

CTIの生態系/市場と対峙する政府のインテリジェンス

防衛研究所 新領域研究会

「サイバー脅威インテリジェンス（CTI）をめぐる内外動向と産官学連携」
討論者コメント資料

2024年3月1日（金）

防衛研究所政策研究部
サイバー安全保障研究室
研究員 瀬戸 崇志

自己紹介

- 研究対象：インテリジェンスと安全保障（機能軸）× 欧州含む環大西洋地域の安全保障（地域軸）
- 研究の方法論：安全保障理論・歴史研究 / 組織・制度論の観察対象としてのcyber/information operations
 - 各国の軍事組織やインテリジェンス機関の**任務・ドクトリン・組織文化**とその（非）**変容要因・過程**のケースとしての関心

これまでの主な研究業績/活動として...

- 「民主主義国家の‘サイバー軍’による攻勢的サイバー作戦能力の整備と運用——米軍とオランダ軍の‘二重の統合’の過程の比較研究——」『安全保障戦略研究』第4巻2号（2024年3月）177-201頁 ([Link](#))
- 「パブリックアトリビューションの‘拡散’と‘多様化’——政策当局間の‘多様化’の国際比較研究——」『安全保障戦略研究』第3巻2号（2023年3月）63-83頁 ([Link](#))
- Weaponized Disclosure of Intelligence in the Russia-Ukraine War: Disclosure Dilemma and Hidden Inheritances from Post-2014 Transatlantic Security Cooperation, *NIDS Commentary*, October 2023 ([Link](#))
- 「情報化時代の‘コバート・アクション（covert action）’——国家による攻撃的サイバー作戦をめぐる課題の歴史的な連続性」研究報告 一般財団法人日本国際政治学会 2022年度研究大会（2022年10月30日）
- 書評論文「志田淳二郎著『ハイブリッド戦争の時代——狙われる民主主義』」『国際安全保障』第50巻2号（2022年9月）122-126頁 ([Link](#))
- 「ロシアのウクライナ侵攻と米英両国のインテリジェンス公表政策—情報機関の「ジレンマ」と2014年以降の安全保障協力の‘系譜’」『NIDSコメンタリー』第224号, 2022年5月 ([Link](#))



画像出典：本人提供

討論者コメント：3つのポイント

両講師の発表内容に通底する点を近年の学術研究の議論を踏まえて整理すると、脅威情報/CTIを取り巻く「生態系」または「市場」の成立は、「政府」に対して次の3つの課題を提起。

① 政府のIntelligence Cycle/Processの水平的延伸

② 政府の「独占的優位」から「市場の一参加者」としての適応

③ 「生態系/市場」での「政府」の機能：3つの視角と論点

①政府のIntelligence Cycle/Processの水平的延伸

古典的な政府のインテリジェンスと、産業界におけるCTIに通底する理念/目的

- 多様な情報（Information）の収集・加工・分析を通じた「プロダクト（intelligence product）」の生産と提供（頒布：dissemination）を通じ、任意のカスタマーの行動のための意思決定を支える（decision support）ための営為〔（石川 2022）（Work 2023）（Work 2020）ほか〕

CTIの特徴①：Informationの収集源+プロダクト生産主体の拡散

- 冷戦期との最大の相違：国家によるプロダクト生産の独占的地位の相対化〔（Broeders and Kavanagh 2023）（Dovner 2022）（Dylan and Maguire 2023）（Romansky and Boudreaux 2021）ほか〕
 - 民間企業/市民社会等の「非国家主体（non-state actor）」の自律性（Cf. 冷戦期：政府の活動の「客体」or「手段」）
- プロダクトの生産者としての国家（政府）の相対化&非国家主体の自律性の向上には、次の要因が大きく作用<参考3>
 - （1）民間の技術/サービスの脅威情報の「センサー」としての機能→民間企業の情報収集活動の独自優位（Steffens 2020）
 - （2）「市場」の成立：CTI概念による「脅威情報」の「財」たる価値の認識→プロダクトのカスタマー/ニーズの多様化〔（瀬戸 2023）（Romansky and Boudreaux 2021）ほか〕

CTIの特徴②：プロダクトのカスタマーおよびニーズの多様化

- CTI/脅威情報：カスタマーは必ずしも政策決定者や法執行機関・軍の運用担当者の意思決定のみに限定されず
 - （例）民間企業と法執行機関：attributionの用途の相違 → 要求水準・必要な時間軸が異なる<参考3>
- 政府の情報機関による、伝統的なインテリジェンス・コミュニティ（IC）の「外」のカスタマーへのプロダクト提供の模索<参考1/6>
 - （例）近年の欧米諸国のインテリジェンス機関（IS）によるJoint Cybersecurity Advisory（JCSA）<参考1/2/7>

② 政府の「独占的優位」から「市場の一参加者」としての適応

脅威情報の「市場」：異なる“intelligence community”の併存と協調/競合関係

- CTI：北米圏で形成されてきた概念は、伝統的な政府のインテリジェンス・コミュニティ(IC)の慣行に起源
- ただし、産業界でのCTI/脅威情報をめぐる市場慣行は、情報機関と異なる出自の構成員による「実践」を通じて発展
 - (例) 脅威インテリジェンス・ベンダー、CERTコミュニティ、産業セクター毎の情報共有コミュニティ (ISAC) など (石川2022)
- 政府のIS/ICは、伝統的なICとは異なるコミュニティも含めた「脅威情報」の取り扱いをめぐる市場の参加者に転換
 - 論点：目的/制度毎のコミュニティ間の合理的断絶 → 特定のコミュニティの枠を超えた情報共有は所与ではない <参考3>

政府のインテリジェンス機関に対する「共同製造」(Peterson 2019) の誘因の付与

- CTIにおける (1) 情報源、(2) プロダクトの生産者、(3) “ ” のカスタマー (消費者) の水平的延伸/拡散
 - 政府のISに対するプロダクトの共同製造 (co-production) (Peterson 2019) の誘因を付与 <参考4>
- 政府ISのIC「外」へのプロダクト提供による「呼び水」→ 産業界/市民社会との相互の情報・言説のフィードバックループの構築
 - 産業界/市民社会のフィードによる収集情報の量的/質的变化 + 第三者検証による信頼性増幅
- 上記モデル：CTIに限らず、近年の政府の戦略的な機密指定解除の内在論理[(Dylan and Maguire 2023) (Seto 2023) (Janjeva,Harris, and Byrne, 2022) ほか]
 - CTIをめぐる例：USCYBERCOMによるVirus Totalへのマルウェア検体公表 <参考6> / NSAのJCSA公表 <参考1/7>
 - CTI以外の例：2022年の露の対宇全面侵攻の前後での米英両国ISの分析結果の戦略的な機密指定解除 <参考8>

③ 「生態系/市場」における「政府」：3つの視角と論点

「生態系/市場」における「監督者」としての政府？

- 公共財の提供/取引環境の整備＋様々な「市場の失敗」の是正を促す最も根源的な政府の機能
 - Q：CTI/脅威情報をめぐる「市場の失敗」はいかに顕在化し、是正手段とは、具体的にはいかなるものなのか？

「生態系/市場」における「生産者/供給サイド」としての政府？

- 近年の欧米諸国の政府当局によるJoint Cybersecurity Advisoryをケースとすれば、
 - 政府の「内在論理」→ 古典マクロ経済学のアナロジーでの公共投資の乗数効果に類する期待 cf.「共同製造」の力学
 - （少なくとも日本での）民間視点の「実績評価」→ 古典ミクロ経済学のアナロジーでの市場歪曲効果をもたらす側面も存在？
 - 現実には双方の側面が混在：Q：いかなる内容/時期/形式であれば、政府の取組は所期の効果を上げるのか？

「生態系/市場」での「消費者/需要サイド」としての政府？

- 「脅威情報」の「財」のメタファー：取引可能な「財」の粒度問題と、市場で取引可能な価値をめぐる問いを提起。
 - 「政府」と「民間」の財の取引：政府の収集・提供可能ないかなる「脅威情報」が民間との交換価値を持つか？ <参考 1/5>
- 「市場」において、政府が「脅威情報」という「財」と交換可能な価値は必ずしも「脅威情報」のみとは限らない。
 - 「民間」が収集・提供する「脅威情報」と釣り合う、政府の交換可能な価値とは何であるのか？ <参考7>

参考1：近年の欧米諸国のインテリジェンス機関による民間へのプロダクト提供の模索



■ オランダ：統合情報保安局(AIVD) / 軍情報保安局 (MIVD)

AIVDとMIVDは、同国NCSC所管の脅威情報共有枠組National Detection Network (NDN) や、CAT5と呼ばれる法執行機関と連携した情報共有枠組に参画。自身の国内外での情報収集活動や各国治安・情報当局から接受した脅威情報を、適宜情報源をサニタイズして国内の民間事業者防護に裨益させるためのアウトリーチ活動を展開。



■ デンマーク：国防情報局 (FE) / 保安情報局 (PET)

2010年代後半、同国NCSOにあたるサイバーセキュリティセンター (CFCS) が、デンマークの国防情報局 (FE : Forsvarets Efterretningstjeneste) を軸に再編。強力な国内法上の権限の下、インテリジェンス機関を高度な標的型攻撃に対するファーストレスポnderにあてる中央集権的体制。

FEは文民系統の保安情報局 (PET : Politiets Efterretningstjeneste) と連携し、重要インフラ事業者へのアウトリーチを展開。法執行機関の立件化を避けたい民間事業者等に対し、諸外国のカウンターパートから接受した脅威情報を駆使しつつ水面下のインシデント対応支援を展開し、同時に事業者のインシデント対応支援で獲得した脅威情報を、将来の事案対処にも役立てるというフィードバック・ループを構築。



■ 米国・英国等：ISによる統合サイバーセキュリティ・アドバイザリー(JCSA)の発出支援

いわゆるファイブアイズ(FVEY)諸国と同盟・同志国の関係機関の連名で発出。特に2010年代後半から、各国インテリジェンス機関も発出に関与。敵対者の攻撃キャンペーンのIoC/TTPや対策手法の情報を公表し、米国・同盟国の官民のネットワーク防衛強化を促すことで、相手方のキャンペーンの妨害と累積的コスト強要を狙う。同盟国等との共同での脅威情報の発出により注目を確保し、また攻撃者の標的産業・意図等のコンテキストを付与。際限の無い脆弱性へのパッチ適用の負担を軽減し、切迫した脅威への優先的対応を支援。

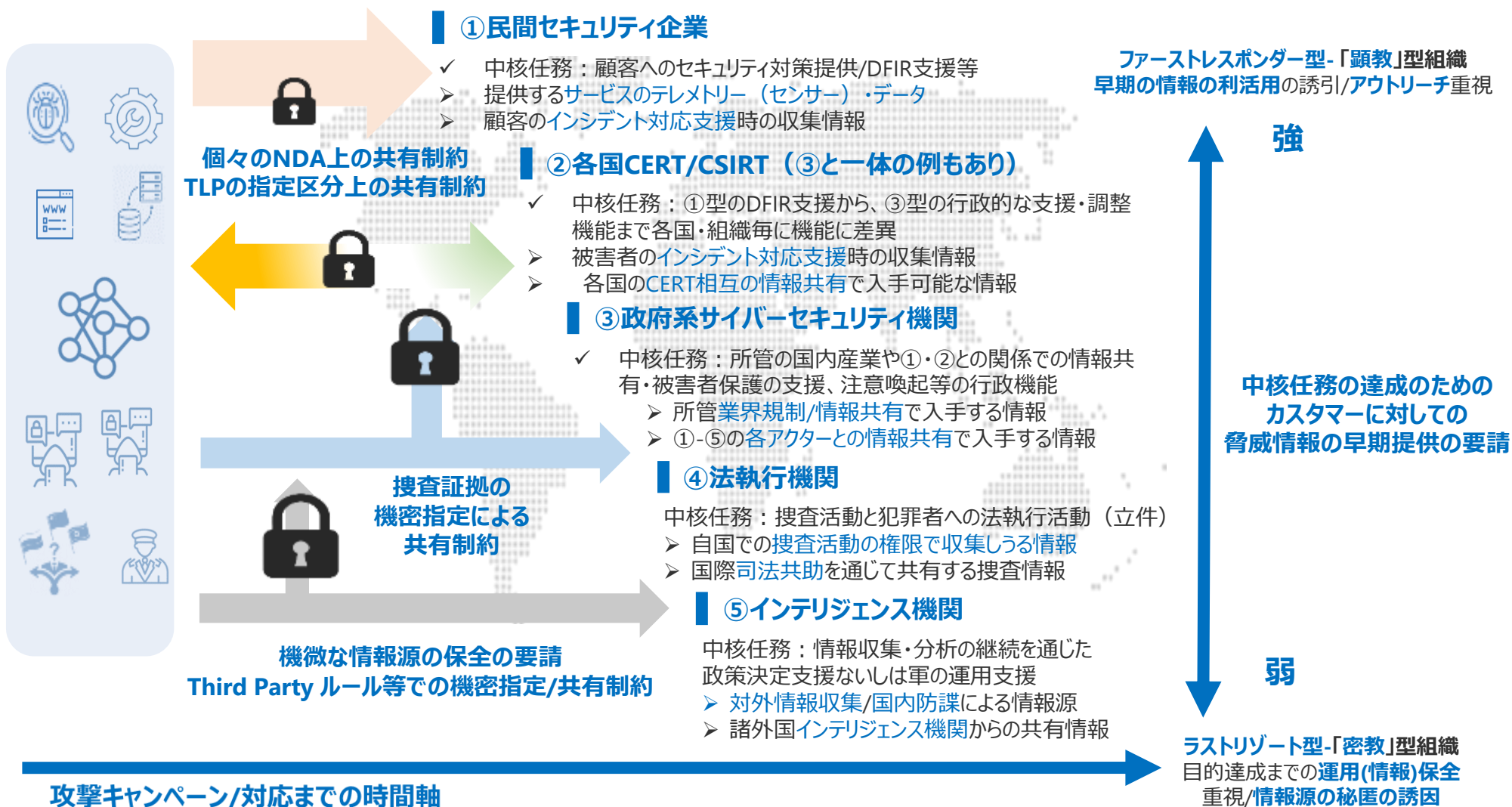


■ 米国：米国サイバー軍国家サイバー任務部隊 (CNMF) によるUnder Advisementプログラム

2018年の中間選挙防護支援の経験を経て、2020年に“Under Advisement (UNAD)”と呼ばれる産業界とのクローズドな脅威情報共有のためのプラットフォームを立ち上げ。米国サイバー軍のなかでも、主に各国を背後とする脅威アクターへの対処・防護を任とするCNMFの要員が実名で参加し、軍民双方が観測している攻撃キャンペーンのIoC/TTPs等についての脅威情報や分析ノウハウを共有。

参考3(1/3) : CTIの生成・利活用をめぐるアクター毎の目的・手続・時間軸の相違

民間セキュリティ企業と政府の法執行機関・インテリジェンス機関は、しばしば同様の攻撃キャンペーンを観測し情報収集・分析をしているが、各アクターが奉ずる伝統的な中核任務に沿って、情報保全の手続や成果物の利活用の時間軸が異なる、複数の情報流通の経路が存在。したがって、各々の経路で収集・分析・活用される情報は、共有が可能/有益な場合であっても、必ずしも経路を跨いで共有されるものではない。



参考3(2/3)：攻撃キャンペーンの観測における情報源と分析手法の比較優劣

アトリビューションのための主たる情報源・分析手法の体系であるMICTICフレームワークに沿って考えたとき、例えば民間企業と政府機関の間では、プロダクト生成のために利用可能な情報源の質・量にそれぞれ比較優位・劣位（例：「T」と「I」）が存在。

略

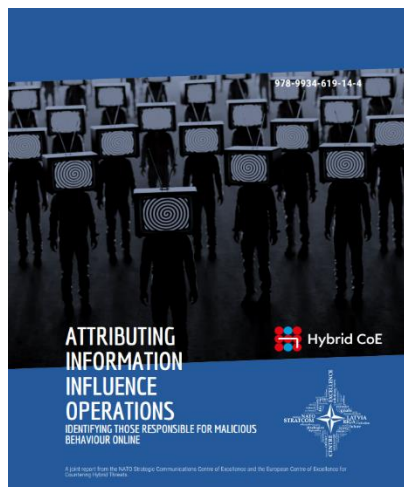
項目名

概要と主たる情報源・技法等

	M	マルウェア (Malware)	■ 攻撃者が利用したマルウェアから採取できる情報源と分析手法。コードの構造、開発環境の言語設定や時間設定、仮想化環境でのマルウェアの挙動と接続先のサーバーの情報、データ転送時の暗号化の特徴など
	I	攻撃インフラ (Infrastructure)	■ 攻撃者が利用するインフラや、その設営段階でのミスが産み出す情報源と分析手法。Whoisプロトコルによる攻撃者のサーバー契約情報の照会、DNS解決を駆使した複数のドメインと一意のIPアドレスの相関分析、攻撃者が利用する特定のサーバーへのアクティブ・スキャンなどを含む。
	C	コントロール・サーバー (Control Server)	■ 攻撃者が利用する攻撃インフラ (I) のなかで、特に重要な機能を果たすサーバーから採取できる情報源。法執行機関の令状によるサーバー事業者からのトラフィック収集や、押収したハードディスクに残された攻撃者のマルウェア運用のためのサーバーの設定情報などを含む。
	T	テレメトリー（センサー） (Telemetry) (民間セキュリティ企業の比較優位)	■ 民間セキュリティ企業が顧客・被害者に提供してきた製品・サービスのセンサー・データとその分析手法の総称。 ■ 民間セキュリティ企業の圧倒的な情報の質・量の優位が存在。特に、北米系を中心に、世界中にサービスを提供するセキュリティ企業は、被害産業・地域・時期の相関（分散）なども含めて、攻撃キャンペーンや（Intrusion Setsの擬人化としての）攻撃グループの動向把握に資するもの。
	I	インテリジェンス活動 (Intelligence) (政府機関の比較優位)	■ 政府のインテリジェンス機関・法執行機関等がその権能でのみ収集し得る情報源と分析手法。捜査活動や対外諜報活動として行うサイバー攻撃、SIGINTやHUMINTによる攻撃者の個人情報や所属機関の情報収集など。 ■ 具体的な実行犯個人や国家機関の関与・責任を高精度な絞り込みに資する情報だが、極めて機微かつ仔細の共有/公表に馴染まないことが通例。
	C	犯行動機 (Cui Bono)	■ 攻撃者が特定の標的に攻撃を行う「動機」に係る情報源と分析手法。（Cui Bonoは犯行動機を指すラテン語）。OSINTを含む地政学的分析を軸に、脅威アクターの背後に居る機関や目的を検証するプロセス。

参考3(3/3) : デジタル影響工作のアトリビューションと証拠/情報源の断片化問題

SNS等を駆使したデジタル影響工作のアトリビューションでも同様に、主体毎の観測優位の差による証拠/情報源の断片化は存在。



NATO戦略的コミュニケーションセンター(NATO StratCom CoE)と欧州ハイブリッド脅威対策センター(Hybrid CoE)の共同研究(2022年7月) のポイント

- 3種の情報源×3つの証拠類型の組み合わせで、立証できるアトリビューションの水準が異なる。
→例えば公開情報源のみでは、背後の国家機関の高い信頼水準でのアトリビューションは困難。
- プラットフォーム企業や政府機関が直面する制約条件のなかで、「特定（分析）」に用いる情報源と、「公表に適した」情報源にはギャップ → 透明性の欠如やバイアス問題等を惹起。
- 各情報源による分析は、相互補完的な存在 → 分析面での官民連携の重要性。

	技術的証拠 (technical)	活動パターン証拠 (behavioral)	文脈証拠 (contextual)	法的・倫理的論点
公開情報源 Open source	ドメインの所有権、 IPアドレス 経済的関係性	アカウント/ページの稼働状況、 単一/複数プラットフォームでの 投稿状況や投稿のシェア/FF関 係などのネットワーク	コンテンツの内容、 言説、言語的特徴、 政治的文脈、動機 (cui bono)	訴訟リスク、研究倫理、研 究者個人が報復されるリス ク
(プラットフォーム企業等の) 私有情報源 Proprietary source	プラットフォーム企業 のバックエンドでの収 集データ	公開情報源と同種だが、プラ ットフォームとして収集可能な、よ り膨大なデータ	公開情報源に加え、 過去のテイクダウンの 実績に基づく情報	政治的・商業的利益の保 護の要請と（個人）デー タ保護をめぐる問題
(政府の) 機密情報源 Classified source	SIGINTならびに令 状(warrant)により 押収された私有 データ	公開・私有情報源に加えて、 SIGINTおよびHUMINT	公開・私有情報源 に加えて、機密指定 された地政学的な 分析	特定の対象国への戦略との 中での一貫性問題、政治 的利益の保護の要請、デー タ（情報収集源）の保護

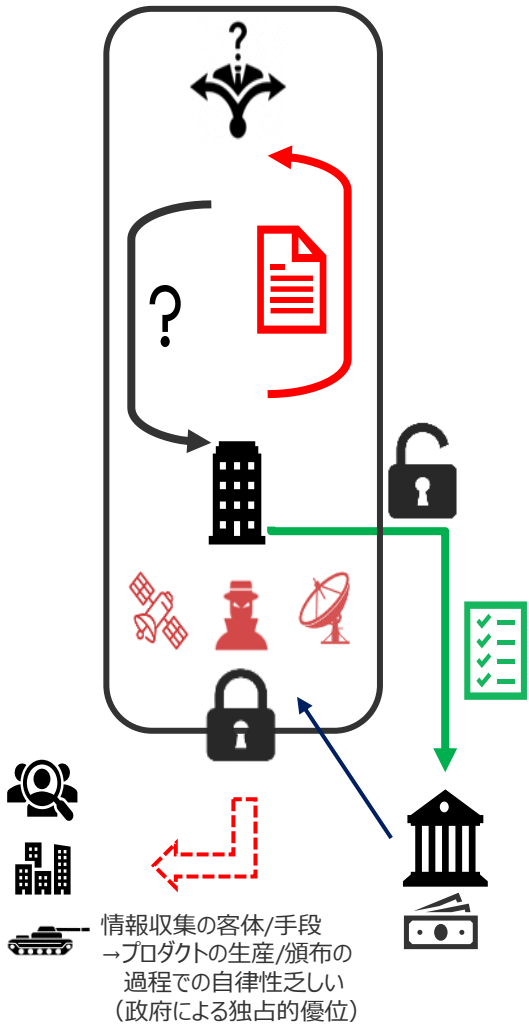
出典：James Pamment and Victoria Smith. 2022. *Attributing Information Influence Operations: Identifying Those Responsible for Malicious Behaviour Online*. Riga, Latvia: NATO Strategic Communications Centre of Excellence. を基に報告者作成

参考4：政府ISの外部とのコミュニケーション類型と「共同製造」モデル（Peterson 2019）

①認知向上(Awareness)

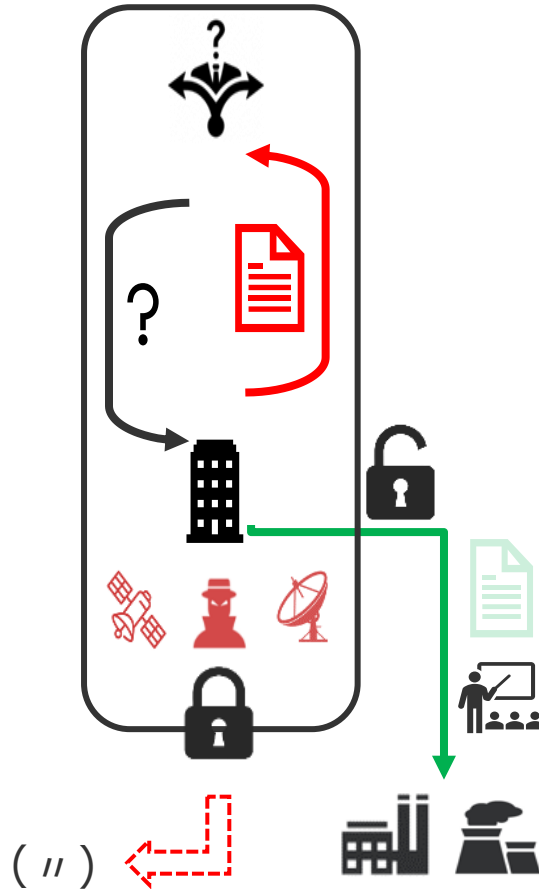
(例) : 年次の議会手続への対応等

枠内：政府のIC



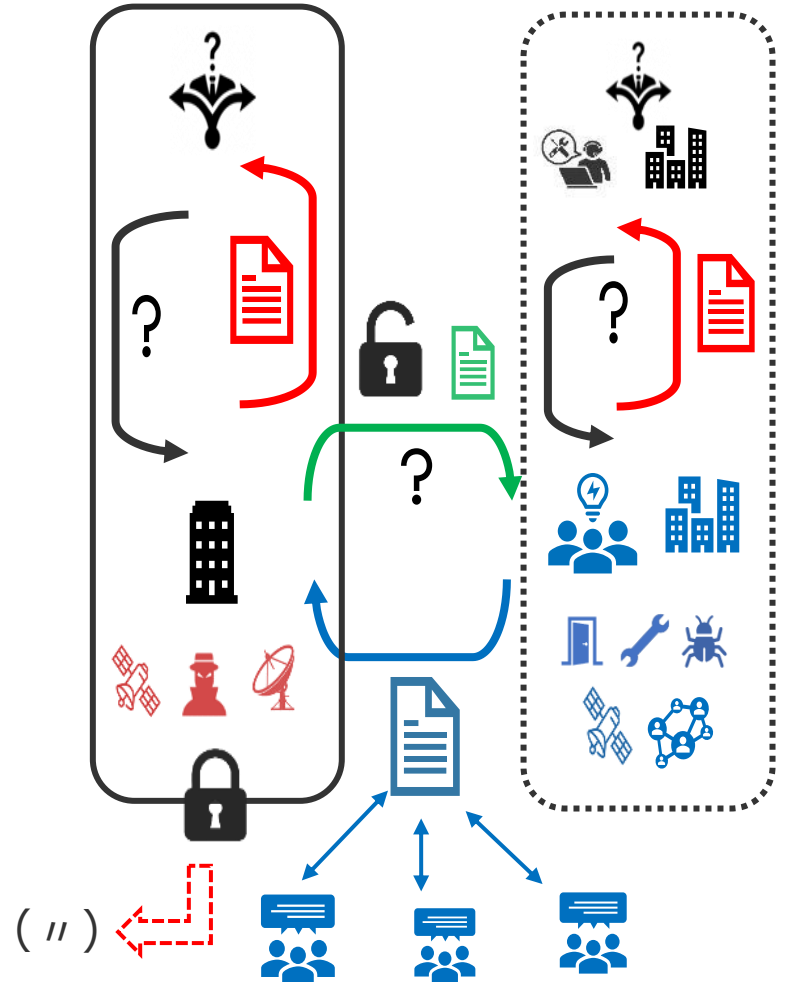
②助言 (Advice)

(例) : テロ対策に向けた
事業者向け注意喚起



③共同製造 (Co-production)

(例) : 近年のJCSA方式での注意喚起 (の理念)



参考5(1/3)：インテリジェンス機関の能力基盤の「比較優位」

①技術情報+攻撃者の能力/意図の統合分析 [(NSA 2022) (NSA 2023) (Ertan 2020) ほか]

- NSAの比較優位：SIGINT機関・対外情報機関としての情報収集・分析の基盤：米国の国外（foreign space）での情報収集活動を通じた多様な攻撃グループの活動様態や戦略目標の情報と、情報通信技術自体への専門知の双方を統合した分析（2021年度NSA年次白書 [2022年2月刊]より）
 （例）SolarWinds事案などの初動対応における集合知による状況把握強化の取組
 - 米国政府とセキュリティ企業側の信頼関係に基づく水面下でのコンタクトを通じて、FireEye社（当時）側が自社サービスのテレメトリーで観測していた国内外の被害状況データ+と、NSA側が独自に観測していたデータの相互参照を通じて全体としての状況把握を強化した由。

②政府間連携での共同発出による注目度/コンテキスト付与による対策の優先度の伝達

- NSA：システム所有者の対策実施に必要な、脅威インテリジェンスのコンテキスト(context)を提供し得るとき、関係省庁やファイブ・アイズ（FVEY）のパートナーとも連携しパブリック・アトリビューションを実施（NSA 2020）
 - 政府機関が特定産業セクターを標的に、他国の政府機関が関与する脅威が進展しているとの具体的なコンテキスト(context)を付し、情報の受け手の範囲や脅威の重大性を明確化。各団体の迅速な対策を促進[（Johnson 2021）（Gazis, O 2020）ほか] [注目度付与の原理は（Riemer 2020）も参照]

③インテリジェンス機関のカウンターパートナーシップ [(Boeke 2016) (Boeke 2017) (Hannigan 2019)]

- 各国政府のサイバーセキュリティ機関は、①英丁白のようにインテリジェンス機関を軸に組成されたもの、②蘭独のようにインテリジェンス機関とは異なる系統の組織を軸に組成されたものの2系統が存在。各国間の脅威情報共有の質量は、系統の近い組織間において緊密となる傾向。
 - オランダやデンマークで両方の情報共有枠組を経験した実務者曰く、（②のトラックよりも）①のトラックから授受できる脅威情報の質・量の向上が見られたとの意見も存在（Boeke 2017）



参考5(2/3) : インテリジェンス機関の能力基盤の比較劣位/内在的制約

比較劣位/内在的制約には、機密指定区分、情報源の保護の要請、カウンターパートとの関係性等ゆえに、民間企業やセキュリティコミュニティと共有可能な情報の粒度・範囲・時期に制約が生じやすいことがある。

First Responder or Last Resort?

The role of the Ministry of Defence in national cyber crisis management in four European countries

Sergei Boeke

1 September 2016



National Detection Network(NDN) (蘭NCSC主管の業種横断的な情報共有枠組)



Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid



弥縫策としての ティアライン(tear-line) 型情報共有による対応

- ✓ 情報源を逆探知しうる仔細を落としたうえで、必要な事業者等によりのみ個別通知。



National Cyber
Security Centre
a part of GCHQ



CENTRE FOR
CYBER SECURITY



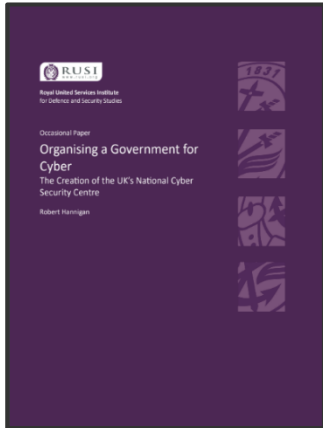
Algemene Inlichtingen-
en Veiligheidsdienst



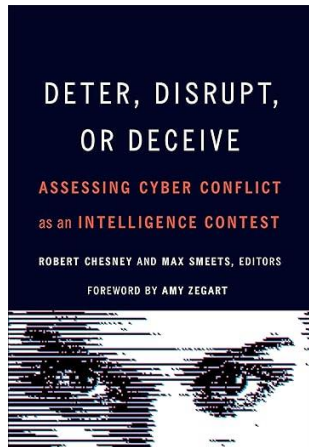
防衛産業系の情報共有枠組 (蘭国防省/MIVDとの機密情報の共有資格が存在)



参考5(3/3) : 英サイバーセキュリティセンター(NCSC)とインテリジェンス機関の組織文化



出典 : Hannigan, Robert. 2019. "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre." RUSI Occasional Paper. Royal United Services Institute for Defence and Security Studies. の内容を要約する形で報告者が作成。



出典 : Ciaran Martin, The Development of the United Kingdom's Cyber Posture, in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed Robert Chesney and Max Smeets (Georgetown University Press, 2022)の内容を要約する形で報告者作成。

NCSC創設に係るR. ハニガン元GCHQ長官回顧録の要点 (Hannigan 2019)

- NCSCの創設の前後では、政府内外で、その情報収集・分析能力や技術的卓越性からしてもGCHQが国内のサイバーセキュリティ政策の一本化に責任を負うべきとの相場観と支持が存在。
- 従前よりGCHQの情報保証部門は政府の関係機関や一部民間のサイバーセキュリティ支援を担ってきたが、必ずしもGCHQでは主流派でなく、そもそもGCHQ全体を英国全体の防護に責任を負うために対外的な関与が可能な組織に完全に作り変えることは、インテリジェンス機関としてのGCHQの性質上、組織文化上の困難な課題を内包。そのためNCSCをGCHQの窓口機関としつつ、GCHQの指揮系統の中に組み込むという選択肢を採用。この組織的編成は、GCHQの情報収集・分析能力の活用は元より、Five Eyes諸国のカウンタパートを中心とするインテリジェンス機関系統の組織間での情報共有でもプラスの作用。
- GCHQの要員による匿名でのHPでのブログ寄稿や情報交換制度など、産業界や民間のセキュリティ・コミュニティとの連携のために求められる「公に開かれた(public-facing) 」組織となりうる取組を強化。

初代NCSCセンター長 Ciaran Martin氏の書籍論文の要点 (Martin 2023)

- GCHQは、英国の首都から離れた地点に位置し、同国で最もセキュリティの厳格な敷地であり、訪問者はGCHQからの招待と途方もないセキュリティチェックを受ける必要。敷地内に対する携帯電話の持ち込みも完全に禁止されており、GCHQ要員との間の迅速なコミュニケーションを取ることすら容易ではない状況にあった。英国のCS戦略に基づく政府と民間とのパートナーシップの重要性の要請にも係わらず、GCHQは—そのデザインと必要性からして、民間セクターとのパートナーシップが容易ではない組織であった。
- NCSCの創設に際しては、新組織を内閣府に置かれた独立組織とするか、GCHQの指揮系統の一部に置くかの論争が存在した。仮に新組織をGCHQとは独立の組織とした場合、(1) ファイブ・アイズ諸国との連携による利得を維持しうるか確証が乏しく、かつ(2) 実働を担うGCHQ要員の忠誠心とキャリア形成上の誘因からはGCHQ外の新組織に要員を送りだすことは、当該要員の離職を招きかねない問題があった。
- 以上の考慮から、NCSCは、GCHQの一部門として置かれつつも、GCHQ本体とは分離された態勢を採用した。インテリジェンス機関が、(情報セキュリティ部門を除き) 法令上義務付けられてきた伝統的な秘密性 (secrecy) の要件が緩和され、NCSCは透明性 (transparency) をデフォルトとする。新組織は、ロンドンに拠点を構えると共に、危機対応と産業界・メディアに対するアウトリーチを可能とするものとなった。

参考6：米国サイバー軍によるVirus Totalへの検体公表の取組の内在論理(1/2)

2020年2月に機密指定が一部解除された米国サイバー軍による2018年/2019年付の行政文書は、米国サイバー軍の隷下にある国家サイバー任務部隊（CNMF）が、Virus Total上で収集したマルウェア検体を公表する施策の目的につき、次の通り説明。

2020年2月の開示文書の構成：2種類の文書 [(USCYBERCOM 2018/2019) (Cox 2020)]

- (1)2018年11月7日作成：Executive Summary（1頁目）。
- (2)2019年7月10日作成：Information Paper(2-6頁目)。

Executive Summaryのポイント（記述から関連箇所抜粋・要約）

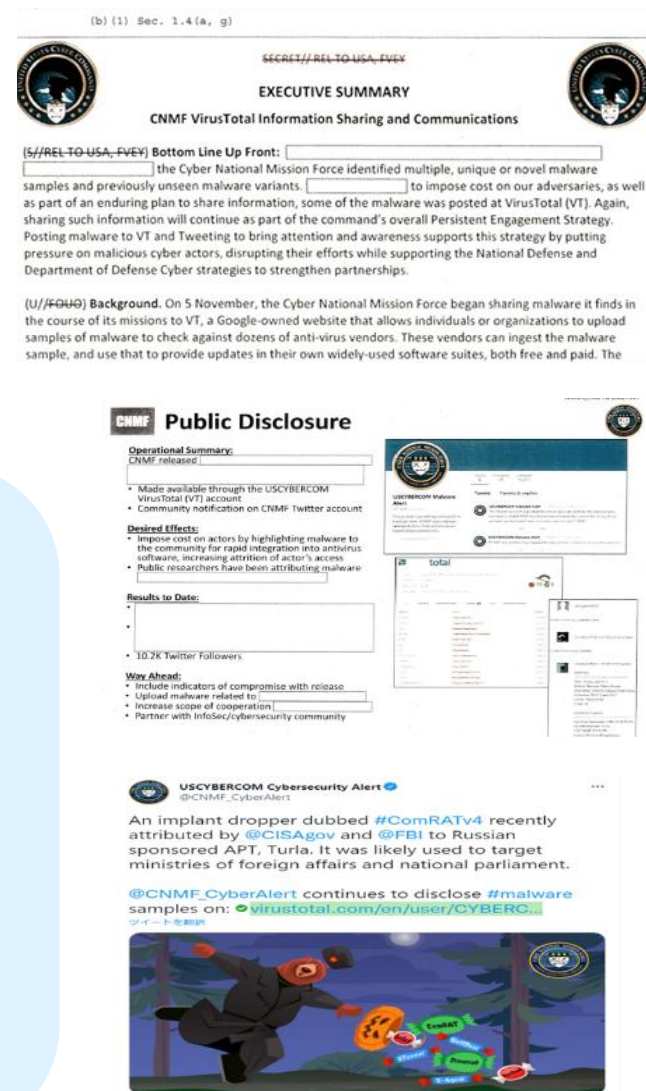
実施内容：国家サイバー任務部隊(CNMF)が任務で収集したマルウェア検体の情報をVirus Total(VT)で公表。（脅威）**アクターのアトリビューション**や（サイバー軍自身の）**SIGINTとTTPの第三者共有の回避**のため、サイバー軍のパブリック・アフェアーズ室（PAO）が支援。**Twitterを注意喚起(媒体)**に活用。

政策目的：概ね次の3点に集約

- (1)脅威アクターの**活動の妨害**（disrupting their efforts）を通じた敵対者に対する**コスト強要**（impose cost）（と抑止）。
- (2)国防総省のサイバー戦略が目標とする**パートナーシップ強化**の追及。
- (3)サイバー軍の「**持続的交戦**」戦略への**認知度・理解の向上**。

対外説明ぶり(narrative)：3つの柱

- (1)国防総省(DOD)は**各省や民間との協働重視**。**情報共有の新手法**を模索。
- (2)サイバーセキュリティ・コミュニティとのマルウェア共有は、共通の**グローバルなサイバーセキュリティを確保する施策**の一貫。
- (3)本施策はDOD・サイバー軍の「**持続的交戦**」戦略の一貫。脅威への**認知度の向上と対策促進**で、現在の活動を阻害し、将来の悪意ある活動を抑止。



参考6：米国サイバー軍によるVirus Totalへの検体公表の取組の内在論理(2/2)

2頁目：Virus Totalの選定理由：サイバーセキュリティ産業・研究者で普及し信頼性のあるクラウド・ソースであり、情報のリーチ範囲が広い。パブリック・エンゲージメントによる迅速なマルウェアの特定と、民間による悪意あるアクターへのアトリビューション、レジリエンス向上、そして敵対者に対するコスト強要に寄与。

2頁目：今後の課題：マルウェアの公表を[－]とシンクロさせ、施策の効果を増幅。敵対者に更なるコスト。

3頁目：情報公開手続 (全12段階のプロセスのうち、一部のみ抜粋)

- 1. CNMFのタスクフォースの分析官によるマルウェア・サンプルの評価：サンプルの独自性(uniqueness)と、公表に適する性質か否か(suitability for release)を決定。
- 3.機密指定解除を要する場合：確立した手続の下で実施。
- 4.サンプルのメタデータを[－]のためにサイバー軍の統合オペレーションセンター(JOC)に共有。[－]のリクエストは、次の情報を含むこと。
 - a. [－] b. 民間での脅威アクターとマルウェアの名称
 - c. マルウェアのサンプルファイル名とハッシュ値[MD5、SHA1、SHA256]
 - d. 適用しうる場合は[－]に紐づけること e. [－]差し止める日付及び意図された公表の[－]
- 6.公表の[－]前に、次の対応を実施すること。
 - a. サンプルを、[－]に対して提供する。(報告者注：約2行程度の不開示箇所：情報の配布先機関と推察)。
 - b. 米国サイバー軍のパブリック・アフェアーズ室に対して通知。c. サイバー軍[－]に対して通知。

4頁-6頁目：オペレーションの要約 (各1枚計3例。不開示箇所が多く事例や詳細は不明だが特筆点のみ抜粋)

- **4頁目：所期の目的** (注：2つの柱：ナンバリングは作成者が便宜上付記)
 - (1)サイバーセキュリティコミュニティでマルウェアを注目させ、早期にウイルス対策ソフトへのシグネチャの登録を促すことで、継続する[－]に対する累積的なダメージ(attrition)を増幅し、[－]に対するコストを課すこと。
 - (2)一般(public)のセキュリティ研究者がマルウェアを[－]にアトリビューションすること。
- **6頁目：今後の方向性** (注：3つの柱：ナンバリングは作成者が便宜上付記)
 - (1) (検体) 公表に伴い(各種の)IoC (indicators of compromise)を含める。(2)[－]に関連するマルウェアをアップロード。(3)[－]との協力の範囲を拡大。(4)サイバーセキュリティ・コミュニティとの協力を拡大する。

参考7(1/2)：近年のFVEY諸国等のJCSAを含む脅威情報「公表」の内在論理

① 諸外国も含む脅威情報のフィードバック・ループ構築 ＝ 特定国/業種を超えた「共同製造」のスケールメリット追求



画像出典：NSA

攻撃キャンペーン/対応までの時間軸

出典：(NSA 2023) (Healey, Jenkins, and, Work.2020) (Hinck and Maurer 2020) (DoJ 2023)ほか、各種先行研究・公開資料を基に報告者が作成。

② 攻撃グループの継戦能力を削ぐ国際共同対処の触媒



Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service

Press Release
Friday, May 9, 2023

Share

For Immediate Release
Office of Public Affairs

Through Operation MEDUSA, the FBI, and the U.S. Attorney's Office for the Eastern District of New York Neutralized the FSB's Premier Cyberespionage Malware Implant in Coordination with Multiple Foreign Governments

画像出典：DoJ

攻撃「ツール・インフラ」の破壊

- 体系化されたIoC/TTP/対策情報を利用した各団体のネットワーク防衛の支援（攻撃手法の効用の低下）
- 攻撃キャンペーンの資金源となる、犯罪収益や暗号資産などの凍結。攻撃キャンペーンを支援する技術・サービスを持つ団体への制裁措置。
- 民間企業や他国法執行機関とも連携したドメイン・C2サーバー/攻撃グループのフォーラムなどの攻撃インフラのテイクダウンなど。

「要員」の活動の制約・妨害

- 国際指名手配による事実上の渡航制限、在外公館カバーを持つインテリジェンス機関の要員（キャンペーンの管理者）の接受拒否で攻撃キャンペーン要員の自由を制約。特に国家機関から委託を受けた、代理人(proxy)が存在する場合に有効との指摘。

「計画」の再編コストの賦課

- 運用保全が重要なインテリジェンス機関の工作活動の計画やネットワークを早期に暴露し、標的団体・社会の警戒を高め、計画の再編に伴う sunk cost を賦課。

参考7(2/2) : 露FSB系攻撃グループ「Trula」のマルウェア「Snake」への共同対処 (2023年)

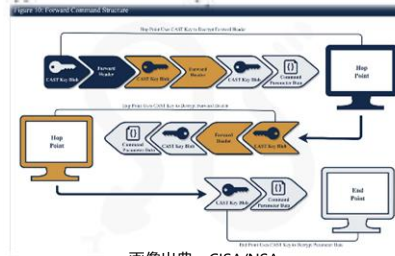
① (+②) ≡ 「Operation MEDUSA」 [(DoJ 2023) (NSA 2023)]

①米国「内」: 捜索令状に基づく被害端末への「PERSEUS」(*)投入: 「Snake」のP2P通信遮断

※PERSEUS: FBIが開発した、「Snake」が感染端末間において暗号化されたP2P通信機能を行う機能を無力化するためのツール

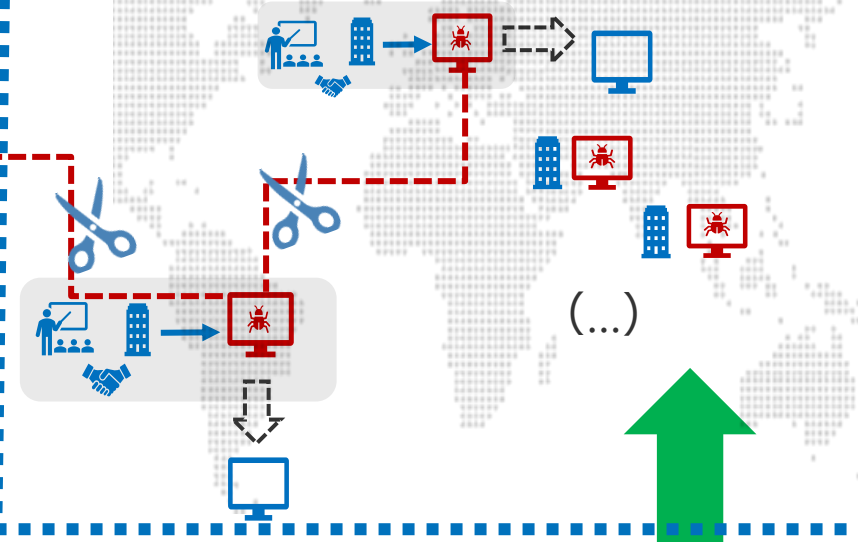
PERSEUS RELEASE

Justice Department Announces Court-Authorized Disruption of Snake Malware Network Controlled by Russia's Federal Security Service



画像出典: CISA/NSA

②米国「外」: 同盟・同志国当局との連携による被害者への通知と「Snake」の無害化 (50か国以上と協働)



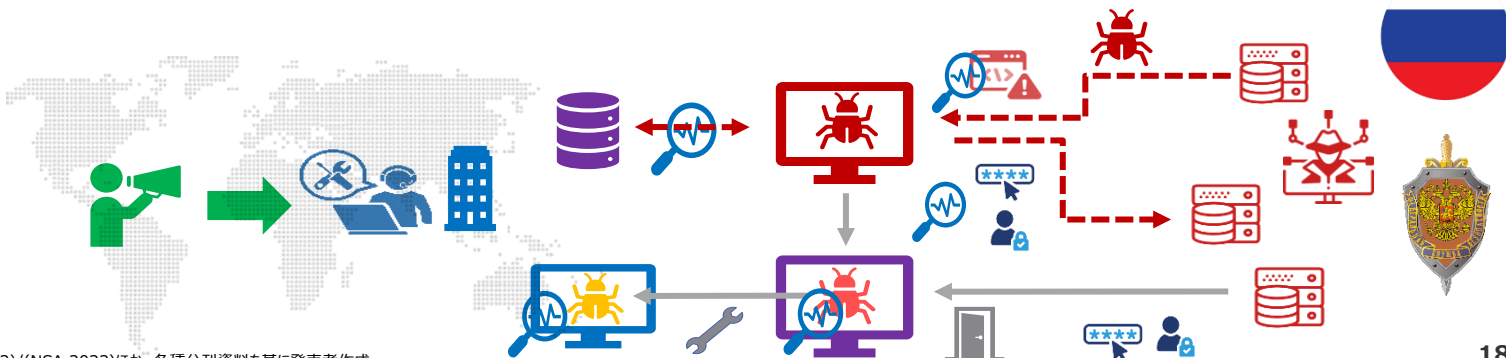
③JCISAに基づく、「Snake」の(現在/将来の)潜在的な被害者への注意喚起

- ・ 意義(1): 把握済の被害者への個別通知/対処でカバーできない範囲のオーディエンスにも注意喚起が可能
- ・ 意義(2): Operation MEDUSA: 「Snake」の感染端末間のP2P通信のみを無力化: 初期侵入経路となる脆弱性や認証情報窃取への対応、あるいは「Trula」が「Snake」を梃に追加で投入した攻撃ツールの無力化には、被害団体/将来の標的団体での検知・予防のための対応が不可欠 (DoJ 2023)



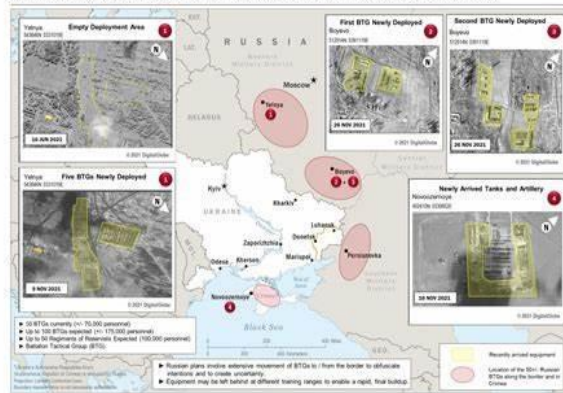
画像出典: CISA/NSA

出典: (DoJ2023)/(NSA 2023)ほか、各種公開資料を基に発表者作成。



参考 8 : 露の対宇全面侵攻前後での米英インテリジェンス機関の取組と「共同製造」

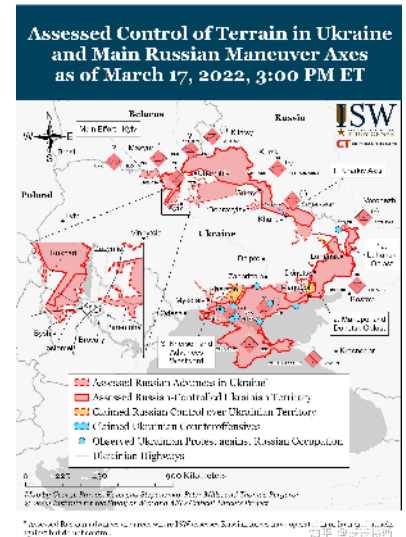
Potential for 175,000 Russian Forces Near Ukraine: Evidence of Recent Artillery, Equipment, Personnel Movements and Planning



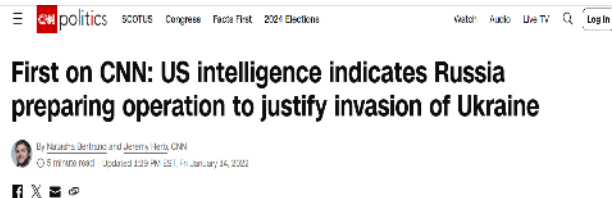
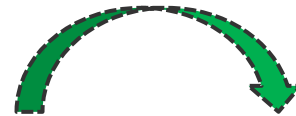
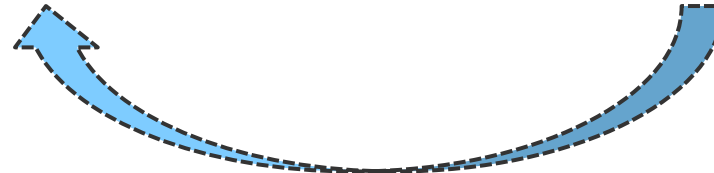
画像出典：New York Times



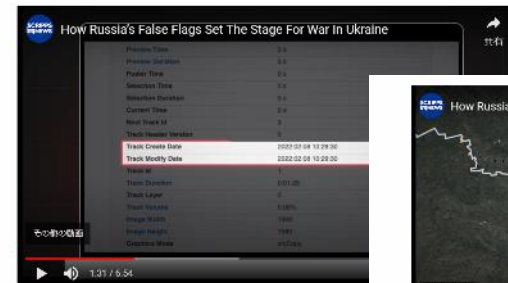
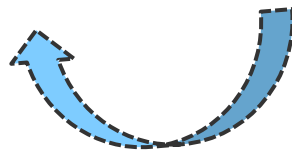
画像出典：UK Defense Intelligence



画像出典：Institute of War (ISW)



画像出典：CNN



画像出典：Bellincat



討論者コメントにおける主要な参考文献一覧(1/1)

- Broeders, D., Boeke, S. and Georgieva, I. 2019. *Foreign intelligence in the Digital Age. Navigating a State of 'Unpeace'*. Policy Brief, (Hague: The Hague Program for Cyber Norms/Leiden University) .
- Broeders, Dennis and Camino Kavanagh, 2023, *Shades of Grey: Cyber Intelligence and (Inter)National Security*, Policy brief (EU Cyber Direct) <https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/XqXCPBb2/shades-of-grey-cyber-intelligence-and-inter-national-security.pdf>
- Boeke, Sergei 2016, *First Responder or Last Resort? The Role of the Ministry of Defence in National Cyber Crisis Management in Four European Countries*, (Hague : Leiden University).
- Boeke, Sergei 2017. "National Cyber Crisis Management: Different European Approaches," *Governance*, vol. 31, no.2.
- Martin, Ciaran 2023. The Development of the United Kingdom's Cyber Posture, in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed Robert Chesney and Max Smeets (Georgetown University Press)
- Cox, Joseph, 2020. 'Internal Docs Show Why the U.S. Military Publishes North Korean and Russian Malware' February 25, 2020, *Vice*: https://www.vice.com/en_us/article/5dmwyx/documents-how-cybercom-publishes-russian-north-korean-malware-virustotal
- Dylan, Huw, and Thomas J. Maguire. 2022. "Secret Intelligence and Public Diplomacy in the Ukraine War." *Survival* 64 (4): 33–74.
- Dovner, Rober 2022. *Hacker, Influencer, Faker, Spy: Intelligence Agencies in the Digital Age* (London: Hurst & Co. Publishers)
- Department of Justice 2023. "Justice Department Announces Court-Authorized Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service," May 9, 2023, <https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network>
- Ertan, Army 2020, "Cyber Attribution: Challenges and Opportunities for Multi-Disciplinary Analysis," *Strife Journal* (14): 13–27.
- Healey, Jason. 2016. "The U.S. Government and Zero-Day Vulnerabilities: From Pre-Heartbleed to Shadow Brokers." *Journal of International Affairs*, November 1.
- Gazis, Olivia. 2020. "NSA Cybersecurity Directorate's Anne Neuberger on Protecting the Elections." CBS News. August 19, 2020.
- Hannigan, Robert. 2019. "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre." RUSI Occasional Paper. Royal United Services Institute for Defence and Security Studies. https://static.rusi.org/20190227_hannigan_final_web.pdf.
- Healey, Jason, Neil Jenkins, and J. D. Work. 2020. "Defenders Disrupting Adversaries: Framework, Dataset, and Case Studies of Disruptive Counter-Cyber Operations." In *12th International Conference on Cyber Conflict. 20/20 Vision: The Next Decade. Proceedings 2020*, 251–74. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence
- Hinck, Garrett, and Tim Maurer. 2020. "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity." *Journal of National Security Law and Policy* 10, no. 3 : 525–561.
- Johnson, Derek B. 2021. "Joint Alerts Are the Flip Side of Persistent Engagement Strategy, Says NSA Cyber Chief." *SC Media*. September 29, 2021.

討論者コメントにおける主要な参考文献一覧(2/2)

- Janjeva, Ardil, Alexander Harris, and Joe Byrne, 2022. *The Future of Open-source Intelligence for UK National Security*, RUSI Occasional Paper (Royal United Services Institute for Defence and Security Studies, Alan Turing Institute's Centre for Emerging Technology and Security).
- National Security Agency. 2022. *2021 NSA Cybersecurity Year in Review*. Fort Meade, Maryland.
- National Security Agency. 2023. *2023 NSA Cybersecurity Year in Review*. Fort Meade, Maryland.
- National Security Agency 2020. *Drovorub Malware Fact Sheet & FAQs*. Fort Meade, Maryland.
- Riemer, Ofek. "Politics Is Not Everything: New Perspectives on the Public Disclosure of Intelligence by States." *Contemporary Security Policy* 42, no. 4 (October 2, 2021): 554–83.
- Petersen, Karen Lund 2019. "Three Concepts of Intelligence Communication: Awareness, Advice or Co-Production?," *Intelligence & National Security* 34, no. 3.
- Pamment, James, and Victoria Smith. 2022. *Attributing Information Influence Operations: Identifying Those Responsible for Malicious Behaviour Online*. Riga, Latvia: NATO Strategic Communications Centre of Excellence. .
- Steffens, T. 2020, *Attribution of Advanced Persistent Threats - How to Identify the Actors Behind Cyber-Espionage*. Weisbaden, Germany: Springer Vieweg.
- Seto, Takashi, 2023, "Weaponized Disclosure of Intelligence in the Russia-Ukraine War: Disclosure Dilemma and Hidden Inheritances from Post-2014 Transatlantic Security Cooperation, *NIDS Commentary*," No.224.
- USCYBERCOM, 2018/2019, "EXECUTIVE SUMMARY CNMF VirusTotal Information Sharing and Communications." Declassified Memorandum . Fort George G. Meade, MD. <https://www.documentcloud.org/documents/6784558-CYBERCOM-Virutotal.html>
- Work, J.D. 2020 "Evaluating Commercial Cyber Intelligence Activity," *International Journal of Intelligence and CounterIntelligence*, 33(2).
- Work, J.D, 2023 "Private Actors and Intelligence Contest in Cyber Conflict," in *Deter, Disrupt, or Deceive: Assessing Cyber Conflict as an Intelligence Contest*, ed Robert Chesney and Max Smeets (Georgetown University Press)
- Wagner, Thomas D. et.al, 2019 "Cyber Threat Intelligence Sharing: Survey and Research Directions," *Computers & Security*, Volume 87.
- Romanosky, Sasha and Benjamin Boudreaux, 2021, "Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government," *International Journal of Intelligence and CounterIntelligence*, Vol. 34, Issue 3, 463-493.
- 石川 朝久 2022 『脅威インテリジェンスの教科書』（技術評論社）
- 佐々木 勇人 2023 「『アクティブ・サイバー・ディフェンス』事始め—攻撃者プロファイリングの意義について」 JSAC2023, https://jsac.jp/cert.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki.jp.pdf.
- 瀬戸 崇志、2023 「パブリック・アトリビューションの“拡散”と“多様化” —政策当局間の「多様化」の国際比較研究—」 『安全保障戦略研究』 第3号2巻。

