論説

衛星通信における宇宙安全保障とサイバー安全保障の交錯

高 屋 友 里

一　はじめに

近年，宇宙空間およびサイバー空間における脅威が国際的に認識されるようになり，国連諸機関において宇宙安全保障（Space Security）およびサイバー安全保障（Cybersecurity）の確保にむけた法規範形成が急がれている。その背景には，①宇宙空間およびサイバー空間の軍事利用の多様化，②両空間を利用するアクターの増加，③衛星をはじめとする宇宙インフラのデジタル化[1]ー衛星の IoT（Internet of Things）化[2]ーがある。その中でも③の影響は大きく，2020 年 9 月 4 日，米国は「宇宙システムのためのサイバーセキュリティ原則」（SPD-5）[3]を打ち出し，宇宙活動おけるサイバー安全保障の重要性を強調した。従来，宇宙空間およびサイバー空間の利用における脅威は，国際宇宙法，国際電気通信法，サイバー行為に関する各法分野（例：国際人道法や国際刑事法）など縦断的に研究されてきたが，宇宙安全保障とサイバ

一安全保障との交錯に着目する研究は始まったばかりである[4]。

このため本稿は，宇宙活動でもあり通信活動でもある衛星通信に焦点を当て，何がすでに禁止され，何が禁止されておらず，何が規範化されるべきかなど，諸規範の整理を試みるものである[5]。検討対象とする国際法規範は，国連宇宙諸条約[6]，および，国際電気通信連合（ITU）[7]が定める諸規範から成るITU 法[8]とする[9]。構成として，まず衛星通信の技術的および法的側面，2 つの空間の法的地位，2 つの安全保障概念を整理し（二），宇宙空間の軍事利用における法的制約を確認しつつ，ITU の有害な混信の禁止規範をサイバー安全保障の観点から再考する（三）。なお，宇宙空間およびサイバー空間の軍事利用に対する国際人道法上の適用可能性は否定しないものの，本稿の射程には含まないこととする。

二　衛星通信と 2 つの安全保障

1. 衛星通信と有害な混信の禁止

衛星通信とは，先端技術である宇宙技術と通信技術とを結合させたものであり，衛星の運用に使用する地上部分，宇宙部分，衛星間の通信システムとで構成される衛星通信システムの通称である[10]。その概念には，地上局から衛星に向けた制御情報の送信（uplink），衛星から地上局へ送られる機体の状態情報の受信（downlink），宇宙ミッション（通信・地球観測・気象観測・測位など）を担う衛星による原データの送信が含まれる[11]。また，月面ローバや火星探査機といった宇宙物体すべてが衛星通信を介して運用されるため，衛星通信とは宇宙活動にとって必要不可欠な構成要素である。

一方，衛星通信に使う無線周波数は有限のため，その国際規制を担う ITU は，無線周波数および静止軌道（Geostationary Orbit）の軌道位置（slot）の割当てや関係国間の国際調整を管轄し，ITU 憲章条約第 45 条 1 項に基づき，通信妨害を引き起こす有害な混信（harmful interference）を明示的に禁止している[12]。

2. 2 つの空間の法的地位

国際法において宇宙空間は定義されていないため，従来の法概念の援用として，ローマ法に起源を持つ公法上の公物の概念－*res communis*－が当てはめられてきた[13]。この概念は，宇宙空間を共有物と捉え，特定の国の領有の対象とはならずに，すべての人間に開かれている領域とするもので，宇宙空間をすべての国家の利益のために平等で共通な権利の対象と考える説である[14]。サイバー空間も同じく *res communis* としてグローバル・コモンズと捉える学説がある[15]。その根拠として，ワールド・ワイド・ウェブ（WWW）創始者がインターネット上の財産権設定を否定するプロトコールを設けている点を指摘する学説もあるが[16]，実際に宇宙空間とサイバー空間とが同じ法的地位とみなすにはいくつか問題がある。

グローバル・コモンズ概念とはもともと国家主権を排除するものではない[17]。国際法上，国際公域とされる公海，南極，宇宙空間（天体を含む），深海底はそれぞれ条約に基づく諸原則（例：平和利用原則）により法的地位が示される一方，サイバー空間の利用に特化した国際条約はまだ存在しない。また，サイバー犯罪やサイバー攻撃といった違法なサイバー行為の発信源が自国の領域内にある場合，当該領域国はサイバー空間の利用において相当の注意義務違反を問われることとなる[18]。つまり，サイバー空間の利用において領域主権に基づく主権概念が存在するのである[19]。このほか，サイバー空間に特有な点として，天然資源の不存在，物理的な境界線の欠如，資源が枯渇することのない点などが挙げられる[20]。

このように宇宙空間とサイバー空間の法的地位は必ずしも一致しないのだが，両空間における安全保障概念には一定の類似性がみられる。この点について次節で述べる。

3. 2 つの安全保障

宇宙安全保障およびサイバー安全保障の概念を整理する。前者は 2001 年米国同時多発テロ事件を契機に米国が創出した用語であり，後者は ITU が 2005 年にサイバー脅威に対抗するため打ち出した用語である。

① 宇宙安全保障

宇宙安全保障は条約上の用語ではなく，宇宙空間の軍事利用を推進する米国が打ち出した政策上の用語であり，その概念は 1946 年に米 RAND 社が発表した「予備設計（Preliminary Design）報告書」[21]まで遡る。同書はミサイル攻撃能力向上における衛星データの有用性を謳うなど，宇宙空間における優位性が国家安全保障の強化に繋がると結論づけた。この概念はその後も受け継がれ，2000 年米国国防権限法[22]によりラムズフェルド宇宙委員会[23]が設置されると，米国の国益を最優先とする宇宙安全保障のほか，宇宙空間における優位性（space superiority）や宇宙コントロール（space control）の概念および用語が打ち出された。2006 年国家宇宙政策（NSPD-49）[24]では，防衛を目的とする衛星によるインテリジェンス活動は宇宙空間の平和利用原則において許容されるとの見解を示した。

2015 年 1 月 9 日，日本も同趣旨の宇宙安全保障を掲げた宇宙基本計画[25]を発表している。当時日本はその定義を示さなかったが，2023 年に発表した宇宙安全保障構想[26]において「宇宙空間を通じた国家安全保障上の目標への貢献」および「宇宙空間を通じて国の平和と繁栄，国民の安全と安心を増進しつつ，同盟国・同志国等とともに，宇宙空間の安定的利用と宇宙空間への自由なアクセスを維持すること」と定義した。

一方，国連軍縮研究所（UNIDIR）は宇宙安全保障を国際の平和と安全の維持および宇宙空間における軍拡競争防止を含む軍縮に関連するものと定義し[27]，また，一部の学説では宇宙空間の自由なアクセスおよび利用を確保することと定義する[28]。このように宇宙安全保障という用語は広く使われるがその定義は国際法上確立しておらず，衛星システムの汎用性の高さに伴い宇宙脅威も多様化するため，その定義は多義的となっている[29]。

② サイバー安全保障

サイバー安全保障に関する国内法政策[30]やソフトローは多く存在するが[31]，サイバー安全保障の用語を用いる国際条約はないため，その定義は確立していない。国連機関として初めてサイバー脅威の低減を試みた ITU は，サイバー安全保障を「サイバー環境，組織，ユーザーの資産を守るために使用される手段，政策，安全保障概念，安全保障セーフガード，ガイドライン，リスク管理アプローチ，措置，訓練，ベスト・プラクティス，保障および技術の

集合体」[32]と定義する。また，国内の省庁によっても定義は異なる。例えば米国商務省は「コンピュータ，電気通信システム，電気通信サービス，有線通信，および電気通信（含まれる情報を含む）の有用性，整合性（integrity），認証（authentication），機密性，および否認防止（nonrepudiation）を確保するための損傷の防止，保護，および修復」[33]と定義する一方，同国国防総省はサイバー空間安全保障（cyberspace security）の用語を用い，「有用性，整合性，認証，機密性，および否認防止を確保する目的で，コンピュータ，電気通信システム，そのほかの情報技術（プラットフォームに内在する情報技術を含む）への不正アクセス，不正利用，損害を生ずることを防ぐためにサイバー空間において講ずる措置」と定義する。サイバー技術アプリケーションの急激な多様化に伴い，サイバー空間の利用において保護すべき利益もユーザーにより変容するため，サイバー安全保障とはサイバー活動もしくは空間に対する脅威の低減を目的とする措置全般を指すこととなる。

また，サイバー安全保障に関する唯一の国際条約[34]は 2001 年サイバー犯罪条約（ブダペスト条約）[35]であり，ITU は同条約の有用性をサイバー安全保障の文脈で確認している。サイバー脅威となるサイバー犯罪とは，不正アクセス（第 2 条），違法なデータ取得・傍受（acquisition）（第 3 条），データの傍受（interception）（第 4 条），システムの妨害（第 5 条），装置の濫用（第 6 条），コンピュータ関連の偽造（第 7 条）およびコンピュータに関連する詐欺（第 8 条）である。同条約は当事国に対しサイバー犯罪に対応する国内法整備を義務づけるが，越境コンピュータにおける捜査[36]やデータの扱い，および，捜査を目的とした通信傍受におけるプライバシー保護[37]が課題となっている。サイバー安全保障の強化・確保においても同じ課題が浮上する。

以上，衛星通信に関する 2 つの安全保障として，宇宙安全保障とサイバー安全保障の概念および定義を確認した。もともと宇宙システムは 2010 年頃までアナログ技術により構成されていたため[38]，宇宙活動はサイバー安全保障の対象外であったが，衛星の IoT 化に伴い，宇宙活動におけるサイバー安全保障の確保という視点が必要となったのである。しかし 2 つの安全保障はともに保障すべき利益（国益・法益・利益など）が ICT 技術の発展に伴い変

容するため，画一的な定義付けは難しい。

三　衛星通信に対する有害な混信の禁止規範の再考

それでは衛星通信をサイバー安全保障の文脈で検討する場合，既存の「有害な混信禁止」規範に及ぼす影響はあるのか。本節では衛星通信に対する脅威となる対抗宇宙能力（counterspace capability）[39]を念頭に，宇宙空間平和利用原則の形骸化を指摘し（1），宇宙空間の軍事利用に対する法的制約を確認するとともに（2），国連で議論される「責任ある行動（responsible behaviors）」決議における成果およびITUの課題を考察する（3）。

1. 宇宙空間平和利用原則の形骸化

1959年南極条約[40]の影響を受けたとされる1967年宇宙条約は，第4条において宇宙空間平和利用原則を定める。しかし戦略的技術の発展に伴い，同原則の規範性が揺らぎつつある。条約発効時，国連は宇宙空間の非核化を目指していたため[41]，本条項は地球軌道の非核化（1文）および天体の完全な非軍事化（2文）に成功したと評される一方，条文の解釈上，宇宙空間で明示的に禁止されるのは大量破壊兵器（WMD）の地球軌道配備のみであり，それ以外の宇宙空間の軍事利用は合法であるとする課題を残した[42]。

例えば，宇宙空間における核実験はすでに1963年部分的核実験禁止条約（PTBT）[43]において禁止されているが，核弾頭搭載の部分軌道爆撃システム（Fractional Orbital Bombardment System: FOBS）が攻撃目標に向けて弾道飛行する際に宇宙空間を通過することは第4条において禁止されない[44]。対衛星破壊（ASAT）実験も然りである[45]。さらに，同原則で用いられる「平和的（peaceful）」の定義も，中露による「非軍事（non-military）」と欧米日による「非侵略的（non-aggressive）」との解釈に分かれ，後者が通説となっている[46]。侵略的でなければ，情報収集をはじめとする防衛目的の宇宙空間の利用は平和利用原則に反しないとする考えに加え，近年における衛星のIoT化により，宇宙空間の軍事利用が急速に拡張している。

その契機となったのが米国による宇宙軍（USSF）の創設である。2017 年 9 月，米国空軍参謀総長ゴールドフィン空軍大将は陸，空，海，宇宙，サイバー, 海底, ソーシャルメディアを戦闘領域として挙げると[47], 2018 年 6 月，トランプ大統領が宇宙軍の創設を発表した[48]。2019 年 2 月，同大統領は宇宙政策指令-4（SPD-4）[49]に署名し，宇宙軍の検討を国防総省に求め，同年 12 月に正式な創設に至った[50]。今や数カ国が宇宙軍を有し，さらに対抗宇宙能力（counterspace capabilities）の開発国も増えたため[51]，宇宙脅威およびサイバー脅威が顕著化している。これらの状況に鑑み，次節では衛星通信に対する対抗宇宙能力の分類および法的制約を概観する。

2. 衛星通信に対する対抗宇宙能力の法的制約

対抗宇宙能力を分類すると，①ASAT 実験のようミサイルによる衝撃力を以て破壊する直接上昇（Direct Ascent）型，②軌道上に配備され攻撃目標に近づく軌道共有（Co-orbital）型，③レーザーや電磁波を用いる指向性エネルギー（Directed Energy）型，④無線周波数エネルギーにより衛星からの通信に混信を生じさせる電子戦（Electronic Warfare）型，⑤コンピュータ・システムを攻撃対象とするソフトウェアやネットワーク技術を使うサイバー（Cyber）型がある[52]。衛星通信における無線周波数の利用に対し有害な混信を及ぼす④は，すでに ITU 憲章第 45 条において禁止されているが，衛星の IoT 化のみならず地上運用局もコンピュータ・システムに制御されるため，⑤に対する脆弱性が増している[53]。このため④と⑤とを同じ対抗宇宙能力もしくはサイバー攻撃と分類する学説もある[54]。また，⑤の対抗宇宙能力により衛星通信を妨害することは技術的に可能であるため, 既存の ITU 法が禁止する有害な混信の定義を確認する。

まず，ITU は「混信」と「有害な混信」とを分けて定義する。混信は「無線通信システムにおける受信時に，放出・放射・誘導（induction）のうち一つもしくはそれらの組み合わせが原因で生じる不必要なエネルギーによる影響（effect）をいい，それはパフォーマンスの低下，解釈の誤り（misinterpretation），当該エネルギーが存在しなければ抽出できたであろう情報の滅失により現れるもの」[55]であり，従来，不必要なエネルギーは技術

的および人的な要因から発せられることも多かった。有害な混信は「無線航行業務その他の安全業務の運用を妨害し，又は無線通信規則に従って行う無線通信業務の運用機能に重大な悪影響を与え，若しくはこれを反復的に中断し若しくは妨害する混信」[56]と定義される。混信の結果として業務（services）の運用の妨害や運用機能に重大な悪影響や妨害をきたす影響を意味しており，代表的な例として通信妨害を引き起こす意図的なジャミングが挙げられる（上記④に該当）。

一方，衛星通信に対する⑤のサイバー脅威を低減するため，ITU は 2001 年サイバー犯罪条約に基づくサイバーセキュリティ強化に取り組むとともに[57]，2023 年 12 月 15 日に開催された世界通信会議（WRC-23）では，宇宙空間における無線資源への公平なアクセスの確保を新たな議題に追加した[58]。しかし衛星通信は，対抗宇宙能力に基づく脅威およびサイバー脅威に晒されていながら，従来の「有害な混信」の定義を以てその低減を図れるか否かは定かでない。なぜなら ITU 法は国際規制とはいえ国家主権を重視する性質のため，意図的な混信を国際違法行為と認定し違反国に制裁を課すといった強制性のある執行機能を有さないからである。対抗宇宙能力として発せられる有害な干渉から有限な通信資源を守るという視点が必要であろう。

3. 国連における TCBM 導入の試み

国連総会第 4 委員会の下に設置される宇宙空間平和利用委員会（UNCOPUOS）は，宇宙空間の平和利用のみを検討する機関のため，宇宙空間の軍事利用に関する事項は検討できない。このため宇宙空間の軍事利用は，国連外に位置するジュネーブ軍縮会議（CD）が宇宙空間軍拡競争回避（PAROS）の文脈で検討し，その報告書は国連総会第 1 委員会に提出されてきた。しかし 2019 年 4 月にインドが実施した ASAT 実験を機に，第 1 委員会が宇宙脅威に関する議論の場となっている。

2020 年，第 1 委員会に対し 22 カ国が共同で「責任ある行動の規範，規則及び原則を通じた宇宙における脅威の低減（責任ある行動）」決議案を提出し，決議 75/36 として採択されたのだが，翌 2021 年 11 月 14 日，ロシアが国際宇宙ステーション（ISS）の軌道上わずか 30km である高度 480km にお

いて ASAT 実験を実施した。大量に生じた宇宙デブリにより ISS 搭乗中の宇宙飛行士は生命の危機に晒されたため，翌月，国連決議 76/231「責任ある行動」決議が採択され，翌 2022 年からオープン・エンド作業部会（OPWG）の招集が決定した。しかし第 1 回 OPWG を前に，2 月 24 日，ウクライナ侵攻の 1 時間前にロシアはウクライナの衛星通信ネットワークを遮断したため，衛星通信に対する宇宙脅威に並びサイバー脅威が顕在化したのである。

OPWG は 2022 年および 2023 年に開催され，宇宙空間における脅威低減に向けた責任ある行動規範に関連する国際法規範を確認したが，ロシアの反対のためにコンセンサスに至らなかった[59]。しかし成果として評価できるのは，破壊的直接上昇 ASAT（DA-ASAT）ミサイル実験に対するモラトリウムの形成である。もともと米国が 2022 年 4 月に提唱し，2024 年までに 34 カ国が賛同したことから，国連総会第 1 委員会において決議 77/41[60]の採択に至った規範である。同決議により，破壊的 DA-ASAT 実験を実施しない国際約束，透明性・信頼醸成措置（TCBM）[61]およびモラトリアムが宇宙空間における軍備競争の回避に関する国際法規範に資するとの認識が共有された。

一方，ITU も 2018 年より通信活動における TCBM の導入に注力している。軍による戦闘作戦としての通信活動は ITU の規制対象とならないが，有限な通信資源の公平な利用の観点から，ITU は無線周波数の軍事利用を制限する法的アプローチを模索し，2018 年に ITU 決議 186「宇宙活動における透明性・信頼醸成措置（TCBM）に関する ITU の役割強化」[62]を採択した。同決議は 2022 年にも改訂され，無線周波数の利用状況における透明性の向上を通じて，宇宙空間における脅威低減を図るものである。

このように宇宙空間およびサイバー空間の安全保障に資する主要な規範として TCBM の有用性が認識されている。しかし TCBM は手段・措置（measures）であり，法規範ではない。軍事活動における透明性の向上が脅威の低減や抑止に繋がるという TCBM の根本的な思想では，2 年以上にわたるロシアのウクライナ侵攻を説明できない。この点に関し，ITU 法における履行制度では，対抗宇宙能力から生じる衛星通信への有害な混信も，技術的には既存の国際モニタリング制度で探知が可能である。TCBM の導入を以て，対抗宇宙能力から生じる有害な混信も ITU 法違反とみなす仕組みが ITU 法

制度に求められる。

四　おわりに

衛星が IoT 化したことを機に，宇宙活動に対するサイバー脅威が増大し，衛星通信は宇宙安全保障およびサイバー安全保障の両方で検討すべき対象となった。宇宙空間における脅威の増大は，1967 年宇宙条約第 4 条が定める宇宙空間平和利用原則が，宇宙軍の創設や対抗宇宙能力の開発を許す解釈となっている点が原因である。一方，国連は「責任ある行動」決議のもと，宇宙脅威の低減に資する既存の国際法規範の確認を急いでおり，そのなかでも TCBM の導入に注力している。しかし TCBM は法規範ではなく，履行確保のための手段・措置に過ぎない。このため，ITU 法制度が有するモニタリング機能に TCBM を導入することで，従来の有害な混信だけでなく，対抗宇宙能力から生じる有害な混信も ITU 法違反とみなし是正する仕組みが模索されるべきである。

---

[1] Rada Popova, "Space Technology and Cybersecurity: Challenges and Technical Approaches for the Regulation of Large Constellations," in: P.J. Blount and Mahulena Hofmann (eds.), *Space Law in a Networked World*, Brill Nijhoff, 2023, p. 105.

[2] P.J. Blount, "Satellites Are Just Things on the Internet of Things," 43 (3) *Journal of Air and space Law*, 2017, pp. 273-294.

[3] U.S. Doc. "The White House, Space Policy Directivee-5: Cybersecurity Principles for Space Systems," available at: https://irp.fas.org/offdocs/nspm/spd-5-fs.pdf (accessed on 1 March 2024).

[4] *See*, supra note 1.

[5] 次を参照のこと。高屋友里「衛星通信に対する有害な混信の禁止と宇宙安全保障ー透明性・信頼醸成措置に着目してー」山本龍彦（監修）石井由梨佳（編）『安全保障』（法律文化社, 2024 年）278-299 頁。

[6] 国連宇宙諸条約とは，1967 年宇宙条約，1968 年宇宙救助返還協定，1972 年宇宙損害賠償条約，1975 年宇宙物体登録条約，1979 年月協定である。Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer

Space, including the Moon and other Celestial Bodies, 27 Jan. 1967, 610 *UNTS* 205 / 6 *ILM* 386 (1967); The Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, 22 April 1968, 19 *UST* 7570 / 672 *UNTS* 119 (1968); The Convention on International Liability for Damage Caused by Space Objects, 29 Mar. 1972, 24 *UST* 2389 / *TIAS* 7762 / 961 *UNTS* 187; The Convention on Registration of Objects Launched into Outer Space, 14 January 1975, 1023 *UNTS* 15; The Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, 18 Dec. 1979, 1363 *UNTS* 3 (1979).

[7] *See*, ITU Doc., "Overview of ITU's History," available at: http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/12.28.71.en.pdf (accessed Dec. 8, 2023).

[8] Convention of the International Telecommunication Union, Geneva, 22 December 1992, 1825 UNTS 1; UKTS 1996 No. 24; Cm. 2539; *ATS* 1994 No. 28; Final Acts of the Additional Plenipotentiary Conference, Geneva, 1992. ITU 憲章条約のほか，世界通信会議で規定される ITU 憲章条約付属無線通信規則や国際無線通信規則を含む。

[9] 学説において，ITU 法体制は国際宇宙法に含まれるとする説と，法規範の形成過程や制度が異なるため別の法体制とみなす説とがあり，本稿は後者の立場をとる。Frans von der Dunk, "Legal aspects of satellite communications, " in Frans von der Dunk with Fabio Tronchetti (eds.), *Handbook of Space Law*, (Edward Elgar Publishing, 2015), p. 492.

[10] Timothy Pratt, Jeremy E. Allnutt, *Satellite Communications*, John Wiley & Sons, 2019. 飯田尚志（編）『衛星通信』（オーム社，1997 年）。

[11] Frans von der Dunk, "Legal aspects of satellite communications," in Frans von der Dunk with Fabio Tronchetti (eds.), *Handbook of Space Law*, (Edward Elgar Publishing, 2015), p. 457.

[12] ITU 憲章第 45 条 1 項 "[A]ll stations, whatever their purpose, must be established and operated in such a manner as not to cause harmful interference to the radio services or communications of other Member States or of recognized operating agencies, or of other duly authorized operating agencies which carry on a radio service, and which operate in accordance with the provisions of the Radio Regulations."

[13] 龍澤邦彦『宇宙法システム－宇宙開発のための法制度』（丸善プラネット株式会社, 2000 年）20-25 頁。

[14] 龍澤『同上』22 頁。

[15] *See*, Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticommons," *Law and Society Approaches to Cyberspace*, Routledge, 2017. 59-139; Abraham M. Denmark and James Mulvenon (eds.), *Contested Commons: The Future of American Power in a Multipolar World*, Centre for a New American Security, 2010, available at:

https://www.jstor.org/stable/pdf/resrep06098.pdf?refreqid=fastly-default%3Ab396c90998fce9906ed2ff3ee92af0c3&ab_segments=&origin=&initiator=&acceptTC=1 (accessed on 3 March 2024).

16 Tim Berners-Lee and Mark Fischetti, *Weaving the Web: The Past, Present and Future of the World Wide Web by Its Inventor*, Texere, 2000, p. 30, 76, 129, quoted in: Nicholas Tsagourias, The legal status of cyberspace: sovereignty redux?, in: Michael N. Schmitt, *Introduction to the Research Handbook on International Law and Cyberspace*, Edward Elgar, 2021, p.28.

17 Nicholas Tsagourias, *supra* note 16, p. 14.

18 赤堀毅『サイバーセキュリティと国際法の基本ー国連における議論を中心にー』（東信堂，2023 年）41 頁。

19 Nicholas Tsagourias, *supra* note 16, p. 13.

20 Nicholas Tsagourias, *supra* note 16, p. 30.

21 *See*, RAND Corporation, *Preliminary Design of an Experimental World-Circling Spaceship*, Report No. SM-11827, 2 May 1946, available at: https://www.rand.org/content/dam/rand/pubs/special_memoranda/2006/SM11827part1.pdf (accessed Aug. 20, 2023).

22 U.S. Public Law 106-65, The U.S. National Defense Authorization Act for Fiscal Year 2000, Oct. 5, 1999.

23 U.S. Doc., "Report of the Commission to Assess United States National Security Space Management and Organization - Pursuant to Public Law 106-65 ("Rumsfeld Commission Report")," 11 January 2000, pp. 1-2, available at: https://aerospace.csis.org/wp-content/uploads/2018/09/RumsfeldCommission.pdf (accessed Dec. 1, 2023).

24 U.S. White House, U.S. National Space Policy, NSPD-49 (Washington, D.C., 2006), available at: https://irp.fas.org/offdocs/nspd/space.html (accessed Dec. 7, 2023).

25 内閣府「宇宙基本計画」（平成 27 年 1 月 9 日 宇宙開発戦略本部決定），available at: https://www8.cao.go.jp/space/plan/plan2/plan2.pdf (accessed Jan. 1, 2024).

26 内閣府「宇宙安全保障構想」（令和 5 年 6 月 13 日 宇宙開発戦略本部決定），available at: https://www8.cao.go.jp/space/anpo/kaitei_fy05/anpo_fy05.pdf (accessed on 2 September 2023).

27 UNIDIR, *A Lexicon for Outer Space Security*, 16 August 2023, p. 40, available at: https://unidir.org/publication/a-lexicon-for-outer-space-security/ (accessed on 2 February 2024).

28 Michael Sarah Estabrooks, "Space Security 2006," in UNIDIR Conference Report of 30-31 March 2006, *Building the Architecture for Sustainable Space Security* (UNIDIR, 2006), p. 93.

29 Ram Jakhu and Karan Singh, "Space Security and Competition for Radio Frequencies and Geostationary Slots," *Zeitschrift für Luft- und Weltraumrecht* 58 Jg. 1/2009, p. 76.

[30] 欧州の関連法政策の例として，European Parliament Resolution of 12 September 2013 on a Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013/2606(RSP)); Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for A High Common Level of Security of Network and Information Systems Across the Union, OJ L 194, 19 July 2016, pp. 1-30.
[31] ソフトローの例として，OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, Paris, 1981), adopted as a Recommendation of the Council of the OECD, 23 September 1980, revised in 2013; United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce with Guide to Enactment 1996 with Additional Article 5 *bis* as adopted in 1998 (United Nations 1999). CETS No. 185.
[32] "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets." *See*, ITU Doc., "Series X: Data Networks, Open System Communications and Security - Overview of cybersecurity," Recommendation ITU-T X. 1205, 2008, p. 2.
[33] US Department of Commerce, NIST, Computer Security Resource Center, "Glossary - cybersecurity," available at: https://csrc.nist.gov/glossary/term/cybersecurity (accessed on 20 March 2024).
[34] Federico Bergamasco, et. al., Cybersecurity: Key Legal Considerations for the Aviation and space Sectors, Wolters Kluwer, 2020, p. 61,
[35] The Convention on Cybercrime, Council of Europe, *European Treaty Series* No. 189, Budapest, 23 November 2001.
[36] 王志安「越境コンピューター捜索の法的地位―サイバー犯罪条約が残した課題―」『駒澤大学』第 3 巻 3 号（2004 年 4 月）114-132 頁。
[37] 通信傍受においてトラフィックデータとコンテンツデータとに明確に区分し処理する技術が確立していないため，サイバー犯罪を突き止める際にコンテンツデータも傍受するとプライバシー侵害が生ずる。夏井高人『サイバー犯罪条約の主要論点』法律論叢 75（2-3）, 2002-12-25, 263 頁。
[38] 2010 年に初めて国際宇宙ステーション（ISS）から宇宙飛行士がインターネットにアクセスしたが，米航空宇宙局（NASA）が提供した衛星リンクを経由し，地上のコンピュータへアクセスしただけであり，もしサイバー攻撃を受けたとしても被害は地上のサーバの損傷だけであった。*See*, Igor Kuksov, "Internet in Space: Is There Net on Mars?," Kaspersky Daily, 13 September 2019, available at: https://www.kaspersky.com/blog/internet-in-space/28267/ (accessed on 30 March 2024).
[39] 対宇宙空間能力と訳する文書もある。
[40] The Antarctic Treaty, 402 *UNTS* 71, 1961.
[41] Bing Cheng, Studies in International Space Law, Clarendon Press Oxford,

1997, p. 244.
[42] Bing Cheng, *ibid.*, p. 244-252.
[43] Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Warter, 5 August 1963, 480 UNTS 43 (PTBT).
[44] Bing Cheng, *supra* note 41, p. 246.
[45] ASAT 実験を禁止していた 1972 年弾道弾迎撃ミサイル（ABM）制限条約は，米国の一方的破棄により 2001 年に失効している。
[46] Jeremy Grunert, The United States Space Force and the Future of American Space Policy - Legal and Policy Implications, Brill Nijhoff, 2022, pp. 22-44.
[47] U.S. Air Force Report, "Air Force Association 2017, Air, Space & Cyber Symposium Remarks by General David L. Goldfein, U.S. Air Force Chief of Staff, 19 September 2017," available at: https://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_2017%20Air_Space_and_Cyber_Symposium.pdf (accessed on 20 March 2024).
[48] Jeremy Grunert, *supra* note 46, p. 1.
[49] U.S. Space Force, Doc., "Space Text of Space Policy Directive-4: Establishment of the United States Space Force," 19 February 2019, available at: https://trumpwhitehouse.archives.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/ (accessed on 21 March 2024).
[50] その後，フランスおよび日本も宇宙軍を創設している（日本は宇宙作戦群と称する）。
[51] 2024 年時点で 14 か国が対抗宇宙能力を開発している。*See*, Secure World Foundation, "Global Counterspace Capabilities: An Open Source Assessment," Annual Report 2024, available at: https://swfound.org/media/207826/swf_global_counterspace_capabilities_2024.pdf (accessed on 31 March 2024).
[52] Secure World Foundation, *ibid.*, p. xxxviii.
[53] Markus Hesse and Marcus Hornung, "Space as a Critical Infrastructure," in: K.-U. Schrogl et al. (eds.), *Handbook of Space Security, Springer*, 2015, p. 190.
[54] Cassandra Steer and Matthew Hersch (eds.), War and Peace in Outer Space: Law, Policy, and Ethics, Oxford University Press, 2021, p. 29. 青木節子「宇宙資産に対するサイバー攻撃に適用可能な国際法の検討」国際法外交雑誌 第 115 巻第 4 号（2017 年）9-12 頁。
[55] 2024 年無線通信規則第 1.166 条 "The effect of unwanted energy due to one or a combination of *emissions*, *radiations*, or inductions upon reception in a *radiocommunication* system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy."
[56] 2024 年無線通信規則第 1.169 条 "*Interference* which endangers the functioning of a *radionavigation service* or of other *safety services* or seriously degrades, obstructs, or repeatedly interrupts a *radiocommunication service* operating in

accordance with Radio Regulations (CS)."

[57] 詳細については次を参照。高屋友里「サイバーテロリズムの防止―通信活動における『有害な干渉禁止原則』の観点より」早稲田大学社会安全政策研究所紀要（11）2018 年 63-82 頁。

[58] ITU, "RA-23 sets agenda for sustainable spectrum use," News, 18 Nov. 2023, available at: https://www.itu.int/hub/2023/11/ra-23-sets-agenda-for-sustainable-spectrum-use/ (accessed on 2 March 2024).

[59] Brian Weeden, "Insight - Takeaways from the UN Open-Ended Working Group on Reducing Space Threats," Secure World Foundation, 12 October 2023, available at: https://swfound.org/news/all-news/2023/10/insight-takeaways-from-the-un-open-ended-working-group-on-reducing-space-threats (accessed on 2 March 2024).

[60] UN Res. A/RES/77/41, 7 December 2022.

[61] TCBM とは，1978 年の国連総会決議 33/91B で明示された信頼醸成措置（CBM）に類似するものであり，国家間での武力紛争のリスク低減を目的とし，法的拘束力は欠くものの 1970 年代初頭から軍縮・軍備管理法において発展してきた履行確保措置である。

[62] ITU Res.186, "Strengthening the role of ITU with regard to transparency and confidence-building measures in outer space activities," 2018, available at: https://www.itu.int/en/council/Documents/basic-texts/RES-186-E.pdf (accessed Sept. 1, 2023).