国民国家、サイバー紛争と THE WEB OF PROFIT

Michael McGuire博士、犯罪学上級講師
Surry大学

内容

序文 Ian Pratt

Global Head of Security for Personal Systems, HP Inc.

国民国家のサイバー紛争やサイバースパイの世界は、もともと秘密主義の世界です。このようなプレイヤーがどのように活動し、どのようなツールを使用し、何に動かされ、どのようにして覇権を握っているのか、その証拠を見つけることは常に困難でした。そこで今回、英国Surrey大学の犯罪学上級講師であるMichael McGuire博士の研究をご紹介し、国家のサイバー領域がどのように進化しているかを明らかにします。

例えば、最近発生したSolarWinds社のサプライチェーン攻撃は、Stuxnet以来、最も巧妙な国家による攻撃であると考えられています。また、Covid-19ワクチンの開発に関する知的財産を盗み出そうとする大胆な試みもいくつかありました。このように、陰に隠れていた国家による干渉の問題が問題となり、脚光を浴びるようになったことで、本報告書はさらにタイムリーなものとなっています。

McGuire博士の研究が示すように、このような緊張の高まりは容易に予見できたはずです。過ヂ20年間、国民国家サイバー活動の厳しさ、開放性、多様性は着実に上昇してきました。その背景には、監視、スパイ活動、破壊活動など、伝統的な軍事・諜報活動の目的でサイバーを利用する動きが広がっていることがあります。また、憂慮すべきことに、本レポートでは、重要インフラに対するサイバー攻撃によって、サイバーとフィジカルの世界が衝突し、悲惨な結果を招く可能性があることも強調しています。

国民国家とサイバー犯罪経済（’The Web of Profit’として知られています）との交わりは、特に興味深い展開です。国民国家は、自分たちの戦略的利益を追求するために、あるいは代理人を利用してサイバー攻撃を「隠蔽」するために、ツール、データ、サービス、人材を購入したり取引したりして、意図的にこのWeb of Profitに関与しています。同様に、2017年にWannaCryのハッカーが使用した悪名高いエクスプロイトであるEternalBlueのように、国民国家が開発したツールもサイバーブラックマーケットに出回っています。

パーソナル・システムのセキュリティ部門のグローバル・ヘッドととして、このレポートには3つの重要なポイントがあります。

01 **罪のない人々がその渦中に巻き込まれています：**国家間の紛争に真空地帯はありません。企業も個人も、直接の標的（例：ワクチンを開発する研究施設）として、あるいはより大きな標的への足がかり（例：SolarWindsのサプライチェーンハッキング）として、そこに吸い込まれています。

02 **サイバー条約は一夜にして成立しません：**国際関係の中でも比較的新しい分野であるため、「ルール」が少なく、グレーゾーンが非常に多い。例えばAPT（Advanced Persistent Threat）グループと国家の境界は曖昧です。サイバー戦争やサイバー兵器に関する合意が得られる日が来ることを期待していますが、現在のところ、この流れを止めることができるものはほとんどありません。

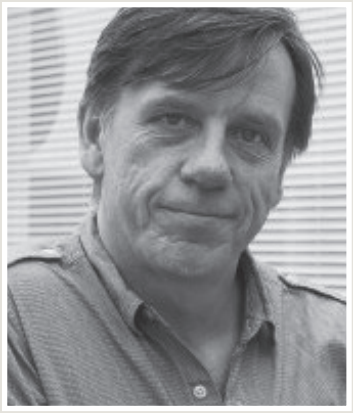
03 **エンドポイントは、依然として最も多い感染経路です：**個人でも企業でも、自分自身を守る必要があります。そのためには、エンドポイントを防御することが最も効果的です。ソーシャルエンジニアリングやフィッシングを利用してターゲットを感染させ、認証情報を盗み出し、永続化するなど、エンドポイントはすべての侵害において最も一般的な感染ポイントとなっています。

国民国家の活動の厳しさ、巧妙さ、規模、範囲が拡大し続ける中、私たちは一歩先を行くためにセキュリティを改革する必要があります。そのためには、より強固なエンドポイント・セキュリティ・アーキテクチャが必要となります。これは、最小限の権限でアクセス制御を行う、きめ細かなセグメンテーションのゼロトラストの原則に基づいて構築されるでしょう。私たちは今、クロスファイアの中にいるのです。ですから、すべての企業が自分自身とそのネットワークを守るためにできることをすることが重要なのです。

> *...最近のSolarWinds社のサプライチェーン攻撃は、Stuxnet以来、最も洗練された国家による攻撃であると広く考えられている。*

> *過ヂ20年間、国民国家のサイバー活動の厳しさ、開放性、多様性は着実に上昇してきた。*

> *国民国家の活動の厳しさ、巧妙さ、規模、範囲が拡大し続ける中、私たちは一歩先を行くためにセキュリティを改革する必要がある。*



エグゼクティブ・サマリー

Michael McGuire博士

犯罪学上級講師、Surry大学

古代中国の軍事思想家である孫子の名著 ***孫子の兵法*** で示されている戦略は、サイバー空間で展開されている国民国家間の新しい種類の争いに豊かな洞察を与えてくれます。特に、「戦わずして人の兵を屈する」ことが戦いの本質であるとする孫子の示唆は的を得ています。

国民国家の裏工作は、その性質上、機密のレベルが高いため、不透明な研究分野として知られていますが、本研究では、公開されている情報（報道で報じられている内部告発者やインサイダー・リークなど）から得られた独自の洞察と非公式の報告、および2019年から2021年の間に発生した200件以上の既知のインシデントの分析を行いました。また、サイバーセキュリティ、インテリジェンス、政府、学界、法執行機関などの関連分野における50人以上の主要な実務家に対する調査から得られた情報や、Web of Profit 調査のフェーズⅡの一環として実施されたダークネット上の情報提供者やその他の秘密の情報源から得られた情報も提供しています。方法論の詳細については、Apnedix Iを参照ください。

“そして、新しい種類のサイバー攻撃、「エクスプロイト」の備蓄、または攻撃ツールと技術の組み合わせ[6]などを開発することを目的とした専用の研究プログラムもあり、これらの戦略的目標を推進するために国家が使用する方法は著しく複雑化してきている。

我々の分析によると：

01 **サイバーベースの国民国家間の争いが拡大していることから、私たちはインターネットが登場して以来、最も「高度サイバー紛争」(ACC)に近い状態にあると言えます。**サイバー攻撃の頻度にしても、ハイブリッド化(サイバーと物理/キネティックの融合が進むこと)現象にしても、既存の地域紛争がサイバー紛争の悪化・促進に果たす役割にしても、不吉な兆候を無視することはますます難しくなっています。

02 **今や各国はサイバースペースにおける戦略的優位性の獲得に向けて、膨大な時間と資源を投入する準備ができています。**[1] サイバーセキュリティへの支出は、米国では11%（2019年 ~ 2021年[2]）、中国では25%（2030年まで[3]）、EUでは50%（2023年まで[4]）、ロシアでは最大200%（2023年まで[5]）増加すると予測されており、サイバー空間における国家の戦略的関心が高まっていることは明らかです。そして、新しい種類のサイバー攻撃、「エクスプロイト」の備蓄、または攻撃ツールと技術の組み合わせ[6]などを開発することを目的とした専用の研究プログラムもあり、これらの戦略的目標を推進するために国家が使用する方法は著しく複雑化してきています。2020年末に行われたSolarWindsのハッキングによる米国のサイバーセキュリティへの大規模な侵入は、おそらく最も壮大で悪名高い最近の例として挙げられます。しかし、その成功にもかかわらず、これははるかに広範な活動の中の1つのインシデントにすぎません。

03 **The Web of Profit（利益の網）とは、世界中に存在する相互に接続された地下のサイバー犯罪経済のことで、オンライン環境における国家間の紛争の特徴を決定します。**多くの国家がWeb of Profitで利用可能なツールやテクニックを積極的に活用しているだけでなく、中には自分たちの関心事を進めるためにサイバー犯罪者を代理人として採用している国もあります。逆に、国家安全保障機関に起源をもつ多くのツールが、サイバー犯罪者の手に渡っています。有名な例としては、2017年にWannaCryのハッカーが使用して世界中に大混乱を引き起こしたNSA EternalBlueエクスプロイトがあります。このようにして、国民国家は、サイバー犯罪経済を構成するWeb of Profitの恩恵を受ける側と貢献を行う側の両方になってます。

---

1 軍事用語では、陸・海・空・宇宙の4つの伝統的な紛争地域を強化するものです。
2 Slye （2020年）
3 Xinhua （2019年）
4 Townsend （2019年） – これは、EUサイバーセキュリティ機関（ENISA）の予算が、この期間中に1,100万ユーロから2,300万ユーロに増加したことを指しています。また、EUはサイバーセキュリティ産業を強化するために、さらに20億ユーロを投じて、最先端のサイバーセキュリティ機器などの資金を調達することを約束しています。
5 Isvestia （2020年）
6 Sunburst/SolarWinds攻撃で見られた、フィッシングメール（手法）とマルウェア（ツール）の組み合わせは、この例に該当します。

政治、戦略、商業、犯罪がかつてないほど融合したことで、ユニークの課題が現れ始めている…

このように、実効性のある規制や、オンラインでの行動の許容基準を策定しようとする国家側のコンセンサスが得られないことは、良いニュースではありません。

04 **また、国民国家は新しい機会をすぐに利用する準備ができています。**過去12ヶ月間に起こったCovid-19パンデミックへの対応は、この準備態勢の典型的なケーススタディとなります。一方で、パンデミックは今回の調査期間中、世界の出来事に大きな影を落とし、旅行や貿易など、国民国家の活動の多くの伝統的な分野に混乱と障害をもたらしました。しかし、国民国家のサイバー紛争については進展を中断させるどころか、激化させています。ワクチンの知的財産権をめぐる争いであれ、サプライチェーンを破壊しようとする試みであれ、Covid-19危機は、国家が戦略的目標を強化するためにサイバーツールを使用する際に、どの程度まで準備しているかを示しています。また、国民国家がCovid-19関連のIPデータを取得するために使用している手法の一部は、物質的利益を追求するためにサイバー犯罪者が最初に試されたもののようなので、上述したサイバー犯罪手法と国民国家のサイバー攻撃との間の関係がさらに明らかになりました。

つまり、伝統的な国際関係とサイバー犯罪経済、そして現在デジタルアンダーグラウンドを動かしているツールやテクニックとの融合です。政治、戦略、商業、犯罪の間のこの前例のない融合は、デジタル世界をどのように規制するか、特に国民国家間の緊張を和らげることができる共通の関心分野をどのように探すかというユニークな課題が現れ始めています。

このように、実効性のある規制や、オンラインでの行動の許容基準を策定しようとする各国のコンセンサスが得られないことは、良いニュースではありません。それどころか、私たちがインターネットから受けるリスクは、これまで考えていたよりもはるかに大きい可能性があることを示しています。そこで、本レポートでは、サイバー・緊張緩和のための最新のオプションについての見解を示しています。ここで議論されているサイバー平和の見込みが薄くなっているように見えることは、サイバー空間における自国の利益を維持しつつ、紛争の拡大を避けるという国民国家の課題を浮き彫りにしています。提言としては、サイバー条約やサイバー協定の締結に向けて政策立案者がより積極的に関与すること、国家の典型的なサイバー兵器やそれに対抗する方法についてサイバーセキュリティの専門家がより積極的に関与すること、企業がデータやネットワーク容量に対する国家の脅威を管理する方法を共有することなどが挙げられます。

不完全なデータを新しい方法で分析し、専門家の知識で補うことで、これから先の内容が、国民国家の脅威に対してより多くの情報を得て、より適切な対応をとるための新たな基盤となるでしょう。

重要な発見：拡大、激化、拡張

拡大

1 頻度＆普及

2017年～2020年の間に「重大な」国家のインシデントが**100%増加**[7]

2020年の**一般に公表されているサイバー攻撃は月に平均10件**以上

専門家[8]の**64%**が2020年はサイバー空間の緊張が**「心配」**または**「非常に心配」**になったと考えている

2 サイバー/フィジカル ハイブリッド化

40%以上のサイバー攻撃がフィジカルおよびデジタルの要素を持っていた

20%が地域紛争と相関していた[9]

激化

最も使われている兵器：

78%
2019年にサプライチェーンを狙った攻撃が増加[10]

37%
の専門家がサプライチェーン攻撃は国家により開発された「最も重大」な攻撃方法と回答

40%
のセキュリティ侵害が現在間接的[11]

2017年～2020年に
27の国家による既知
のサプライチェーン攻撃があった[12]

既知の国家の標的：

- 企業 35%
- サイバー防御機構[13] 25%
- メディアと通信 14%
- 政府機関あるいは監督官庁 12%
- 重要インフラ[14] 10%

7 CSIS（2020年）も同様な集計をしています。
8 エグゼクティブ・サマリーと方法論の専門家パネルからの発見
9 Brown（2020年）
10 Symantec（2019年）
11 Accenture（2020年）
12 Herr et al（2020年）
13 サイバー防御機構とは、国家のサイバーセキュリティを保護する責任を負う機関、サービス、ハードウェア、ソフトウェアの集合体と定義されます。これには、英国NCSC（National Cyber Security Centre）、米国CISA（Cybersecurity and Infrastructure Agency）、各国のCERT（Computer Emergency Response Team）、GCHQやNSAのような情報収集機関、民間のインターネットサービスプロバイダー（ISP）、保護ドメインネームシステム（DNS）のように政府のユーザーが疑わしいサイトにアクセスするのをブロックするソフトウェア、政府のファイヤーウォール、テイクダウンサービスなどが含まれます。
14 その他のデータ（O Malley, 2020年）では、2019年～2020年の間に、北米の企業の36%が国家の脅威を報告していることが示されており、この結果を裏付けるものとなっています。

拡張 I
サイバー犯罪経済

20% 高度な兵器を利用したサイバー攻撃

50% 低予算のツールの利用

65% 国家がサイバー犯罪から利益を得ていると考えている専門家

58% 国家がサイバー犯罪者をリクルートするのは一般的だという専門家

拡張 II
Covid-19

専門家の**75%**が、Covid-19は国家が活用すべき「重要な新しい機会」であると回答

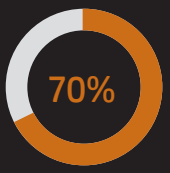
2020年7月～9月にかけて、2020年1月～6月と比較して、国家のインシデントが**40%**増加

製薬会社へのサイバー攻撃が**50%**増加[15]

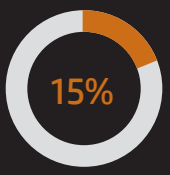
5万件以上の2020年2月～5月に新たに作成されたCovid-19関連サイトが不正に関与[16]

202017年11月以降に医療機関に対するサイバー攻撃が**45%**増加[17]

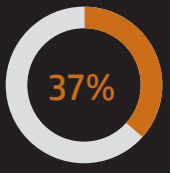
サイバー戦争か、サイバー平和か？
果たしてサイバー条約は成立するのか？



サイバー戦争の拡大を防ぐためには、サイバー条約が必要だという回答

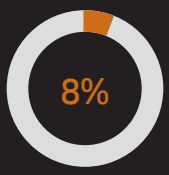


今後5～10年の間に合意が得られるだろうという回答

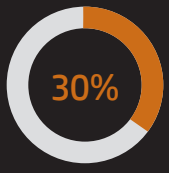


10～20年かかるだろうという回答

20年以上かかるだろうという回答



わからないという回答



どのような時間枠でもサイバー条約が成立する見込みはないという回答

15 Coker （2020年）
16 Chandler （2020年）, Lancaster （2020年）
17 Lancaster （2020年）

1.1

競争、紛争、あるいは高度サイバー紛争（「サイバー戦争」）？

この研究では、国家間の競争がどのようなエスカレーションのレベルで解釈されるべきかについてのより正確な評価を行うために、特別な分析ツールを開発し、現在の緊張状態を明確にマッピングしました。このツールでは、3つの異なるレベルを使用します。

(i) ***サイバー競争：***国家がサイバー空間を積極的に利用して、競争相手に対する優位性を獲得すること。経済的アクターが行うのと同様ですが、認識されている行動規範や制限は少ない。例えば、ドメインネームシステムを支配しようとする試みなど。

(ii) ***サイバー紛争：***国家間のオンライン競争が激化し、経済的優位性よりも戦略的目標が優先されるようになった状態。協定や合意は重視されないが、あからさまな争いには発展しない。例えば、情報やその他の戦略的に有用なデータを得るために、競争相手のネットワークを調査しようとすること。

(iii) ***高度サイバー紛争（ACC）：***各国がデジタル攻撃と反撃を繰り返すようになること。例えば、ネットワークを侵害し、機能を喪失させることを目的とした高度なサイバー攻撃など。オン / オフラインのターゲットが曖昧になり、電力網や水道などの物理的資産にも注目する。サイバー攻撃への報復として通常兵器を使用する可能性。

次に、従来の研究で考えられていた伝統的な文脈での高度な（キネティックな）紛争に至るまでの一連の典型的な指標を特定し、これをデジタルの文脈に合わせて調整しました。[18] その指標とは、***サイバー兵器の数と洗練度を高めようとする積極的な試みの証拠***や、***国家が戦争による領土的利益を求めている証拠***などです。これらの指標をサイバー世界での類似性と関連付け、過去20年間の3つの時期（2000年、2010年、2020年）にこれらの指標がどの程度有効であったかを評価することで、現在展開されている状況がどの程度深刻であるかをより正確に定量化することができました。

18 例えばJackson and Morelli（2009年）や Hegre et al（2011年）を参照ください。

高度サイバー紛争ヒートゲージ

高度な紛争/戦争への過程を示す伝統的な指標	サイバー・パラレルとその事例	2000年	2010年	2020年
戦争をしない最小限の理由しか無いという認識	標準的なサイバー・セキュリティツールでは、国家を標的としたサイバー攻撃を防ぐことができない。これまでのところ、サイバー攻撃に対する報復は、ライバルの情報システムへの攻撃に限られている。			
競争相手の行為が戦争行為であるという認識	英国の司法長官は、西側諸国はネットワークへの侵入を「戦争の原因」と見なすだろうと発表。[19]			
戦争で得られる利益が潜在的なコストを上回るという感覚	2009年以降の緊張の高まり以来、サイバー攻撃の増加に対する制裁措置は進展していない。			
各国が戦争による経済的利益を期待している証拠	多くの国民国家は、収入増やその他の経済的利益のためにサイバー紛争を追求。			
侮辱されたことに対する報復	ネットワーク侵入に対応する積極的な準備ができていることを示す証拠が増えた。			
競争相手とのコミュニケーションや行動規範への合意の失敗	サイバー兵器に関する国際的な合意がないこと。			
「ユース・バルジ」（若者の増加：戦争に参加できる人口の増加）	情報技術に長けた若年層の増加により、国民国家による展開が可能となる。			
国家が戦争によって領土的利益を求めている証拠	ライバルのネットワークやデジタル資産を「占拠」または併合しようとする行為（例えば、長期間隠れるマルウェアを仕込む）が一般的になる			
兵器の数や種類を増やそうとする積極的な試みの証拠	サイバー兵器の数は、2000年～2020年の間に10,000%を超える割合で増加[20]していると推定される。			
宗教的/思想的な意見の相違	サイバー攻撃が既存の意見の対立を激化させること、以外には明らかな類似点は無し。			
過去の紛争に起因する不平不満	オフラインの不平不満のサイバー空間への頻繁な投稿			

19 Hall（2018年）

20 2000年に知られていたマルウェアの種類と国家による潜在的な使用の評価に基づいた数字、2020年との比較

指標が4つ未満の場合、専門家パネルは、この状況を攻撃的な*サイバー競争*の一形態に過ぎないと評価しました。指標が4～8個の場合は、より進んだ競争であり、*サイバー紛争*に相当すると評価しました。8つ以上の指標がある場合は、*高度サイバー紛争*（ACC）に近いか、すでになっていると判断し、俗に言うサイバー戦争としました。

この種の指標は、過去20年間の緊張の高まりを明確に示すのに有効です。2000年には、明確な指標が4つ以下しかなかったため、サイバースペースにおける国家間の関係は、まだ競争上の優位性を得ることが主目的でした。2010年には、約7つの指標が議論の余地なく当てはまり、よりあからさまな紛争ベースの関係に移行しつつあることを示しています。2020年には、少なくとも11の要素が揃うことになり、現在の予測は憂慮すべきものとなっています。兵器の増加や、敵対的なネットワークへの侵入を「戦争行為」とみなすという政府代表の認識[21]などの指標が累積的に増加しており、我々は危険な段階に移行しています。同じように、あるいはそれ以上に問題なのは、こうした緊張の高まりがもたらす潜在的な重大性について、一般の人々の認識が不足していることです。

2.1

サイバースペースにおける国民国家：国民国家のサイバー紛争の特徴

現在、国民国家はデジタルネットワークを利用して、通常の行動規範から外れた方法で積極的に影響力を競い合っているため、こうした戦略的ダイナミクスを特定し、特徴づけることがますます重要になっています。今回の調査では、国民国家のサイバー紛争の特徴として、少なくとも10個の特徴を抽出しました。

(i) **非対称：**小国は大国にうまく立ち向かうことができます。
   a. 今回分析したインシデントの**70%**以上は、15～20人未満のグループに攻撃されたり、紛争に巻き込まれたりした国家を対象としたものです。

(ii) **見えない：**サイバー戦士は、隊列を組んで行進し忠誠を示す旗をつけて行進することはありません。
   a. 証拠が明らかな場合でも、今日までどの国もサイバー攻撃を告白していないという100%の否定率がこれを強調しています。

(iii) **分子的：**闘争には複数のエージェントが関与することがあり、その組み合わせも多い。
   a. 例えば、（複数の可能性がある）国民国家、その国家が使用する代理人や傭兵、裏工作を行う諜報機関、（ハニーポットを使って）サイバー攻撃に対応あるいはサイバー攻撃を実施するサイバーセキュリティ企業、さらにはサイバー犯罪グループなどがあります。

(iv) **多次元的：**サイバー紛争では、ライバル企業の情報システムやサイバー防御を超えて、物理的な資産にまでサイバー攻撃が及ぶケースが増えています。
   a. 調査で分析されたインシデントの**40%**以上は、物理的およびデジタル的要素を持つ資産への攻撃でした。

(v) **グローカル**[22]**：**サイバー紛争は、地域的な闘争とグローバルな闘争との間に大きな相互依存関係があることを示しており、前者が後者の踏み台になることがよくあります。
   a. 今回分析したインシデントの約**20%**は、地域的なサイバー紛争に端を発していました。

21 この種の主張は、最近ではイギリスの司法長官（Hall, 2018年）やEU（Muncaster, 2017年）が行っています。同様に、米国では、ネットワークを侵害しようとする試みは、特定の状況下では「武力攻撃を構成する」可能性があると宣言しています（Wolfe, 2019年）。
22 この言葉はRobertson（1994年）に由来しています。

(vi) **パーソナル：**国民国家は戦略的なサイバー利益を追求するために、脅威をもたらすと考えられる個人を直接標的にする準備をますます整えています。
   a. 最近の例として、2018年にAmazonのCEOであるJeff Bezos氏の写真が国民国家の関係者によってハッキングされて公開されたこと[23]や、国民国家に脅威を与えていると考えられる個人に対して広範なデジタル監視が行われていること[24]などが挙げられます。

(vii) **多面的：**サイバー紛争は、貿易戦争のような他の種類の非軍事的紛争を他に反映させる役割を果たすようになり、同時に相互の緊張を増幅させています。

(viii) **ハイブリッド化 ：**サイバー作戦は、物理的な紛争と連動して、あるいはそれに対応して行われることが多くなっています。

(ix) **曖昧：**サイバー紛争の中で、敵と味方を分けるのは難しいことです。
   a. 例えば、2013年にCIAの内部告発者であるEdward Snowden氏が発表した内容によると、NSAがドイツのAngela Merkel,首相をはじめ、EUの上級幹部、その他35人の世界のリーダー、そして7,000万人以上のフランス国民の電話や通信を盗聴していたことが明らかになりました。[25]

(x) **文化的：**選挙への影響やソーシャルメディア上での態度の「認知的ハッキヌグ」など、サイバー紛争は従来の戦争よりもはるかに敵国社会の社会文化構造に破壊的な影響を与えます。
   a. 例えば、ソーシャルメディアに掲載された偽のストーリーは、真実のストーリーよりもはるかに多くの「いいね！」を獲得し共有され、長く保存され、配信範囲も広くなる傾向があることが、多くの研究で示されています。[26]

23 Merriman （2019年）
24 Ignatius （2018年）
25 Ball （2013年）
26 例えば、Silverman（2016年）を参照ください。

2.2

戦略、目標、標的、ツール

個々のサイバー攻撃を識別することも重要ですが、国民国家のサイバー紛争への取り組みをより完全に理解するためには、データのギャップを埋めて、重要なパターンやダイナミクスを見極める必要があります。

この研究のために、私たちは**NSiC**（Nation States in Cyberspace）という分析手法を開発しました。NSiCのアプローチは、合成と単純化のプロセスを用いて、サイバースペース内での国家のサイバー攻撃の原動力となる多くの複雑な決定と動機を分析者がすぐに理解できるようにします。これを達成するために、4つの重要な**'SOTTT'**変数が国家の行動をマッピングするために使用されます。

戦略 → **目的** → **標的** → **ツール&テクニック**

このようにして、NSiCはインシデントのより統合された構図を提供し、より明確な分析と比較を可能にします。さらに、典型的なサイバー紛争がどのように発生し、維持されているかについて、より統合された包括的な理解が得られます。4つの変数はそれぞれ以下のように説明されます。

戦略

サイバー犯罪と国家の活動との間には密接な関係がある一方で、追求されている***戦略***、つまり優位性を獲得するための全体的かつ長期的な計画と行動には違いがあります。戦略をより深く理解することで、国家が特定の方法でサイバーツールを利用する理由を知ることができ、より多くの情報に基づいた対応が可能になります。我々は、インシデント・データベースから得られた国家の様々な攻撃行動を分析することで、サイバー紛争で優位に立つために国家が用いていると思われる14の異なる戦略を特定しました。このリストは明らかに単純化されたものですが（国民国家は状況に応じて他の方法や複数の方法で活動することもあるでしょう）、国民国家がどのように（そしてなぜ）特定の戦略的オプションを他のものよりも好むのかを理解するための有用な一覧表となります。

> ***戦略をより深く理解することで、国家が特定の方法でサイバーツールを利用する理由を知ることができ、より多くの情報に基づいた対応が可能になる。***

戦略	特徴
支配	サイバースペースを全領域でコントロールすることで得られる優位性
蓄積	通貨やデータなどの資産を構築することで得られる優位性
侵入	デジタル、物理的、認知的な保護を侵害することで得られる優位性
報復	攻撃的な行動には必ず反作用があることを敵に思い知らせることで得られる優位性
吸収	技術や資産を模倣・継承することで得られる優位性
促進	他の国家に機能を与えることで得られる優位性
保護	デジタル、物理または政治的構造を維持 / 強化することで得られる優位性
抽出	ライバルのデータなどの資産を不正に取得することで得られる優位性
破壊	敵の防御に混乱をもたらすことで得られる優位性
交渉	コンセンサスを得ることで得られる優位性
消ㅋ	脅威を恒久的に除ㅋすることで得られる優位性 - 現実または認識
補強	既存のリソースの構造を強化することで得られる優位性
浸透	ライバルのシステムに秘密裏にアクセスすることで得られる優位性
誇示	力や能力を誇示することで得られる優位性

図1-サイバースペースで採用される典型的な国民国家の戦略

例えば、支配戦略は、サイバースペースをコントロールをしようとする明示的な試みによって国家が優位に立つことを可能にし、抽出戦略は、ライバルのデジタル資産を不正に取得することによって優位に立つことを可能にします。

目的

国民国家は、長期的な戦略に加えて、より短期的な目的を追求することが多い。そのため、効果的な分析を行うためには、目的と戦略の組み合わせが必要となります。サイバー空間における国家の行動を形成する4つの典型的な目的が、我々のインシデント・データベースと本研究で得られた調査データの分析から導き出されました。以下の表にその詳細を示します。

目的	小目的	例
取得	**インテリジェンス**	軍事、産業、政治的な秘密/インテリジェンスの取得。例えば、製造業におけるサイバー攻撃の約95％は、現在、取得目的のスパイ活動と関連しています。[27]
	データ	2018/19年に発生した情報漏洩の約20～25％は、国家のアクターが関与していると考えられます。[28]
	収益	一部の国家では、輸出収益の30％に相当する収益をサイバー攻撃によって得ている可能性があります（Appendix II参照）
	ステータス	2014年のソニー・ピクチャーズのハッキングのように、能力を示すことが目的の象徴的サイバー攻撃。[29]
無力化	**破壊**	敵の資産にダメージを与えたり、機能を停止させたりすること - 例えば、Disttrackマルウェアを使用した湾岸石油会社に対するShamoonのサイバー攻撃では、ファイルが消去され、システムが機能しなくなりました。[30]
	混乱	ネットワーク機能の低下。インターネットの停止やネットワークの中断により、米国では年間約24億ドルのコストが発生すると推定されています。[31]
形成	**オピニオン**	「認知的ハッキング」 - 社会的対立や分断を広めるために偽情報を発信することなど。例えば、過激派の意見を広めたり、選挙プロセスを混乱させたりするため[32]に、国家が「ツイッターボット」を使用するケースが増えています。‘
	政権交代	例えば、ウクライナでは対立する国家が民族主義政府に介入し、ベネズエラでは電力などの重要インフラへのサイバー攻撃の可能性を含めた介入が行われています。[33]
ハイブリッド化	**戦術支援**	通常戦力の成功を補強するためのサイバー能力の利用 例：2019年の米国によるイランのミサイル能力へのサイバー攻撃。[34]

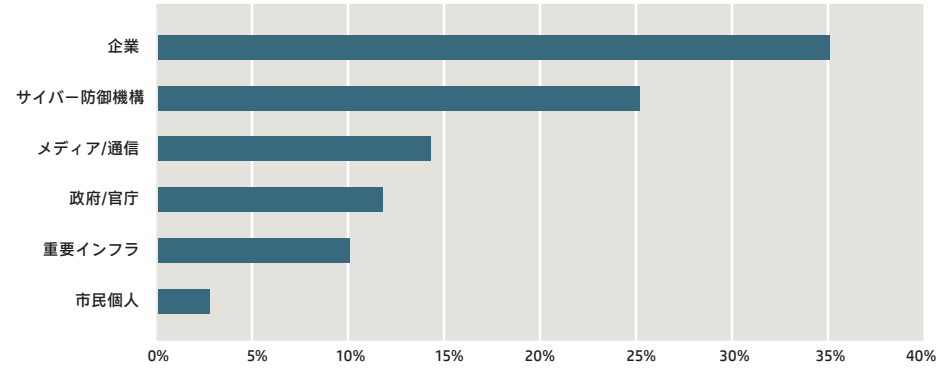
表1：サイバー紛争における国家の目的[35]

27 SOFF （2017年）
28 Verizon （2019年）
29 Elkind （2015年）
30 ENISA （2019年）
31 West （2016年）
32 Guglielmi （2020年）
33 Leetaru （2019年）
34 Lewis & Unal （2019年）
35 なお、これらは相互に排他的である必要はありません。国民国家はデータを得る目的と同時にインテリジェンスや収益といった副次的な目的も持っているかもしれません。

標的

戦略と目的は、サイバースペースにおける国民国家の行動を理解する上で重要な第3の要素、つまり典型的なサイバー攻撃の***標的***によって結び付けられます。我々のインシデント・データベースの分析と、この分野における他の研究[36]とを関連付けることにより、最も一般的に標的とされる資産のいくつかは、以下のように特定されました。.

国民国家によるサイバー攻撃で最も頻繁に標的とされるのは（分析されたサイバー攻撃の35%を占める）企業や法人。



グラフ1：国民国家によるサイバー攻撃の最も一般的なターゲット

… Covid-19ウイルスに関する知的財産（ワクチン開発に関する情報など）を取得しようとする試みは、報告されているPfizerのような製薬会社に対するハッキングやランサムウェアによる攻撃が約50%増加したことに関連している。

企業 – 国民国家によるサイバー攻撃で最も頻繁に標的にされるのは（**分析されたサイバー攻撃の35%**を占める）企業や法人です。セクターや規模にかかわらず、企業は、従来のサイバー犯罪者からのリスクと同様に、国家からのリスクに直面しているようです。知的財産やビジネス・インテリジェンスを得ることは、テクノロジー企業や製薬・バイオテクノロジー企業が特にリスクを抱えていることから、一つの明白な動機となっています。2020/21年のデータによると、Covid-19のパンデミックがこの傾向を悪化させています。例えば、Covid-19ウイルスに関する知的財産（ワクチン開発に関する情報など）を取得しようとする試みは、報告されているPfiz erのような製薬会社に対するハッキングやランサムウェアによる攻撃が約**50%**増加したこと[37]に関連しています。また、研究所に対するスパイ活動や医療機関の破壊も並行して行われており、2020年11月以降、研究所やCovid-19の患者を治療する病院に対するサイバー攻撃が**45%**増加していると言われています。[38] このような活動には国家が明確に関連しており、2019年から2020年の間にサイバースパイ活動に関与した悪意のあるアクターの約**38%**が国家に帰属しています。[39]

国家によるサイバー攻撃の脅威から安全な企業はないと思われます。例えば、知的財産権の窃盗を専門とするAPT10グループ（別名：***Menupass***または***Red Apollo***）[40]は、主要産業の顧客のデータを取得するために米国の法律事務所にハッキングしたこともあります。[41] APT10は、IT業界、大手アパレル企業、航空宇宙、重工業なども標的にしています。[42] 中小企業も同様に危険にさらされており、2017/18年にAPT28グループ（***Fancy Bear***、***Sofacy***、***Pawn Storm***などと呼ばれる）が行ったサイバー攻撃が注目を集めました。数千台もの中小企業や家庭用のルーターがハッキングされ、同グループの支配下に置かれました。[43] APT28は、2016年の選挙期間中の米国民主党へのハッキングに関連していたことがありますが、最近ではおそらく認証情報を取得したり、電子メールから有用なデータを抽出したりするために、企業やその他の分野の脆弱な電子メールサーバーを調査し始めています。44 また、APT28は、OfficeプリンターやビデオデコーダなどのIoT機器を利用して企業ネットワークへのアクセスを獲得することについても探っています。2019年には、同グループがVoIP電話と共にこうした機器を利用して、ネットワーク上の他の脆弱なマシンを侵害しようとした証拠が出ています。

APT28は、OfficeプリンターやビデオデコーダなどのIoT機器を利用して企業ネットワークへのアクセスを獲得することについても探っている。

36 例えば、CrowdStrike（2019年）、FireEye（2019年）などを参照ください。
37 Coker （2020年）
38 Lancaster （2020年）
39 ENISA （2020年）
40 APTグループは、様々な名称で呼ばれることが多く、また情報源によって一貫性がないことに注意してください。本報告書では、**番号を付けた**後に、そのグループに関連する最も一般的な名前を2～3個付ける方法を採用しています。
41 Leyden （2019年）
42 NSCS （2018年）
43 Lucero （2018)年）
44 Muncaster （2020年）

IoTデバイスを乗っ取るために単純なSSHブルートフォース/辞書攻撃を行うKajiのような新しいマルウェアの系統は、効果的なエンドポイントセキュリティと継続的なテストが、国民国家の脅威から企業ネットワークを守るために不可欠なツールとなっている理由をさらに強調している。

次に多かった標的は、国家のサイバー防御機構（サイバー攻撃の25%）で、これに対して個別の政府や官庁への攻撃はインシデントの約12%を占めている。

Lojaxのようなマルウェアは、OSの起動や読み込みを行うUEFI（Unified Extensible Firmware Interface）と呼ばれる最も深い操作レベルに位置することができるため、より致命的な脅威となる可能性がある。

このようにして、制限されたアカウントにアクセスして、より多くの貴重なデータが取得される可能性があります。[45] IoTデバイスを乗っ取るために単純なSSHブルートフォース/辞書攻撃を行うKajiのような新しいマルウェアの系統[46]は、効果的なエンドポイントセキュリティと継続的なテストが、国民国家の脅威から企業ネットワークを守るために不可欠なツールとなっている理由をさらに強調しています。

他には企業の電子メールの脆弱性を狙ったサイバー攻撃があり、2021年にはHafnium Advanced Persistent Threat（APT）グループが様々なゼロデイエクスプロイトを展開してMicrosoft Exchangeサーバーを標的にしました。Hafnium APT攻撃グループは、様々なゼロデイ脆弱性を利用してMicrosoft Exchangeサーバーを標的にし、電子メールを侵害してデータを盗み出し、長期間にわたってリモートアクセスを可能にするマルウェアを仕込みました。銀行、金融機関、電力会社などの企業や、小規模なホテルなどの中堅企業を含む、2万以上の組織が標的となりました。[47]

国家のサイバー攻撃に対する企業の脆弱性を示す最も新しい例は、2020年にSolarWinds社のOrionソフトウェアを使っていた企業が標的となったものです。このソフトウェアはサプライチェーン攻撃に利用され、米国の大手企業のシステムへの検知されないアクセスを可能にする正規の認証情報の取得を可能にしました。**15,000**社以上のSolarWindsの顧客がネットワークを侵害されましたが、その中にはFotune500企業の顧客も含まれており、特にITセクターのCisco、FireEye、Intel、Microsoftなども含まれていました。[48]

サイバー防御機構と政府機関へのサイバー攻撃[49] - 次に多かった標的は、国家のサイバー防御機構（サイバー攻撃の**25%**）で、これに対して個別の政府や官庁への攻撃はインシデントの約**12%**を占めていました。明らかに、国家はそれが防御の強度を試そうとするものあれ、業務の妨害であれ、重要データの流出であれ、自国のサイバーセキュリティ/サイバー防衛システムに対するサイバー攻撃に定期的に対処する必要があります。このため、サイバーセキュリティのテストは、政府機関に対するより直接的な攻撃と組み合わせて行われることが多くなるでしょう。例えば、米国のサイバー軍が2018年に行った‘Synthetic Theology’作戦は、脅威インテリジェンスのために他国のネットワークを調査するものでした。[50] また、より広範なインターネットインフラ自体を標的とすることにも関心が高まっています。例えば、2019年には、このようなサイバー攻撃の例が2つありました。1つは、スヌーピングやトラフィックのリダイレクトなどを可能にするDomain Name（DNS）の構造を狙ったもの。もう1つは、すべての通話ログデータを取得するためにモバイルネットワークを攻撃するものでした。Lojaxのようなマルウェアは、OSの起動や読み込みを行うUEFI（Unified Extensible Firmware Interface）と呼ばれる最も深い操作レベルに位置することができるため、より致命的な脅威となる可能性があります。[51] つまり、再インストールはもちろん、ハードドライブを消去してもマルウェアを除去することはできません。これまで事例は少なく、外交官やNGOを対象としたサイバースパイ攻撃に関連していましたが、マルウェアが汎用的なサイバー兵器として大きな可能性を秘めていることは明らかです。

敵対する政府の活動を理解したり、混乱させたりすることは、Turlaグループのような一部のAPT攻撃グループが特に重視しています。Turlaは2018年にハーグの化学兵器機関や英国の国防科学技術研究所（DSTL）のコンピュータシステムをハッキングしようとしたことに関係していました。[52] 2020年には、英国、米国、カナダの主要大学20校を対象としたランサムウェア攻撃（成功）に関連していますが、これは新たな攻撃ベクトルの一例に過ぎず、2018年～2020年の間に英国の大学だけで年間平均約1,000件のサイバー攻撃が行われていると言われています。[53] また、2020年のSunburstのサプライチェーン攻撃では、米国国土安全保障省、米国国務省、米国国立衛生研究所、米国商務省、米国財務省などの主要な政府機関への侵入も行われました。

メディア & 通信 - 敵対する国家のメディアや通信システムへのアクセスを得ることは、ますます魅力的な選択肢となっており、国家のサイバー攻撃の約**14%**を占めています。

45 Vavra（2019年）
46 Daws（2020年）
47 Seal（2021年）
48 Krebs（2021年）
49 サイバー防御機構とは主要なネットワーク、インフラ、その他のデジタル資産を保護するために利用されるツールと技術の両方を意味します。
50 Nakashima（2019年）
51 Higgins（2020年）
52 Crerar et al（2018年）& Gov. UK（2018年）
53 Coughlan（2020年）

現在、毎日1,000件以上の放送局へのハッキング未遂事件が発生しており、さらに広範囲な通信システムへの攻撃も発生しているようだ。

最近の一連の事件は、こうした疑念を裏付けるものであり、我々のデータによると、インフラに対するサイバー攻撃は現在、国家のインシデントの少なくとも10%を占めている。

…忘れてはならないのは、サイバー紛争に内在する力の非対称性により、報復、浸透、排除の戦略が、時に国民国家による市民個人への直接的なサイバー攻撃を伴うことがあるということだ。

議論に影響を与えたり、ライバル国の一般市民が入手できる情報の質を落としたり、あるいは単純な監視や情報収集を行ったりすることは、すべて戦略的な動機になります。2015年にフランスのTV5 Mondeがハッキングされ、12のチャンネルが18時間にわたって停止したことは有名な例です。[54] 最近では、Sandworm APTがウクライナのメディア企業のコンピュータを攻撃した例があります。[55] 現在、毎日1,000件以上の放送局へのハッキング未遂事件が発生しており[56]、さらに広範囲な通信システムへの攻撃も発生しているようです。例えば、BBCのような伝統的なニュースサイトが偽情報を流すために偽装されているだけでなく[57]、WhatsApp、WeChat、Telegramなどの新しい暗号化されたメッセージングツールが国家によってますます狙われるようになっています。2019年には、米国と同盟関係にある少なくとも20カ国の政府や軍の高官のWhatsAppアカウントがハッキングされ[58]、2020年には、「国家に支援されたアクター」が、電話番号とTwitterのユーザー名を結びつけることで、投稿のバイラル効果を高めていたことがTwitterで報告されました。[59] 外交文書のような秘密の通信を入手することも、もう一つの傾向です。例えば、最近、英国の元駐米大使が政府の重要なメッセージを流出させましたが、これは敵対的なサイバーパワーによるものである可能性が非常に高いようです。[60]

重要インフラ - 送電網や上水道システムなどの重要インフラは、長い間、潜在的な標的としてコメンテーターの想像力をかきたててきました。最近の一連の事件は、こうした疑念を裏付けるものであり、我々のデータによると、インフラに対するサイバー攻撃は現在、国家のインシデントの少なくとも**10%**を占めています。2019年に公益事業、エネルギー、健康、運輸部門のセキュリティスタッフを対象に実施した調査[61]では、90%が2017年から2019年の間に少なくとも1回、自社の設備に対する成功した攻撃があったと報告していることが明らかになりました。例えば、2014年のBlack Energyマルウェア感染による米国エネルギー事業者への侵入[62]は、2018年にSandworm APTやVoodoo Bear APTが同じマルウェアを使ってウクライナのさまざまなエネルギーインフラに行った攻撃の最終リハーサルだったと思われます。また、ウクライナの鉄道発券システムも同じグループによって侵害されました。さらに、海運会社や航空会社に気候情報を提供する気象システムへのサイバー攻撃も報告されています。[63]

市民個人 - 最後に忘れてはならないのは、サイバー紛争に内在する力の非対称性により、報復、浸透、排除の戦略が、時に国民国家による市民個人への直接的なサイバー攻撃を伴うことがあるということです。このような攻撃は数量的には少ないかもしれませんが（今回分析したサンプルの5%未満）、長期的には重要な影響を及ぼす可能性があります。個人の暗殺や評判への攻撃は長い間、国民国家によって行われてきましたが、デジタルネットワークの出現により新たな選択肢が生まれ、しばしば物理的活動と連動して行われるようになりました。確定的な証拠は限られていますが、この種の事件としてよく記録されているものがあります。例えば、2017年に、マルウェアに感染したツイートが、Twitterを使って米国国防省の職員とその家族に送られました。このメッセージは、個人の関心事に訴えるように注意深くターゲットを絞っていたと思われ、その結果、約70%のクリック率を記録しました。その結果、政府の機密情報が入った家庭用機器が危険にさらされました。[64] 特定の国で破壊的と見なされたジャーナリストは監視の対象となり[65]、高名な人物も標的となりました。例えば，AmazonのCEOであるJeff Bezosの名誉を傷つけようと，（ハッキングされた）危険な写真を流通させようとしたことは，敵対的国家のアクターと関連しています。[66]

上記のような主要なターゲット以外にも、不可解な例を見落とすべきではありません。例えば、競合する社会を混乱させることを目的とした**浸透**戦略では、社会文化的なプロセスや制度、特に選挙を標的とする試みが増えています。[67]

ツール & テクニック

戦略や目的と標的の組み合わせを成功させるためには、適切なサイバー兵器の選択が重要です。しかし、どのようなサイバー兵器を利用するかは必ずしも明確ではありませんでした。サイバー兵器とは、ツールやテクニックのことを指します。システムにダメージを与えたり、単にデータを盗んだりするような破壊的な能力を指す場合もあれば[68]、ソーシャルメディア上で世論に影響を与えようとするツールを含む場合もあります。

54 Corera （2016年）
55 RTS （2016年）& Hern （2016年）
56 Snoddy （2016年）
57 Elliott （2019年）
58 Reuters （2019年）
59 Doffman （2020年）
60 Jones （2018年）
61 Simmons （2019年）
62 Greenberg （2017年）
63 BBC （2015年）
64 Bosetta （2018年）
65 Ignatius （2018年）
66 Kirschgaessner （2020年）
67 例えば、 Shane （2018年）, BBC （2019年）& JTA （2019年）参照。
68 例えば、 Uren et al （2018年）参照。

この曖昧さから、本研究ではツールとテクニックを、使用されるコンテキストなどの他の要素とともに、サイバー兵器全体の特徴の一部として扱う、より一般的なサイバー兵器の**類型化を**試みました。この類型化では、サイバー兵器を、その目的、サイバー兵器の種類、洗練度（開発に最も長い時間と資源を必要とするものが5、最も少ない時間と資源を必要とするものが1）、用途の観点から定義しています。

この表は、サイバー兵器マトリックスの一例に過ぎず（他にも考えられます）、国家の戦略や目的は様々であるため、一つの目的に一つの兵器を分類するのは誤解を招きかねません。したがって、マルウェアやDDoS攻撃がサイバー兵器になるのは、特定の方法で使用されたり、高度にカスタマイズされた場合に限られます。マトリックスの目的はいくつかの要素を組み合わせることで、サイバー兵器をより総合的に考えることです。

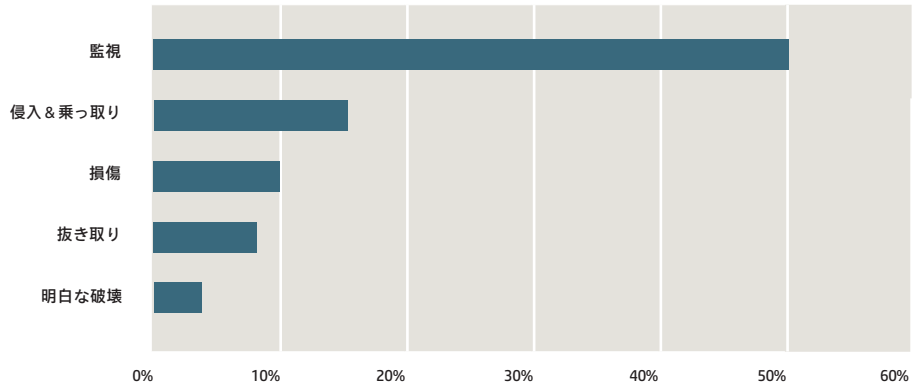
目的	サイバー兵器	洗練度	用途
取得			
インテリジェンス	ハードウェア バックドア	4	‘Lojax’ マルウェア - ルートキットのように動作しますが、コンピュータの基盤であるUEFIを攻撃するマルウェアです。OSの再インストールでも消ヰできず、サイバースパイ活動との関連も指摘されています。[69]
インテリジェンス	RAT （リモートアクセス型トロイの木馬）	3	PlugX RA - 2019年、APT10グループが東南アジアの政府機関や民間企業に対するサイバー攻撃で利用しました。[70]
データ	キーロガー	3	QWERTYキーロギング・マルウェア-大量監視用途のNSA REGINサイバー兵器 [71] のプラグインです。
収益	ランサムウェア	2	SamSamランサムウェア - アトランタやサンディエゴなどの都市に対する国家のサイバー攻撃と関連しています。[72]　2018年11月までに600万ドル以上を稼ぎました。
ステータス	論理爆弾	2	ソニー・ピクチャーズに仕込まれたマルウェアです。北朝鮮の指導者を風刺した映画の公開後に「爆発」し、4,000台以上のコンピュータが消ヰされました。[73]
無力化			
混乱	DDoS/ボットネット	2	2018年 Github software hosting co.へのDDoS攻撃 - 過ヰ最大規模の1.35 tbpsのトラフィックが発生し、一時的にサービスが停止。2015年にも同様のDDoS攻撃が行われている [74] ことから、国家のアクターによるものである疑いが強い。
混乱	ワイパー マルウェア	3	NotPetyaマルウェア - 2016年末に出現し、2017年に急速に広まり、ランサムウェアを偽装していました。実際には、システムに最大の混乱をもたらすことを目的としたエンドポイントのワイパーでした。[75]
破壊	ワームと 標的型マルウェア	5	Disttrackワーム - 湾岸の石油会社を標的としたサイバー攻撃Shamoonで使用された高度なマルウェアで、データの削除や業務の妨害を行いました。
破壊	マルウェア フレームワーク （様々なツールを組み込んだもの）	4	Tritonサイバー兵器 - サウジアラビアの石油化学プラントの安全システムを乗っ取るために使用されました。一つ以上の国家に帰属します。[76]

表2：サイバー兵器マトリックスの一例

69 Goodin （2019年）
70 Stewart （2019年）
71 Smith （2015年）
72 Hoff man （2019年）
73 Elkind （2015年）
74 Tannam （2018年）
75 Thomson （2017年）
76 Sherman & Zoob （2018年）

> ***…監視の用途での利用（兵器使用の約50%）は、現在、損傷（10%）または明日な破壊（4%）のための使用をはるかに上回っている。***

サイバー兵器を単一の定義ではなく、要素のマトリクスで分類することの利点は、他の多くの種類のサイバー兵器を分析し比較できることです。例えば、ここに記載されていない他の潜在的な種類のサイバー兵器には、エクスプロイト、バックドア、トロイの木馬、ルートキットなどが含まれます。[77] 我々のデータベースにあるインシデントを分析し、これを他の情報[78]と照合することで、国民国家によるサイバー兵器の最も一般的な使用方法を特定することができました。



グラフ2：国民国家によるサイバー兵器の最も一般的な使用法

これらの結果は、サイバー兵器がいかに伝統的な兵器使用のパターンに準拠していないかを強調しています。例えば、監視の用途での利用（兵器使用の約**50%**）は、現在、損傷（**10%**）または明白な破壊（**4%**）のための使用をはるかに上回っています。同様に、ラテラル・ムーブ（横展開：価値のあるデータやシステムへの足場を広げ、強固にしようとする試み[79]）やRAT（リモートアクセス型トロイの木馬）の利用など、ネットワークへの侵入や乗っ取りは、データや資産を盗む抜き取り（約**8%**）よりも頻繁に行われているようです。

この分析から、さらに3つの重要な見解が得られました。

(i) より洗練されたサイバー兵器の必要性を回避する「媒介型攻撃」の傾向が強まっています。政府機関への侵入を目的としてソフトウェアサプライヤーの脆弱性を狙う「サプライチェーン攻撃」の現象は、最も深刻な例の一つです。例えば、国家によるNotPetya攻撃は、ウクライナの会計ソフトを利用して同国のインフラを標的にした攻撃で、FedExやMerckなどの多国籍企業の業務を停止させるなど、広範囲に拡散した結果、100億ドル以上の損害をもたらしました。2020年後半、前述のSolarWinds[80]のハッキング事件は、サプライチェーン攻撃の中でも最も深刻なものの一つとなりました。それは、侵害された政府機関の範囲が広かっただけでなく、単一ではなく**2つの**国家アクターによるエクスプロイトと考えられており、元政府職員によると、米国の安全保障に「大規模な」影響を与えたからです。[81] サプライチェーン攻撃を受けたエンティティの数は、2020年後半には**100%**以上増加していると推定されます。[82]

77 DeVore & Lee （2017年）
78 例えば、Lightcyber (2016年)のネットワーク・トラフィック・レポートやManess et al (2017年)のインシデント・データベースを参照ください。
79 NCSC （2018年）
80 Korolov （2021年）
81 Reuters （2021年）
82 ITRC （2020年）

サプライチェーン攻撃を受けたエンティティの数は、2020年後半には100%以上増加していると推定される。

…現代の世界では、戦争の実践と犯罪の実行が密接に絡み合っており、サイバー兵器はこの境界の曖昧さの中心となっている。

(ii) サイバー兵器は、ありふれたサイバー犯罪の実行に使われるツールと、いかに互換性があるか。レポートが示唆しているように、現代の世界では、戦争の実践と犯罪の実行が密接に絡み合っており、サイバー兵器はこの境界の曖昧さの中心となっています。

(iii) 我々はより洗練された、カスタマイズされたサイバー兵器の開発に着手したばかりであるという事実。既存のツールがさらに改良される可能性があるだけでなく、将来のサイバー戦争の結果に決定的な影響を与える可能性のある「第2世代」のサイバー兵器が登場しています。これらの新しい兵器は、コンピューティングパワーの強化、より高度なAI、より完全なサイバー/フィジカル統合を利用しています。以下に5つの例を紹介します。

第2世代のサイバー兵器	戦略的用途の可能性
「ブーメラン」マルウェア	「捕獲される」とその所有者に戻ってくることができるマルウェア。中国はすでにこの方法に成功しているという証拠があります。[83]
武器化したチャットボット	より説得力のあるフィッシング・メッセージの配信、新たな事象への迅速な対応、Twitterなどのソーシャルメディアを通じたメッセージ・レスポンスの送信、他のボットへの攻撃などの機能が強化されたAIデバイス。[84]
サイバーフィジカル戦争におけるディープフェイク	実際に起きていることが歪めるために、デジタル戦場データの改変（例えば、顔や声など）を行う。[85]
ドローンの群れ	ハッキング、Wi-FiやBluetoothなどの通信妨害、監視活動が可能なドローン群。[86]
量子コンピューティング	ほとんどすべての暗号化されたシステムを破ることができる、飛躍的な（量子ベースの）計算能力を持つデバイス。[87] 中国は、この分野で大規模な研究を行っていることが知られており、すでに欧米の専門知識を凌駕している可能性があります。[88]

表3：サイバー兵器の新しい方向性

83 Cushing （2019年）
84 Wall （2018年）
85 South （2018年）
86 O’Neill （2018年）
87 Walden & Kashefi （2019年）、Katwala （2018年）も参照。
88 Katwala （2018年）

2.3

サイバースペースにおける国民国家 ： 国民国家によるサイバー攻撃の分析

NSiCで指摘されているような要素は、サイバー紛争がなぜ従来のキネティックな紛争とは大きく異なるのかを説明するのに役立ちます。通常の戦争の目的は、勝利を得ること、あるいは少なくとも「勝者」が自分の意志を貫くために敵を十分に弱体化させることでした。しかし、サイバー紛争では明確な勝利を目指すことはほとんどありません。つまり、陸・海・空を問わず、「戦場の優位性」を中心とした軍事戦略は無意味になります。

例えば、下の図が示すように、サイバー攻撃は1回で終わるものではなく、通常は、計画・攻撃前のステージから、攻撃そのものやそのフォローアップまで、少なくとも4つのステージで構成されています。.

> ***…しかし、サイバー紛争では明確な勝利を目指すことはほとんどありません。つまり、陸・海・空を問わず、「戦場の優位性」を中心とした軍事戦略は無意味になる。***

計画	攻撃前	攻撃	フォローアップ
能力の開発（トレーニング、投資、研究開発など）	予行演習	特定の攻撃ベクトルの適用 （ソーシャルエンジニアリング、ドライブ・バイなど）	採り当てた弱点の継続的な検査
標的の選定	ハッキングの練習	ペイロードの配信	土込んだ資産の継続的な活性化
弱点の評価	ターゲットの弱体化		フォローアップ攻撃
キー・ツールの兵器化	スキルの向上		さらなる兵器化
	弱点のテスト		
	事前の防御機能低下		

図2: 典型的な国家によるサイバー攻撃のステージ

3.1

拡張 - 国民国家と THE WEB OF PROFIT

今回の研究で最も印象的だったのは、国民国家のサイバー紛争が、Web of Profitと呼ばれる（不正な）デジタル経済の典型的な活動の多くと織り交ぜられているように見えるという、これまでに知られていない面でした。これを反映して、サイバー犯罪者が使用するツールやテクニックと、国家が使用するツールやテクニックが相互にクロスオーバーしています。

調査では、このシフトの少なくとも4つの側面が明らかにされました。

(i) **サイバー犯罪の手法の採用：**もともとハッカーが使い、やがてサイバー犯罪者が用いていた手法（SQLサイバー攻撃、DDoSの使用、感染拡大の試みなど）が、国家の戦略的オプションとして広く採用されています。

例えば、IMF、国連、米国国務省などの国際機関に対するDDoS攻撃は、2017年～2018年の間に**200%**以上増加したと記録されています。[89] このようなサイバー攻撃の動機は、従来のサイバー犯罪の観点からは説明できません。

多くのサイバー攻撃に見られる専門性は、国家がサイバー犯罪者を代理人として直接雇用しているだけでなく、その人的リソースの犯罪技術を向上させていることが多いことを示唆しています。

> ***今回の研究で最も印象的だったのは、国民国家のサイバー紛争が、Web of Profitと呼ばれる（不正な）デジタル経済の典型的な活動の多くと織り交ぜられているように見えるという、これまでに知られていない面だった。***

89 D'mello （2019年）

> *国家によるサイバー攻撃に対する従来の防御策は、あまり効果的ではなく、少なくとも全てのウイルス対策ツールの39%が回避されるという検証がされている。*

> *…約50%はダークネットやその他のサイバー犯罪市場で簡単に購入できる低予算の簡単なツールを使用していました。約20%は、標的型マルウェアや兵器化されたエクスプロイトなどのより高度なカスタムメイドの兵器を使用しており、おそらく国家のサイバーセキュリティプログラマーが開発したものだった。*

> *…現在売上の10～15%が「非典型的」購入者や他のクライアントの代理人として行動する者に支払われている。*

> *…SolarWinds社のハッキングで複数の米国政府機関から盗まれたデータが、ダークネット上で100万ドル以上で販売されていると言われている。*

例えば、国家によるサイバー攻撃は、サイバー犯罪者による攻撃よりもはるかに効率的で、ほとんどのネットワークに侵入するのに平均20分しかかからないと言われています。[90] また、阻止することも非常に困難です。国家によるサイバー攻撃に対する従来の防御策は、あまり効果的ではなく、少なくとも全てのウイルス対策ツールの39%が回避されるという検証がされています。[91]

(ii) **サイバー犯罪ツールの統合：**サイバー犯罪者が標準的に使用しているツール（マルウェア、キーロギング、監視装置など）が、国家によって取得され、兵器化されています。
例えば、2010年～2020年の間に行われたサイバー攻撃のサンプルを分析したところ、約**50%**はダークネットやその他のサイバー犯罪市場で簡単に購入できる低予算の簡単なツールを使用していました。約**20%**は、標的型マルウェアや兵器化されたエクスプロイトなどのより高度なカスタムメイドの兵器を使用しており、おそらく国家のサイバーセキュリティプログラマーが開発したものでした。さらに**30%**は、出所が不明または特定できないものであることがわかりました。
国家がダークネットやその他の秘密の情報源を通じて入手する、監視されていない既製のサイバー兵器の取引は、重要な意味を持つかも知れませんが、明確に証明することは不可能です。今回の調査のためにインタビューしたダークネットベンダーのサンプルや、ダークネットのサイバー脅威に関する前回のレポートによると、現在売上の**10～15%**が「非典型的」購入者や他のクライアントの代理人として行動する者に支払われてます。[92] その中には、ゼロデイエクスプロイトなどのツールを「ストックしておく」事も含まれています。[93]
また、現在多くのダークネット市場は、国家の境界線に従い運営されており、商品リストは当該国家の言語で表示され、商品は国内の生産者や消費者の特定のニーズに合わせてカスタマイズされていることも明らかになっています。[94]

(iii) **サイバー犯罪者による国家のデジタル資源の取引と利用：**デジタル資源の流れは逆になり始めています。その結果、もともと国家が開発した高度なハッキング・ツールや政府機関が作成したデータをサイバー犯罪者が利用することが多くなっています。政府が積極的にハッキング・ツールを共有しているケースさえあります。例えば、ペネトレーションテストツールPowerShell Empireは、ハッカーに人気があり、英国国立サイバーセキュリティセンターが発表した最も危険な一般向けハッキング・ツールの5つのうちの1つに選ばれています。[95] しかし、このツールは国家がスポンサーとなっているAPTグループがクラウドサービスを危険にさらすために広く利用していることも事実で、2020年にはCovid-19のフィッシングメールを介して広がりを見せています。[96]
一方、EternalBlue は悪名高いShadow Brokersによる情報漏えい事件で米国家安全保障局（NSA）から流出したエクスプロイトの一つで、現在世界中の 500 万台以上のコンピュータを危険に曝しています。そして、世界の企業や政府に数十億ドルの損害を与え、サイバー犯罪者に5億ドル以上の収益をもたらしました。[97]
最近では、SolarWinds社のハッキングで複数の米国政府機関から盗まれたデータが、ダークネット上で100万ドル以上で販売されていると言われています。[98]

(iv) **国民国家はサイバー犯罪経済から利益を得ている：**サイバー犯罪活動をベースとした経済は非常に大きな価値を持っているため、一部の国家は直接的な収入を得るために、あるいは間接的な利益を得るためにこれに関与しています。例えば、デジタル通貨の（不正な）取得、データの窃盗と取引、知的財産や企業秘密の窃盗、あるいは単純なデバイスのセールスなど、いずれもサイバーセキュリティとサイバー兵器の境界を曖昧にするようなものです。その結果得られる収益は、国内総生産（GDP）、外貨準備高、輸出額など、伝統的な国民国家の経済指標にますます大きな影響を与えているようです。

90 Kundaliya（2019年）
91 Ashford（2018年）
92 McGuire（2019年）
93 cf Maxwell（2017年）
94 Osbourne（2016年）
95 NCSC（2018年）
96 Jay（2020年）
97 cf Perloth & Shane（2019年）
98 Abrams（2021年）

3.2

収益創出と THE WEB OF PROFIT

武器生産量の増加が国のGDPに影響を与えるように、軍国化は確実に経済に影響を与えます。国民国家間のサイバー紛争は、この関係に新たな側面を加えているようです。これまでのレポートで、私たちはサイバー犯罪の経済規模が非常に大きく、保守的に見積もっても、年間**1.5兆ドル**の収益を創出しいることを明らかにしました。[99] このサイバー犯罪経済の規模（全体）は、Fortune 500企業の利益を上回るだけでなく、多くの国家のGDPをも上回っていることを考えると、このような収益の流れを悪用する誘惑があるのは明らかです。

“このサイバー犯罪経済の規模（全体）は、Fortune 500企業の利益を上回るだけでなく、多くの国家のGDPをも上回っていることを考えると、このような収益の流れを悪用する誘惑があるのは明らかだ。

代表的な収入源としては、以下のようなものが考えられます。

- 営業秘密の盗難またはデータ取引
- 通貨の窃盗
- デジタルマネーロンダリング
- （合法的に）儲かるセキュリティツール業界

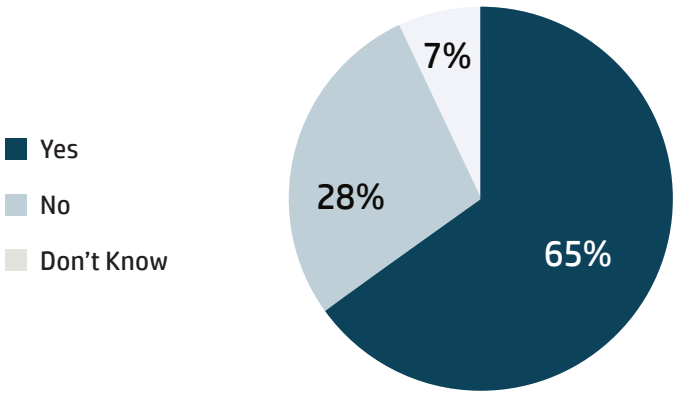
サイバー犯罪経済を利用していることが比較的証明されている例として、北朝鮮（DPRK）のケースがあります。多くの専門家は、サイバー犯罪で収益を上げる方法とデジタルイノベーションを組み合わせることができているとみています。暗号通貨の窃盗、ランサムウェアの運用、マネーロンダリングなどの形態を取っていますが、彼らのアプローチは銀行強盗でした。例えば、2017年に行われた暗号通貨取引所へのサイバー攻撃では、北朝鮮のAPTグループLazarusが5億7,100万ドルに相当する収益を上げたことの確かな証拠が得られています。このグループは、フィッシングなどの手法を用いて取引所にアクセスし、北朝鮮政府の限られた外貨獲得手段を補うための有用な手段を提供しました。同様に、おそらく政府が支援していると思われる北朝鮮のグループが、2016年にバングラデシュ中央銀行の職員のSWIFT認証情報を利用して8,100万ドルの送金を企てた攻撃に関与していましたが、これは同グループによる東南アジアの銀行からの一連の強盗未遂事件の1つでした。[100] 2018年、同グループはATMのハッキングに目を向け、特別にカスタマイズしたトロイの木馬を使って、要求に応じて数百万ドルを払い出すことに成功しました。[101] 国連の2021年の報告書によると、2020年に北朝鮮がサイバー窃盗で得た3億ドル以上が、核ならびに弾道ミサイル計画の資金に使われたとされています。[102]

“…専門家アンケートの回答者の約3分の2（65%）は、国家がサイバー犯罪で金儲けをすることは可能だと考えている…

国民国家がサイバー犯罪に直接関与しているという印象が広まっているようです。専門家アンケートの回答者の約3分の2**（65%）**は、国家がサイバー犯罪で金儲けをすることは可能だと考えており、この意見は主要な国際サイバーセキュリティ機関も認めています。例えば、NSAの代表者は、「国家が銀行強盗をしている」と明確に指摘しており、それもコンピュータ[103]を使って行っているとしています。

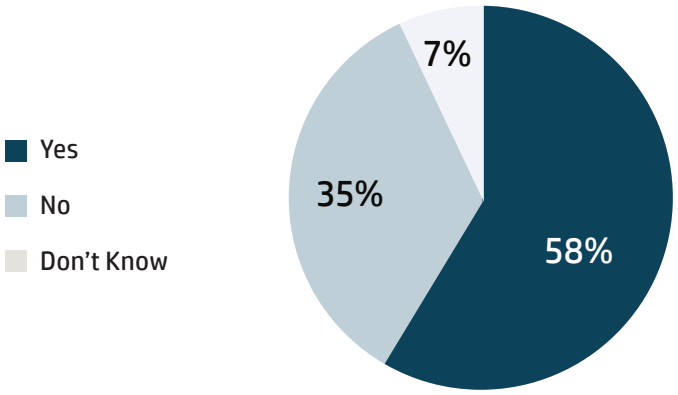
99 McGuire（2018年）
100 Zetter（2016年）
101 Schwartz（2018年）
102 Roth and Berlinger（2021年）
103 Pollard（2017年）

58%の専門家が、国家がサイバー犯罪者をサイバー攻撃の代理人として採用することは珍しいことではないと回答している。



グラフ3：「国家がサイバー犯罪で儲けていると思うか」という質問に対する専門家の回答

また、今回の調査では、多くの専門家が、国家とサイバー犯罪者の共謀はごくありふれたことであると考えていることがわかりました。58%の専門家が、国家がサイバー犯罪者をサイバー攻撃の代理人として採用することは珍しいことではないと回答しています。あからさまなサイバー犯罪者であれ、単なる秘密の政府機関であれ、代理人の使用は、能力を拡大するだけでなく、もっともらしい否認を可能にします。[104] GCHQ の元長官Robert Hanniganは、この疑念を裏付けるように、「これらのグループは同じ部屋に座って昼間は国家活動を行い、夜は犯罪を行っている。これは、利益と政治的意図の興味深いよせあつめだ。」と言っています。[105]



グラフ4：「国家がサイバー犯罪者をリクルートしていると思うか」という質問に対する専門家の回答

国家がサイバー犯罪からどの***レベル***の収入を得ているのかを推定することは、推定につかう信頼できる情報が非常に限られているため、当然ながら非常に困難です。しかしながら、IP窃盗や暗号通貨のハッキングのような特定の種類の不正な収益源を見て、これらをより伝統的な経済指標と関連付けることで、国民国家のアクターにとってのサイバー犯罪の利益を経験的に推定することは可能です。

104 Maurer （2018年）
105 Schwartz （2018年）

4.1

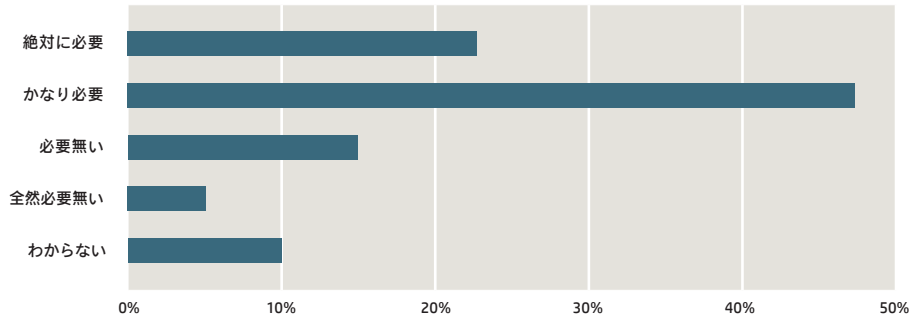
“

回答者の30%は、実現可能な協定や条約の見通しについて懐疑的な見方をしている。

サイバー戦争とサイバー平和

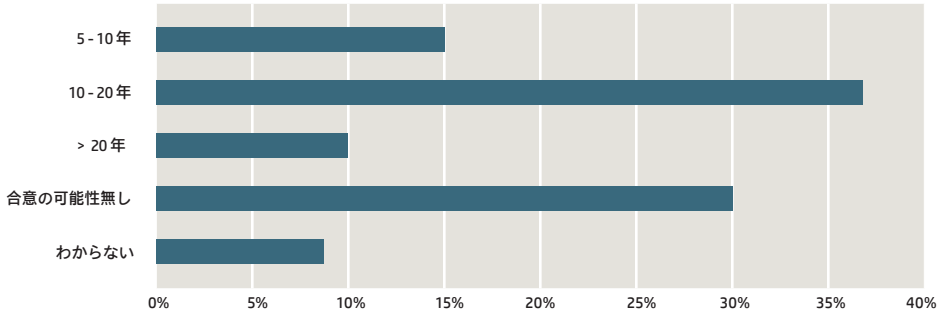
これまでのセクションは、現在私たちが直面しているリスクがどれほど重大なものかを示唆していました。一方で、「高度サイバー紛争ヒートゲージ」は、（許容できる）サイバー競争と（許容できない）高度な紛争の形態の区別が曖昧になっていることを示しています。一方、SOTTT分析では、洗練されたサイバーツールと軍事的な戦略目標との関連性が高まっていることが明らかになりました。その結果、これ以上のエスカレーションを阻止する必要性が高まっているのです。

この懸念は、今回の調査でも反映されており、専門家の**70%**が、国民国家がより深刻な形態のオンライン紛争に巻き込まれることを避けるためには、何らかの形の合意やサイバー条約が必要であると考えています。



グラフ5：「サイバー条約はどれぐらい必要か」という質問に対する専門家の回答

このような合意がなされるまでの期間については、意外な答えが返ってきました。ほとんどの回答者（52%）は、今後5年から10年、または10年から20年の間に可能性があると考えていました。ある回答者は、このタイムスケールが妥当であると指摘し、「より深刻になる可能性のある衝突を回避するために前進することが、すべての当事者の利益になる」と述べています。また、別の回答者は、「もし実現しなければ、誰もその後の事態に備えることはできないだろう」と述べています。



グラフ6：「実行可能なサイバー条約を締結するための最も可能性の高いタイムスケール」という質問に対する専門家の回答

しかし、そのような協定はどのような形を取るのでしょうか？一つの包括的な協定を結ぶのか、それとも様々な条約や協定をパッチワークのように組み合わせるのか。ジュネーブ条約のような通常の戦争を規定する協定を単純に拡張するだけなのか。それとも、よりサイバーに特化した形をとる必要があるのか。このような複雑な問題があるためか、回答者の30%は、実現可能な協定や条約の見通しについて懐疑的な見方をしています。

最低限、2つの重要な要素が一致することが、合意の成功につながると考えられます。

(i) ***範囲***：関係する管轄の全ての当事者と対象となる具体的な活動。

(ii) ***コンセンサス***：形成すべき原則の種類についての合意。この原則には、武器の制限などの予防に関するものだけでなく、サイバー戦争の実 了に関するものもあります。

これらの要素を考慮して、現在、国民国家が利用可能な合意のための選択肢を表にしました（下表参照）。これらはすべてを網羅しているわけではありませんが、コンセンサスを得て緊張を和らげるために利用できる構成要素の一例を示しています。この表は2つの分野をカバーしています。

一つ目は、より高度な形態のサイバー紛争が発生する前に、行動を規制するために利用できる合意です。これらの中には、単にサイバーセキュリティやサイバー犯罪に対するより良い協力関係を確保することを目的としたものもあります。また、より明確に紛争の予防を目的としたものもあります。

二つ目は、より高度な形態のサイバー紛争（「サイバー戦争」）が発生した場合に、行動を規制するために利用できる合意です。

この表では、次のレベルで協定の範囲を区別しています。国内、産業、国家/国際。

レベル	現在/提案されている」合意の例	範囲	内容
高度なサイバーコンフリクトに先立つ行動基準 / コンセンサス			
国内	米国 脆弱性エクイティプロセス (VEP)	透明性と国家の脅威を軽減するために、国と政府機関が協力すること。	米国政府とその機関に対し、Apple、Cisco、Juniper、Fortinet などの大手企業にサイバー脆弱性を開示するよう求める一方、情報機関がゼロデイに関する情報を保持することを認める。
産業	サイバーセキュリティ技術協定	デジタルテック産業が国家の脅威を軽減するために協力する。	サイバー空間の安全性、安定性、回復力を高めるために、特に国家の脅威に対して、デジタル技術企業間の協力を促進することを目的とする。 HP、Facebook、Dell、BT、Microsoft、Hitachi、Panasonic、Cisco、Nokia、RSA、Orangeなど、150社を超える企業が加盟している。
産業	Siemens 信頼性憲章	国家の脅威に対するオンラインの安全性を確保するための業界標準を作成する。	個人、企業、インフラにとってより安全なネットワークを実現するための3つの目標を中心に、「サイバーセキュリティに関する最低限の一般的基準を設定する」ことを目的としている。 データ保護：損害の限定：信頼性の高い基盤
産業＆国家	サイバー空間の信頼性と安全性のための「パリ・コール」	国家の脅威を軽減するための産業界と国家が協力する。	悪意のあるオンライン活動に対する国際的な安全性の強化、選挙プロセスへの干渉の防止、非国家主体によるオンライン傭兵活動や攻撃行為に対する対策の強化、関連する国際基準の強化への協力を求める。 51カ国、HPを含む347社、92の非営利団体、大学、協力団体が加盟している。
国家/国際	（ブダペスト）サイバー犯罪に関する条約	国家の脅威を軽減するために、サイバー犯罪との戦いにおけるコンセンサスと協力関係を強化する。	条約には65カ国が加盟しており、加盟国間でオンライン犯罪に対する国内法や政策を調和させることを目的としている。条約は行動規範よりも犯罪を重視しており、ロシア、中国、インド、ブラジルなどの主要なサイバーパワーは、戦略上の懸念から加盟を拒否している。
国家/国際	（提案中の）国連サイバー犯罪条約	国家の脅威を軽減するために、サイバー犯罪との戦いにおけるコンセンサスと協力関係を強化する。	2020年初頭にロシア、中国などが提案。その後、2021年5月に全地域を代表する専門家によるアドホック委員会を開催し、「犯罪目的の情報通信技術の利用に対抗するための包括的な国際条約」の詳細を検討することが予定されている。[105]
国家/国際	国連GGEプロセス	サイバー空間での行動規範に関するコンセンサスを形成する。	国連の政府専門家グループ（GGE）は、デジタルネットワーク上で許容される行為や規範について、すべての加盟国間でより大きなコンセンサスを得ることを目的としてる。
高度サイバー紛争（サイバー戦争）における行動基準 / コンセンサス			
戦闘員	タリン・マニュアル 2.0	高度なサイバー紛争（サイバー戦争）における国民国家の行動基準を作ること。	NATOの支援の下、国際的な法律専門家によって作成され、規定的なガイドではなく、法律の再解釈を目的としています。より広範な紛争の側面（例：認知的ハッキング）に適用できるよう、サイバー戦争ではなく、サイバー作戦に焦点を当てています。「主権、管轄権、デューデリジェンス、介入の禁止」などの問題に対して、既存の原則がどのように適用されるかを検討している。

表4：サイバー条約に関する現在/提案中の枠組み

106 UN（2021年）

4.2 サイバー犯罪防止条約の新たな選択肢？

2020年に、「犯罪目的のための情報通信技術の使用に対抗する」ことを目的とした「サイバー犯罪条約」の新たな提案が国連に提出され、枠組みの模索において重要な進展があると思われました。[107] この提案は、79票対60票、33人の棄権で採択 [108] されましたが、国際的なコンセンサスの欠如に加え、戦略的目標の実現に向けて各国が競い合っていることから、この構想が普遍的な承認を得る可能性は、他に示された選択肢と同様に低いと考えられます。

問題は、ロシアがスポンサーとなり、中国がバックアップしたこの提案が、インターネットの切断や言論の自由の犯罪化を許すものであることです。NGOや権利団体のグループは、この提案がサイバー犯罪に対抗するものであると同時に権利を損なうものであると、国連に抗議の手紙を出しました。また、加盟していない国家の好みに合わせて、ブダペスト条約の代わりを作ろうとしているのではないかという疑念もあります。

楽観的に考えれば、1998年以降、ロシアが国連総会で情報セキュリティに関する決議案を積極的に作成してきたことは、非西洋諸国がより根本的なサイバー平和の実現に向けて真剣に取り組んでいるのではないかという期待を抱かせます。また、ロシアは2003年に国連の政府専門家グループ（GGE）の報告書に、サイバー紛争を減らすための協力分野を特定するための動きを提案することにも貢献しました。この報告書への支持は得られなかったものの、2010年には、国際社会が規範や信頼性向上のための手段を開発し、議論することを推将するGGE報告書が発表されました。[109]

4.3 課題と論点

これらの枠組みを実現するためには、さまざまな課題があります。例えば、以下のようなものです。

(i) 国家安全保障のニーズと企業のニーズの間で適切なバランスを取ることは、不安定さを伴うなようです。例えば、米国の「脆弱性エクイティプロセス」は、現在、政府の利益に大きく貢献していると考えられています。ガバナンスは、国家安全保障会議（NSC）が議長を務め、国土安全保障省や商務省など、米国の重要なインフラのセキュリティに最も関心のある機関を含む他の機関の代表者が参加する委員会の手に委ねられています。この委員会の決定により、政府がAppleやMicrosoftなどのシステムに存在する毎年約45件の既知の脆弱性を産業界から隠蔽していることが、継続的な問題となっています。

(ii) 産業界の行動を規制することを目的としたSiemens憲章のような協定は、その範囲が非常に限られており、背後にある明確な原則もほとんどありません。また、実効性を持たせるためには、産業界からより多くの加盟企業を募り、より明確な制裁措置を講じる必要があります。

(iii) パリ・コールのような、より国際的な枠組みについても同様の懸念があります。米国、ロシア、中国、イラン、イスラエル、北朝鮮といった主要なサイバー超大国が加盟していないことが目立ちますが、彼らの合意がなければ、このような合意が影響力を持つのは難しいでしょう。

(iv) したがって、完全にグローバルな合意が不可欠ですが、国連のGGEプロセスのようなアプローチは、いくつかの重要な側面において、良く言えば限定的、悪く言うと重大な側面が欠如しています。

107 Hakmeh & Peters （2020年）
108 Stolton （2020年）
109 Barrera （2017年）

> 例えば、サイバースペースにおける人権の尊重などについては、ある程度の合意が得られていますが、それ以外の重要な問題については、まだ合意が得られていないものが多くあります。また、サイバー空間における国家の責任や自衛権をどのように規定するかについても大きな疑問が残っています。

大枠の中だけではありますが、何らかの合意がなされているということは、高度サイバー紛争へのエスカレーションが回避されるかもしれないという期待が持てます。

しかしながら、既存の議論があまりにも範囲が狭く、コンセンサスに欠けていることも気になります。また、多くの提案が、伝統的な政治的コンセンサスではなく、犯罪/サイバー犯罪に関するものであることも注目に値します。このことは、本レポートで述べられている、犯罪と政治が微妙に混ざり合った、まったく新しい国際関係のあり方に我々が到達していることを裏付けているのではないでしょうか。

従って、サイバー戦争（あるいはそれ以上）に至るような悪循環の継続を阻止するためには、今後数年間で取り組まなければならない少なくとも10の重要な論点が残っています。

(i) 既存の協定を、象徴的な意思表示から、加盟国を拘束するようなものに変えるにはどうすればよいか？

(ii) 本レポートで調査したオンライン紛争の多くを引き起こしているサイバー超大国が、紛争削減のための真剣な取り組みを行うことは可能でしょうか？

(iii) 地域のサイバー紛争がグローバルな段階に飛び火するのを防ぐ方法はあるのでしょうか？

(iv) グローバルなサイバー犯罪の問題は、グローバルな戦略的利益の問題とどのように切り離すことができるのでしょうか？特に、サイバー犯罪者のツールやテクニックの使用にはどのような制限をすべきでしょうか？

(v) サイバー代理人グループの責任とは何で、サイバー兵器の使用にどのような制限をするべきでしょうか？どのような形態の「軍縮」が可能でしょうか？

(vi) コンセンサスを得るための試みは、超国家的なレベルで行われるべきなのでしょうか、それとも草の根活動家が行うべきなのでしょうか？

(vii) 合意のためにどのような検証を行うことができ、違反を仲裁するためにどのような機関を受け入れることができるでしょうか？

(viii) 民間人に対してどのような義務や保護が考慮されるでしょうか？

(ix) サイバー紛争によって被った被害に対する補償制度は実現可能でしょうか？

(x) 一線を越えてしまうようなことが万が一起こった場合、どのような対応が可能でしょうか – 「サイバー戦争犯罪」はあり得るでしょうか？[110]

既存の議論があまりにも範囲が狭く、コンセンサスに欠けていることも気になります。また、多くの提案が、伝統的な政治的コンセンサスではなく、犯罪/サイバー犯罪に関するものであることも注目に値する。

110 RAND（2019年）

5.1

結果と提言

今回の調査で、我々は国民国家が情報技術を利用する上で、重要な転換点にいることがわかりました。政治的な対立を超えて国家はサイバースペースを積極的に利用する準備ができているように見えますが、多くの場合その結果をほとんど気にしていません。

その結果、ますます多くの被害者がこのクロスファイアに巻き込まれることになります。都市や地方自治体は、国家の代理人として活動する影のグループによって、ネットワークの停止、身代金の要求、データの喪失に直面しています。重要なインフラが狙われると、サイバー世界とフィジカル世界が融合した、人命を失うような壊滅的な結果を招くリスクに曝されます。メディアや情報システムが標的にされると、事実と出来事を区別することや、民主主義の方向性について適切な情報に基づいた判断を下すことが困難になります。また、一部の国家では法の尊重が失われ、個人が情報技術を利用した大規模な監視や強制的なコントロールに直面し、国家の権力にあまりに挑戦しているとみなされる場合には、サイバーターゲットによる暗殺の可能性さえあります。

したがって、バランスがより高度な形態のサイバー紛争に傾いているのではないかという指摘は、サイバーセキュリティの実務に携わるステークホルダーだけでなく、私たち全員が懸念すべきことです。同様に懸念されるのは、急成長するサイバー犯罪経済に関連するWeb of Profitの利用が、これらの問題に果たす役割です。この1.5兆ドルの経済の中で、国民国家はサイバー犯罪から直接あるいは間接的に利益を得ているだけでなく、サイバー犯罪のツールやテクニックを使って軍事力を強化し、犯罪グループを使って戦略的な目的を推進する準備ができているようです。

現在、私たちが直面している紛争と犯罪の融合は、確実に前例がなく情報社会の不確実な未来を示唆しています。国際関係の場に犯罪の典型的な関係、特に法の支配の軽視が入り込むと、（宣言の無いまま）永遠に続く紛争状態を生み出す危険性があり、これを解決することは不可能かもしれません。

この点を踏まえて、本研究では、適用可能な以下の提言を行います。

(i) 政策立案者は、サイバー条約やサイバー協定の締結に向けて、より積極的に取り組む必要があります。

(ii) このような条約が有効に機能するためには、サイバー空間における国民国家の正当な利益がより広く認識される必要があります。ただし、その認識は個々の国家の戦略的目的を過度に反映したものではありません。

(iii) このような条約が有効に機能するためには、サイバー空間における国民国家の正当な利益がより広く認識される必要があります。ただし、その認識は個々の国家の戦略的目的を過度に反映したものではありません。

(iv) 国際金融当局は、マネーロンダリングのような国家のサイバー犯罪を助長する行為に対処するために、国家間の協力を得ることにもっと積極的に関与すべきです。

(v) サイバーセキュリティの専門家は、典型的な国家のサイバー兵器に関するインテリジェンスを蓄積し、それらに対抗する方法を見つけることに、より積極的に取り組む必要があります。

(vi) サイバーセキュリティの専門家は、典型的な国家のサイバー兵器に関するインテリジェンスを蓄積し、それらに対抗する方法を見つけることに、より積極的に取り組む必要があります。

(vii) 個々の市民は、サイバー空間で協力する方法を見つけるために、政府にもっと積極的に働きかけるべきです。

> ***政治的な対立を超えて国家はサイバースペースを積極的に利用する準備ができているように見えますが、多くの場合その結果をほとんど気にしていない。***

> ***重要なインフラが狙われると、サイバー世界とフィジカル世界が融合した、人命を失うような壊滅的な結果を招くリスクに曝される。***

> ***この1.5兆ドルの経済の中で、国民国家はサイバー犯罪から直接あるいは間接的に利益を得ているだけでなく、サイバー犯罪のツールやテクニックを使って軍事力を強化し、犯罪グループを使って戦略的な目的を推進する準備ができているようだ。***

参考文献

Abrams, L., 2021, Solar Leaks site claims to sell data stolen in SolarWinds attacks, Bleeping Computer, 12/01/2021

Accenture, 2020 Cybersecurity Report

Ashford, W., 2018, Cyber criminals catching up with Nation State attacks, Computer Weekly, 26/02/2018

Ball, J., 2013, NSA monitored calls of 35 world leaders after US o ffi cial handed over contacts, Guardian, 25/10/2013

Barrera, M., 2017, The Achievable Multinational Cyber Treaty, Air University Press

BBC, 2015, China denies Australia Bureau of Meteorology ‘hack’, 02/12/2015

BBC, 2019, Australian political parties hit by ‘state actor’ hack, PM says, 16/02/2019

BBC, 2019b, German politicians targeted in mass data attack, 04/01/2019

BBC, 2021 Trump bans Alipay and seven other Chinese apps, 06/01/2021

Bosetta, M., 2018, The Weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy, Columbia Journal of International Aff airs, 20/09/2018 CFR,

2019, Cyber Operations Tracker, Council on Foreign Relations

Chandler, S., 2020, Google Registers Record Two Million Phishing Websites In 2020, Forbes 25/11/2020

Coker, J., 2020, Attacks on Pharma Rise Amid Targeting of #COVID19 Vaccine Development, Infosecurity, 19/11/2020

Corera, J., 2016, How France’s TV5 was almost destroyed by ‘Russian hackers’ BBC 10/10/2016

Coughlan, S., 2020 Cyber threat to disrupt start of university term, BBC 17/09/2020

Crerar, P., Henley, J., & Wintour, P., 2018, Russia accused of cyberattack on chemical weapons watchdog, Guardian, 04/10/2018

Crowdstrike, 2019, 2019 Global Threat Report

CSIS, 2020, Signifi cant Cyber Incidents, Center for Strategic and International Studies

Cushing, T., 2019, Chinese Spies Intercepted NSA Malware Attack, Weaponized It Against Targets Around The World, Techdirt, 08/05/2019

D’mello, A., 2019, Threat intelligence report shows new IoT vulnerabilities, Nation State actors and a rise in DDoS frequency, Vanilla Plus, 28/02/2019

DeVore, M., & Lee, S., 2017, APT (advanced persistent threats) and infl uence: cyber weapons and the changing calculus of confl ict The Journal of East Asian Aff airs, 31, 1pp. 39-64

Doff man, Z., 2020, Twitter Confi rms ‘Nation-State’ Attack, Forbes, 04/02/2020

Elkind, P., 2015, Sony Pictures: Inside the Hack of the Century, Fortune, 27/06/2015

Elliott, C., 2019, Here Are The Real Fake News Sites, Forbes, 21/02/2019

ENISA, 2019, Shamoon Campaigns with Disttrack, European Union Agency for Cybersecurity, 07/01/2019

ENISA, 2020, Cyber espionage, ENISA Threat Landscape, 01/2019-04/2020

FireEye, 2019, M-Trends 2019 Special Report

GFI, 2019, Global Firepower index, see: https://www.globalfi repower.com/countries-listing.asp

Goodin, D., 2019, Unkillable LoJax rootkit campaign remains active, Arstechnica, 16/01/2019

Gov.uk, 2018, UK exposes Russian cyber attacks, Press Release, 04/10/2018

Greenberg A., 2017, Your Guide to Russia’s Infrastructure Hacking Teams, WIRED, 12/07/2017

Guglielmi, G., 2020, The next-generation bots interfering with the US election, Nature, 28/10/2020

Hakmeh, J., & Peters, A., 2020, A New UN Cybercrime Treaty?, Council on Foreign Relations, GuestBlog, 13/01/2020

Hall, K., 2018, Brit Attorney General: Nation State cyberattack is an act of war, The Register, 23/05/2018

Hegre et al., 2011, Predicting Armed Confl ict, 2010 – 2050 International Studies Quarterly 57(2): 250 – 270

Hern, A., 2016, Ukrainian blackout caused by hackers that attacked media company, researchers say, Guardian, 07/01/2016

Herr et al., 2020, Breaking trust: Shades of crisis across an insecure software supply chain, Atlantic Council, 26/07/2020

Hoff man, K., 2019, True crime: SamSam ransomware I am, SC Media, 01/02/2019

Ignatius, D., 2018, How a chilling Saudi cyberwar ensnared Jamal Khashoggi, Washington Post, 18/12/18

Izvestia, 2020, Russia will increase spending on information security, 02/10/2020

ITRC, 2020, Data Breach Report, Identity Theft Resource Center

Jackson and Morelli, 2009, The Reasons for Wars – an Updated Survey, in Handbook on the Political Economy of War, edited by Chris Coyne, Elgar Publishing Jay,

J., 2020, Microsoft issues fresh warning about Nation State actor Gadolinium, Teiss, 25/09/2020

Jones, C., 2018, EU communications hack linked to Chinese spies, ITPro, 19/12/2018

JTA, 2019, Israel’ s national broadcaster accuses Hamas of Eurovision hack, Jewish News, 18/05/2019

Katwala, A., 2018, Why China’ s perfectly placed to be quantum computing’ s superpower, WIRED, 14/11/2018

Kirschgaessner, S., 2020, Jeff Bezos hack, The Guardian, 22/01/2020

Korolov, M., 2021, What are Supply Chain Attacks, and How to Guard Against Them, DataCenter Knowledge, 12/01/2021

Krebs, B., 2021, SolarWinds: What Hit Us Could Hit Others, Krebs on Security, 12/01/2021

Kundaliya, D., 2019, Russian state-sponsored attackers take just 20 minutes to infi ltrate networks, claims CrowdStrike, Computing, 20/02/2019

Lancaster, K., 2020a, 10 facts about Nation State cyberattacks, ID Agent, 19/11/2020

Lancaster, K., 2020b, Sudden Spike in Healthcare Cyberattacks May Be Nation-State Hackers, ID Agent, 29/10/2020

Lewis, P., & Unal, B., 2019, The Destabilizing Danger of Cyberattacks on Missile Systems, Chatham House, Expert Comment, 02/07/2019

Leyden, J., 2019, Chinese cyber spies ‘target international businesses to pilfer trade secrets’, Daily Swig, 07/02/2019

Lightcyber, 2016, Cyberweapons 2016 Report

Lucero, L., 2018, F.B.I.’ s Urgent Request: Reboot Your Router to Stop Russia-Linked Malware, New York Times, 27/05/2018

Maurer, T., 2018a, Why the Russian Government Turns a Blind Eye to Cybercriminals, Slate, 02/02/2018

Maurer, T., 2018b, Cyber Mercenaries: The State, Hackers, And Power, New York and Cambridge: Cambridge University Press.

Maxwell, P., 2017, Stockpiling Zero-Day Exploits: The Next International Weapons Taboo, 2th International Conference on Cyber Warfare and Security, Dayton, OH March 2017

McGuire, M., 2018, Into the Web of Profi t, Bromium, 20/04/2018, see https://www.bromium.com/resource/into-the-web-of-profi t/

McGuire, M., 2019, Into the Web of Profi t: Behind the Dark Net Black Mirror, Bromium, 05/06/2019, see https://www.bromium.com/resource/into-the-web-of-profi t-behind-the-dark-net-black-mirror/

Merriman, C., 2019, Amazon’ s Jeff Bezos was hacked by Saudi Arabia, investigation fi nds, Inquirer, 01/04/2019

MIT, 2019, Atlas of Economic Complexity, accessible at: https://oec.world/en/

Muncaster, P., 2017, EU to Declare Cyber-Attacks “Act of War”, Infosecurity, 31/10/2017

Muncaster, P., 2020, Russian APT28 Group Changes Tack to Probe Email Servers, Infosecurity, 20/03/2020

Nakashima, E., 2019, At nations’ request, US Cyber Command probes foreign networks to hunt election security threats, Washington Post, 07/05/2019 NCSC,

2018a, Preventing Lateral Movement, UK National Cybersecurity Centre, Advisory note, 08/02/2018

NCSC, 2018b, APT10 continues to target UK organisations across wide range of sectors, Alert, 20/12/2018

NCSC, 2020, NCSC defends UK from more than 700 cyber attacks, News item, 03/11/2020

Howell O’ Neill, P., 2018, Drones emerge as new dimension in cyberwar, Cyberscoop, 05/02/2018

O’ Malley, M., 2020 Concerned about Nation State Cyberattacks?, Security Magazine, 26/03/2020

Osbourne, C. 2016, Dark Web drugs, data dumps and death: Which countries specialize in what services?, ZDNet, 02/03/2016

Perlroth, N. & Shane, S., 2019, In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc, New York Times, 25/05/2019

Pollard, N., 2017, Ghosts in the Machine that Can Rob You Blind, The Cipher Brief, 03/12/2017

RAND, 2019, Accountability in Cyberspace: The Problem of Attribution, 14/04/2019

Reuters, 2019, Government o ffi cials around the globe targeted for hacking through WhatsApp – sources, 31/10/2019

Reuters, 2021, Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency, 02/02/2021

Robertson, R., 1994, Globalisation or glocalisation? The Journal of International Communication 1, pp 33-52

Roth and Berlinger, 2021, North Korean hackers stole more than $300 million to pay for nuclear weapons, says confi dential UN report , CNN, 09/02/2021 RTS,

2016, The hackers stalking TV networks, Royal Television Society, November 2016

Schwartz, M., 2018a, Cybercrime Groups and Nation State Attackers Blur Together, BankInfo Security, 18/06/2019

Schwartz, M., 2018b, Lazarus ‘FASTCash’ Bank Hackers Wield AIX Trojan, BankInfo Security, 12/11/2018

Seal, T., 2021, Microsoft Exchange Zero-Day Attackers Spy on U.S. Targets, Threatpost, 03/03/2021

Shane, S., 2018, Russia Isn’ t the Only One Meddling in Elections. We Do It, Too, New York Times, 17/02/2018

Sherman & Zoob, 2018, The Triton Cyber Weapon, RealClearDefense, 04/04/2018

Silverman, C., 2016, This analysis shows how viral fake election news stories outperformed real news on Facebook, Buzzfeed News, 16/11/2016

Simmons, D. 2019, Cyber-attacks ‘damage’ national infrastructure, BBC 05/04/2019

Slye, J., 2020, The FY 2021 Federal Budget Sustains Cybersecurity Funding, Govwin

Smith, M., 2015, Researchers link QWERTY keylogger code to NSA and Five Eye’ s Regin espionage malware, CSO, 27/01/2015

Snoddy, R., 2016, The hackers stalking TV networks, Television Magazine, November 2016

SOFF, 2017, State sponsored cyber attacks, Swedish Security and Defence Industry Association

South, T., 2018, New cyber weapons are here and no one is prepared, experts say, Army Times, 09/04/2018

Stewart, R., 2019, Chinese-linked APT10 adds new Quasar RAT and PlugX variants to its arsenal Cyware, 28/05/2019

Stolton, S., 2020, UN backing of controversial cybercrime treaty raises suspicions, Euractive, 23/01/2020

Sun Tzu, 2018, The Art of War, CreateSpace Independent Publishing

Symantec, 2019 Internet Security Threat Report 2019

Tannam, E., 2018, GitHub falls victim to world’ s largest DDoS attack: What you should know, Silicon Republic, 02/03/2019

Thomson, I., 2017, Everything you need to know about the Petya, er, NotPetya nasty trashing PCs worldwide, The Register, 28/06/2017

UN, 2021, Ad hoc committee established by General Assembly resolution 74/247: Postponement. See: https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

Uren, T., Hogeveen, B., Hanson, F. et al., 2018, Defi ning off ensive cyber capabilities, Australian Strategic Policy Institute, 04/07/2018

Voo, J. et al., 2020, National Cyber Power Index 2020, Harvard College, available at: https://www.belfercenter.org/sites/default/fi les/2020-09/NCPI_2020.pdf

Walden, P. & Kashefi , E., 2019, Cyber Security in the Quantum Era. Communications of the ACM, April 2019, 62, 4, p. 120

Wall, M., 2018, Is this the year ‘weaponised’ AI bots do battle?, BBC, 05/01/2018

Wolfe, D., 2019, A cyberattack in Japan could now bring the US into war, Quartz, 20/04/2019

Xinhua, 2019, China to lead global cybersecurity market growth in next 5 years, China.org.cn, 09/09/2019

Zetter, K., 2016, That Insane, $81M Bangladesh Bank Heist? Here’ s What We Know, WIRED, 17/05/2016

APPENDIX – 方法論

国民国家間のオンライン紛争を調査する際、その数の少なさと信頼性の低さはよく知られており、その秘密度を考慮すると意外性はありません。多くのデータは各国政府によって機密扱いにされており、そのため研究者がアクセスすることはできません。また、アクセス可能な場合でも、慎重かつある程度の懐疑心を持って取り扱わなければなりません。もし国民国家が情報の非公開に満足しているとしたら、それはなぜなのか、誰のためになるのかを考えなければなりません。また、西欧社会の研究者が入手できる情報は、西欧社会の利益に大きく傾斜していることも注目すべきです。多くの点で、私たちはアメリカやイギリスについてよりも、ロシアや中国のサイバー作戦についての方がよく知っています。

この調査では、主に4つの情報源を利用しました。

(i) 二次情報源、内部告発者、内部情報から得られたパブリック・ドメインにある文書化されたレポート。

(ii) 関連分野の第一線で活躍する50人の実務家を対象としたアンケートから得られた専門家の知見。具体的には以下の分野です。

英国法執行機関	5人の回答者
欧州および国際的な法執行機関	5人の回答者
政府	4人の回答者
インテリジェンス機関	6人の回答者
サイバーセキュリティ業界	10人の回答者
メディア・ジャーナリズム	5人の回答者
NGO	5人の回答者
学術研究機関	10人の回答者

本報告書で取り上げられている問題は非常に秘密度が高いものであるため、回答は匿名かつ帰属を伏せた上で提供されています。

(iii) ダークネット上の情報提供者やその他の秘密の情報源との非公式、非構造化インタビュー。

(iv) オンライン上の国民国家間の紛争に関連した約200件のインシデントの帰納的な分析。[111]

利用可能な生の、そして多くの場合限られた二次データからの洞察は、可能な限り信頼性の高い推論の範囲で「ギャップを埋める」ように設計された新しい分析ツールによって強化されました。例えば、NSiC（Nation States in Cyberspace）アプローチは、国家間のサイバー紛争の複雑さを、「SOTTT」変数として定義された4つの主要パターンに分解するのに役立ちました。

S – サイバー空間での優位性を獲得するために国民国家が立てた***戦略***

O – 戦略的優位性を求めるための国民国家の***目的***

T – これらの闘争の主な***標的***

T – 主要な***ツール***（サイバー兵器）

T – 国家がこれらのために利用している***テクニック***（攻撃ベクター）

111 この調査のために集められた事件のリストは、2つの既存のデータベース（CSIS 2020とCFR 2019を参照）、他の二次資料で言及されている国家の潜在的な攻撃、およびこの調査で相談した専門家のオフレコの見解を利用しました。