サイバー防衛支援とウクライナ

教訓とこれからについて

ASPEN DIGITAL
aspen institute

国際的に不安定な時代において、デジタル社会の安全性とレジリエンス(回復力)は深刻な課題に直面しています。このような不安定な情勢は、サイバー空間での侵略に対抗する各国の政府の対処能力を低下させています。この拡大する空白を埋めるため、民間セクターによるサイバー防衛支援の実施は、変化し、その重要性はますます高まっています。

欧米やその同盟国では、デジタル領域の主要な生産者、運営者、保護者の役割を民間セクターが担っています。過去3年間、欧米企業は単独、あるいは団結して、ロシアの再侵攻に直面したウクライナだけでなく、世界中のデジタル環境を保護するためにも、サイバー防衛を提供してきました。欧米企業が国際的なデジタル環境全体でサイバー防衛とレジリエンス支援を主導する必要性は、今後ますます高まると思われます。本稿では、これらの取り組みを導くための教訓を提示します。

ACKNOWLEDGMENTS

作者

Greg Rattray
Executive Director, Cyber Defense Assistance Collaborative (CDAC)

Seungmin (Helen) Lee Director of Intelligent Cyber Research (ICR), Next Peak

貢献者

Yameen Huq
Director, Cybersecurity Programs, Aspen Digital

アスペン米国サイバーセキュリティグループ

共同グループ長

Yvette Clarke
U.S. House of Representatives

Christopher Krebs
Chief Intelligence & Public Policy Officer, SentinelOne

Gary Steele
President, Go-to-Market, Cisco and GM, Splunk

Kemba Walden
President, Paladin Global Institute

Yasmin Green
CEO, Jigsaw, Google

スタッフ

Yameen Huq
Director, Cybersecurity Programs, Aspen Digital

Sasha O'Connell
Senior Director, Cybersecurity Programs, Aspen Digital

Nicole Tisdale
Senior Advisor, Cybersecurity Programs, Aspen Digital

John P. Carlin
Strategic Advisor and Chair Emeritus for Cybersecurity, Aspen Digital

Stefani Jones
Director, Cybersecurity Programs, Aspen Digital

本書は、アスペン研究所の米国サイバーセキュリティグループのメンバーと協議して作成されました。同グループのメンバーは、アスペン・デジタルのサイバーセキュリティ政策スタッフ、専門家、アドバイザーにアイデアや提言を提示しました。これらの提言は、官民両部門における深い専門知識がなければ不可能であったでしょう。この専門知識は、サイバーセキュリティをどのように改善するかについて、引き続き重要な課題となっています。

アスペン研究所の米国サイバーセキュリティグループ

アスペン研究所の米国サイバーセキュリティグループは、サイバー空間およびその他の領域において、米国の機関、インフラ、個人を保護し、安全な未来を推進する、官民を横断するフォーラムです。

はじめに

2022年2月のロシアによるウクライナへの再侵攻は、欧米諸国がこの侵略に抵抗するきっかけとなりました。戦争は未だサイバー空間を含む多くの戦線で継続していますが、リソースの制約と疲労が深刻化しており、支援活動は減速しています。同時に、ウクライナのデジタル領域は、現在の紛争の遂行と紛争後の重要な懸念事項の両面において、引き続き攻撃の焦点となっています。

2023年2月にアスペン研究所が発表した論文「The Cyber Defense Assistance Imperative: Lessons from Ukraine(サイバー防衛支援の必須事項:ウクライナからの教訓)」[1] では、民間セクターがウクライナのサイバー防衛をどのように支援したか、その影響について考察し、そのプロセスから得られた重要な教訓を導き出しています。ロシア近郊のバルト三国、モルドバ、ポーランド、また東アジアでは台湾、フィリピンなどの地政学的な火種が、サイバー要素を伴ってエスカレートする中、CDA（サイバー防衛支援)に対する将来的な潜在的な課題について深く理解することが極めて重要です。ウクライナのデジタルレジリエンスは、現在の紛争を乗り越えるための交渉及び維持の面で、極めて重要です。同様に、強固なサイバー防衛とデジタルレジリエンスは、2024年5月に発表された米国の国際サイバー戦略で述べられているように、他の潜在的な引火点における危機の安定性を向上させることができます[2]。

「官民パートナーシップは、サイバーおよびデジタル外交に不可欠であり、柔軟性と適応性が必要です。危機的状況下におけるサイバー防衛サービスや製品の拡張、供給、ライセンス供与のための新たな方法が必要になる可能性があります..」

ウクライナでは、運用支援によって強化された効果的で適応性の高いサイバー防衛とレジリエンスの必要性が依然として不可欠です。ウクライナで行われた取り組みは、同様の地政学的状況にある米国とその同盟国が目標を達成するためにも必要であることを明らかにしています。本稿では、前回の報告書のアップデートと追加調査の結果を提供します。

[1] https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf
[2] https://www.state.gov/united-states-international-cyberspace-and-digital-policy-strategy/#cyber-attacks

サイバー空間におけるロシア・ウクライナ紛争の進展

ウクライナのサイバー防衛は、ロシアのサイバー攻撃の頻度と強度が増しているにもかかわらず、高いレジリエンスを維持しています。2023年末には、ウクライナ最大の通信事業者であるキエフスターが「ウクライナのネットワークに対する最も深刻な破壊的サイバー攻撃の1つ」[3] を経験しました[4] 。2024年上半期、ウクライナで発生したサイバーインシデントは1,739件で、2023年下半期の1,463件から19%増加しました[5] 。2024年末には、ウクライナの国家設備をオフラインにしてしまうという、ロシアがウクライナに対して行った攻撃の中で最も深刻な攻撃が実施されました[6] 。ロシアとウクライナのサイバー作戦の性質も進化し続けています。ウクライナのコンピューター緊急対応チーム(CERT-UA)[7] は、2024年3月にロシア政府が支援するソルントセペック社がウクライナのインターネットプロバイダーであるTriacom、Misto TV、Linktelecom、KIMに対してサイバー攻撃を行ったことからもわかるように、ロシアのサイバー作戦は通信業界を標的にすることに注力していると発表しました[8] 。2024年、ロシアはウクライナ[9]およびヨーロッパ[10] における偽情報キャンペーンにも焦点を当て、ウクライナの決意を弱め、ウクライナへの外国からの支援を阻止しようとしました。ロシアはまた、紛争に直接関与する組織に対して、さまざまなサイバースパイ活動を実施しました[11] 。これに対して、ウクライナは、ロシアの国営企業や民間企業を攻撃して情報を収集し、混乱を引き起こすという積極的なアプローチを採用し始めました[12]。

[3] https://therecord.media/russians-infiltrated-kyivstar-months-before
[4] The Kyivstar hack is a sophisticated cyberattack, allegedly conducted by Russian state-controlled hacker group Sandworm, against Ukraine's internet infrastructure which resulted in disruption to communications, networks, and connectivity.
[5] https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report
[6] https://www.csoonline.com/article/3629407/russia-fires-its-biggest-cyberweapon-against-ukraine.html
[7] https://cip.gov.ua/ua/news/kiberoperaciyi-rf-novi-cili-instrumenti-ta-grupi-analitika-khakerskikh-atak-proti-ukrayini-za-2-pivrichchya-2023-roku%E2%80%8B
[8] https://cyberscoop.com/russian-military-intelligence-may-have-deployed-wiper-against-multiple-ukrainian-isps/
[9] https://thehill.com/policy/international/4484030-russian-hackers-attack-ukrainian-media-outlets/
[10] https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/
[11] https://cip.gov.ua/en/news/cyber-operations-rf-h1-2024-report
[12] https://therecord.media/ukraine-cyberattacks-aiding-ground-war-russia

ウクライナ政府は現在、親ウクライナ派のハクティビストと協力してロシアの組織を標的にする活動を公に行っており、2024年10月には、ウクライナ軍情報部（HUR）とつながりのある親ウクライナ派のハッカー集団BO Teamが、ロシアの司法管轄裁判所のウェブサイトを標的にして閉鎖しました[13]。

双方によるサイバー攻撃は、今後さらにエスカレートする可能性があり、ロシアがエストニアなどのウクライナの同盟国に対してサイバー攻撃をエスカレートさせる可能性も懸念されています。過去3年間にわたり、ロシアによる破壊工作の深刻さは増減を繰り返してきましたが、全体的には上昇傾向にあります。重要なのは、たとえ合意によって従来の軍事紛争が停止したとしても、緊張状態は継続する可能性があるという点です。

ウクライナへのサイバー防衛支援（CDA）の推移

世界中の政府および民間セクター（主に米国と欧州に拠点を置く組織）が、ウクライナにサイバー防衛支援（CDA）を提供しています。初期の取り組みは、ウクライナが分散型サービス拒否（DDoS）攻撃をかわし、耐障害性の高いクラウドベースのデジタルサービスを確立するなど、ウクライナにおけるロシアのサイバー攻撃の状況を把握することに重点をおいており、ネットワークへのロシアの侵入排除を行う上で極めて重要な役割を担っていました。CDAC（サイバー防衛支援協力）[14] やその他の民間企業は、信頼を構築するために、ウクライナの組織が要請した支援を緊急度に応じて提供することに取り組みました。しかし、支援活動の長期的な有効性と持続可能性に関する懸念は、取り組みへの要求が拡大するにつれ生じていきました。

公共圏において、米国政府は2022年2月から2024年8月の間に、8200万ドル以上のサイバー支援をウクライナに提供しました[15] が、サイバー支援プログラムは広く対象をもうけてお

[13] https://therecord.media/russian-court-websites-down-attack-claimed-pro-ukraine-group

[14] https://crdfglobal-cdac.org/

[15] https://www.state.gov/proceedings-of-the-2023-u-s-ukraine-cyber-dialogue/#:~:text=As%20part%20of%20this%20support,over%20%24120%20million%20since%202016. The source has been archived, current as of Jan 22. 2025, but was available in August 2024.

り、紛争後の復興に重点をあてています[16] 。また、米国政府は、ウクライナへの支援をめぐる党派的な対立[17] の高まりや、支援の重点化や世界的な地政学的コミットメントの観点でも優先事項の相違が存在しています。
さらに、トランプ政権が発足したことで、ウクライナへのサイバー防衛支援の見通しにどのような影響が及ぶかは現時点では不明です。トランプ大統領は2025年1月21日時点で、すべての対外援助を90日間凍結しています。本報告書執筆時点では、CDAC やその他の取り組みを通じた民間セクターの支援は継続されています。

国際的にも、各国ウクライナのサイバー防衛を支援し続けています。例えば、英国は2023年6月に1600万ユーロと2年間の支援延長を表明しました[18] 。さらに、同じ考えを持つ国々が協力し、次のようなウクライナのサイバー防衛を支援するための正式なメカニズムを確立しています。

- **タリン・メカニズム:**[19] 米国、カナダ、デンマーク、エストニア、フランス、ドイツ、オランダ、ポーランド、スウェーデン、英国は、2023年12月にウクライナ政府と、重要インフラに焦点を当てた非軍事的サイバー防衛能力構築支援の調整と促進を目的とした取組みを正式に確立しました。この取り組みでは、ウクライナの国家サイバー支援要件を優先的に選別することを求めていますが、西側の支援国は個々の国家支援の取り組みを調整します。メカニズムの進化に伴い、民間セクターの関与をどのように調整し、高度なサイバー防衛能力をタイムリーに展開するかの試行錯誤は続いています。2024年12月20日、タリン・メカニズムは共同声明を発表し、メカニズムの記念日を祝うとともに、この取り組みが2億ユーロを超える外国からの援助を集めたことを強調しました。また、「ウクライナを支援するための新たな手段を、必要な限り追求し続ける」とも述べています[20]。

[16] https://therecord.media/us-cyber-ambassador-fick-cyber-aid-to-ukraine-kyiv
[17] https://www.pewresearch.org/global/2024/05/08/growing-partisan-divisions-over-nato-and-ukraine/
[18] https://www.gov.uk/government/news/uk-to-give-ukraine-major-boost-to-mount-counteroffensive
[19] https://www.state.gov/formalization-of-the-tallinn-mechanism-to-coordinate-civilian-cyber-assistance-to-ukraine/
[20] https://vm.ee/en/news/joint-statement-tallinn-mechanism

- **IT連合:**[21] エストニア、ルクセンブルク、ベルギー、デンマーク、アイスランド、イタリア、ラトビア、リトアニア、オランダを含む10カ国の欧州諸国は、ウクライナ国防省および軍の情報技術（IT）インフラを今後6年間支援することを目的として、2024年2月に連合を正式に発足させました。連合の取り組みは、ウクライナ軍のITおよび通信に関するあらゆるニーズを網羅しています。2024年5月には、IT連合はウクライナに通信ハードウェアを納入し、ルクセンブルク、アイスランド、エストニア、ベルギーは新たに2200万ユーロの支援を行いました[22] 。米国は連合の正式な参加はしておらず、活動をオブザーバーとして見守っています。

  タリン・メカニズムの登場により、政府主導のCDAが直面する課題と好機の両方を明らかにしています。この取り組みは、ウクライナのサイバー防衛要件の確立を促す上で効果的であることが証明されました。タリン・メカニズムに関する議論は2023年初頭に開始されました。参加各国政府による取り組みの立ち上げと調整のペースが遅いのは、多国間外交で伝統的におこなわれてきた慎重なプロセスに起因します。契約プロセスにおける同様の遅れは、戦略的に影響力のある支援の提供に民間セクターを組み入れる妨げになる可能性があります。

民間セクターには、さまざまなレベルで企業と政府間の調整を行っているCDAの情報源が存在します。CDACはウクライナへの支援の調整を継続しており、32の民間企業から25のウクライナの組織に対して、2600件以上のサイバー防衛ツールや、1600件以上のトレーニングクレジットまたは訓練セッションをなど、4000万ドル以上の支援の提供を行っています[23]。 CDAC以外では、ロシアがウクライナのデータセンターや電力網を爆撃している間、マイクロソフトやその他のクラウドベースのサービスがデジタルサービスを提供しました[24] 。ロシアが比較的洗練されていないDDOS攻撃を使用してウクライナのデジタル政府、銀行、通信サービスを抑制した際には、Cloudflareが対DDoSサービスを提供しました[25]。

[21] https://kyivindependent.com/it-coalition-members-sign-cooperation-agreement-in-support-of-ukraine/
[22] https://www.mil.gov.ua/en/news/2024/05/31/the-it-coalition-led/
[23] CDAC internal tracker current as of October 23, 2024.
[24] https://blogs.microsoft.com/on-the-issues/2022/11/03/our-tech-support-ukraine/
[25] https://blog.cloudflare.com/ukraine-update

多くの政府が民間セクターの組織と契約を結び、幅広いサイバー能力を提供し、インシデント対応とハンティング業務を実施しています。

CDACによる運用能力の提供に向けた画期的な取り組みは、紛争開始から数週間以内に開始されました。特に、CDACは協力企業およびカスタムの脅威インテリジェンスプラットフォームを通じて、攻撃対象領域の監視と、脅威インテリジェンスを提供しています[26] 。2022年のCDACインテリジェンス支援の取り組みにより、ウクライナ国家特別通信サービス（SSSCIP）、SBU、国家サイバーセキュリティクラスター（NCCC）などのウクライナの組織は、攻撃対象領域を毎日監視し、ロシアの特定の脅威と攻撃の特徴に関する情報提供を毎日受け取ることができ、攻撃に対する防衛力と攻撃からの迅速なレジリエンスを強化することができました。
2023年末までに、Recorded Future社は、ウクライナ：特に重要インフラに対して、1,000万ドル以上の情報データ、Intelligence Cloudソフトウェアプラットフォーム、ロシアの戦争犯罪捜査を提供しました。同社は2024年にはさらに1,300万ドル分を支援しました[27] 。パートナー企業であるThreatQuotient社、Recorded Future社、Mandiant社、およびCyber Threat Alliance（CTA）社との連携により、CDACは、ウクライナ政府および民間セクターのさまざまな受信者向けに脅威インテリジェンスの重複排除と優先付けを行う、脅威インテリジェンスの集中型収集・配信システムを開発しました。このプラットフォームは官民連携の象徴であり、米国土安全保障省のサイバーセキュリティ・インフラセキュリティ庁（CISA）が民間企業とともに、以下のように、更新情報を提供しています。

CISA副所長のクレイトン・ロマンス氏は『CISAは引き続きウクライナにいるパートナーを支援し、サイバー防衛を強化するためにあらゆる情報やサービスを提供していきます。CDACのような主要パートナーと協力することで、情報共有を促進し、政府と産業界の最高の能力を結集して、この困難な時期にあるウクライナを支援することができます。』と、述べています。

[26] https://crdfglobal-cdac.org/case-study-threat-intelligence-sharing/
[27] https://www.recordedfuture.com/press-releases/recorded-future-continues-provide-intelligence-ukraine

CDACの参加者は、ウクライナの長期的なサイバー防衛能力も強化しています。提供された主なツールには、セキュリティ情報およびイベント管理（SIEM）システム、エンド検出対応（EDR）ツール、脆弱性スキャナーなどが含まれます。SANS研究所は、ウクライナにサイバー訓練と教育を提供することで、必要な人材を育成するためのリソースの開発と共有に取り組んできました[28]。

支援の提供にとどまらず、CDACは、サイバー空間における戦略的および運用上の課題に効果的に対処可能な強力なコミュニティを構築し、協調的な組織のモデルとなることで、タリンメカニズムやIT連合などの他のメカニズムに統合できるツール、サービス、トレーニングを提供しています。継続中のCDAC会議や、50を超える民間および政府関係者の四半期ごとの会合を通じてCDACは、サイバー防衛イニシアティブに関する情報交換を行うユニークなフォーラムを提供し、また、何がうまくいっていて、どのような課題があるのかについて活発な対話を行うための信頼関係を維持しています。

2024年の前半、CDACは、コロンビア大学国際公共政策大学院と共同で、CDAの効果を測定するための新しいフレームワークを作成しましました。ここでは、関連するオープンソースの研究、既存の評価フレームワークのレビュー、および専門家のインタビューに基づいており、CDAの運用、戦略、組織の有効性を評価するための3段階のアプローチを提案しています。段階的なアプローチにより、紛争のさまざまな局面における効果を測定できます。このアプローチは、運用上の成功、効率性、戦略的計画、軋轢、持続可能性という5つの主要な柱から構成されており、参加者が支援の対象をより適切に絞り、潜在的なCDA資金提供者が表明するプログラムの有効性に関する懸念に対処するのに役立っています[29]。

進展がみられ、新たなメカニズムが確立されたにもかかわらず、優先順位の高いCDAの要請や支援の有効性に関するフィードバックを受ける上での障壁は依然として存在しています。紛争勃発以来、多くのウクライナの組織は、重複する支援を求め、時には矛盾する要請リストを要件に合わない支援組織に提出してきました。

[28] https://www.sans.org/blog/ukraine-russia-conflict-cyber-resource-center/
[29] https://crdfglobal-cdac.org/cda-evaluation-framework/

また、ウクライナの組織における指導者の入替が続いたことで、調整が遅れ、支援者に躊躇が生まれてきています。CDACの「Blue Force Tracking, Assessment, and Coordination (ブルー・フォース・トラッキング、評価、調整)」の取り組みは、官民の支援提供者の関心を集めていますが、資金不足で停滞気味であり、その情報収集も場当たり的なものにとどまっています。紛争が当初の想定を上回る長さで続いているため、当初は単発の活動として想定されていたツールのライセンスやトレーニングについては、継続と更新の必要性が生じています。これらの取り組みの構造的な長期的維持に関する各国政府との対話は、ウクライナの状況にもかかわらず、ゆっくりと進んでいます。

紛争の進行に伴い、CDACやその他の民間セクターの取り組みはより広く認知され、賞賛されるようになりましたが、このような支援の提供状況や、その効果の追跡および測定は依然として困難です。サイバー支援の提供者は、契約上の取り決め、企業のセキュリティ上の懸念、紛争への関与に対する世間の認識などのさまざまな理由から、提供した支援に関する具体的な情報の提供に消極的になる場合があります。多くの場合、受給者には、支援の影響についてフィードバックを提供する時間や能力がありません。CDAの有効性を測定するために必要なレポート作成とデータ収集には、リソースと計画が必要です[30]。

2025年初頭の観測によると、民間セクターは、インテリジェンス支援、ソフトウェアライセンス、トレーニングプログラム、その他の支援など、初期のCDA活動を通じて提供された能力を概ね維持しています。しかし、新たな要請や取り組みのレベルは大幅に低下しています。この状況に影響を与えている要因には、1）ウクライナのデジタルレジリエンスの成功、2）サイバー領域におけるロシアのサイバーの非効率性に対する認識、3）一部の支援提供者の疲弊、4）大規模支援を支える資金不足、5）取り組みのシステム化、6）支援活動への不確実な影響、などがあります[31]。ウクライナに対するサイバー支援の焦点を、短期的なサイバー防衛ギャップの解消とするべきか、あるいは長期的なデジタルレジリエンスとするべきかについては、さまざまな見解があります。優先事項の整合性と取組みの調整は依然として理想論にとどまってしまっています。

[30] https://crdfglobal-cdac.org/cda-evaluation-framework/
[31] CDAC Blue Force Tracker and operations

教訓と今後の取り組み

ロシアとウクライナとの戦争は、今後のCDAイニシアティブにとっていくつかの教訓をもたらしました。第一弾のアスペン論文では、3つの主な教訓が示されました。1）CDAの支援受領者と提供者との間に早期に連携と信頼関係を構築する必要性、2）能力提供者を特定、集結、組織化する必要性、3）CDAの活動と優先事項を整合させる必要性。 これらは、当該論文が発表されて以来、現在もなお教訓として守られており、CDAの支援提供者は、これらの教訓を政策と行動に完全に組み込むべく、現在も取り組んでいます。

CDAの肯定的な面として、ウクライナの多くの支援受領者と支援提供を行っている西側諸国および企業との間に強い信頼関係が存在していることが挙げられます。このような信頼関係は、ウクライナ側の要望に応えること、そして情報や技術を継続的かつ成熟した形で提供するためにウクライナと協力することで、主に構築されました。優先事項の調整が依然として課題となっているにもかかわらず、タリン・メカニズム、IT連合、CDACは、能力提供者を組織化するための場を提供し続けています。

これらの初期の調査結果に加え、過去2年半にわたりウクライナ紛争でCDAの提供という苦難の経験から、少なくとも5つの追加的な教訓が得られました。

1) 優先順位付けされた要件リストと提供体制の確立を目指す

活動の調整と優先順位の確立が可能になるため、支援受領国は、潜在的な支援提供者に対して統合された優先順位付けされた要件リストを作成することが最も望ましくあります。国家のサイバー優先事項の確立はどのような状況でも難しいため、そのような取り組みは、最もリスクの高い国家の最も重要な資産に最も大きな影響を与える支援の特定に実質的に焦点を当てるべきです。

この目標は、支援受領国の政治体制、サイバー成熟度、また紛争や緊急事態などの性質によって、達成することが困難な場合があります。ウクライナでは、紛争の初期段階における緊急状態により、達成が難しくなりました。この知見は、可能な限り、動的対立の発生前にこのような評価を実施すべきであると主張しています。また、ウクライナでは、優先順位のついた要件リストを作成するうえで、自己評価を実施する能力が欠如していたため、困難に見舞われました。したがって、CDAは、ニーズを適切に理解するための評価サービスの提供を行うことができます。タリン・メカニズムは、このような優先順

位付けされた要件に対する適切なインセンティブを提供するとともに、戦略的影響を追求するレベルでリソースを集約する能力を提供するのに役立っています。

さらに、以前に提供された支援に関する状況認識を持つことで、重複や非効率性を回避し、どの支援が効果的であるかをより深く理解することができます。しかし、活動の存在、焦点、効果に関する支援提供者と受益者の双方の認識のずれや、支援の分散的な提供は、状況認識の妨げとなってしまっています。

2) 欧米諸国による加速化されたCDAのための継続的な資金調達メカニズムの確立

民間セクターが深く関与するCDAの提供には前例がほとんどないため、ロシア・ウクライナ戦争が勃発する以前の米国には、長期的なサイバー能力構築の取り組みとは異なるCDAを特定、支援、提供するための正式なメカニズムは存在していませんでした。正式なメカニズムが組織され始めたのは、紛争開始から約2年後の2023年後半になってからです。資金調達メカニズムの欠如と差し迫った危機が過ぎ去ったという感覚により、民間セクターによる自主的な支援の萎縮に繋がっていきました。

さらに、ウクライナに対するCDAは、他地域の新たな紛争の可能性対して優先順位が下げられており、現在は米国内政治の影響を受けています。CDA活動に対する長期的で専用の資金調達メカニズムがあれば、こうした変動性を減らすのに役立つでしょう。さらに、長期的な資金調達は、世界的な安定への支援、費用対効果の高いCDAの提供、そして被支援国へのセクターレベルの改善の提供に重点を置くべきです。

3) 状況認識とインテリジェンスツールの提供に向けたCDA能力の強化

CDACは、Looking Glass社（現Zero Fox社）によるアタックサーフェスの監視、ThreatQuotient社およびRecorded Future社のインテリジェンスプラットフォームなど、状況認識やインテリジェンスツールの提供に役立つさまざまなツールやサービスを提供してきました。Tenable社の戦略的能力およびプログラム担当副社長兼CTO（最高技術責任者）のクリストファー・デイ氏は、次のように説明しています：

『防衛を担う者にとって視認性は重要です。ここでいう視認性とは、運用環境から収集した技術的なサイバー遠隔測定データや、運用環境に関するデータ、さらには敵対者に関する情報を意味します。何も知らない、あるいは自社のシステムに対する攻撃を目視できない攻撃者を阻止することは困難です。具体的には、欧米の政府や民間情報機関がウクライナに照準を合わせたことで、ロシアがウクライナのネットワークやシステムに対して攻撃的なサイバー作戦を実行することが非常に困難になりました。』

4) リソース割当ての為、サイバー能力構築、CDA、サイバーレジリエンスの区別を行う

一連の活動が重複しているため、サイバーセキュリティ支援の種類間の明確な区分はやや恣意的です。

しかし、サイバー能力構築、CDA、サイバーレジリエンスの区別は、リソース割り当て、および関連するタイミングと優先順位の決定に役に立ちます。サイバー能力開発には、通常、法律や規制、トレーニング、労働力開発が含まれ、紛争が発生する前に効果的な国家サイバー政策と組織が実施されるように支援します。

CDAとは、インシデント対応や攻撃対象領域の監視などの活動を含む、標的型攻撃を阻止する能力を持つ政府や重要インフラ組織を支援することを指します。サイバーレジリエンスは、政府や重要インフラを支えるクラウドなどのデジタルインフラを向上させるための長期的な取り組みです。

CYBER CAPACITY BUILDING	→	CYBER DEFENSE ASSISTANCE (CDA)	→	CYBER RESILIENCE EFFORTS
紛争前		紛争時		紛争後
法律・規制		サイバー防衛重きを置く		長期的な復興への取り組み
訓練・労働力開発		標的型攻撃を阻止する		デジタルインフラの改善
国家サイバー政策・組織		インテリジェンス、ASM、セキュリティ運用、インシデント対応を含む		

これらの活動はスペクトルに沿って存在しており、サイバー空間における国家の防衛には、適切なタイミングで全体にわたる連続的な取り組みが必要となります。したがって、政策立案者およびサイバーセキュリティ業界は、支援のカテゴリーごとの定義を策定し、被支援国にとってバランスのとれたパッケージを確保するべきです。

5) 紛争に備えて、重点的に取り組む運用ラインを確立する。

2023年のアスペン研究所のCDAに関する論文[32] では、支援を受ける側と支援を行う側との早期のつながりと信頼関係を構築する必要性、および能力提供者を特定、集結、組織化する必要性が強調されました。支援を受ける側と支援を行う側は、さらに一歩進んで、机上演習、レッドチームの取り組み、セキュリティ・オペレーション・センター（SOC）の強化、その他の運用作業において協力し、従来の紛争の中でサイバー作戦から防衛する能力を開発することで、潜在的な紛争に備えて事前に準備する必要があります。効果的な準備を行うには、ステークホルダーの関与と、活動の焦点を絞り、計画を立て、実行するための調整ハブが必要です。CDACのような組織は、適切なリソースが確保されれば、メンバー企業、潜在的な支援受益者、政府機関を巻き込んで、このような活動を調整することができます。

今後の潜在的な見通し

ウクライナ紛争の結果と終結時期は依然として不透明ですが、バルト三国、モルドバ、ポーランドがロシアの次の集中的な侵略の標的になる可能性があります。モルドバはウクライナとルーマニアの間に位置する小国で、ロシアとは歴史的なつながりがあり、ロシアはウクライナに戦争を仕掛けているにもかかわらず、モルドバの親欧米派のマイア・サンドゥ大統領の政権を不安定化させるためのサイバー作戦も同時並行で行っています[33] 。バルト諸国も同様の状況にあり、2007年のエストニアの状況と似ています[34]。今年の初め、ロシアの国会議員で下院議員のアレクセイ・ジュラヴリョフは、ポーランドが他の旧ソ連領と同様に、ロシアの次の標的になる可能性を示唆しました[35]。

[32] https://www.aspeninstitute.org/wp-content/uploads/2023/02/Aspen-Digital_The-Cyber-Defense-Assistance-Imperative-Lessons-from-Ukraine.pdf
[33] https://www.csis.org/analysis/moldovas-fate-tied-ukraines-now-time-west-go-big-moldova
[34] https://www.nytimes.com/2007/05/29/technology/29estonia.html
[35] https://www.newsweek.com/putin-ally-says-poland-next-ukraine-war-rant-russian-tv-1860470

2024年5月、ポーランドのCERT（CERT-PL）は、ロシアの軍事情報機関（GRU）と関連のあるハッカー集団APT28が、広範囲にわたるスパイ活動とマルウェアキャンペーンでポーランドを標的にしているとコメントしました[36]。これらの国々はウクライナと同様の脅威に直面しており、ウクライナ情勢がさらに展開するにつれ、サイバー攻撃が増加する可能性があります。ウクライナのために開発されているサイバー防衛コミュニティと組織体制は、バルト三国、モルドバ、ポーランドでも活用できます。

東アジアにおける地政学的な緊張も高まっています。昨年末、中国の習近平国家主席は、2027年という公表されたタイムラインには同意していないものの、将来的に中国と台湾を再統一する意向を公に宣言しました[37]。台湾海峡で緊張が高まれば、中国はサイバー攻撃を利用して台湾を威嚇するなど[38]、同盟国の支援を妨害する可能性があると、多くのアナリストが予測しています。台湾では1日あたり240万件以上のサイバー攻撃の標的となっており、2023年の1日平均120万件の2倍に当たります[39]。サイバースパイ活動と混乱を行う中国の取り組みは、米国でも増加しており、2024年のソルト・タイフーン・キャンペーンは少なくとも9つの米国の通信会社に影響を与え[40] オーストラリア[41] と日本[42]でも明確に認識されています。中国はまた、フィリピンに対する誤情報とハッキングキャンペーンを強化しています[43]。台湾海峡危機の際には、既存のサイバー防衛コミュニティを活用することができますが、一部の専門家は、米国企業の中国との経済関係が米国の民間部門による台湾支援の妨げになると懸念しています[44]。しかし、CDACのような多くの欧米のテクノロジー企業やサイバーセキュリティ企業は、すでに中国とのほとんどの関係を断ち切っており、その多くが台湾の支援に関与しています。同盟国であるオーストラリアや日本などの民間セクターを巻き込む可能性もあります。

[36] https://therecord.media/poland-cyber-espionage-russia-gru
[37] https://www.nbcnews.com/news/china/xi-warned-biden-summit-beijing-will-reunify-taiwan-china-rcna130087
[38] https://thediplomat.com/2024/02/in-a-crisis-could-china-coerce-taiwan-through-cyberspace/
[39] https://www.darkreading.com/cyber-risk/as-tensions-with-china-mount-taiwan-sees-surge-in-cyberattacks
[40] https://www.darkreading.com/cyberattacks-data-breaches/china-salt-typhoon-charter-windstream-telecom-victims
[41] https://itwire.com/guest-articles/guest-opinion/a-wake-up-call-for-australia%E2%80%99s-telecom-sector-lessons-from-the-u-s-salt-typhoon-hack.html
[42] https://www.asahi.com/ajw/articles/15570789
[43] https://www.darkreading.com/cyberattacks-data-breaches/philippines-pummeled-by-assortment-of-cyberattacks-tied-to-china
[44] https://cset.georgetown.edu/publication/which-ties-will-bind/

結論

将来の紛争において、民間セクター主導のサイバー支援とサイバー防衛の重要性は明らかです。ウクライナにおける過去3年間の紛争は、サイバー防衛支援の調整を支援する新たなメカニズムや組織を生み出すことになりました。ウクライナにおけるCDA活動の進化は、支援を受ける側の国が透明性のある優先順位付けされた要件を提示する必要性、長期的な資金調達メカニズムを確立することの重要性、運用に重点を置いた支援の価値、そして紛争に備えてあらかじめ取り組みの方向性を定めておく必要性を示しました。ロシア周辺および東アジアにおける地政学的な緊張が、サイバー領域へ拡大し続けている中、米国が危機を管理し、必要に応じて同盟国や友好国を効果的に防衛するためには、これらの教訓が極めて重要となります。

ASPEN DIGITAL
aspen institute