米国政府アカウンタビリティ室

議会関係者への報告

2024 年 1 月 GAO-24-105563

サイバー外交

米国の利益を支え、優先順位を高めることを目的とした国の取り組み

GAO Highlights

GAO-24-105563 のハイライト（議会宛報告書

GAO がこの調査を行った理由

国際貿易、コミュニケーション、重要インフラのデジタル技術への依存度が高まるにつれ、米国とその同盟国は、海外からのサイバー脅威の激化に直面している。国家や非国家主体は、民主主義を弱体化させる無責任な行動のプラットフォームとしてサイバー空間をますます利用している。国務省は、サイバー空間における米国の利益を促進するために、米国政府の国際的な取り組みを主導している。2022 年 4 月、国務省は、サイバー空間、デジタル技術、デジタル政策に関連する国家安全保障上の課題、経済的機会、米国の価値観への影響に取り組むことを使命とする CDP を立ち上げた。

2023 会計年度のジェームズ・M・インホフ国防認可法には、GAO がサイバー空間における利益を促進するための米国の外交努力およびその他の関連事項をレビューする条項が含まれている。本報告書では、特に(1)国際協定やフォーラムの利用を含め、サイバー空間に関する米国の利益を促進するために国務省が行っている活動、(2)サイバー外交の目標を達成するために、国務省の組織変更がどの程度役立っているか、あるいはどのような課題を提示しているか、について検証する。

国務省の活動を特定するため、GAO はプログラム文書を分析し、国務省の職員と戦略目標の実施について話し合った。国務省の組織変更を調査するため、GAO は以下の分析を行った。

国務省の改革計画とその実施状況を文書化し、GAO が改革に重要であると指摘した特定の慣行に国務省がどの程度取り組んでいるかを評価した。

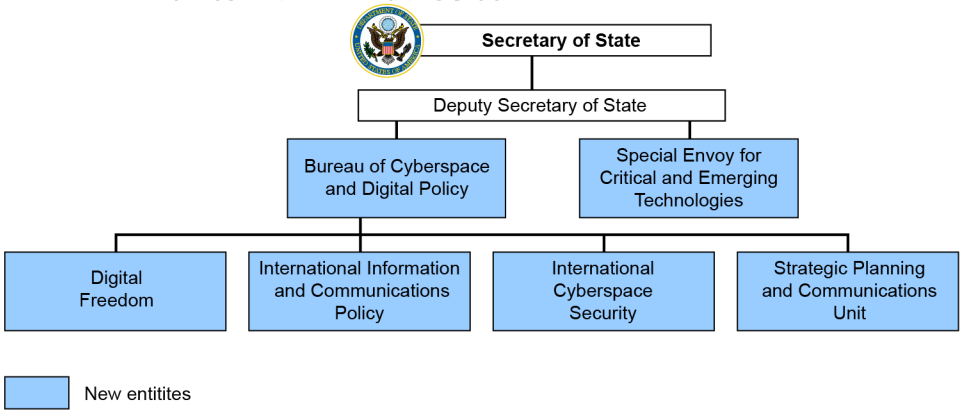
GAO-24-105563 を参照のこと。詳細は、ラテシャ・ラブ＝グレイヤー 電話：(202) 5124409 または lovegrayerl@gao.gov まで。

GAO の調査結果

国務省は、2023 年国家サイバーセキュリティ戦略で特定された目標を支援することを目的とし て、さまざまな外交・対外支援活動を行っている。具体的には、責任ある国家行動の規範を強化し、容認できない国家行動を抑止し、サイバー政策を推進することを目的とした多国間のフォーラムや協定に関与している。例えば、米国は国連政府専門家グループおよびオープンエンド・ワーキング・グループと協力し、平時の規範と信頼醸成措置を含むサイバー空間での行動に関する枠組みを策定した。国務省職員によれば、ルール違反者に結果を強制することを含め、サイバー空間における規範を確立することは、サイバー空間における悪行の代償を高め、悪行を抑止することになるという。また、デンマークと協力して「民主主義のための技術に関するコペンハーゲン誓約」を推進するなど、米国のサイバー規範と政策に沿った二国間活動も行っている。この誓約は、ネット上での言論の自由に対する権威主義的抑圧に対抗し、世界的にデジタルの自由を推進することを意図している。さらに国務省は、世界中のパートナーの能力を強化するために、研修や技術支援などの対外援助をプロバイダとして提供している。

国務省は 2022 年 4 月、サイバー空間の優先順位を高めるためにサイバー空間・デジタル政策局（CDP）を設立し、新局が米国のサイバー利益を促進するために直面するいくつかの課題に対処するための措置を講じている。米国はサイバー空間関連活動の努力と指導力を、特命全権大使が率いる CDP に一本化した。以前は、国務省内の複数の事業体がサイバー外交の責任を分担していた。GAO は、この変更がサイバー外交の目標を達成するために、国務省の立場をより良くするのに役立っていることを明らかにした。例えば、CDP の大使レベルのリーダーシップは、より高いレベルの外国政府高官とのエンゲージメントを可能にし、サイバーに関する米国の知名度を世界的に高めた。GAO はまた、同局の設立にあたり、関連する先進的な改革手法に取り組んでいることも明らかにした。例えば、国務省には、定員、リソース、変更管理に取り組む専門の実行チームがある。CDP は、局とそのパートナーとの間の役割を明確にする必要があるなど、改革された体制の下でサイバー目標を追求する上でまだ課題に直面している。 しかし、CDP の職員は、それらに対処するためのステップを特定している。

サイバーの優先順位を高めるために国が新たな事業体を設立



Source: GAO based on Department of State documentation (data); Department of State (seal). | GAO-24-105563

目次

略語 5

議会への対応 6

背景 8

サイバー外交 8

サイバー外交に関する GAO の先行研究 8

既存のサイバー外交戦略 8

国家は、さまざまな外交・対外援助活動を通じて、サイバー利権の促進に努める。 10

多国間フォーラムや協定における国家の外交的関与は、責任ある国家行動の規範を促進することを目的としている。 13

国家は、サイバー空間における責任ある行動の規範を確立または強化するための多国間協定を支持する。 14

米国は二国間で連携してサイバー規範と政策を推進する 16

対外援助活動の目的は、トレーニングや技術支援による協力の強化とサイバー・レジリエンスの構築である。 16

国務省の改革努力は、サイバー外交の目標を高め、先進的な慣行と一致させるのに役立った。 23

国務省、サイバー外交を優先する新局を設置 23

国務省の新局は、戦略目標の達成に向けて課題に取り組んでいる。 25

国務省は関連する先進的改革プラクティスに従った新サイバー局設立時 26

行政機関のコメント 29

附属書 I. 目的、範囲、方法論 31

附属書 II：米国国際開発庁からのコメント 33

附属書 III：GAO の連絡先とスタッフ 34

謝辞 34

スタッフの謝辞 34

略語

CDP	Bureau of Cyberspace and Digital Policy	サイバー空間とデジタル政策局
DCCP	Digital Connectivity and Cybersecurity Partnership	デジタル接続とサイバーセキュリティ・パートナーシップ
DRL	Bureau of Democracy, Human Rights, and Labor	民主主義・人権・労働局
FOC	Freedom Online Coalition	オンライン自由連合
GGE	Group of Governmental Experts	政府専門家グループ
GLEN	U.S. Transnational and High-Tech Crime Global Law Enforcement Network	米国国際・ハイテク犯罪グローバル法執行ネットワーク
INL	Bureau of International Narcotics and Law Enforcemen Affairs	国際麻薬・法執行局
ITU	International Telecommunication Union	国際電気通信連合
OAS	Organization of American States	米州機構
OEWG	Open Ended Working Group	オープン・エンド・ワーキング・グループ
S/TECH	Office of the Special Envoy for Critical and Emerging Technology	重要・新興技術特使事務所
TTC	Trade and Technology Council	貿易技術理事会
UN	United Nations	国際連合

これは米国政府の著作物であり、米国における著作権保護の対象ではない。公表された成果物は、GAO の許可を得ることなく、その全体を複製、配布することができる。ただし、本著作物には著作権で保護された画像やその他の素材が含まれている場合があるため、この素材を個別に複製する場合は、著作権者の許可が必要となる場合がある。

441 G St.

ワシントン DC 20548

2024 年 1 月 11 日

議会への対応

米国とその同盟国は、ウクライナ戦争、中国との競争、ロシアとの紛争に象徴されるように、国際貿易、コミュニケーション、重要インフラのデジタル技術への依存度が高まる中、激化する対外サイバー脅威に直面している。国家や非国家主体は、重要なインフラや市民を標的にしたり、民主主義や国際機構を弱体化させたり、グローバル経済における公正な競争を損なったりする無責任な行動のプラットフォームとして、サイバー空間をますます利用するようになっている。ロシアによる民間インフラへの攻撃的なサイバー攻撃や、ウクライナ戦争中に行われた偽情報キャンペーンは、そのリスクを物語っている。同時に、グローバルな舞台は、コネクティビティ、民主主義、平和、法の支配、持続可能な開発、人権と基本的自由の享受を促進するデジタル技術の可能性に対する信念を含め、米国の重要な価値観をデジタル・エコシステムに浸透させる積極的な機会を提供している。

国務省は、サイバー空間における米国の利益を促進するために、米国政府の国際的な取り組みを主導している。2021 年 10 月、ブリンケン国務長官は、サイバー空間と新興技術について、米国はデジタル・サイバー革命を形成し、それがわが国民に役立ち、わが国の利益を守り、わが国の競争力を高め、わが国の価値観を堅持するようにすることに大きな利害関係があると発言した。国務省のサイバー外交戦略目標には、同盟の構築、能力の強化、規範の強化が含まれる。これらの目的を達成するため、2022 年 4 月にサイバー空間・デジタル政策局（CDP）を新設した。

2023 会計年度のジェームズ・M・インホフ国防認可法には、サイバー空間における自国の利益を促進するための米国の外交努力や、その他の関連事項を見直すという条項が含まれていた。[1]われわれはまた、これらのテーマについて検討するよう、別途要請を受けた。本報告書では以下を検証する：1) 国際協定やフォーラムの利用を含め、サイバー外交の戦略を実施するために国が行っている活動と、その影響について報告されていること、2) サイバー外交の目標を達成するために、組織の変更が国にとってどの程度役立っているか、あるいはどのような課題を提示しているか、である。

サイバー空間に関する米国の利益を促進するために国務省が実施している活動を特定するため、2020 年から 2023 年まで進行中、および最近終了した活動に焦点を当てた。我々はプログラム文書を分析し、米国国際開発庁（USAID）、国防総省（DOD）、国土安全保障省（DHS）を含む国および関連機関の職員と戦略目標およびその実施について話し合った。選定したプログラムの結果を検討し、その影響について報告されていることを確認するため、国務省職員と話をした。

国務省がサイバー外交の目標を達成するために、組織の変更がどの程度役立ったか、あるいはどの程度課題となったかを検証するため、国務省の根拠、実施、計画、組織の変更に関する文書を調査し、CDP の設立を分析した。われわれは、GAO

[1] パブ.L. No. 117-263, § 9504, 136 Stat. 3903 (Dec 23, 2022).

の先行研究で概説された選択された政府改革慣行にどの程度取り組んでいるかを評価することで、組織変更を評価した。[2] また、新統合局とそのハイレベル・リーダーシップの形成により、国務省が得た利益の主な例を特定した。我々の調査範囲と方法論の詳細については、附属書 I を参照されたい。

当検査院は、一般に公正妥当と認められた政府監査の基準に準拠して、2021 年 11 月から 2024 年 1 月にかけて本業績監査を実施した。これらの標準は、当検査院が、監査の目的 に照らして合理的な根拠を有する十分かつ適切な証拠を入手するために、監査を計画し実施することを求めている。当検査院は、入手した証拠が当検査院の監査目的に基づく所見と結論のための合理的な基礎を提供すると信じている。

[2] GAO、ガバナンス再編：省庁改革の取り組みを評価するための重要な質問、GAO-18-427（ワシントン D.C.：2018 年 6 月 13 日）。

背景

サイバー外交

サイバー外交」という言葉は、サイバー空間における米国の幅広い関心を包含している。国務省職員や非政府組織（NGO）代表者によると、サイバー外交の公式な定義は存在しない。本報告書では、「サイバー外交」とは、国務省が主導するサイバー空間における米国の利益を国際的に支援する取り組みであると考える。このような取り組みには、米国の対外援助を相手国に提供し、サイバー犯罪撲滅、サイバー空間における責任ある行動規範の確立、技術標準の策定を目的とした活動を含む多国間および二国間交流に関与することが含まれる。CDP は、さまざまなサイバー外交活動の指導、管理、支援を通じて、サイバー外交を実施する上で、国務省において主導的な役割を果たしている。国務省職員によると、同省のサイバー外交には、外交努力を通じて、相互運用可能で信頼性の高いグローバル・インターネットに対する前向きなビジョンを推進することも含まれるという。このような努力は、米国とそのパートナーの紛争リスクを軽減し、サイバー空間の安全と安定を達成するために働く。

サイバー外交に関する GAO の先行研究

年 9 月、われわれはサイバー局設立に関する当時の国務省の計画について報告した。[3]我々は、国務省が国際サイバー外交に貢献する他の連邦政府機関を計画策定に関与させていないことを発見した。我々は、国がサイバー局を設立する計画に関連する連邦政府機関を参加させ、彼らの意見を聞き、潜在的なリスクを特定するよう勧告した。我々の勧告とこれまでの作業を考慮し、2021 年の 5 月と 6 月に、国は国防総省、商務省、国土安全保障省を含む関連連邦機関の高官、国家安全保障会議と国家サイバー局長室の高官と会談した。これらの協議の中で、国はこれらの機関の見解を入手し、リスクを特定し、我々の勧告を実施した。

2021 年 1 月、我々は国務省のサイバー局提案に関する別の報告書を発表した。[4]われわれは、国務省が提案書を作成するためにデータと証拠を利用していないことを明らかにした。我々は、データと証拠がなければ、国務省の提案が効果的に優先順位を設定し、局が意図した目標を達成するために適切なリソースを割り当てる保証がないと判断した。我々は、国務省に対し、現在の提案、あるいはサイバー局設立のための新たな提案を正当化するために、データと証拠を用いるよう勧告した。我々の勧告と過去の報告書を受け、国務省は人員とスキルのギャップを特定するために質的な内部評価を実施し、また局設立の提案書を作成するために数カ月にわたるプロセスで、内部および外部の利害関係者とともに証拠とデータに基づくレビューを実施した。データと証拠に基づくレビューを実施することで、国務省の最終提案が意図した結果を達成できることを確認することができた。

既存のサイバー外交戦略

[3]GAO「サイバー外交」参照：国務省はサイバー空間安全保障・新興技術局設立計画の策定に関係連邦政府機関を関与させていない」（GAO-20-607R、ワシントン D.C.：2020 年 9 月 22 日）。

[4]GAO, *Cyber Diplomacy*：*GAO*-21-266R（ワシントン D.C.：2021 年 1 月 28 日）参照。

国務省職員によれば、同省にはサイバー外交の努力を方向付ける単一の統一戦略がない。その代わりに、2023 年国家サイバーセキュリティ戦略、2022-2026 年国務省・USAID 共同戦略計画など、複数の戦略を用いている。その代わりに、2023 年国家サイバーセキュリティ戦略や 2022-2026 年国家と USAID の共同戦略計画など、複数の戦略を用いている。[5]

2023 年 3 月の国家サイバーセキュリティ戦略は、行政府による最新の国家レベルの戦略ガイダンス文書である。国家サイバーセキュリティ戦略は、サイバー外交活動の展開と実施の方向性を示すために利用されている。同戦略は 5 つの柱で構成され、防御可能でレジリエンスが高く、米国の価値観に沿ったデジタル・エコシステムを確保するための協力強化の必要性を強調している。国家サイバーセキュリティ戦略の 5 本目の柱は、責任ある国家行動を促進し、オープンで自由、グローバル、相互運用可能、信頼性が高く、安全なインターネットを維持するための国際的パートナーシップの構築に焦点を当てている。国家のサイバー外交活動は第五の柱に該当する：この柱は、特に連合体の構築、能力の強化、規範の強化などを含む戦略的目標を記述している。この柱は 5 つの戦略目標で構成されている。これらには、デジタル・エコシステムへの脅威に対抗するための連携構築、国際パートナーの能力強化、同盟国やパートナーを支援する米国の能力拡大などの目標が含まれる。2023 年 7 月、ホワイトハウスは国家サイバーセキュリティ戦略実施計画を発表し、米国政府全体の行動を調整するためのロードマップを提供した。実施計画では、国家サイバーセキュリティ戦略に関連するイニシアチブ、担当機関の特定、および完了までの関連スケジュールが説明されている。例えば、実施計画では、国家サイバーセキュリティ戦略の柱 V の 12 のイニシアティブのうち、7 つのイニシアティブの責任機関として国務省を特定している。これらのイニシアティブには、「国際サイバー空間およびデジタル政策戦略」を発表するイニシアティブが含まれるが、国務省当局者によると、これは CDP が主導する進行中の取り組みである。

2022 年 3 月、国務省と USAID は 2022-2026 会計年度の共同戦略計画（JSP）を発表した。この計画は、両組織のビジョンと方向性、そして米国の外交政策と開発援助をどのように実施するかを示している。JSP には、サイバー問題に関するいくつかの戦略目標と実績目標がある。これらには、安定したサイバー空間の促進、米国と同盟国のサイバー脅威能力の強化、米国の技術的リーダーシップと競争力の支援が含まれる。もう一つの目的は、米国が新興技術の最先端を走り続けることを確実にすることである。JSP は、軍備管理局、検証・コンプライアンス局、経済・ビジネス局などの他の事業体と連携して、CDP をこれらの取り組みの主導者に指名している。

[5]2023 年 6 月、国は CDP の機能局戦略を発表し、その戦略的目標と目的を概説し、サイバー外交における国の優先的取り組みを伝えた。

国家は、さまざまな外交・対外援助活動を通じて、サイバー利権の促進に努める。

国務省は、2023 年国家サイバーセキュリティ戦略に示された米国の目標に沿ったさまざまな外交・対外支援活動を実施していることがわかった。本報告書では、外交活動を、サイバー規範、技術標準を確立し、サイバー目標に関する国際的なコンセンサスを構築するために、多国間または二国間の場で行われる活動と定義する。対外援助活動とは、能力構築、信頼醸成措置、その他を含むサイバーおよびデジタル関連のトピックに関する技術支援や訓練を支援する、国から資金提供される活動と定義する（表 1 を参照）。国はまた、これらの活動の一部の影響について報告している。例えば、国家はサイバー犯罪と闘うためのブダペスト条約により多くの国を加盟させるという目標を掲げている。[6]ナイジェリアが最近、2022 年に同条約に加盟したことは、同国に対する国の外交的関与と技術支援の努力の効果の一例であると、国当局者や関連文書は述べている。

表 1：2023 年サイバーセキュリティ戦略目標を支援する米国務省の外交・対外援助活動の例

戦略目標 5.1 デジタル・エコシステムへの脅威に対抗するための連合を構築する

外交活動の例

- 国際安全保障の文脈におけるサイバー空間での責任ある国家行動の促進に関する米国政府専門家グループおよび国際安全保障の文脈における情報通信分野の発展に関するオープンエンド型作業部会に参加する。
- 国連が後援する 2 つの主要なサイバー関連イニシアティブである「安全保障」を支援する。民主主義を強化し、人権を擁護することを目的とした政策および対外支援イニシアティブである「民主主義再生のためのサミット大統領イニシアティブ」に関連する取り組みを支援し、民主主義のためのテクノロジーを推進するイニシアティブを含む。同様に、市民やインフラを危険にさらす新たな脅威に立ち向かうために 81 カ国が支持する公約「パリ・コール」や、自由、革新、信頼を支えるオープンで自由、グローバル、相互運用可能、信頼性が高く安全なインターネットを推進するために 60 カ国以上が支持する公約「インターネットの未来のための宣言」で概説された原則を推進する。
- 米・EU 貿易技術評議会や国際電気通信連合などの組織に参加し、技術標準が米国の価値観に合致していることを確認し、国際標準化活動や戦略的課題に関する自発的な情報共有を支援する。
- フリーダム・オンライン連合（Freedom Online Coalition）は、国連などの場での共同声明を通じて世界的な規範を形成し、コンセンサスを構築してインターネットの自由を推進するために活動する 37 カ国のグループである。

対外援助活動の例

[6] ブダペスト条約は、コンピューター関連犯罪に対処するための多国間条約である。この条約は世界的な性格を持ち、2001 年にすべての国に署名が開放された。現在の締約国は 68 カ国である。

- 欧州評議会が主導するオクトパス・プロジェクトを支援し、各国の国内サイバー犯罪および電子証拠法制をブダペスト条約の標準と整合させ、国際的なサイバー犯罪協力を推進するための研修と技術支援を提供する。
- 米国、欧州、アジア、コスタリカの協力を得て、安全で信頼できるインフラのためのコスタリカの青写真をどのように自国の市場に適応させることができるかについて、ラテンアメリカのパートナーに情報を提供し、協力体制を構築するための専門家によるワークショップを実施する。

戦略目標 5.2 国際パートナーの能力強化

外交活動の例

- ウクライナとの二国間対話に参加し、ウクライナのサイバー防衛を支援するという米国のコミットメントを再確認する。

対外援助活動の例

- 司法省と提携し、国際的なサイバー犯罪協力を強化するグローバル法執行ネットワークの活動を支援する。
- デジタル・コネクティビティ・サイバーセキュリティ・パートナーシップの活動に参加し、発展途上国に技術支援やトレーニングを提供している。

戦略目標 5.3 同盟国やパートナーを支援する米国の能力を拡大する

外交活動の例

- 批准されれば、サイバー犯罪と闘うための国際協力を促進することになる国連サイバー犯罪条約の交渉プロセスを支持し、関与する。

対外援助活動の例

- 米州機構加盟国のサイバーセキュリティ能力を強化するため、サイバーレジリエンス活動を支援する。

戦略目標 5.4 責任ある国家行動の世界的規範を強化するための連合を構築する

外交活動の例

- 法律の調和、証拠収集の標準化、加盟国間のサイバー犯罪に関する法執行協力の強化を目的とするブダペスト条約の原則を支持し、推進する。
- コペンハーゲンの「民主主義のための技術に関する誓約」を支持し、デジタル・フリーの優先事項と責任ある技術利用を促進する。

対外援助活動の例

- 参加者を教育し、サイバー外交の行動規範を確認するため、ジョージ・C・マーシャル・センターを通じてサイバー法と国際法のコースに資金を提供する。

戦略目標 5.5 情報・コミュニケーション・運用技術製品および供給品のグローバル・サプライチェーンを確保する。

外交活動の例

- ブロードバンド携帯電話ネットワークの第 4 世代および第 5 世代技術標準である安全な 4G および 5G ネットワークの開発を促進することに合意するアルバニアとの二国間覚書に署名する。

対外援助活動の例

- 5G や次世代通信ネットワークの安全確保に取り組んでいる国々を対象とした 5G セキュリティキャンペーンを支援し、信頼できないベンダーに対する認識を高める。
- 安全な 5G 配備を支援するため、コスタリカと二国間で関与する。

多国間フォーラムや協定における国家の外交的関与は、責任ある国家行動の規範を促進することを目的としている。

国家は、責任ある国家行動の規範を強化し、容認できない国家行動を抑止し、米国の目標に沿ったサイバー政策を推進するために、多国間フォーラムに参加し、多国間協定を支援している。加盟国が承認した責任ある国家行動を強化するために、CDP は国連などの多国間組織と協力する責任があると、加盟国当局は我々に語った。

国際安全保障の文脈におけるサイバー空間での責任ある国家行動の促進に関する 2021 年国連報告書」は、規範とは国際社会の期待を反映するものであり、国際法に合致した責任ある国家行動の標準を定めるものであると説明している。[7]例えば、2021 年国連報告書には、安定性を高め、国際安全保障を脅かす可能性のある行為を防止するための情報通信技術政策の強化などの措置の策定と適用において、各国が協力することを求める規範が盛り込まれている。同報告書はまた、情報通信技術の悪用から生じる紛争を防ぐために、各国が協力を促進するための政策を強化するよう勧告している。国務省の担当者は、ルール違反者に対して結果を強制することを含め、このようなサイバー規範を確立することで、サイバー空間における悪行の代償を高め、不正行為を抑止することができると語っている。

国家は多国間フォーラムで協力体制を築き、サイバー目標に沿った規範を強化する。

米国は、（1）米国のデジタル・エコシステムに対する脅威に対抗し、（2）責任ある国家行動の世界的規範を強化するために、米国の戦略的目標を共有する国々の連合体構築に取り組んでいる。例えば、オープン、フリー、グローバル、相互運用性、信頼性、安全性の高いインターネットを推進する政策を調整するために、米国の目標を共有する国々を結集している。具体的には、サイバー空間における責任ある国家行動の促進に関する国連政府専門家グループ（GGE）や、情報通信に関するオープン・エンド・ワーキング・グループ（OEWG）とのコンセンサス・レポートの作成において、同省は世界各国の代表団をリードしたと CDP 関係者は述べている。[8]GGE と OEWG は、サイバー空間における米国の利益を促進するために、国が参加している 2 つの主要な国連主催のサイバー関連イニシアチブである。CDP 関係者によると、GGE と OEWG のこれらの合意報告書は、作成された最も重要なサイバー協定とみなされている。

GGE と OEWG から得られたコンセンサス・リポートは、国家の責任ある行動に関する国際規範の強化に関連する米国の目標を前進させるのに役立っていると、関係者は我々に語った。例えば、GGE のコンセンサス・レポートは、サイバー空間へ

[7] 国連文書。A/76/135 「国際安全保障の文脈におけるサイバー空間での責任ある国家行動の促進に関する政府専門家グループ」。2021 年 7 月 14 日。国連政府専門家グループ（GGE）は 2004 年以来 6 回開催され、2010 年、2013 年、2015 年、そして最近では 2021 年に 4 つのコンセンサス・レポートを作成した。2015 年の GGE 報告書では、サイバー空間における国家の行動に関する 11 の自主的規範が列挙され、2021 年の GGE 報告書では、採択された勧告、規範、サイバー空間における国家の責任ある行動のための原則の枠組みがさらに定義された。このコンセンサス報告書は、サイバー空間における責任ある国家行動の枠組みを定義し、サイバー空間における国際法の適用可能性など、これまでの GGE コンセンサス報告書の結論を再確認するものである。

[8] 国連 OEWG の最初の会合は 2019 年から 2021 年まで開催され、GGE と並行して進められた。OEWG は GGE が策定した規範を支持し、途上国を含む各国がサイバー規範を策定・普及するための、より包括的なフォーラムを提供した。2020 年、国連総会は情報通信技術の使用に関する 5 年間の新たな OEWG を設置した。2021 年から 2025 年にかけての OEWG の任務は、責任ある国家行動のルール、規範、原則をさらに発展させ、データセキュリティ、信頼醸成措置、キャパシティ・ビルディングをさらに研究するとともに、そうした措置についての共通理解を促進すること、などであった。

の国際法の適用可能性を確立し、責任ある国家行動の規範の枠組みを確立した。同様に、OEWG は GGE に書かれた自主的な規範を再確認し、さらに各国がインターネットの一般的な可用性と完全性を確保するよう努めることを確認した。

国はまた、技術標準がコンセンサスに基づき透明性のある方法で開発されることを確実にするために、多国間の技術標準設定団体に参加している。例えば、貿易技術評議会（TTC）を通じて EU と協調し、国際標準化活動に関する情報を共有する仕組みを構築している。CDP はまた、情報通信技術の安全保障と競争力に関する TTC 作業部会を通じて、重要技術や新興技術に関して TTC と協力している。CDP は、信頼できる電気通信サプライヤーのためのアドボカシー活動や、6G のための共有原則の策定に関して欧州委員会と連携している。[9]これらの活動は、技術要件の標準化に向けて、透明性のある民間主導のコンセンサスに基づくアプローチを強化するものである。

国家は、サイバー空間における責任ある行動の規範を確立または強化するための多国間協定を支持する。

国際電気通信連合（ITU）の事務総長に米国人が選出されたことで、トップダウンの権威主義的な標準設定アプローチとは対照的に、オープンで相互運用可能なインターネットおよび電気通信政策のコンセプトを維持することができたと、政府関係者は語った。ITU のような標準設定団体に米国や志を同じくする国々から職員を選出することは、ITU をより強く、より効果的で、米国の目標に沿ったものにするための改革を実施することで、私たちのデジタル・エコシステムへの脅威に対抗する一助となる。

2011 年、国務省の民主主義・人権・労働局（DRL）は、インターネットの自由に関するコンセンサスを構築し、注目を集めるための多国間フォーラムであるフリーダム・オンライン連合（FOC）を設立した。国務省職員によれば、米国は 2023 年に FOC の議長国を引き継ぎ、米国の目標やイニシアチブを推進するために外交ネットワークを活用するという。DRL の職員は、FOC は決議案について統一戦線を組み、国連など他の場で使用する文言を開発したと述べた。CDP の関係者は、関連する問題領域で DRL と協力し、特定の業務について専門知識を提供することで支援を提供することもあると述べた。例えば、2022 年秋の広範な抗議行動におけるイランのインターネット閉鎖を非難する FOC 共同声明の採択交渉は、国務省が主導した。国家の行動に責任を持たせ、その行動に結果を課すことで、国家の責任ある行動規範を強化するという戦略目標に合致している。

国家は、米国の目標を共有する国々や産業界、学界、市民社会と協力することにより、原則、規範、戦略的目標を推進するために多国間協定を利用している。国務省の報告によると、交渉への参加は、多国間協定の範囲、内容、効果を形成するのに役立っている。例えば、国務省国際麻薬・法執行局（INL）は、現在も進行中の国連サイバー犯罪条約の交渉では、コンセンサスに基づく意思決定が守られ、米国の慣行と一致する世界的な規範や標準の採用に役立つ可能性があると報告している。

国務省の当局者によれば、国務省が国際社会をリードし、国連に加盟している国同士のイニシアチブを受け入れ、肯定しているという。過去 10 年にわたって策定されたこのイニシアチブは、「サイバー空間における国家の責任ある行動のための枠組み」（フレームワーク）と呼ばれている。フレームワークは、国連 GGE で確立され、OEWG のコンセンサス報告書で再

[9]6G は、5G の後継となる無線通信ネットワークで、2030 年の開始が見込まれている。6G は、5G に比べて拡張性が強化され、無線スペクトラムの利用が拡大し、さまざまな接続タイプにダイナミックにアクセスできるようになる。これにより、ドローンやロボットなどの先端技術をサポートするのに不可欠な、より高い信頼性と接続の低下を減らすことが可能になる。

確認された一連のサイバー規範である。フレームワークは、国際法、デジタル領域で国家が何をすべきで、何をすべきでないかを定める自主的規範、透明性、予測可能性、安定性を強化する信頼醸成措置という 3 つの柱で構成されている。これらの柱は、責任ある国家の行動に関する世界的な規範を強化し、国際的なパートナーの能力を強化するという戦略目標に沿ったものである。加盟国がフレームワークを理解し、実施するのを引き続き支援する予定であり、フレームワークを支援することが引き続き重要な優先事項であると、加盟国は我々に語った。

また、欧州評議会の「サイバー犯罪に関するブダペスト条約」への加盟を促進する活動も行っている。この条約は、法律を調和させ、証拠収集を標準化し、加盟国間の協力を強化することを目的としている。これらの概念は、条約に記載された標準を加盟国に課すことにより、世界的な規範を強化するという戦略的目的に合致している。国/INL は、発展途上国の条約加盟を支援する欧州評議会サイバー犯罪事務所への資金提供など、技術面やその他の支援を行っている。また、たとえ条約に加盟していない国であっても、条約の規定に沿った法律を制定するよう各国に働きかけているという。国家はサイバー外交の進展を評価する指標の一つとして、条約の加盟国数を追跡している。ナイジェリアが 2022 年に同条約に加盟したことは、INL の外交的関与と技術支援の努力の効果を示す一例であると、国/INL 関係者は述べた。同条約は普遍的な批准に近いものではないため、どの国も加盟を決定することは重要であると、国務省職員は我々に語った。

2019 年 12 月、国連はサイバー犯罪条約交渉のための専門家による特別委員会の設置を議決した。[10]国務省/INL は、他の米国機関のサイバー犯罪政策、技術、法執行の専門家とともに、米国の省庁間の取り組みを主導し、交渉に関与し、影響を及ぼす。交渉プロセスの調整を担当する国連委員会は、コンセンサスに基づく文書の作成を目指し、2024 年初頭までに最終的な文言を決定する予定である。サイバー犯罪条約の制定に向けた努力は、同盟国やパートナーを支援する米国の能力を拡大し、責任ある国家行動の世界的規範を強化するという戦略目標に沿ったものである。国務省職員は、交渉の努力は合意に基づく意思決定を守ることを優先し、米国の利益と慣行に沿った世界規範の採用を推進するのに役立つと報告している。

国家は、米国のサイバー目標を推進するため、2018 年パリ・コールや 2022 年インターネットの未来のための宣言など、様々なイニシアティブに参加した。パリ・コールは、サイバー空間の安全を確保するための 9 つの原則で構成されており、署名者は、国家、民間セクターのパートナー、市民社会など、サイバー空間における責任ある行動を採用するために支援し、協力することを約束する。国務省によると、「インターネットの未来のための宣言」は、オープンで、競争、プライバシー、人権の尊重を促進するインターネットを実現するために、60 カ国以上が署名国に約束する政治的コミットメントである。国務省職員は、これらのイニシアチブを支援する活動は、フレームワークに対する米国のコミットメントを強化し、国際的な立場を一致させ、オープン、フリー、グローバル、相互運用性、信頼性、安全なインターネットを目指す米国のサイバー目標を推進するための声明や外交努力を調整することで、世界的な知名度やパートナーシップを高めると述べた。国務省当局者によると、同省は「インターネットの未来のための宣言」を起草し、国際的なパートナーの賛同を得る上で重要な役割を果たしたという。また、このイニシアチブは、これらの原則を支持する志を同じくする国際的な支持を構築し、米国の目標を推進するためのプラットフォームとしての役割を果たすと述べた。

[10] 10A/Res/74/247（2019 年 12 月 27 日）。

同様に国家は、民主主義の強化、権威主義からの擁護、汚職との闘い、人権の促進に重点を置く、民主主義のためのサミットと、関連する「民主主義再生のための大統領イニシアティブ」[11] を支援している。例えば、民主的価値観とガバナンスに有利な技術革新を奨励するという大統領イニシアチブの公約を支持し、政府は 2022 年 12 月に、民主主義を支援する技術開発をイノベーターに奨励するイベントを共催した。

米国は二国間で連携してサイバー規範と政策を推進する

国務省はまた、米国の利益を促進し、サイバー空間におけるグローバルなコンセンサスを支援するために、多くの継続的な二国間活動を維持している。CDP は、政府間サイバー・ダイアログのような活動を通じて、望ましい成果を達成するための二国間外交を促進していると、国務省職員は我々に語った。国務省職員によると、このような関与は、共通の政策成果を達成するための集団的戦略に関する世界的な協調を促すという。例えば、2022 年にはデンマークと協力して、世界中のデジタル権威主義に対抗し、デジタルの自由を促進する「民主主義のための技術に関するコペンハーゲン誓約」（誓約）を推進した。最初の二国間努力に続き、この誓約は 100 カ国以上の市民社会組織、民間事業体、政府からなる署名者を集め、責任あるテクノロジーの使用に関する米国の承認した目標と価値を推進した。これらの努力は、デジタル権威主義などのデジタル・エコシステムに対する脅威に対抗するための連合を構築するという戦略的目標に沿ったものである。

2021 年 6 月、米国とアルバニアは、協力関係を強化し、安全な 4G および 5G ネットワークの開発を促進し、それらのネットワークを敵対勢力から保護することに合意する覚書を締結した。覚書では、信頼できないベンダーが開発した 5G ネットワークを使用すると、相互運用性や情報共有の機会に悪影響を及ぼす可能性があるとし、既存のネットワークで信頼できない情報通信技術を使用しないよう奨励している。国務長官は、このパートナーシップは、機密技術について信頼できるベンダーと協力することの重要性について、この地域に強い模範を示したと述べた。この取り組みは、敵対する政府から影響を受ける可能性のある技術による米国の国家安全保障への過度なリスクを防ぐため、5G ネットワークにおいて信頼できるベンダーへの移行を奨励することで、情報・コミュニケーション・運用技術製品およびサービスのグローバル・サプライチェーンの安全を確保するという戦略目標に沿ったものである。

2023 年 6 月、米・ウクライナ・サイバー・ダイアログが開催された。この対話の中で、国務省はウクライナのサイバー防衛を支援し、サイバー事件や脅威を検知、抑止、対応するウクライナの能力を強化することを再確認した。このウクライナ支援へのコミットメントの一環として、ウクライナに対する 3700 万ドルのサイバー支援を発表した。これらの取り組みは、国際的なパートナーの能力を強化するという戦略目標に沿ったものである。

対外援助活動の目的は、トレーニングや技術支援による協力の強化とサイバー・レジリエンスの構築である。

[11] サミット・フォー・デモクラシーは、権威主義を擁護し、腐敗と闘い、人権尊重を推進することを目的とした、米国主催の一連のバーチャル・サミットである。ホワイトハウスは 2021 年 12 月に第 1 回サミットを、2023 年 3 月に第 2 回サミットを開催した。

第 1 回民主主義サミットにおいて、ホワイトハウスは「民主主義再生のための大統領イニシアティブ」を発表した。このイニシアティブは、志を同じくする政府や非政府のパートナーとともに、民主主義のレジリエンスを維持し、成長させる努力を拡大することによって、世界的に民主主義を支援し、人権を擁護する政策および対外援助のイニシアティブで構成されている。

国務省は、パートナーの能力を強化し、確立されたサイバー規範を促進するために、訓練や技術支援などの対外援助をプロバイダとして提供している。CDP は、フレームワークに沿った行動を強化したり、パートナー国がサイバー規範を理解するのを助けたりするなど、米国のサイバー政策目標の達成を支援するために、適切なプログラムをパートナー国に提供する取り組みを主導していると、国務省職員は我々に語った。また、米国のサイバー政策目標に沿ったサイバーセキュリティのベストプラクティスを促進する技術支援活動を支援するための資金もプロバイダとして提供している。例えば、ドイツ系米国人の安全保障・防衛教育機関であり、相手国間の理解を促進するジョージ・C・マーシャル・センターとの提携により、サイバーセキュリティの能力構築と国際法に関する一連の訓練コースに資金を提供した。同センターに外国の専門家を招き、フレームワーク、平和規範、サイバー攻撃帰属などの概念について教育・解説を行った。研修コースではサイバーセキュリティの問題が取り上げられ、参加者は複雑な技術的・政策的トピックに対処するためのスキルやベストプラクティスに触れた。

2021 年 5 月、同センターは 17 カ国の政府から 39 人のサイバーセキュリティ・リーダーを招き、悪意あるサイバー活動の加害者を集団的に帰属させる方法に関する初のコースを開催した（図 1 参照）。国務省職員は、集団的帰属は報復の可能性を減らし、申し立ての完全性を強化し、告発された国からの否定の信憑性を減らすのに役立つと述べた。国務省職員によれば、このコースは、政策手段としての公的帰属についての理解を深めることによって、サイバー脅威に協力的に対応する外国パートナーの能力を強化することを意図したものであり、脅威行為者の責任を追及するために悪意のあるサイバー活動を帰属させることの重要性を強調したものであった。このコースと国の継続的な訓練努力は、サイバー空間に関連する国際パートナーの能力を強化するという戦略目標に沿ったものである。

図 1：ジョージ・マーシャル・センターで行われた、世界のサイバーセキュリティ・リーダーを対象とした国務省サイバー外交トレーニングの発表資料

Source: Department of State. | GAO-24-105563

司法省との協力の下、国務省/INL は、米国国際ハイテク犯罪グローバル法執行ネットワーク（GLEN）への資金提供を通じて、研修や技術支援によりサイバー犯罪や知的財産の窃盗と闘う取り組みを支援している。GLEN は、知的財産やサイバー犯罪と闘うために、外国の法執行機関や司法のパートナーに訓練や技術支援を提供し、国際組織犯罪を含むあらゆる犯罪と闘うための電子証拠の収集と使用に関するスキルを構築し、緊急の支援と長期的な機構改革を促進するための的を絞った支

援を提供している。国務省職員は、GLEN を通じて提供される技術支援は国際協力を強化し、サイバー犯罪の能力開発を外国の司法当局者に提供し、現場で活用してもらうものであると報告した。例えば、GLEN を支援する資金の一部は、ランサムウェアの脅威への対処を支援するため、地域の暗号通貨ワーキンググループの拡大を促進したと、国は報告した。以前にも報告したように、国務省と司法省は、GLEN を通じて外国の法執行機関パートナーに地域ワークショップなどのトレーニングを提供するなど、外国のサイバー犯罪対策能力を高めるためのさまざまな活動を行っている。[12]

国/INL 当局者はまた、技術支援はサイバー犯罪と闘うための法の支配に基づくアプローチを促進し、ブダペスト条約などの既存のサイバー犯罪関連文書の価値を強調すると報告した。2007 年から 2019 年にかけて、GLEN の構成要素である国際コンピュータハッキング・知的財産（ICHIP）弁護士アドバイザーの数は 1 人から 12 人に増加した。[13]GLEN を通じ、ICHIP 弁護士アドバイザーは、研修ワークショップ、立法審査、能力開発などを通じて研修や技術支援を提供することができる。ICHIP 弁護士アドバイザーを派遣することで、パートナー国との協力・調整を強化することができる。また、GLEN は警察当局との関係を強化し、国際的なサイバー犯罪の協力と取り締まりを強化するのに役立つと、国家当局は述べている。これらの活動は、国際的なパートナーの能力を強化し、技術アドバイザーによる訓練や支援を通じて法執行能力と有効性を高め、国際的なサイバー犯罪協力を進めることによって、脅威に対抗するための連合を構築するという戦略目標に合致している。[14]

State/INL は、2014 年に設立された欧州評議会のサイバー犯罪プログラムであるオクトパス・プロジェクトに資金を提供しており、発展途上国の法律をブダペスト・サイバー犯罪条約に合致するよう強化している。このイニシアチブは継続中で、途上国が条約への加盟を要請できるよう、研修や技術支援を提供している。このような対外援助を提供することは、各国が必要なインフラ防御を導入するのに役立つと、国務省関係者は述べている。このイニシアチブは、発展途上国が自国の法律を条約加盟に必要な標準に合わせることができるよう、政策助言、訓練、技術支援を提供することにより、国際パートナーの能力を強化するという戦略目標に沿ったものである。このプログラムを支援している間に、条約の締約国は 40 カ国から 68 カ国に増えたと国は報告した。

米州は、米州機構（OAS）加盟国の全体的なサイバーレジリエンスを改善し、関係者間の協力と協調を強化する取り組みを通じて、サイバー能力構築の強化を支援している。米州政府高官は、サイバーセキュリティ問題に関する OAS 作業部会議長として、CDP は OAS と協力し、サイバーセキュリティ対策に関する地域対話を構築していると述べた。例えば、国務省

---

[12] GAO, *Global Cybercrime* : *Federal Agency Efforts to Address International Partners' Capacity to Combat Crime*, GAO-23-104768, (Washington, D.C.: Mar 1, 2023)を参照。

[13] ICHIP プログラムは、海外に弁護士を派遣し、法執行当局の能力評価、研修の開発・実施、機構の構築・強化、地域動向の監視を行っている。

[14] 2023 年 3 月、われわれは国務省、司法省、国土安全保障省がサイバー犯罪と闘う国際的なパートナーの能力を構築するために行っている取り組みと、これらの取り組みに対する主要な課題について報告した。これらの協力活動には、現在の脅威に関する情報を海外のパートナーと共有することや、海外の法執行機関にサイバー・トレーニングを提供することなどが含まれていた。しかし、対外援助を担当する主要機関として、国務省はこれらの活動が外国のサイバー犯罪対策に効果的であったかどうかを十分に評価していなかった。我々はそうするよう勧告した。国はこの勧告に同意し、今後取るべき行動を識別した。われわれの勧告は、国がこれらの行動を完了するまで、未解決のままである。詳細は GAO-23-104768 を参照されたい。

職員は、OAS 信頼性対策作業部会の現在の議長であると述べた。その後、加盟国と OAS は、サイバー規範に関する既存の協定に従った実際的な措置の実施に取り組むと、国当局は述べている。

国はまた、信頼醸成措置の策定に情報を提供するために、サイバー脅威に関する知識や情報へのアクセスを増やすことを意図した能力構築プロジェクトへの資金提供などの活動を通じて OAS を支援していると報告した。OAS のプロジェクト提案報告書は、サイバーレジリエンスの改善は、オープンで自由、グローバル、相互運用性、信頼性、安全性の高いインターネットという重要な信条を推進することで、能力構築という米国のサイバー目的を支援すると述べている。[15]OAS は、米国の援助が地域パートナーのサイバー能力を強化し、サイバー問題に関する合意形成を支援すると報告した。

政府がガバナンスを主導し、USAID が共同議長を務めるデジタル・コネクティビティ・サイバーセキュリティ・パートナーシップ（DCCP）は、オープンで相互運用性が高く、安全で信頼性の高いインターネットを推進するための、政府機関全体のグローバルなイニシアティブである。国は DCCP の活動に資金をプロバイダしており、DCCP は国際パートナーの能力を強化するという戦略目標に合致している。DCCP は、(1)包括的でマルチステークホルダーなインターネット・ガバナンス・モデルの推進、(2)レジリエンスな情報通信技術インフラへの投資の促進によるコネクションの構築、(3)サイバーセキュリティのベストプラクティスの導入と実施の促進によるサイバーセキュリティの強化によって、デジタル・エコシステムへの脅威に対抗している。

DCCP はまた、国際パートナーの情報通信技術エコシステムの強化に関連する対外援助活動も管理しており、これは 2022 年 CHIPS（Creating Helpful Incentives to Produce Semiconductors）法によって設立された国際技術安全保障・イノベーション基金の一部によって支援されている。[16]CDP 関係者によると、これらの資金の取得者として、CDP は志を同じくするパートナーを支援するため、サイバーとデジタルに焦点を当てた対外支援を大幅に強化することができたという。

国務省職員によると、このパートナーシップのプログラムは、国務省が支援するサイバー関連の対外援助活動のかなりの部分を占めている。USAID 当局者によると、2019 年 9 月から 2024 年 9 月まで実施されるデジタル・アジア・アクセラレータ（DAA）プログラムは、米国のテクノロジー企業のノウハウと現地組織の専門知識や文脈的知識を活用した、特に成功した DCCP 活動であるという。DAA は、オープンで相互運用性があり、信頼性が高く、安全なインターネットを推進し、サイバーセキュリティを向上させるという目標を支援するために設計されたもので、デジタル・セーフティの実践を改善し、東南アジアの利害関係者がデジタル経済政策の問題に関与する能力を高め、主要な聴衆にリーチするためのさまざまな形態のプログラミング・ツールを開発した。関係者の報告によると、プログラミング活動を通じて 24,500 人がデジタル・スキルに関するトレーニングを修了し、プログラムによって 230 万人以上がデジタル・セーフティに関する情報にアクセスできるようになった。

国家はまた、二国間ベースで対外援助を提供している。例えば、コスタリカの 5G 展開のためのデジタルインフラと機器のアップグレードを支援するため、国は技術的助言、指導、関与を行った。国務省職員は、リソースと関与により、信頼でき

---

[15] 米州機構対テロ米州委員会サイバーセキュリティ・プログラム。米国は *OAS* 加盟国のサイバーセキュリティ能力を継続的に強化するための支援を行う。2021 年 8 月

[16] パブ.L. No. 117.167, Div. A, § 102(c), 136 Stat 1375 (Aug. 2022).この基金は、安全で信頼できる電気通信ネットワークの開発と採用を促進し、半導体のサプライチェーンの安全性と多様化を確保するため、2023 会計年度から 5 年間にわたり毎年 1 億ドルずつ、5 億ドルを国務省にプロバイダするものである。

る電気通信ベンダーとの契約が成功することを期待していると述べた。この取り組みは、情報・コミュニケーション・運用技術製品および供給品のグローバル・サプライチェーンの安全確保という戦略目標に沿ったものである。

さらに、2023 年 3 月、政府は、コスタリカの政府ネットワークに対するランサムウェア攻撃が 1 年にわたり繰り返され、医療、徴税、税関などの重要なサービスに影響を与え、国家非常事態に至ったことを受け、悪意ある行為者からの脅威に対するコスタリカのサイバー防衛を強化するため、2500 万ドルのサイバーセキュリティ支援パッケージを発表した。この資金は、サイバー脅威を監視、防止、検知、調査、対応するための集中型セキュリティ・オペレーションセンターの設立と装備、サイバーセキュリティ訓練業務、サイバーセキュリティ・ツール、長期的な能力構築のための当面の支援を提供することを目的としている。この支援は、サイバー攻撃を調査、対応、復旧するパートナー国の能力を支援することにより、同盟国やパートナーを支援する米国の能力を拡大するという戦略目標に沿ったものである。

政府関係者によると、専門知識を活用し、見識を広め、政府全体として対外援助活動を実施するために、非公式な調整努力に加えて、正式な省庁間協定（IAA）を通じて他の省庁とも協力している。CDP は現在、商務省、内務省、国防総省、国土安全保障省（DHS）、連邦コミュニケーション委員会を含む 11 のサイバー関連 IAA を管理している。[17]これらの協定は、キャパシティビルディング、技術支援、訓練の促進に重点を置いている（表 2 参照）。例えば、商務省との IAA は、ガイダンス、専門知識、技術支援を提供することで、信頼できないベンダーの認識を高めるための、国務省のグローバル 5G セキュリティキャンペーンを支援することに重点を置いている。具体的には、商務省は、5G セキュリティ関連の様々なトピックや国家安全保障法制に関するベストプラクティス・ガイドや二国間技術支援を提供する。これらの活動は、情報・通信・運用技術製品や供給品のグローバル・サプライ・チェーンを確保し、5G セキュリティを推進することで、オープンで相互運用可能かつセキュアなインターネットを提唱するという戦略目標に沿ったものである。

表 2：表：米国務省サイバー空間・デジタル政策局が管理するサイバー外交関連の省庁間協定一覧

行政機関	プログラム概要	資金調達予定額	履行期間
商務省	米国が開発したサイバーセキュリティのベストプラクティスとフレームワークの適用と導入に ついて、外国の民間政府、外国の産業界パートナー、その他の外国の民間利害関係者を適宜関与 させる。このプログラムの目標は、米国の整合的なフレームワークやガイドラインを検討し、持続的に採用する可能性を通じて、自国および地域のサイバーセキュリティを構築するためのパートナー国の能力と能力を開発し、支援することである。	$20,000,000	09/23/2020-9/30/2025

[17] サイバー空間・デジタル政策局が管理する省庁間協定に加え、他の局もサイバー活動に関連する省庁間協定を管理することがある。

表 2：表：米国務省サイバー空間・デジタル政策局が管理するサイバー外交関連の省庁間協定一覧

行政機関	プログラム概要	資金調達予定額	履行期間
商務省	世界中でデータの流れを可能にする一貫性のある包括的なアプローチの作成を支援するソフトウェアツールの開発を促進する。この取り組みはまた、プライバシーを保護するための相互運用可能なアプローチの採用を支援するために働く。	$1,250,000	09/30/2019–09/30/2023
商務省	国務省の 5G セキュリティキャンペーンを支援するため、法律および規制に関するアドバイスを提供する。商務部は、ベストプラクティス、国家安全保障法制、通信ネットワークにおける信頼できないベンダーの禁止措置に関する助言と情報提供で国務省を支援する。	$2,250,000	09/24/2020–09/30/2023
商務省	西半球問題地域における安全保障インターネットと情報通信技術開発に関する国務省のアドボカシー活動を支援するため、指導、専門知識、分析、技術支援を提供する。	$1,645,000	09/24/2020–09/30/2023
国防総省（DOD）	各国政府および地域の関係者が、民間ネットワークやインターネット通信インフラに対するサイバーセキュリティの脅威に対処する能力を改善する。	$50,000,000	10/01/2015–08/30/2025
国防総省	上級・中級レベルのサイバーセキュリティ戦略、政策、意識に関する教育を、ワークショップやセミナーなどの常駐コースやアウトリーチイベントを通じて、パートナー国政府の参加者に提供し、現在および新たなサイバー脅威に対する理解を向上させ、緩和戦略や政策解決策を策定し、立法や規制の改善に影響を与える。	$20,000,000	10/01/2017–09/30/2025
国土安全保障省 (DHS) - サイバーセキュリティ・インフラセキュリティ庁 (CISA)	産業制御システムのサイバーセキュリティ能力を強化するためのトレーニングとリソースを提供する。この能力は、既存のネットワークを防御し、サイバー脅威を早期に検知し、サイバーイベントをより効果的に分析する能力に焦点を当てる。	$1,400,000	09/30/2020–09/30/2023

表 2：表：米国務省サイバー空間・デジタル政策局が管理するサイバー外交関連の省庁間協定一覧

行政機関	プログラム概要	資金調達予定額	履行期間
DHS - CISA	対象国の重要インフラ保護能力を構築し、国際環境におけるサイバーセキュリティ問題への取り組みを支援するとともに、同盟国や同様の考えを持つ国々の取り組みを支援する。	$500,000	09/30/2021–09/29/2026
連邦コミュニケーション委員会（FCC）	DCCP の目標や 5G キャンペーンを直接支援する会議、技術協議会、研修、その他の活動に参加する FCC 職員の出張を支援する。	$75,000	07/21/2020–09/30/2023
内務省	請負業者は、DCCP のモニタリングと評価の枠組みが、プロジェクトのスケジュールや、目標、範囲、成果物を定義するプロジェクト憲章を持つなど、国務省のプログラム設計方針に準拠していることを確認する。	$1,047,468	09/30/2021–09/30/2022
米国国際開発庁	世界的なサイバーセキュリティ能力構築のニーズに対応し、改善する。このプログラムは、サイバー空間とデジタル政策におけるパートナー国の能力と能力を開発し、支援することを目的としている。	$3,100,000	10/01/2022–09/30/2024

出典国務省による省庁間協定。 | GAO23-105563

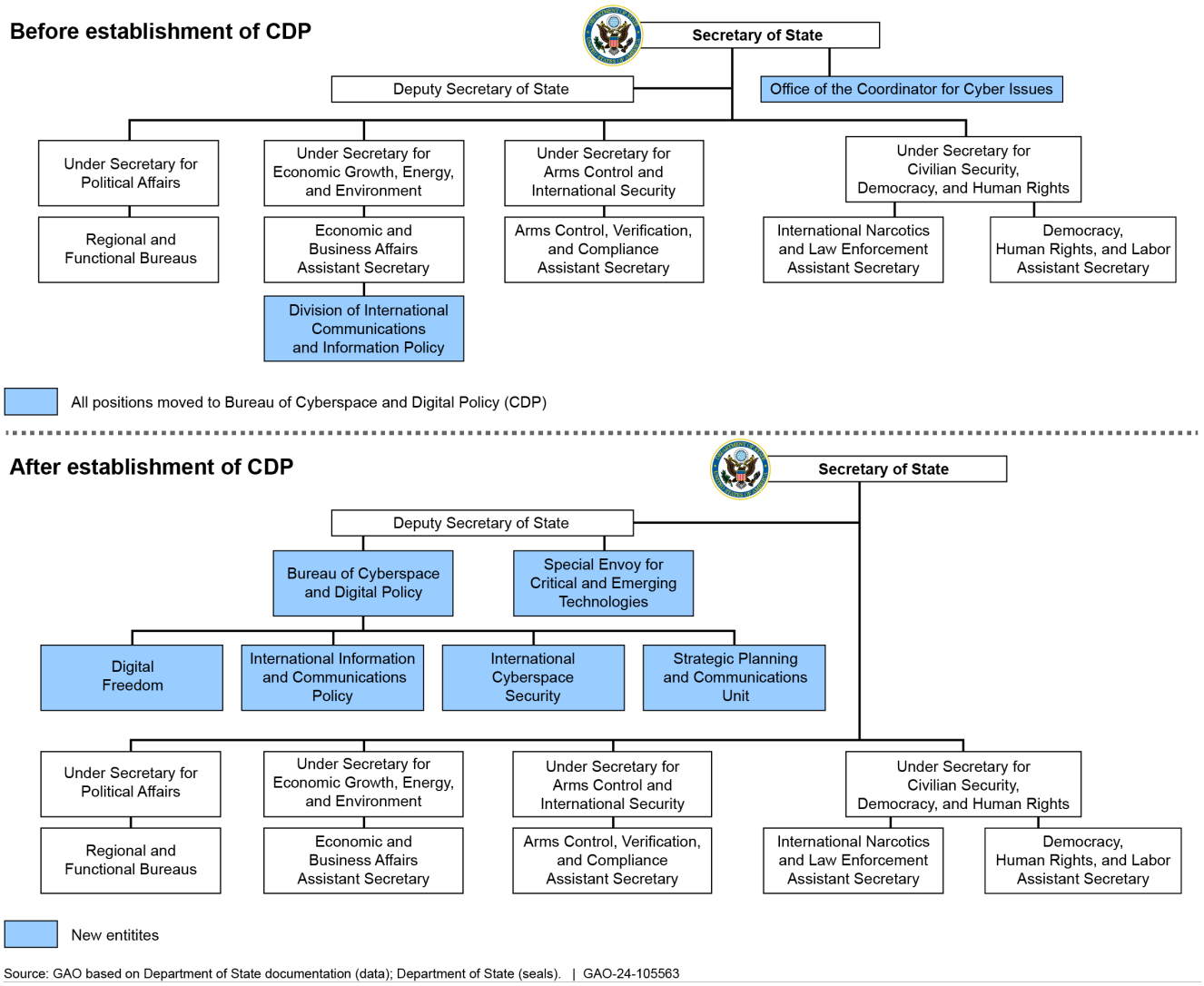
注：この表は、サイバー空間・デジタル政策局が管理する省庁間協定のみを代表者としている。他の局もサイバー活動に関連する省庁間協定を管理している可能性があるが、ここでは報告していない。

国務省の改革努力は、サイバー外交の目標を高め、先進的な慣行と一致させるのに役立った。

国務省、サイバー外交を優先する新局を設置

2022 年 4 月、国務省はサイバー空間・デジタル政策局（CDP）を新設し、サイバー空間、デジタル技術、デジタル政策に関連する国家安全保障上の課題、経済的機会、米国の価値観への影響に取り組むことを使命とした。米国は、サイバー空間関連活動の努力と指導力を一元化することで、サイバー空間を米国外交の組織的コンセプトとして高めるため、上院で承認された特命大使を長とする CDP を創設した。関係者によれば、これまで国務省はサイバー問題調整官事務所（S/CCI）やその他の事業体にサイバー問題の責任を分散させていた（図 2 参照）。

図 2：サイバー外交体制の統合を反映した国務省組織図の要素



Source: GAO based on Department of State documentation (data); Department of State (seals). | GAO-24-105563

サイバー空間・デジタル政策担当特命全権大使は、国務省の上級管理職の中でサイバー空間政策を担当する最高責任者であり、国務長官のサイバー空間・デジタル問題に関するアドバイザーでもある。

国務省関係者によれば、CDP がハイレベルの指導者を擁する局レベルの事業体として設立されたことで、サイバー外交の重要性が浮き彫りになったという。例えば、ある認可当局は、サイバー問題に関する大使レベルのリーダーシップと権限ができたことで、より高いレベルの外国政府高官との関与が可能になり、サイバーに関する米国の世界的な知名度が高まったと語った。就任以来、大使はサイバー目標の推進に関して様々な国の上級指導者と関わってきた。一例として、大使は 2023 年 8 月、ベンガルールで開催された G20 デジタル経済閣僚会合に米国代表団を率いて出席し、インドの G20 議長国が設定した優先分野を含むデジタル経済のトピックに関する米国の見解を強調するとともに、技術起業家や産業界、市民社会の代表者らと会談した。

さらに、CDP が局としての地位を得たことで、以前には存在しなかった上級レベルの支援、リソース、関与が提供され、国務省内でのサイバー問題の地位が強化された。例えば、国務省高官によれば、CDP の設立により、サイバー政策問題に対す

る認識と技術的リテラシーが内部で高まり、国務省全体のサイバー問題に対する発言力と正当性が高まったという。CDP の責任者によると、2023 年に世界各国の駐在大使が集まる年次首席公使会議でサイバーに関するセッションが行われたが、完全に満席になったという。国務省職員はまた、組織の統合と新たな役割の定義が、官僚主義を切り崩し、サイバー問題がより注目されるようになったと述べている。

CDP には 3 つのポリシー・ユニットがある：

- **国際サイバー空間安全保障：**多国間、地域、二国間フォーラムにおける国際サイバー空間安全保障に関する外交関与を含め、サイバー空間の安定と安全保障を促進するための国の取り組みを 37 人のスタッフで主導する。
- **国際情報通信政策：**5G を含む競争力のある安全なネットワークを推進し、ライセンス、制裁の執行、サプライチェーンの安全保障を通じて電気通信サービスとインフラを保護する。
- **デジタル・フリーダム：**世界のインターネットの自由を促進するため、プライバシー、政府介入、人権、市民参加に関する加盟国の活動を 6 人のスタッフで支援する。

国務省の新局は、戦略目標の達成に向けて課題に取り組んでいる。

米国政府関係者によると、CDP の戦略計画・コミュニケーションユニットは、同局の戦略計画、パブリック・ディプロマシー、メディア、立法活動を担当し、デジタル・コネクティビティ・サイバーセキュリティ・パートナーシップを通じた対外援助プログラムを管理している。

CDP は国務省の主要業務勘定「外交プログラム」から資金を調達し、機能局の運営プログラムを支援する「外交政策・支援」カテゴリーに毎年資金を要求している。2022 会計年度には、同局と 92 の役職を支援するため、CDP に 1800 万ドルが割り当てられた。その後の要求では、新たな役職に充てるための追加増額を要求し、2023 会計年度には CDP に 2100 万ドルを割り当てた。

同局設立後の 2023 年 1 月には、重要・新興技術を米国の外交政策と外交に統合するため、国務長官室内に重要・新興技術特使室（S/TECH）も設置された。S/TECH は、重要・新興技術に関する外交政策と外交を主導し、人工知能、バイオテクノロジー、量子情報技術に焦点を当てている。CDP と S/TECH はともに副長官に報告し、S/TECH は CDP の特命大使を通じて報告する。

国務省当局者によると、CDP は戦略的目標を追求する中で、役割の明確化や職員の雇用などの課題に取り組んでいる。国務省職員によれば、新体制のもとでサイバー問題に対する責任は明確化されたものの、役割は依然として意図的に共有され、部局全体で補完的であるため、明確化は継続的な課題である。さらに、サイバー問題は外交のほぼすべての側面に関連する可能性があるため、専門知識が十分に活用されるよう、問題の認識と可視性を確保するための国務省内のコミュニケーションは、関連する重要な課題であると述べた。例えば、CDP のデジタル・フリーダム・ユニットと民主主義・人権・労働局（DRL）は、インターネット上の言論の自由や公正なアクセスなど、似たような分野を扱っている。CDP の役割は、技術政策に関する専門知識を提供し、他の米国ユニットと協力してトピックに関する補完的な立場を打ち出し、声明やその他の活動でパートナー諸国と関与することであるのに対し、DRL の役割は、二国間および多国間の外交を通じて、また市民社会主導のプロジェクトに資金を提供することによって、インターネットの自由を推進することである。

政府関係者によれば、サイバー外交の定義が世界的に合意されていないこと、また外国政府、多国間アクター、市民社会、民間セクターがサイバーに関するトピックについて組織する方法が多様であることが、いくつかのサイバー問題に関する役

割と責任を特定する上で直面する課題の一因となっている。国務省職員は、定期的な会議や非公式な会話など、構造化された、あるいは構造化されていないメカニズムが、これらの問題に関する CDP と他の局や事務所とのコミュニケーションを促進していると述べた。さらに、複数の局がある問題に関与している場合、担当者はその場その場で役割を明確にしている。このようなアプローチは、対立やコミュニケーションの断絶を避けるのに役立っていると、私たちが話を聞いた国務省の局の職員は述べている。

CDP はまた、米国政府全体の省庁間プロセスにおける国家の役割を明確にすることにも取り組んでいる。CDP は、国務省がサイバー外交の主導権を維持し、他の米政府機関と協調して行動するよう働きかけている。例えば、国務省は最近、米サイバー軍司令部、国家サイバー局長室、サイバーセキュリティ・インフラセキュリティ保障庁の高官からなる代表団を率いてウクライナの副大臣と会談し、前述のようにウクライナに対する 3700 万ドルの非軍事サイバー支援を発表した。

国務省職員によると、CDP は現在、人員配置され、完全に稼働しているが、成長計画を達成するために、既存職員の訓練とさらなる雇用が必要だという。現在のスキルギャップに対処するため、CDP は国際サイバーセキュリティ・パートナーシップ・イニシアチブ、情報コミュニケーション政策業務、デジタル・フリーダム政策業務、省庁間 調整、対外援助業務、二国間／多国間関与などの専門分野に関する知識共有プログラムを実施 した。CDP はまた、国務省外務研究所のサイバー・デジタル政策担当官コースを設立し、世界中の職員が容易にアクセスし利用できるよう、コンテンツをオンデマンドでバーチャルにプロバイダすることにも取り組んでいる。CDP の責任者は、2024 年末までに訓練を受けたサイバー・デジタル政策担当官をすべての大使館に配置することを目標としていると語った。また、職員が職務にマッチし、識別のためのインセンティブが与えられるよう、国務省全体でサイバー・スキルを識別する仕組みも構築している。さらに

また、大使の選考基準として、サイバー関連の話題に堪能であることを追加した。さらに、同省内のサイバー外交の重要性を強調するため、毎年「技術外交の功績」賞を授与することにした。また、採用ニーズに対応するため、CDP はプロセスを迅速化するための追加的な施策を実施・検討しており、人材パイプラインを構築するため、産業界、学界、他省庁とのパートナーシップの構築に取り組んでいる。

国務省は関連する先進的改革プラクティスに従った新サイバー局設立時

GAO の省庁改革の取り組みに関する先行研究では、連邦政府の組織改革や業務の効率化・効果改善の取り組みについて、主導的な改革手法が特定されている。　連邦政府の組織改革や、業務の合理化・効率化・効果改善のための取り組みについて、先進的な改革プラクティスを紹介している。[18]一般的な慣行の中から、国務省の改革努力の実施に関連し、適用可能なものに焦点を当てた。

CDP の創設にあたり、国務省は 8 つの先進的な改革手法に取り組んだ（表 3 参照）。

表 3：国務省はサイバー空間・デジタル政策局を設立するにあたり、関連する先進的な改革プラクティスに取り組んだ。

[18]GAO-18-427。

改革の実践と問題	GAO の評価
リーダーシップ：当該機関は、提案されている改革の実施に責任を負うリーダーを指名しているか。	対応済み
説明責任：改革が成功裏に実施された場合、その指導者はどのように責任を負うのか。	対応済み
実施チーム：改革プロセスを管理するために、人員、資源、変更管理などの能力を備えた専任の実施チームを設置したか。	対応済み
実施計画：改革の機運を高め、進捗状況を示すために、どのような実施目標とスケジュールが設定されているか。言い換えれば、実施進捗を追跡するための主要なマイルストーンや成果物を含む実施計画を策定しているか。	対応済み
従業員のエンゲージメント：改革中および改革後、従業員のエンゲージメントを維持・強化するために、どのような計画を立てているのか。	対応済み
多様性：改革において、あるいは人員削減を検討する際に、その機関は具体的にどのように多様性を管理し、包括的な職場環境を確保しようと計画しているのか。	対応済み
戦略的労働力計画：提案されている改革や再編成に必要な、スキルやコンピテンシーを含む資源や能力が確保されるかどうかを判断するために、当該省庁はどの程度、戦略的労働力計画を実施したか。	対応済み
採用：専門性が高く、採用が難しい職種を採用するためのカスタマイズされた戦略など、効果的な募集・採用のための重要な実践が改革にどの程度盛り込まれたか？	対応済み

出典 GAO による国務省データの分析。| GAO-23-105563

国務省によるこの慣行への取り組みの詳細については、以下の通りである：

リーダーシップ：国務省は、特命全権大使、首席次官補、事務局長を含む改革努力のリーダーを指名した。

説明責任：CDP は、国務省の他の局と同様、各職員と協力して上司が設定した業績目標の監視と報告を含む業績計画プロセスを通じて説明責任を負う。このプロセスを支援するため、CDP は機能局戦略（FBS）を策定し、サイバー政策を世界的に推進し、米国政府内のデジタル外交政策を高めることに関する目標、目的、小目標を特定した。CDP は、四半期ごとのパフォーマンス指標とマイルストーンを用いて進捗を追跡することを含む戦略実施計画を策定した。CDP は、CDP が存在する以前にサイバー外交の役割を担っていた部署がどのように実績を報告していたかと同様の方法で、米国の年次保証書（Statement of Assurance）プロセスで実績を報告する。

実施チーム：国務省は、キャパシティ・スタッフィング、リソース、チェンジ・マネジメントに特化した専門知識と能力を持つワーキンググループからなる実施チームを設立した。例えば、コミュニケーション・チェンジマネジメントワーキンググループは、CDP の創設によって直接影響を受ける人々、国務省全体のスタッフ、および外部の聴衆との関わりを担当した。このグループを率いたのは、国務省の広報担当の最高幹部、旧サイバー問題調整官室のスタッフ、旧情報通信政策ディビジョンのスタッフで、プロセス管理とコミュニケーションの経験者であった。

実施計画：国務省は、改革作業前と作業中に必要な一連のタスクを特定し、進捗状況を追跡するためのマイルストーンを策定し、実施計画の要素に取り組んだ。具体的には、CDP は、タスクが記載された開始前計画を作成し、改革の取り組み中に、目標、小目標、それぞれに関与する関連部門を特定するアセスメントを作成し、望ましい最終状態を追跡するための見出しを付けた。2022 年 9 月、CDP は戦略の見直しを行い、CDP の目標に沿った目標とマイルストーンを作成した。さらに、CDP は FBS を利用して進捗状況を追跡するという。

従業員エンゲージメント：CDP は、設立直後にオフサイトを実施し、ビジョン、バリュー、目標との整合性に関する従業員のフィードバックを募った。また、毎月のアンバサダー・タウンホール、毎週のチーム・コール、バーチャルの「ランチ&ラーン」シリーズ、その他のエンゲージメント活動も実施した。CDP は、従業員のエンゲージメントを維持するために、さらなるコミュニケーションツールや、さまざまなワーキンググループ、共有ワークステーションを備えたオープンコンセプトの同居スペースなどのアプローチを引き続き模索している。

多様性 DEIA（多様性、公平性、インクルージョン、アクセシビリティ）戦略計画と協調して、CDP は DEIA 協議会を設立し、ベストプラクティスの使用を確実にするための採用活動に重点を置いて、DEIA 局の戦略を見直し、調整する。

戦略的労働力計画 GAO の先行研究では、労働力計画への戦略的アプローチについて説明している。[19]国務省/CDP は、以下のように戦略的な人員計画に取り組んだ。

- CDP は、国務省におけるサイバー空間の習熟度ギャップを埋めるための文書である CDP 訓練・現場支援戦略（TFSS）の中で、現在および将来の目標を達成するために必要となる重要なスキルと能力を特定している。例えば、基本的なレベルのスキルの 1 つは、サイバーとデジタル政策の用語の概念を持つことであり、もう 1 つは、サイバーとデジタル政策の問題が米国の安全保障、経済競争力、価値にどのように影響するかを理解することである。
- TFSS は、スキルの格差に対処するための戦略について概説しており、これには、対面式の公式トレーニングコースの実施、付随するバーチャルコースの作成、地域ワークショップの実施といったアプローチが含まれる。
- TFSS は、労働力計画戦略をサポートするために必要な内部能力を構築するための、資金やスタッフを含むリソースを特定する。
- CDP 職員によると、スキル格差の解消に向けた進捗状況を監視・評価するため、CDP は 2022 年 11 月に習熟度に関するベースライン調査を実施し、今後も定期的に調査を実施して変化を測定し、それに応じて調整を行う予定である。CDP はまた、米国の研修部門であるフォーリン・サービス・インスティテュート（FSA）と共同で実施した研修後の調査を通じて、スキル格差をモニターしている。

採用：国務省は直接雇用などの特別採用認可を利用した。

認可のほか、外務情報技術フェローシップ・プログラムのような特別プログラムもあり、ミッションの優先事項に対応している。前述したように、CDP は、プロセスを迅速化するための特別採用の仕組みをさらに検討し、人材パイプラインを構築するために、産業界、学界、他機関とのパートナーシップの構築に取り組んでいる。

---

[19] GAO, High-Risk Series : An Update, p. 51, GAO-13-283, (Washington, D.C.: Feb. 2013)を参照のこと。

行政機関のコメント

本報告書のドラフトを国務省、USAID、国防総省、国土安全保障省（DHS）に提供し、レビューとコメントを求めた。USAID は附属書 II に再掲するコメントを寄せた。国務省と DHS は技術的なコメントを提供し、我々はそれを適宜取り入れた。

この報告書のコピーを適切な議会に送付する。

委員会、国務省長官、USAID 長官、国防長官、国土安全保障長官に報告した。また、報告書は GAO のウェブサイト（https://www.gao.gov）で無料で入手できる。

本報告書についてご質問のある方は、(202) 512-4409 または LoveGrayerL@gao.gov までご連絡いただきたい。米国議会関係部および広報部の連絡先は、本報告書の最終ページに記載されている。本報告書に主要な貢献をした GAO スタッフは、附属書 III に記載されている。

ラテシャ・ラブ＝グレイヤー

国際・貿易部長

対応済みリスト

ベンジャミン・カーディン氏

会長

ジェームズ・E・リッシュ

ランキング・メンバー

米国上院外交委員会

マイケル・マッコール

会長

グレゴリー・ミークス ランキング・メンバー

外務委員会

代表者

ロバート・メネンデス

米国上院

附属書 I. 目的、範囲、方法論

本報告書では、(1)国際協定や国際フォーラムの利用を含め、サイバー空間に関する米国の利益を促進するために国務省が行っている活動と、その影響について報告されていること、(2)サイバー外交の目標を達成するために、国務省の組織変更がどの程度役立っているか、あるいはどのような課題を提示しているか、について検証する。

サイバー空間に関する米国の利益を促進するために国が行っている活動を特定するために、2017 年から現在までの国のサイバー外交活動に関する文書をレビューし、2020 年から 2023 年までの進行中および最近の活動に焦点を当てた。複数の省庁がサイバー外交活動を支援する対外援助活動を実施する可能性があるが、我々は、国務省が主導または資金を提供するサイバー外交活動、あるいは報告義務や正式な省庁間協定など、国務省との構造的な関係を有するサイバー外交活動に焦点を絞って監査作業を行った。我々は、サイバー外交プログラムや活動を、2018 年国家サイバー戦略の柱 III「強さによる平和の維持」または柱 IV「アメリカの影響力の促進」で特定されたサイバー外交目標に貢献するものと定義した。

情報提供の要請は 2023 年国家サイバーセキュリティ戦略の公表前に行われたが、2023 年国家サイ バーセキュリティ戦略の柱 V の戦略目標との整合性を判断するために、国および他の省庁が特定した活動お よびプログラムを分析した：なぜなら、この柱は国際的なサイバー対策に焦点を当てているからである。我々の報告書の目的上、2018 年国家サイバー戦略と 2023 年国家サイバーセキュリティ戦略に含まれる戦略目標は、国際的なサイバー目標に関して類似したテーマと概念を捉えていると判断した。我々はプログラム文書を分析し、米国国際開発庁（USAID）、国防総省（DOD）、国土安全保障省（DHS）を含む国および関連機関の職員と戦略目標とその実施について議論した。

我々は、国が支援しているサイバー外交活動の範囲と影響を示すために、多国間フォーラム、多国間協定、二国間協定、対外援助活動を特定した。我々は、選択したプログラムの結果を検討し、影響について報告されていることを確認するために、国務省職員と話をした。検討した活動の中には、サイバー空間・デジタル政策局（CDP）が設立される前に始まったものもあるが、国務省のサイバー外交の取り組みを例示するものである。さらに、CDP はこれらの活動を引き続き支援している。従って、本報告書ではこれらの活動についても適宜言及している。

国務省がサイバー外交の目標を達成するために、組織の変更がどの程度役立ったか、あるいはどの程度課題となったかを検証するため、国務省の合理的根拠、計画、組織の変更に関する文書を分析し、関係者に話を聞いた。具体的には、CDP の実施計画、目標の評価、戦略レビュー、CDP 設立に関するメモ、訓練と現場支援戦略、CDP の人員計画などの文書を検討した。また、国務省が書面で回答した詳細な質問から情報を収集した。また、政府関係者や非政府組織の代表者から、課題や優先事項、それらに対処するためのアプローチについて話を聞いた。我々は、GAO の先行研究で概説された、選択された政府改革のプラクティスに国がどの程度取り組んでいるかを評価することで、組織変更を評価した。組織改革がサイバー外交の目標達成にどの程度役立ったかを検証するため、目標達成のために適用可能な政府改革手法にどのように取り組んだかを評価した。国務省の組織改革に関連し、合理的に実施できるものであれば、適用可能であると判断した。

当検査院は、一般に公正妥当と認められた政府監査の基準に準拠して、2021 年 11 月から 2024 年 1 月にかけて本業績監査を実施した。これらの標準は、当検査院が、監査の目的 に照らして合理的な根拠を有する十分かつ適切な証拠を入手するために、監査を計画し実施することを求めている。当検査院は、入手した証拠が当検査院の監査目的に基づく所見と結論のための合理的な基礎を提供すると信じ ている。

USAID
FROM THE AMERICAN PEOPLE

Latesha Love-Grayer
Director, International Affairs and Trade
U.S. Government Accountability Office
441 G Street, N.W.
Washington, D.C. 20226

December 11, 2023

Re: CYBER DIPLOMACY State's Efforts Aim to Support U.S. Interests and Elevate Priorities (GAO-24-105563)

Dear Ms. Love-Grayer:

I am pleased to provide the formal response of the U.S. Agency for International Development (USAID) to the draft report produced by the U.S. Government Accountability Office (GAO) titled, CYBER DIPLOMACY State's Efforts Aim to Support U.S. Interests and Elevate Priorities (GAO-24-105563).

We thank you for the draft report, which highlights the enormous importance of international cyber diplomacy and related development efforts for U.S. national interests.

The draft report is relevant to USAID given our work with the Department of State on cybersecurity issues through the Digital Connectivity and Cybersecurity Partnership (DCCP). This has included efforts such as Promoting American Approaches to Information and Communication Technology (ICT) Policy and Regulation (ProICT), an activity that provides technical assistance and capacity-building to help developing country governments establish ICT policy and regulatory frameworks that will enable an inclusive digital economy. In addition, the Digital Asia Accelerator (DAA) activity aims to advance economic development by increasing business' and citizens' capacities to use digital technology safely and effectively across Southeast Asia. These are but a few of the cyber and digital capacity building efforts on which we are actively collaborating.

I am transmitting this letter from USAID for inclusion in the GAO's final report. USAID does not have any comments. Thank you for the opportunity to respond to the draft report, and for the courtesies extended by your staff while conducting this engagement.

Sincerely,

Colleen Allen

Colleen Allen
Assistant Administrator
Bureau for Management

謝辞

スタッフの謝辞

上記の担当者に加え、ロブ・ボール（アシスタント・ディレクター）、マーク・カステラノ（アナリスト・イン・チャージ）、ニール・ドハーティ、マーク・ダウリング、トーマス・フレンド、クシュ・マルホトラ、ドナ・モーガン、アンドリュー・スタヴィスキー、サラ・ヴィール、ジナ・ユーが本報告書に重要な貢献をした。

GAO の使命

政府アカウンタビリティ室は議会の監査、評価、調査部門であり、憲法上の責任を果たす議会を支援し、米国民のために連邦政府のパフォーマンスと説明責任を改善するために存在する。GAO は公的資金の使途を調査し、連邦政府のプログラムや政策を評価し、議会が十分な情報に基づいた監督、政策、資金調達の決定を行えるよう、分析、勧告、その他の支援を提供している。GAO の良き政府へのコミットメントは、説明責任、誠実さ、信頼性というコアバリューに反映されている。

GAO 報告書および証言のコピーを入手する

GAO 文書のコピーを無料で入手する最も早く簡単な方法は、ウェブサイトを利用することである。GAO は毎週平日の午後、新たに発表された報告書、証言、通信文書などをウェブサイトに掲載している。また、GAO の電子メール・アップデートを購読すれば、新しく掲載された製品の通知を受け取ることができる。

電話で注文する

GAO の各出版物の価格は、GAO の実際の制作・配布コストを反映しており、出版物のページ数、カラー印刷か白黒印刷かによって異なる。価格と注文情報は、GAO のウェブサイト（https://www.gao.gov/ordering.htm）に掲載されている。

ご注文は、(202) 512-6000、フリーダイヤル (866) 801-7077、または TDD (202) 512-2537 まで。

アメリカン・エキスプレス、ディスカバー・カード、マスターカード、ビザ、小切手、郵便為替での支払いが可能。詳細は電話で問い合わせを。

GAO とつながる

Facebook、Flickr、Twitter、YouTube で GAO とつながろう。

RSS フィードまたは E メールアップデートを購読する。ポッドキャストを聴く

GAO のウェブサイト https://www.gao.gov。

連邦プログラムにおける不正、浪費、濫用を報告する件

FraudNet に連絡する：

ウェブサイト：https://www.gao.gov/about/what-gao-does/fraudnet

自動応答システム： (800) 424-5454 または (202) 512-7700

議会関係

A.Nicole Clowers, Managing Director, ClowersA@gao.gov, (202) 512-4400, 米国政府アカウンタビリティ室, 441 G Street NW, Room 7125, Washington, DC 20548.

パブリック・アフェアーズ

チャック・ヤング、マネージング・ディレクター、youngc1@gao.gov、(202) 512-4800

米国政府アカウンタビリティ室 441 G Street NW, Room 7149 Washington, DC 20548

戦略的プランニングと渉外

Stephen J. Sanford, Managing Director, spel@gao.gov, (202) 512-4707 米国政府アカウンタビリティ室, 441 G Street NW, Room 7814,Washington, DC 20548

再生紙に印刷すること。