航法メッセージも暗号化されておらず、そのフォーマットはIS-GPS-200というインターフェース仕様書（ICD）で完全に公開されている 。これにより、攻撃者はもっともらしい偽の航法メッセージを構築し、受信機を欺いて偽の位置を計算させることができる。

1.2.2 アキレス腱：微弱な信号電力

GPS衛星は高度20,000 km以上の宇宙空間を周回しており、そこから送信される信号は、地球の電離層や対流圏を通過する過程で大きく減衰する 。その結果、地上の受信機アンテナに到達する時点での信号電力は、-120 dBmから-130 dBm程度と極めて微弱になる 。これは、背景雑音レベルを下回るほどの弱さである 。
ある比較によれば、標準的な100ワットの電球の電力は、受信機アンテナにおけるGPS信号の電力の10^{18}倍にも達する 。この極端な微弱性は、GPSシステムの根本的なアキレス腱である。なぜなら、地上の送信機は、ごくわずかな電力で本物の衛星信号を容易に圧倒（オーバーパワー）できるからである 。これにより、ジャミング（妨害）やスプーフィングが、電力的な観点からは非常に容易に実行可能となっている 。

1.3 認証メカニズムの欠如

民生用GPSの脆弱性を決定づける最後の要素は、暗号技術に基づく認証メカニズムが完全に欠如していることである 。レガシーなL1 C/A信号には、受信した信号が本当にGPS衛星から送信されたものであるか、またその内容が改ざんされていないかを検証する手段が一切組み込まれていない 。受信機は、単に「GPS信号のように見える」信号、すなわち正しい周波数で、既知のC/Aコード構造を持ち、妥当な航法メッセージを含んだ信号を、無条件に信頼するしかない。この「盲目的な信頼」こそが、スプーフィング攻撃者が悪用する最大の脆弱性である。対照的に、軍事用のP(Y)コードは暗号化されており、権限のないユーザーによるなりすましを防ぐように設計されている 。
これらの脆弱性を総合すると、民生用GPSは、そのオープンな設計思想と認証の欠如により、意図的な欺瞞に対して本質的に無防備なシステムであると言える。当初、このオープン性は世界的な普及を促進し、計り知れない経済的利益をもたらした 。しかし、技術が進歩し、脅威が多様化した現代において、その設計思想自体がシステム全体のリスクとなっている。問題は単純な「バグ」ではなく、アーキテクチャレベルでのトレードオフの結果であり、そのリスクが顕在化した今、PNTに対する考え方を「信頼されるユーティリティ」から「ゼロトラスト」へと根本的に転換する必要性が生じている 。

第2章 スプーフィング技術の進化：シミュレータからソフトウェア無線へ

GPSスプーフィングの脅威の性質は、それを実行するために必要な技術の進化と密接に関連している。かつては国家レベルの能力を必要とする高度な攻撃であったが、技術の民主化により、その様相は劇的に変化した。この章では、スプーフィングツールの技術的変遷を追い、それが脅威のランドスケープをいかに変えたかを分析する。

2.1 専用ハードウェアの時代

初期のスプーフィング能力は、高価で大規模な研究室グレードのGNSS信号シミュレータに依存していた 。これらの装置は、衛星信号を極めて高い忠実度で生成・シミュレートするために設計された専門的な計測機器であり、その価格は数万ドルから数十万ドルにも及んだ 。
このため、スプーフィング攻撃を実行できるアクターは、国家の軍事・情報機関や、潤沢な資金を持

つ研究機関、あるいは大手防衛産業などに事実上限定されていた 。脅威は存在したものの、その実行者はごく少数であり、攻撃の対象も主に国家安全保障に関わる高価値なターゲットに限られていた。一般の民生分野や商業活動に対する脅威としては、まだ現実味の薄いものであった。

2.2 SDR革命：欺瞞の民主化

この状況を一変させたのが、ソフトウェア無線（Software-Defined Radio, SDR）技術の登場と普及である。SDRとは、従来ハードウェアで実装されていた変復調、フィルタリング、信号生成といった無線通信の物理層機能を、ソフトウェアによって汎用プロセッサ上で実現する技術である 。
2010年代以降、HackRF、bladeRF、USRPといった、数万円から十数万円程度で購入可能な低コストの商用オフザシェルフ（COTS）SDRプラットフォームが市場に登場した 。これら安価なハードウェアと、gps-sdr-simのようなオープンソースのGPS信号生成ソフトウェアを組み合わせることで、専門家でなくとも比較的容易にGPSスプーferを構築できるようになった 。
このSDRによる技術革命は、スプーフィング攻撃の参入障壁を劇的に引き下げ、「脅威の民主化」とも呼べる状況を生み出した 。かつては国家の専有物であった高度な電子攻撃能力が、今や犯罪者、テロリスト、さらには技術的好奇心を持つ個人（ホビイスト）の手にも届くようになったのである 。

2.3 SDRによって可能になった攻撃モダリティ

SDRの柔軟性は、攻撃者に多様な攻撃手法の選択肢を与えた。

- リプレイ攻撃（ミーコニング）: 最も単純な攻撃形態であり、攻撃者はSDRを用いて特定の場所や時間における本物のGPS信号を録音し、それを後で別の場所や時間に再放送する 。これにより、受信機は録音された時点の位置・時刻情報を現在地のものとして誤認する。SDRの登場により、この種の攻撃は極めて簡単に実行可能となった 。
- 生成攻撃: より高度な攻撃形態であり、攻撃者はソフトウェアを用いて、自身が意図する偽の軌道に対応した、完全に新しい合成GPS信号を生成する 。この手法では、受信機を静的な偽の位置に固定するだけでなく、動的に移動させ、特定の目的地へ誘導することも可能となる。次章で詳述するシームレス・テイクオーバー攻撃には、この生成攻撃の能力が不可欠である 。

この技術的変遷は、単なるコスト削減以上の意味を持つ。それは、GPSスプーフィングという脅威の性質そのものを、予測可能で対処しやすい「戦略的」脅威から、拡散的で予測困難な「戦術的・非対称」脅威へと変質させた。国家が地政学的な優位性のためにスプーフィングを行うシナリオ に加え、個人が数百ドルのSDRを用いて高価な積荷を積んだコンテナをハイジャックする 、あるいは競合他社のドローンを妨害するといった、より小規模で戦術的な動機に基づく攻撃が現実のものとなった。
この脅威の非対称化は、法執行機関や規制当局に新たな課題を突きつけている。軍事資産を国家の脅威から守るための防衛策と、一台の商用トラックをSDRを持つ一人の犯罪者から守るための防衛策とでは、求められるスケーラビリティやコスト効率が全く異なるからである。

第3章 シームレス・テイクオーバー攻撃の解剖

GPSスプーフィングの中でも最も高度かつ危険な形態が「シームレス・テイクオーバー」攻撃である。この攻撃の目的は、ターゲットとなる受信機に攻撃を一切感知させることなく、すなわち、航法解の喪失（ロック喪失）やその他の警告を引き起こすことなく、その制御を密かに奪取することにある 。この章では、この巧妙な攻撃を成功させるために要求される厳格な技術的要件を、定量的なデータに基づいて詳細に分析する。

3.1 顕在的スプーフィング vs. 潜在的スプーフィング：攻撃者の選択

スプーフィング攻撃は、その実行方法によって大きく二つに分類される。

- 顕在的スプーフィング（ジャム・ゼン・スプーフ）：これは比較的単純な手法である。攻撃者はまず、強力なジャミング信号を送信して、ターゲット受信機の正規衛星信号へのロックを強制的に解除させる。受信機が信号を失い再捕捉モードに入った後、攻撃者は強力な偽信号を送信し、受信機にそれを捕捉させる 。この方法は実行が容易である一方、ロック喪失という明確な異常事態を発生させるため、受信機側（ひいてはオペレーター）に攻撃の存在を警告してしまうという欠点がある。
- 潜在的スプーフィング（シームレス・テイクオーバー）：こちらは、受信機の追跡ループを欺き、正規信号から偽信号へと滑らかに「乗り換え」させることを目指す。成功すれば、受信機もオペレーターも、航法情報が偽造されていることに気づかないまま、攻撃者の意図する偽の軌道へと誘導される 。その隠密性の高さから、最も深刻な脅威と見なされている。

3.2 技術的な難関：シームレス・テイクオーバーの要件

シームレス・テイクオーバーの成功は、送信電力の大きさではなく、極めて高い精度での信号制御にかかっている。実験的研究に基づき、その成功には以下の3つのステップと、それぞれに対応する厳格な技術的要件が必要であることが示されている 。

3.2.1 ステップ1：信号の精密な同期

攻撃の第一段階は、生成する偽信号を、受信機が現在受信している本物の衛星信号と、複数の領域で完全に同期させることである 。

- コード位相の同期：攻撃者が生成する偽信号のC/Aコードの位相は、本物の信号の位相と極めて精密に一致している必要がある。実験データによれば、この同期精度は**75**ナノ秒以下でなければならない 。これより大きなオフセットが存在すると、受信機のDLL（Delay-Locked Loop）がロックを失い、攻撃は失敗に終わる。75ナノ秒という時間は、光速で換算すると約22.5mの距離に相当し、攻撃者はターゲットまでの距離をこの精度で把握している必要があることを意味する 。
- キャリア位相の同期：同様に、1.57542 GHzの搬送波の位相も、本物の信号と同期させる必要がある。悪意のある攻撃者が完全なキャリア位相同期を達成することは極めて困難であるとされるが 、受信機のPLL（Phase-Locked Loop）を欺くためには、可能な限り高い精度での同期が求められる。
- データビットの同期：攻撃者は、50 bpsで送信される航法メッセージのデータビットをリアルタイムで予測し、偽信号に含めなければならない。データビットの不一致は、受信機側で容易に検出され、攻撃の露見につながる 。

3.2.2 ステップ2：電力制御による「ドラッグオフ」

信号の同期が完了すると、攻撃者は偽信号の電力を徐々に増加させていく 。ここでの鍵は、絶妙な電力制御にある。

- 偽信号の電力は、本物の信号よりもわずかに強いだけで十分である。実験によれば、本物の信号に対して**+2dB**程度の相対電力があれば、受信機の追跡ループを捕捉するのに十分であり、かつ、単純な電力レベル監視による異常検知を回避できるほど低いレベルに抑えられる 。
- このわずかな電力差により、受信機のDLL/PLLの相関ピークは、本物の信号から偽の信号へと滑らかに引きずられ（ドラッグオフ）、受信機はロックを失うことなく偽信号を追跡し始める 。

3.2.3 ステップ3：軌道の操作

受信機の追跡ループを完全に掌握した後、攻撃者は偽信号のタイミングをゆっくりと、かつ巧妙に変化させる。これにより、受信機が計算する擬似距離が操作され、結果として算出される位置・速度情報が攻撃者の意図通りに改ざんされる。この段階に至れば、攻撃者はターゲットを任意の偽の軌道へと誘導することが可能となる 。

3.3 攻撃者の知識問題

シームレス・テイクオーバーを成功させるためには、攻撃者はターゲットの位置と速度をリアルタイムで正確に把握している必要がある 。これは、前述の精密な信号同期を実現するための前提条件である。実験では、攻撃開始時に想定する偽の位置が、ターゲットの真の位置から**500**メートル以内でなければ円滑な乗っ取りが難しく、真に潜在的な攻撃とするには100メートル以内の精度が求められることが示されている 。
このため、最も効果的な攻撃手法として「レシーバー・スプーfer」アーキテクチャが採用される。このアーキテクチャでは、攻撃者の装置がまず受信機として機能し、ターゲット周辺の正規GPS信号を受信して、ターゲットの状態（位置、速度、受信している衛星の状況など）を正確に推定する。その情報をもとに、完全に同期した偽信号を生成し、送信機として機能し始める 。
この攻撃手法の高度さは、裏を返せば攻撃者にとっての脆弱性をも内包している。すなわち、シームレス・テイクオーバーの成功に不可欠な「受信してから送信する」という特異な動作は、それ自体が探知可能な異常なRFシグネチャとなる。また、高精度な同期のためにはターゲットへの物理的な近接が要求されることが多く、これは攻撃者の戦術的な脆弱性となり、発見・特定されるリスクを高める。したがって、最も高度な攻撃を可能にするアーキテクチャそのものが、防御側にとっての新たな探知の機会を提供しているのである。

表**1**：シームレス**GPS**テイクオーバー攻撃の技術的要件

パラメータ	要求精度	失敗した場合の結果	典拠
相対信号電力	正規信号に対し +2dB 以上	パワーモニターによる検知、テイクオーバー失敗	
コード位相同期（一定時間オフセット）	75ナノ秒（ns）以下	ロック喪失、測位位置の跳躍	
初期位置精度	500メートル（m）以下	検知可能な測位位置の跳躍、中間エラー	
相対時間オフセット（複数アンテナ使用時）	80ナノ秒（ns）以下	ロック喪失	

第4章 欺瞞のケーススタディ：概念実証から地政学的兵器まで

GPSスプーフィングはもはや理論上の脅威ではない。学術的な実証実験から国家間の紛争における実用まで、その事例は多岐にわたる。この章では、具体的な事例を分析し、スプーフィング技術がどのように実装され、どのような影響を及ぼすのかを明らかにする。

4.1 学術的な概念実証：テキサス大学の実験

GPSスプーフィングの脅威を世に知らしめたのは、テキサス大学オースティン校のトッド・ハンフリーズ助教授（当時）が率いる研究チームによる一連の画期的な実験であった。

4.1.1 2012年 UAVハイジャック実験

2012年6月、ハンフリーズ教授のチームは、米国国土安全保障省（DHS）の要請を受け、ニューメキシコ州のホワイトサンズ・ミサイル実験場にて、UAV（無人航空機）の乗っ取り実験を公開で実施した。

- ターゲットと手法： ターゲットは、法執行機関などで使用される高度なナビゲーションシステム（GPS、IMU、高度計、磁力計を統合）を搭載したHornet Mini UAVであった 。チームは、約1km離れた丘の上から自作のスプーferを用い、ホバリング中のUAVに向けて偽のGPS信号を送信した 。このスプーferは、まず受信機として機能し、UAVが受信している正規信号のコード位相やキャリア位相、ドップラー周波数などを正確に把握した後、それと完全に同期した偽信号を生成する「レシーバー・スプーfer」アーキテクチャを採用していた 。
- 結果： 偽信号の電力を徐々に強めることで、UAVのナビゲーションシステムは完全に掌握された。攻撃者は、UAVが意図せず上昇しているかのように誤認させ、UAVのオートパイロットは高度を下げようと機体を急降下させた。地上に激突する寸前で、安全パイロットが手動操縦に切り替えて機体を救った 。この実験は、複数のセンサーを統合した高度なシステムであっても、GPSを主要な信頼の基点（トラストアンカー）としている限り、スプーフィングに対して脆弱であることを明確に証明した。

4.1.2 2013年 超大型ヨット乗っ取り実験

翌2013年、チームはさらに大胆な実験を地中海で実施した。ターゲットは、8,000万ドル相当の超大型ヨット「ホワイト・ローズ・オブ・ドラックス号」であった 。

- 攻撃シナリオ： チームは、ブリーフケースサイズの小型スプーferをヨットの上部甲板に設置し、船の2つのGPSアンテナに向けて偽信号を送信した 。攻撃は極めて巧妙かつ潜在的に行われた。船の航法装置には一切の警報が表示されず、電子海図上ではヨットは予定された航路を一直線に進んでいるように見えた 。
- 認知バイアスの悪用： 実際には、偽信号によって船はわずかに針路をずらされており、乗組員が電子海図の表示を信じて「コース修正」を行うたびに、船はさらに予定航路から逸脱していった。乗組員は、船が実際に旋回している物理的な感覚を覚えながらも、デジタルの表示を優先してしまった 。これは、人間が自動化システムからの情報を無批判に信頼してしまう「オートメーション・バイアス」という認知バイアスを巧みに突いた攻撃であり、ヒューマン・マシン・インターフェースにおける深刻な脆弱性を示唆した。最終的に、ヨットは本来の航路から数百メートルも離れた平行なコースを航行させられていた 。

4.2 国家によるスプーフィング：ロシア連邦の事例

学術的な実証にとどまらず、GPSスプーフィングは国家による電子戦（EW）のツールとして常態的に使用されている。特にロシア連邦による活動は、その規模と持続性において顕著である。

4.2.1 黒海およびモスクワでのインシデント

- 黒海「空港スプーフィング」： 2017年6月、黒海を航行中の20隻以上の船舶が、自船の位置が25海里（約46km）も離れた内陸のゲレンジーク空港にあるとGPSに表示されるという奇妙な

現象を報告した 。これは大規模かつ顕在的な攻撃であり、特定のターゲットを精密に誘導するのではなく、広範囲にわたって混乱を引き起こすことを目的としていた。

- モスクワ「クレムリン・バブル」: モスクワ中心部、特にクレムリン周辺では、GPS信号が恒常的に32km離れたヴヌーコヴォ国際空港の位置を示すようにスプーフィングされていることが報告されている 。この「空港スプーフィング」という特異な手口は、多くの市販ドローンに搭載されているジオフェンシング機能を悪用した、一種の粗雑な対ドローン防衛策である可能性が高い。ドローンは、自身が空港の近くにいると誤認すると、安全機能が作動して自動的に着陸するか、離陸地点に引き返すようにプログラムされているためである 。

4.2.2 C4ADSレポート「我らの上には星のみ」の分析

非営利分析機関C4ADSが2019年に発表したレポート「Above Us Only Stars」は、ロシアによるスプーフィング活動の全体像を明らかにした 。

- 規模と範囲: 2016年2月から2018年11月にかけて、ロシア国内、クリミア、シリアなど10カ所で、1,311隻の民間船舶に影響を与えた9,883件の疑わしいスプーフィング事例を特定した 。
- 目的の分類: レポートは、スプーフィングの目的を以下の3つに分類している。
    1. 要人警護（**VIP Protection**）: ロシア首脳の動向とスプーフィング活動の発生が密接に相関しており、連邦警護庁（FSO）が運用する移動式システムによるものと推定される 。
    2. 戦略的施設防護（**Facility Protection**）: 黒海の沿岸にあるプーチン大統領の宮殿と噂される施設など、特定の重要施設の周辺で持続的なスプーフィングが確認されている 。
    3. 軍事作戦・空域拒否（**Military Operations**）: シリアのフメイミム空軍基地など、実際の紛争地域において、敵対勢力の航空機などに対してサービス拒否（DoS）環境を作り出すために使用されている 。

4.2.3 ロシアの電子戦（**EW**）システム

これらの活動を支えているのが、ロシアが開発・配備する高度な電子戦システムである。

表**2**: ロシアの主要な電子戦システムの既知能力

システム名	プラットフォーム	主要機能	対象周波数/システム	有効範囲	典拠
Krasukha-4	BAZ-6910-022 車両	ジャミング	航空機/衛星レーダー (X, Ku, Ka帯)	最大300 km	
R-330Zh Zhitel	移動式車両	ジャミング、探知	GPS, SATCOM (Inmarsat, Iridium), GSM	20-30 km	
Leer-3	Orlan-10 UAV 搭載	ジャミング、SIGINT	GSM (携帯電話通信)	-	
Tirada-2	移動式車両	ジャミング	衛星通信	-	

4.3 民間部門への影響: 航空および海運

スプーフィングの脅威は、もはや軍事・安全保障分野に限定されない。

- 航空分野: 東欧、バルト海、中東地域を中心に、民間航空機を標的としたジャミングやスプーフィングが急増している 。これらのインシデントでは、航法システムの完全な喪失、慣性基準装置（IRS）の故障、オートパイロットの解除といった深刻な事態が発生し、乗員は推測航法や航空交通管制（ATC）による誘導への依存を余儀なくされている 。
- 海運分野: 黒海や中国沿岸でのインシデントに加え、ホルムズ海峡などでは国家（イランなどが疑われている）が関与するスプーフィング攻撃が発生している 。また、スプーフィングは、船舶を誤った場所へ誘導して積荷を強奪したり、制裁逃れなどの違法行為を隠蔽したりするための海事犯罪のツールとしても利用されている 。

これらの事例は、スプーフィング攻撃の意図が多様であることを示している。単純なドローン抑止から、特定のターゲットの乗っ取り、そして広範囲な商業・軍事活動の妨害まで、その目的は多岐にわたる。この「意図の多様性」は、防御側が直面する課題の複雑さを物語っている。画一的な対策では不十分であり、保護対象となる資産が直面する最も可能性の高い脅威の種類に合わせて、防御戦略を調整する必要がある。

表**3**: 主要な**GPS**スプーフィングインシデントの概要

インシデント/年	ターゲット	攻撃タイプ	推定攻撃者	観測された影響	典拠
UT-Austin UAV (2012)	UAV	シームレス・テイクオーバー	学術研究者	車両の乗っ取り	
UT-Austin Yacht (2013)	ヨット	シームレス・テイクオーバー	学術研究者	車両の乗っ取り、偽の直線航路表示	
モスクワ・クレムリン **(2016-)**	民生用GPS利用者	顕在的な位置スプーフィング	ロシアFSO/軍	偽の位置（空港）を報告	
黒海 **(2017)**	海上船舶	顕在的な位置スプーフィング	ロシア軍	偽の位置（空港）を報告	
中国「クロップサークル」**(2019)**	海上船舶	顕在的な位置スプーフィング	中国の国家/非国家主体	「クロップサークル」状の偽位置パターン	
東地中海/バルト海 **(2022-)**	民間航空機	ジャミング/スプーフィング	不明（国家主体が疑われる）	航法システムの喪失	

第**5**章 対スプーフィング兵器庫: 多層防御戦略

GPSスプーフィングに対する万能の解決策は存在しない。効果的な防御は、単一の技術に依存するのではなく、PNT（測位・航法・時刻）エコシステムの様々な段階で機能する複数の防御層を組み合わせる「多層防御（Defense-in-Depth）」のアプローチを必要とする。この章では、現在利用可能または開発中の主要な対スプーフィング技術を、その動作原理、有効性、限界とともに体系的に概説する。

5.1 基礎層: 受信機自律信頼性監視（**RAIM**）

受信機自律信頼性監視（Receiver Autonomous Integrity Monitoring, RAIM）は、GPS受信機に組み込まれた最も基本的な自己診断機能である 。RAIMは、測位計算に必要以上の数の衛星（通常5機以上）からの信号を受信している場合に、その冗長性を利用して測定値の一貫性をチェックする 。いずれかの衛星からの信号が他の信号と大きく矛盾する場合、その信号を異常と判断し、警告を発するか、測位計算から除外する。

しかし、RAIMには致命的な脆弱性が存在する。それは、攻撃者が偽の位置情報と幾何学的に完全に整合性のとれた偽の衛星信号群（フルコンステレーション）を生成する、高度な「コヒーレント・スプーフィング」攻撃に対しては全く無力であることだ 。この場合、すべての偽信号は互いに矛盾なく偽の位置を指し示すため、擬似距離の残差は小さく、RAIMは異常を検知できない 。

5.2 高度な受信機ベースの防御

RAIMの限界を克服するため、受信機内部の信号処理レベルで機能する、より高度な防御技術が開発されている。

- 信号電力監視: 最も単純なチェック方法であり、受信信号強度の急激かつ大幅な増加を検知することで、力任せの攻撃を特定する 。しかし、巧妙な攻撃者は、正規信号の電力レベルに合わせるか、徐々に電力を増加させることで、この単純な検知を回避できる 。
- 複数アンテナシステムと到来方向（**AoA**）分析: これは極めて強力な防御策の一つである。本物の衛星信号は、空の異なる方向から到来する。対照的に、スプーフィング信号は、たとえ複数の衛星を偽装していても、通常は単一の地上送信機から発信されるため、すべて同じ方向から到来する 。アンテナアレイ（複数のアンテナを搭載したシステム）を用いることで、この幾何学的な不一致を検出し、スプーフィング攻撃を特定できる 。
- 信号フィンガープリンティング: 本物の衛星信号には、衛星に搭載された原子時計や信号生成ハードウェアの微細な個体差に起因する、固有の「指紋（フィンガープリント）」が存在する 。これは、攻撃者が生成するクリーンな合成信号には存在しない特徴である。このフィンガープリントを分析することで、信号の真贋を判定することが可能となる 。
- 高度な相関関数分析（**SPREE**）: この技術は、受信信号と受信機内部で生成したレプリカコードとの相関関数の「形状」を分析する。本物の信号と偽の信号が同時に存在する場合、相関ピークは歪む。SPREE（Spoofing-Resistant GPS Receiver）と呼ばれる受信機は、「補助ピーク追跡（Auxiliary Peak Tracking）」という手法を用いる。これは、1つの衛星に対して複数の受信チャンネルを割り当て、強力なピーク（偽信号）と微弱なピーク（本物の信号）の両方を同時に追跡することで、攻撃の存在を検知するものである 。

5.3 暗号化の盾：信号認証技術

民生用信号の根本的な脆弱性（認証の欠如）に対処するため、信号そのものに暗号技術を導入する取り組みが進められている。

- **Galileo Open Service Navigation Message Authentication (OSNMA)**:
  - 原理: 欧州のGalileoシステムが提供するサービスで、E1-B信号で放送される航法メッセージ（I/NAV）に対して暗号技術による認証を提供する 。TESLA（Timed Efficient Stream Loss-tolerant Authentication）プロトコルに基づき、遅延公開される鍵を用いてメッセージ認証コード（MAC）を検証することで、航法データが改ざんされていないことを保証する 。これはデータの真正性を保証するものであり、測距信号自体の真正性を保証するものではない。
  - 現状: 2024年6月に公開試験フェーズが完了し、初期サービスの提供開始が間近に迫っている 。Septentrio、u-blox、STMicroelectronicsといった主要メーカーから、OSNMA対応の受信機が市場に投入され始めている 。
  - 脆弱性: OSNMAは、単純なリプレイ攻撃や、より高度な攻撃（受信機の時刻認識を操作してTESLAプロトコルの時刻同期要件を迂回する攻撃）に対して脆弱であることが指摘されている 。
- **GPS Chips-Message Robust Authentication (CHIMERA)**:
  - 原理: 米国がGPS L1C信号向けに提案している、より高度な認証方式。航法メッセージ（データ）と拡散符号（測距信号）の両方を認証することを目指している 。拡散符号に

暗号化されたマーカーを「パンクチャリング（穿孔）」することで、信号とデータを時間的に強固に結びつけ、単純なリプレイ攻撃を困難にする 。
    - 現状：まだ実験段階にあり、NTS-3（Navigation Technology Satellite-3）衛星での試験が計画されている 。実用化には至っていない。

5.4 システムレベルの防御：マルチセンサー・フュージョン

最も効果的な防御は、GPS/GNSS以外の独立したセンサー情報を利用して、PNT解のクロスチェックを行うことである 。GPSによる測位情報が他のセンサー情報と著しく矛盾する場合、スプーフィング攻撃の可能性が高いと判断できる 。

- 慣性計測装置（**IMU**）：加速度計とジャイロスコープで構成されるIMUは、物体の相対的な動き（加速度と角速度）を計測する。IMUは短期的には非常に正確なPNTデータを提供するが、時間とともに誤差が累積（ドリフト）する。GPSとIMUを緊密に統合したシステム（タイトカップリング）では、GPSの解がIMUの示す物理的に可能な動きと矛盾した場合（例えば、瞬間的な位置の跳躍など）、スプーフィングを検知できる 。
- その他のセンサー：Lidar、レーダー、カメラ（ビジュアルオドメトリ）、さらにはWi-Fiや携帯電話の基地局といった「機会信号（Signals of Opportunity）」からの情報を統合することで、さらに多くの冗長性が生まれ、システムのレジリエンスが向上する 。

これらの防御策は、単独で機能するものではなく、組み合わせて使用することでその真価を発揮する。例えば、OSNMAはリプレイ攻撃に脆弱だが、IMUとのフュージョンはその種の攻撃を検知できる可能性がある。このように、多層防御の各レイヤーが互いの弱点を補完し合うことで、システム全体の堅牢性が向上するのである。

表**4**：対スプーフィング技術の比較分析

技術	検知原理	シームレス・テイクオーバーへの有効性	実装コスト/複雑性	典拠
RAIM	冗長な測定値の一貫性チェック	低（コヒーレント攻撃に無効）	低	
信号電力監視	電力レベルの異常検知	低（巧妙な攻撃には無効）	低	
AoA（複数アンテナ）	信号到来方向の幾何学的不一致	高	高	
SPREE	相関関数の二重ピーク追跡	高	中	
信号フィンガープリンティング	送信機ハードウェアの固有署名	中～高	中	
OSNMA (Galileo)	データ暗号認証	中（リプレイ/時刻攻撃に脆弱）	低（ソフトウェア）	
Chimera (GPS)	データ＋信号暗号認証	高	中（将来技術）	
IMUフュージョン	慣性情報とのクロスチェック	高	中	

これらの技術の中で、OSNMAやChimeraのような暗号認証は特に有望視されているが、新たな脆弱性の側面も浮き彫りにしている。これらのシステムは、「トラストアンカー」と呼ばれる、受信機内に安全に保管されなければならない公開鍵に依存している 。このトラストアンカーが、製造段階でのサ

プライチェーン攻撃、悪意のあるファームウェアアップデート、物理的な改ざんなどによって侵害されれば、暗号認証システム全体が崩壊する 。攻撃者は自身の鍵を署名した偽信号を生成し、受信機はそれを本物として受け入れてしまう。これは、PNTセキュリティの問題が、単なるRF信号処理の問題から、デバイス自体の物理的・サイバー的セキュリティを含む、より広範なサイバーフィジカルセキュリティの問題へと移行したことを意味している。信号を保護するだけでは不十分であり、その信号の真正性を検証するための信頼の基点（トラストアンカー）のライフサイクル全体を保護する必要があるのだ。

第6章 次なるフロンティア：AI、スウォーム、そして認知戦

スプーフィングと対スプーフィングの「いたちごっこ」は、新たな技術領域へと拡大し続けている。人工知能（AI）、自律システムの群制御（スウォーム）、そして人間の認知を標的とする戦術は、PNTセキュリティの未来を形作る重要な要素である。

6.1 人工知能という両刃の剣

AI、特に機械学習（ML）と深層学習（DL）は、スプーフィング攻防の両面に革命をもたらす可能性を秘めている。

- 攻撃のための**AI**：深層強化学習（DRL）などの技術を用いることで、より適応的で知的なスプーフィング攻撃を構築できる 。AI駆動のスプーferは、ターゲットとなる受信機の追跡ループやセンサーフュージョンアルゴリズムの特定の脆弱性をリアルタイムで学習し、最適な欺瞞戦略を自動的に生成することが可能になる 。これにより、汎用的な防御策を回避する、オーダーメイドの攻撃が実現し得る。
- 防御のための**AI**：逆に、AIはより堅牢な検知システムの構築にも貢献する。LSTM（長短期記憶）、SVM（サポートベクターマシン）、オートエンコーダといった機械学習モデルは、C/N0、AGC、擬似距離残差、IMUデータなど、多次元の時系列データに潜む、スプーフィング攻撃特有の微細な異常パターンを学習・識別できる 。これにより、単純な閾値ベースの検知手法では見逃してしまうような、巧妙で低電力な攻撃も検出可能となる 。

6.2 スウォームへの挑戦：分散型欺瞞

UAVスウォームのような分散型自律システムの普及は、新たな防衛上の課題を提示している 。

- 単純なスウォーム攻撃：攻撃者は単一の送信機を使い、スウォームを構成する全メンバーを同じ偽の位置にスプーフィングすることができる。この場合、各メンバーが報告する座標が同一になるという不自然な状態が生じるため、比較的容易に検知可能である 。
- 高度なスウォーム攻撃：より巧妙な攻撃者は、複数の送信機を協調させるか、あるいは極めて精緻に計算された信号を送信することで、スウォームの相対的な位置関係（フォーメーション）を維持したまま、群全体を偽の目的地へ誘導する。この種の攻撃は、UWB（超広帯域無線）のような独立した測距手段や、群内での合意形成（コンセンサス）に基づく異常検知アルゴリズムがなければ、検出が極めて困難となる 。

6.3 認知戦としての**GPS**スプーフィング

最も深刻な考察は、GPSスプーフィングを単なる機械に対する技術的攻撃としてではなく、人間のオペレーターやヒューマン・マシン・チームの「認知」を標的とした心理的攻撃、すなわち「認知戦」の一形態として捉えることである 。
この攻撃の真の目的は、航法システムを乗っ取ること自体ではなく、オペレーターの信頼を蝕み、疑

念を植え付け、意思決定プロセスを操作することにある 。スプーフィングは、人間の認知バイアスを巧みに悪用する。

- オートメーション・バイアス: 自動化システムからの情報を、他の矛盾する情報（例えば、自身の身体感覚）よりも過度に信頼し、無批判に受け入れてしまう傾向。2013年のヨット実験で、乗組員が船の旋回を体で感じながらも、正常に見える電子海図を信じてしまったのが典型例である 。
- 確証バイアス: 自身の既存の信念や期待を裏付ける情報を優先的に探し、受け入れてしまう傾向。攻撃者がターゲットの予定航路に沿った、ごくわずかなズレを伴う偽情報を提供した場合、オペレーターはそれを正常な誤差とみなし、攻撃の兆候を見逃す可能性が高まる 。
- 探索の満足（**Satisfaction of Search**）: 一つの問題を発見すると、他の問題を探すのをやめてしまう傾向。オペレーターがスプーフィングによって引き起こされた小さな異常を修正したことで満足し、それがより大きな進行中の攻撃の一部であることを見抜けなくなる可能性がある。

これらのバイアスを悪用されると、人間は自ら誤った判断を下し、システムの安全性を損なう最後の砦としての役割を果たせなくなる。この観点から見ると、GPSスプーフィングは、PNTデータの認識論、すなわち「我々はいかにして、自らの位置を『知る』のか？」という根本的な問いを突きつける。伝統的に、PNTデータは「正当化された真なる信念（Justified True Belief）」として扱われてきた 。しかし、スプーフィングは、一見すると「正当化されている」ように見える（GPS信号の形をしている）が、「真ではない」信念を提供する。これにより、問題は工学的な計算から認識論的な課題へと移行する。すなわち、システム（あるいは人間）は、潜在的に矛盾し、信頼性の低い複数の情報源から、いかにして自己の状態に関する強固な信念を構築できるのか、という問いである 。
この課題に対する答えは、システムが単なる計算機ではなく、一種の「認識主体（epistemic agent）」として機能する必要があることを示唆している。つまり、システムは、GPS、IMU、視覚情報など、利用可能なすべての情報源の信頼性を、それらの整合性、物理的な妥当性、過去の実績などに基づいて能動的に評価しなければならない 。これは、「PNT信頼性推論エンジン（PNT Trust Inference Engine）」 や「マネージド・トラスト」アーキテクチャ といった概念につながる。そこでは、信頼は無条件に仮定されるものではなく、航法解の算出プロセスの中核として、継続的に計算・管理されるべき変数となる。問題はもはや「位置を計算すること」ではなく、「計算された位置への信念を正当化すること」なのである。

第7章 レジリエンスの設計：PNTセキュリティへの統合的アプローチ

GPSスプーフィングという複雑な脅威に対抗するためには、技術的な防御策だけでなく、ヒューマン・マシン・インターフェース（HMI）、オペレーターの訓練、そして国家レベルのインフラ戦略に至るまで、包括的かつ統合的なアプローチが不可欠である。この最終章では、様々なステークホルダーに向けた、PNTレジリエンスを構築するための具体的な提言を行う。

7.1 システム設計者へ：レジリエントなHMIの設計原則

HMIは、技術的な防御が破られた際の最後の砦である。したがって、その設計は、PNTが侵害された環境下でオペレーターの認知バイアスを軽減し、的確な状況認識と意思決定を支援することに主眼を置くべきである。

- 状態の明確な表示の原則: HMIは、PNTシステムの現在の状態と信頼性レベルを、曖昧さなくオペレーターに伝えなければならない。これには、現在使用している測位ソース（GPS、Galileo、IMU単独航法など）、信号が認証されているか（OSNMAなど）、そしてシステムが現在の解に対してどの程度の信頼を置いているかを、直感的に理解できる形で表示することが

含まれる 。

- 段階的開示の原則: 情報過多は、特に危機的状況下ではオペレーターの判断を麻痺させる。HMIは、通常時は意思決定に必要な情報のみを表示し、より詳細な診断データは要求に応じてアクセスできるように設計されるべきである（プログレッシブ・ディスクロージャー）。
- 認知的強制の原則: インターフェースは、オペレーターを危険な操作から遠ざけ、システムの警告を無視するような操作には明確な確認を要求するように設計されるべきである。正しい操作を容易にし、誤った操作を困難にすることが、安全性の向上につながる 。
- 信頼性較正の原則: HMIは、オペレーターが自動化システムの能力と限界について正確なメンタルモデルを構築するのを助けるべきである。システムの不確実性や過去のパフォーマンスに関する情報を表示することで、オペレーターはシステムへの信頼度を適切に較正（キャリブレーション）することができる 。

7.2 オペレーターへ: 認知的レジリエンスのための訓練

オペレーターの訓練は、標準的な手順の習熟にとどまらず、スプーフィングがもたらす心理的影響に積極的に対処するものでなければならない。

- シナリオベース訓練: パイロットや航海士は、高忠実度のシミュレータを用いて、現実的なスプーフィングシナリオに定期的に直面させるべきである。これにより、攻撃の微細な兆候を認識し、回復手順を実践する能力を養うことができる 。
- クロスチェックの徹底: 「信頼せよ、されど検証せよ」という文化を醸成することが不可欠である。GPSによる位置情報を、地上航法支援施設（navaids）、レーダー、天測、慣性基準装置（IRS）など、利用可能なあらゆる代替手段とクロスチェックすることを、緊急時だけでなく標準的な手順として義務付けるべきである 。
- 認知バイアスへの意識向上: オートメーション・バイアスや確証バイアスといった認知的な落とし穴について、オペレーターに明確に教育する。これにより、自身やクルーがこれらのバイアスの影響下にあることを認識し、積極的に対抗することが可能になる 。

7.3 政策立案者へ: 中央集権型 vs. 分散型PNTの弁証法

国家レベルでのPNTレジリエンスを確保するためには、インフラストラクチャの構造そのものについての戦略的考察が求められる。

- 中央集権の脆弱性: 現在の世界は、GPSやGalileoといった少数の衛星ベースのシステムに過度に依存している。これは、システム全体にわたるリスク、すなわち、これらのシステムの一つに攻撃や障害が発生した場合、その影響が世界規模で連鎖的に波及する脆弱性を生み出している 。
- 分散化の可能性: 真にレジリエントな国家PNTアーキテクチャは、多様な分散型技術を組み込んだ「システム・オブ・システムズ」でなければならない。これにより、衛星システムを補完し、バックアップを提供することが可能となる。具体的な技術としては、以下のようなものが挙げられる。
    - 地上系**RF**システム: eLoran（強化型ロラン）のような、衛星とは全く異なる物理原理に基づく地上波航法システム 。
    - 機会信号（**SoOp**）: 携帯電話基地局、Wi-Fiアクセスポイント、テレビ放送塔など、既存の通信・放送インフラから発信される信号を利用する測位技術。
    - クラウドソース型干渉検知網: gpsjam.orgのような航空機のADS-Bデータを利用したシステムや、多数のスマートフォンから情報を収集するシステムにより、広範囲の干渉をリアルタイムで検知・可視化する 。
    - 分散型台帳技術（**DLT**）: ブロックチェーンなどのDLTを用いて、PNT情報をピアツーピアで安全に検証する、新しい分散型PNTの概念 。

- 戦略的課題：課題はGPSを置き換えることではなく、それをいかに補強するかである。しかし、商業ユーザーは、義務付けられたり、明確なインセンティブがなければ、冗長なPNTシステムに追加のコストを支払うことに消極的である 。この市場の障壁を克服するためには、米国運輸省（DOT）による補完的PNT技術の実証実験 のような、政府による政策的な投資と推進が不可欠となる。

最終的に、本レポートが導き出す結論は、PNTセキュリティにおける「銀の弾丸」は存在しないということである。真のレジリエンスは、単一の優れた技術によってもたらされるのではなく、多様で階層化されたシステムが生み出す「創発的な特性」である。多層防御の各レイヤーが互いの弱点を補うことで、システムは堅牢性を獲得する。中央集権的な衛星システムと分散型の地上システム、機械による検証と人間による監督、そしてRF、慣性、視覚といった異なる物理的検知様式。これらの間の弁証法的な相互作用こそが、巧妙で多角的な攻撃に耐えうるシステムを構築する鍵となる。したがって、国家のPNT政策は、単一の「GPS代替システム」を追求するのではなく、豊かで多様性に富み、相互運用可能なPNTエコシステムの育成に注力すべきである。その目標は、無敵のシステムを作ることではなく、優雅に失敗し、危機的状況下でも最低限の信頼性を維持できるシステムを構築することにある。

引用文献

1. GPS System Vulnerabilities and Countermeasures - Blue Goat Cyber, https://bluegoatcyber.com/blog/gps-system-vulnerabilities-and-countermeasures/ 2. Civil GPS Systems and Potential Vulnerabilities - DTIC, https://apps.dtic.mil/sti/tr/pdf/ADA440372.pdf 3. Civil GPS Systems and Potential Vulnerabilities - ResearchGate, https://www.researchgate.net/publication/235161476_Civil_GPS_Systems_and_Potential_Vulnerabilities 4. Understanding Vulnerabilities of Positioning, Navigation, and Timing - CISA, https://www.cisa.gov/sites/default/files/2023-04/fs_positioning-navigation-timing-vulnerabilities_508.pdf 5. A simple model for GPS C/A-code self-interference - NAVIGATION, https://navi.ion.org/content/67/2/319 6. GPS signals - Wikipedia, https://en.wikipedia.org/wiki/GPS_signals 7. GPS Spoofing - Tufts Sites, https://sites.tufts.edu/eeseniordesignhandbook/files/2017/05/Red_Chapman.pdf 8. What Is GPS Spoofing and How Do You Defend Against It? | Okta, https://www.okta.com/identity-101/gps-spoofing/ 9. What are the GPS / GNSS signals? - Medium, https://medium.com/@mikeg888/what-are-the-gps-gnss-signals-4bdd032887fc 10. en.wikipedia.org, https://en.wikipedia.org/wiki/GPS_signals#:~:text=Modulation%20codes-,Coarse%2Facquisition%20code,the%20carrier%20as%20previously%20described. 11. GPS Spoofing: low-cost GPS emulator - TIB AV-Portal - TIB.eu, https://av.tib.eu/media/36387 12. (PDF) Low-cost GPS simulator – GPS spoofing by SDR - ResearchGate, https://www.researchgate.net/publication/286330869_Low-cost_GPS_simulator_-_GPS_spoofing_by_SDR 13. GPS Navigation Message - Navipedia - GSSC, https://gssc.esa.int/navipedia/index.php/GPS_Navigation_Message 14. Are we doing enough to fix GPS vulnerability? - Blog - Adtran, https://www.blog.adtran.com/en/are-we-doing-enough-to-fix-gps-vulnerability 15. GNSS Interference and Security: Impacts on Critical Infrastructure and Mitigation Strategies, https://www.researchgate.net/publication/389331703_GNSS_Interference_and_Security_Impacts_on_Critical_Infrastructure_and_Mitigation_Strategies 16. GPS-Spoofing Attack Detection Mechanism for UAV Swarms - ResearchGate, https://www.researchgate.net/publication/371875186_GPS-Spoofing_Attack_Detection_Mechanism_for_UAV_Swarms 17. When is it safe to use the gps spoofer : r/hackrf - Reddit,

https://www.reddit.com/r/hackrf/comments/1einwy0/when_is_it_safe_to_use_the_gps_spoofer/ 18. Aviations GPS Spoofing & How to Avoid It | APG - Aircraft Performance Group, https://flyapg.com/blog/what-is-gps-spoofing 19. A Practical GPS Location Spoofing Attack in Road Navigation Scenario - Yuanchao Shu, https://yshu.org/paper/hotmobile17gps.pdf 20. What is spoofing and how to ensure GPS security? - Septentrio, https://www.septentrio.com/en/learn-more/insights/what-spoofing-and-how-ensure-gps-security 21. (PDF) Vulnerabilities of civilian Global Navigation Satellite Systems (GNSS) signals: A review - ResearchGate, https://www.researchgate.net/publication/290159860_Vulnerabilities_of_civilian_Global_Navigation_Satellite_Systems_GNSS_signals_A_review 22. GPS-Spoofing Attacks and Countermeasures - Antispoofing Wiki, https://antispoofing.org/gps-spoofing-attacks-and-countermeasures/ 23. The P and C/A Codes | GEOG 862: GPS and GNSS for Geospatial Professionals - Dutton Institute, https://www.e-education.psu.edu/geog862/node/1741 24. Report: The economic impact on the UK of a disruption to GNSS - GOV.UK, https://www.gov.uk/government/publications/report-the-economic-impact-on-the-uk-of-a-disruption-to-gnss 25. Economic Benefits of the Global Positioning System (GPS) - Office of Space Commerce, https://www.space.commerce.gov/wp-content/uploads/2019-08-gps-presentation.pdf 26. Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture - Homeland Security, https://www.dhs.gov/sites/default/files/2022-06/22_0609_st_resilient_pnt_ra.pdf 27. On the Requirements for Successful GPS Spoofing Attacks, https://www.cs.ox.ac.uk/files/6489/gps.pdf 28. GNSS Spoofing Scenarios with SDRs | GPSPATRON.com, https://gpspatron.com/gnss-spoofing-scenarios-with-sdrs/ 29. GPS spoofing - NavtechGPS, https://www.navtechgps.com/wp-content/uploads/assets/1/7/Spoofing_Article_Rev7.pdf 30. GNSS Signal Simulator, https://gnss-learning.org/wp-content/uploads/2022/08/14_Simulator_rev1.pdf 31. GPS Signal Reception and Spoofing Based on Software-Defined Radio Devices, https://www.researchgate.net/publication/367265928_GPS_Signal_Reception_and_Spoofing_Based_on_Software-Defined_Radio_Devices 32. Spoofing attack - Wikipedia, https://en.wikipedia.org/wiki/Spoofing_attack 33. GPS Spoofing: Pioneered in Russia - Grey Dynamics, https://greydynamics.com/gps-spoofing-pioneered-in-russia/ 34. Implementing SDR-based GNSS/GPS simulators - Embedded, https://www.embedded.com/implementing-sdr-based-gnss-gps-simulators/ 35. Russia May Be Testing Its GPS Spoofing Capabilities Around The Black Sea - The War Zone, https://www.twz.com/13549/russia-may-be-testing-its-gps-spoofing-capabilities-around-the-black-sea 36. Above Us Only Stars - C4ADS, https://c4ads.org/reports/above-us-only-stars/ 37. GPS Jamming and Spoofing Maritime's Biggest Cyber-Threat - Regulations.gov, https://downloads.regulations.gov/USCG-2014-1020-0007/attachment_1.pdf 38. arXiv:1603.05462v1 [cs.CR] 17 Mar 2016 - Aanjhan Ranganathan, https://arxiv.org/abs/1603.05462 39. GNSS Spoofing and Detection, https://radionavlab.ae.utexas.edu/images/stories/files/papers/gnss_spoofing_detection.pdf 40. Toughening Techniques for GPS Receivers: Navigation Message Authentication, https://www.gps.gov/governance/advisory/meetings/2015-06/humphreys.pdf 41. GPS Spoofing Experiment Knocks Ship off Course - Inside GNSS, https://insidegnss.com/gps-spoofing-experiment-knocks-ship-off-course/ 42. A GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver - MDPI,

https://www.mdpi.com/1424-8220/19/18/3993 43. Advanced Anti-Spoofing Methods in Tracking Loop | The Journal of Navigation, https://www.cambridge.org/core/journals/journal-of-navigation/article/advanced-antispoofing-methods-in-tracking-loop/9E64492AAB75B1A2228AD7217F9AAE28 44. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks - Radionavigation Laboratory, https://radionavlab.ae.utexas.edu/images/stories/files/papers/PMUAndUAVSpoofingION2012.pdf 45. Todd Humphreys' Research Team Demonstrates First Successful GPS Spoofing of UAV, https://www.ae.utexas.edu/news/todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing 46. UAVs Vulnerable to Civil GPS Spoofing - Inside GNSS - Global Navigation Satellite Systems Engineering, Policy, and Design, https://insidegnss.com/uavs-vulnerable-to-civil-gps-spoofing/ 47. UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/ 48. University of Texas Team Hijacks $80 Million Yacht With Cheap GPS Spoofing Gear, https://www.nextgov.com/digital-government/2013/07/university-texas-team-hijacks-80-million-yacht-cheap-gps-spoofing-gear/67625/ 49. University of Texas team takes control of a yacht by spoofing its GPS - New Atlas, https://newatlas.com/gps-spoofing-yacht-control/28644/ 50. Position, Navigation, and Timing Weaponization in the Maritime Domain: Orientation in the Era of Great Systems Conflict - NDU Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation/ 51. Mass GPS Spoofing Attack in the Black Sea? - Maritime Executive - RNTF, https://rntfnd.org/2017/07/12/mass-gps-spoofing-attack-in-the-black-sea-maritime-executive/ 52. New Report Details GNSS Spoofing Including Denial-of-Service Attacks, https://insidegnss.com/new-report-details-gnss-spoofing-including-denial-of-service-attacks/ 53. Observations of GNSS Spoofing in Russia in 2023-2024 - Stanford University, https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Lo_ION_ITM_2025_Russia_Spoofing.pdf 54. Exposing GPS Spoofing in Russia and Syria - C4ADS, https://c4ads.org/wp-content/uploads/2022/05/AboveUsOnlyStars-Report.pdf 55. Analysis: Which Russian Electronic Warfare Systems Jam US Excalibur & HIMARS Ammunition in Ukraine - Army Recognition, https://armyrecognition.com/focus-analysis-conflicts/army/analysis-defense-and-security-industry/analysis-which-russian-electronic-warfare-systems-jam-us-excalibur-himars-ammunition-in-ukraine-2 56. GPS interference threatening flights, ships: What is happening, possible solutions, https://indianexpress.com/article/explained/explained-sci-tech/how-gps-interference-threatens-global-transportation-10094956/ 57. GNSS Jamming and Spoofing Events Present a Growing Danger to Aviation, https://www.ainonline.com/aviation-news/air-transport/2024-03-04/gnss-jamming-and-spoofing-events-present-growing-danger 58. Understanding GPS spoofing in shipping: How to stay protected - Safety4Sea, https://safety4sea.com/cm-understanding-gps-spoofing-in-shipping-how-to-stay-protected/ 59. Cyber attacks: who targets the maritime industry and why? - Thetius, https://thetius.com/cyber-attacks-who-targets-the-maritime-industry-and-why/ 60. GPS Jamming, Spoofing and Hacking | NorthStandard | Marine Insurance, https://north-standard.com/insights-and-resources/resources/articles/gps-jamming-spoofing-and-hacking 61. EU to upgrade GPS systems as Russian jamming efforts spark response - Defense News,

https://www.defensenews.com/global/europe/2025/03/12/eu-to-upgrade-gps-systems-as-russian-jamming-efforts-spark-response/ 62. Global Navigation Satellite Systems Signal Vulnerabilities in Unmanned Aerial Vehicle Operations: Impact of Affordable Software-Defined Radio - MDPI, https://www.mdpi.com/2504-446X/8/3/109 63. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing | Journal of Applied Research and Technology. JART - Elsevier, https://www.elsevier.es/en-revista-journal-applied-research-technology-jart-81-articulo-detection-mitigation-gps-spoofing-based-S1665642315300043 64. Optimization and Performance of Multi-Criteria Collaborative Integrity Control in Degraded GNSS Environments - CEUR-WS.org, https://ceur-ws.org/Vol-3980/paper8.pdf 65. Characterization of the Ability of Low-Cost GNSS Receiver to Detect Spoofing Using Clock Bias - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC10007427/ 66. GNSS Spoofing Detection using Two-Antenna Differential Carrier Phase - Radionavigation Laboratory, https://radionavlab.ae.utexas.edu/images/stories/files/papers/Psiaki_WROD_2014.pdf 67. A Survey of Spoofer Detection Techniques via Radio Frequency Fingerprinting with Focus on the GNSS Pre-Correlation Sampled Data - PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC8123360/ 68. GNSS Receiver Fingerprinting for Security-Enhanced Applications - ResearchGate, https://www.researchgate.net/publication/308968248_GNSS_Receiver_Fingerprinting_for_Security-Enhanced_Applications 69. A Spoofing Resistant GPS Receiver - SPREE, https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/system-security-group-dam/research/publications/pub2016/spoof-detector.pdf 70. Galileo Open Service Navigation Message Authentication (OSNMA) | European GNSS Service Centre (GSC), https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma 71. Introducing GNSS Navigation Message Authentication, https://gnss-sdr.org/osnma/ 72. Galileo is getting ready for the upcoming OSNMA operational declaration | European GNSS Service Centre (GSC), https://www.gsc-europa.eu/news/galileo-is-getting-ready-for-the-upcoming-osnma-operational-declaration 73. Practical Spoofing Attacks on Galileo Open Service Navigation Message Authentication, https://arxiv.org/html/2501.09246v1 74. Receivers implementing Galileo OSNMA | European GNSS Service Centre (GSC), https://www.gsc-europa.eu/support-todevelopers/galileo-compatible-devices/receivers-implementing-galileo-osnma 75. Out-of-the-box spoofing mitigation with Galileo's OSNMA service | - u-blox, https://www.u-blox.com/en/blogs/insights/spoofing-mitigation-galileo-osnma 76. [2501.09246] Practical Spoofing Attacks on Galileo Open Service Navigation Message Authentication - arXiv, https://arxiv.org/abs/2501.09246 77. GPS Chimera: A Software Receiver Implementation - The Institute of Navigation, https://www.ion.org/publications/abstract.cfm?articleID=18127 78. Chips-Message Robust Authentication (Chimera) for GPS Civilian Signals - ResearchGate, https://www.researchgate.net/publication/329011274_Chips-Message_Robust_Authentication_Chimera_for_GPS_Civilian_Signals 79. Satellite Navigation Signal Authentication in GNSS: A Survey on Technology Evolution, Status, and Perspective for BDS - MDPI, https://www.mdpi.com/2072-4292/15/5/1462 80. GPS Spoofing Detection using RAIM with INS Coupling - NavLab, http://www.navlab.iit.edu/uploads/5/9/7/3/59735535/khanafseh_plans_2014_final.pdf 81. GPS IMU Sensor Fusion: Elevating Precision in Modern Navigation Systems, https://www.pnisensor.com/gps-imu-sensor-fusion-elevating-precision-in-modern-navigation-systems/ 82. Experimental Validation of Sensor Fusion-based GNSS Spoofing Attack Detection Framework for Autonomous Vehicles - arXiv, https://arxiv.org/pdf/2401.01304 83. Sensor Fusion

Module Using IMU and GPS Sensors For Autonomous Car | Request PDF, https://www.researchgate.net/publication/348165680_Sensor_Fusion_Module_Using_IMU_and_GPS_Sensors_For_Autonomous_Car 84. Multi-Sensor Fusion of GNSS receivers, inertial sensor and cameras for Precise and Reliable Positioning - ANavS, https://anavs.com/pdfs/HenBur15-COFAT-2015.pdf 85. An Outline of Multi-Sensor Fusion Methods for Mobile Agents Indoor Navigation - PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC7956205/ 86. Protection and Fundamental Vulnerability of GNSS - DiVA portal, https://www.diva-portal.org/smash/get/diva2:429026/FULLTEXT01.pdf 87. Trust Anchor Lifecycle Attack Protection - Department of Energy, https://www.energy.gov/sites/prod/files/2017/04/f34/SNL_Trust%20Anchor%20Lifecycle%20Attack%20Protection_FactSheet.pdf 88. [2506.08445] GPS Spoofing Attacks on AI-based Navigation Systems with Obstacle Avoidance in UAV - arXiv, https://arxiv.org/abs/2506.08445 89. GPS Spoofing Attacks on AI-based Navigation Systems with Obstacle Avoidance in UAV - arXiv, http://www.arxiv.org/pdf/2506.08445 90. GPS Spoofing Attacks on AI-based Navigation Systems with Obstacle Avoidance in UAV, https://arxiv.org/html/2506.08445v1 91. Self-supervised federated GNSS spoofing detection with opportunistic data - arXiv, https://arxiv.org/html/2505.06171v1 92. [2501.02352] GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning - arXiv, https://arxiv.org/abs/2501.02352 93. Use of Supervised Machine Learning for GNSS Signal Spoofing Detection with Validation on Real-World Meaconing and Spoofing Data—Part I - MDPI, https://www.mdpi.com/1424-8220/20/4/1171 94. GNSS Spoofing Detection Based on Wavelets and Machine Learning - MDPI, https://www.mdpi.com/2079-9292/14/12/2391 95. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions - PubMed Central, https://pmc.ncbi.nlm.nih.gov/articles/PMC8114815/ 96. (PDF) UAV Swarm GNSS Spoofing Defense Method Based on Consensus Artificial Potential Field - ResearchGate, https://www.researchgate.net/publication/387188199_UAV_Swarm_GNSS_Spoofing_Defense_Method_Based_on_Consensus_Artificial_Potential_Field 97. Detection and Mitigation of Position Spoofing Attacks on Cooperative UAV Swarm Formations - arXiv, https://arxiv.org/html/2312.03787v1 98. Cognitive warfare: the new battlefield exploiting our brains - Polytechnique Insights, https://www.polytechnique-insights.com/en/columns/geopolitics/cognitive-warfare-the-new-battlefield-exploiting-our-brains/ 99. Mitigating and Responding to Cognitive Warfare - dtic.mil, https://apps.dtic.mil/sti/trecms/pdf/AD1200226.pdf 100. Cognitive Bias | SKYbrary Aviation Safety, https://skybrary.aero/articles/cognitive-bias 101. Investigation on the impact of human-automation interaction in maritime operations, https://www.researchgate.net/publication/323734349_Investigation_on_the_impact_of_human-automation_interaction_in_maritime_operations 102. Human Cognitive Bias Identification for Generating Safety Requirements in Safety Critical Systems, https://www.ijrte.org/wp-content/uploads/papers/v8i6/F9598038620.pdf 103. A Human Study of Cognitive Biases in Web Application Security - arXiv, https://arxiv.org/html/2505.12018v2 104. (PDF) Epistemological Conception of Trust - ResearchGate, https://www.researchgate.net/publication/362668187_Epistemological_Conception_of_Trust 105. The Ethics and Epistemology of Trust - Internet Encyclopedia of Philosophy, https://iep.utm.edu/trust/ 106. Measurement of Trust in Automation: A Narrative Review and Reference Guide - Frontiers, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2021.604977/full 107.

How navigation systems transform epistemic virtues: Knowledge, issues and solutions - PhilArchive, https://philarchive.org/archive/GILHNS 108. Positioning, Navigation, and Timing Trust Inference Engine - Inside GNSS, https://insidegnss.com/positioning-navigation-and-timing-trust-inference-engine/ 109. HMI Design Thinking: Applying UX Principles to Mission-Critical Interfaces, https://www.aufaitux.com/blog/hmi-design-thinking-ux-mission-critical-interfaces/ 110. Principles for External Human–Machine Interfaces - MDPI, https://www.mdpi.com/2078-2489/14/8/463 111. Trust in automated vehicles: constructs, psychological processes, and assessment - Frontiers, https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1279271/full 112. Trust in an Autonomous Guidance System and Resulting Behavior for a Planetary Rover Task - ResearchGate, https://www.researchgate.net/publication/370796278_Trust_in_an_Autonomous_Guidance_System_and_Resulting_Behavior_for_a_Planetary_Rover_Task 113. Cognitive Engineering in Training: Monitoring and Pilot-Automation Coordination in Complex Environments, https://ntrs.nasa.gov/citations/20230002763 114. Automation Bias and Countermeasures in Flight Crews - NASA Technical Reports Server (NTRS), https://ntrs.nasa.gov/citations/20020043049 115. Pilot, OEM Share Best Practices to Fight GPS Spoofing Attacks | NBAA, https://nbaa.org/news/business-aviation-insider/2025-03/pilot-oem-share-best-practices-to-fight-gps-spoofing-attacks/ 116. Analysis of the Development Status of eLoran Time Service System in China - MDPI, https://www.mdpi.com/2076-3417/13/23/12703 117. GPSJam | Bellingcat's Online Investigation Toolkit - GitBook, https://bellingcat.gitbook.io/toolkit/more/all-tools/gpsjam 118. Crowdsourcing GNSS jamming detection and localization - Stanford University, https://web.stanford.edu/group/scpnt/gpslab/pubs/papers/Strizic_IONITM_2018_CrowdsourceSmartphone.pdf 119. Sharing and Crowdsourcing GNSS Data to Monitor and Protect the GNSS RF Environment - UNOOSA, https://www.unoosa.org/documents/pdf/psa/activities/2022/GNSS2022/IDM10/GNSS2022_03_IDM_05.pdf 120. [2306.06143] Integrating Usage Control into Distributed Ledger Technology for Internet of Things Privacy - arXiv, https://arxiv.org/abs/2306.06143 121. [2006.04754] Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials - arXiv, https://arxiv.org/abs/2006.04754 122. Report on Positioning, Navigation, and Timing (PNT) Backup and Complementary Capabilities to the Global Positioning System (GPS) - CISA, https://www.cisa.gov/sites/default/files/publications/report-on-pnt-backup-complementary-capabilities-to-gps_508.pdf 123. Complementary PNT and GPS Backup Technologies Demonstration Report | US Department of Transportation, https://www.transportation.gov/administrations/assistant-secretary-research-and-technology/complementary-pnt-and-gps-backup