

国家のサイバー攻撃と パブリック・アトリビューション

2021年9月14日 研究会報告
防衛省防衛研究所グローバル安全保障研究室
瀬戸 崇志

※本発表の内容は個人の見解であり、所属組織または防衛省を代表するものではありません。
スライド・図表等の無断利用はご遠慮ください。

本日の報告の構成・目的・導入

本日の報告の構成（約20分）[]内は拙稿での対応箇所目安

- 1 パブリック・アトリビューション（PA）研究の「射程/視角」[第1節-2節]
- 2 「政策対応」としてのPA－ 主要な「機能」をめぐる議論と論点 [第3節]
- 3 PA研究からみたSolarWinds事案対応－ PAの政治性の縮図？ [第4節]
- 4 むすびにかえて—今後の研究上の論点・課題[むすび＋ 第1節-2節＋脚注等]

導入と報告全体を通じた問いかけ

Q1 PA研究の対象=アトリビューションの「**古典的論点**」？：**なぜ**この数年、新名称で改めて**着目**？

Q2 国際政治学・安全保障研究基盤のPA研究が（目下）**何を議論している（ない）か**？

[導入]「パブリック」アトリビューションへの言及の増加とその含意？

- PA：特に国家のサイバー活動(cyber operations)の**アトリビューションの結果（判断）の「公表」と「非公表」**。これによる敵対者・関係者との「**コミュニケーション**」をめぐる「**政策対応**」+ アトリビューションの「**政治的側面**」や「**政策過程**」の問題に着目する概念。
- アトリビューションの**一部**かつ**古典的論点**[Rid Buchanan2015][Guitton 2017]？



学術研究－最広義：アトリビューションの（結果の）「公表(publicize)」サイバー空間における悪意ある活動の使用機材、特定の攻撃の実行者、そして最終的な責任を有する敵対者(国) (responsible adversary) の情報を公表**する行為 [Egloff & Smeets 2021] (定義の源流は[Lin 2016])**



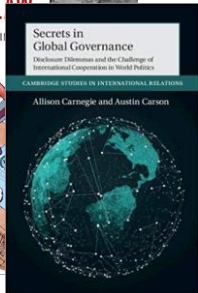
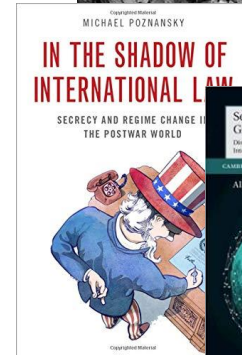
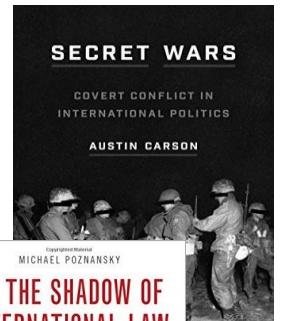
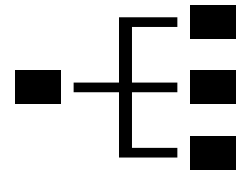
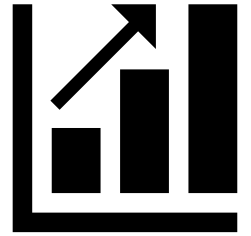
日本政府『サイバー空間における脅威の概況2021』（2021年4月）
攻撃実行者と背後にいる国家機関を**特定**した上で、**公開の場**（起訴や制裁を含む）で当該国を名指して**非難**する（中略）取組。



豪州政府『サイバー・重要技術国際関与戦略』（2021年4月）

（悪意あるサイバー活動への）対処は法執行、経済、外交又は適切な場合には軍事的手段も行使。対処は豪州の国益に資する場合のみ実施し、**非公開で行われる場合もある(will not always be public)**(p.41)。（対処は抑止の一部であり）対処の目的は**責任ある国家の行動(responsible state behavior)**の促進による、平和・安定的な国際環境の護持(p.41)。**国家に対するパブリック・アトリビューションは、豪州の対処手段(toolkit of responses)**の一つ (p.42)。

- ① パブリック・アトリビューション（PA）研究の「視角/射程」 [第1節-2節]
- ② 「政策対応」としてのPA－ 主要な「機能」をめぐる議論と論点 [第3節]
- ③ PA研究からみたSolarWinds事案対応－ PAの政治性の縮図？ [第4節]
- ④ むすびにかえて－今後の研究上の論点・課題[むすび＋ 第1節-2節＋脚注など]



1. 観測可能なアトリビューションの公表の事例数の増加

1. 各種データセット・実証研究の過程で観測される純増の傾向。

- ・米外交問題評議会データベースの登録数等。特に2016年頃の増加傾向指摘の研究多数。

2. 政策対応の活発化：国家によるアトリビューションの米国以外への拡散

- ・17年末以降のアトリビューション連合(attribution coalition)方式
- ・米国・英国と一体化しない単独/並行対応の事例 (独・仏・日など)

2. 事例間や同一事例内での公表/非公表をめぐる主体毎の対応の差への関心

1. 国際的な大規模サイバー事案での“被害国”間での対応の差 (例：EU加盟国内の対応差)
2. 企業/報道/在野専門家のPAを政府が公認(追認)しない例 (例：SingHealth事案)

3. 「国際関係における秘匿性」論との合流・相互発展

1. 「国際関係における秘匿性(secrecy in international relations)」論 (以下SIIR) [Carnegie 2021]

- 2016年頃から米英を軸に発展する国際関係論 (IR)・安全保障研究・インテリジェンス研究/諜報史の学際研究領域。冷戦期の他国への非公然(covert)な軍事介入、大量破壊兵器不拡散、国際機関加盟国の情報共有まで、多様な実証・理論研究を蓄積。特に次の共通の問い/視座を共有。
 1. なぜ国家は、公然性/透明性が重要とされる政策領域で自身の行動や保有情報を秘匿するか。
 2. なぜ国家は、他国の非公然な政策の事実を把握しつつ、それを暴露して対応を取らないか。
 3. なぜ〃他国・報道機関等の暴露後も、自国の行為を「公認しない(unacknowledge)」か？

2. 近年のアトリビューション研究：上記領域の実証研究の成果(理論) (特に2-3)を受容して発展

[Carson 2018] [Poznansky & Prekoski 2018] [Giles & Haltman 2019] [Baram & Sommer 2019] [Egloff 2020]など

アトリビューション問題の2つの定型句 (cliché)

1. 誰がやったのか (Who did it?)
2. 困難だが、不可能ではない (Difficult, but not impossible)

「本歌取り」をしたうえでのPA(研究)の問題意識

1'. 誰がやったのかを知ったとき、何をなすか？

What do you do when you know who did it ? [Egloff 2020]

2'. 困難だが不可能ではない。しかし（仮に可能でも）国家は結果を公表（認）すべきか。

("). However, ***should states make it publicized/acknowledged*** (even if it's possible) ?

& YES(NO)ならば、「なぜ[why]」「どのように[how]」 (非)公表（認）に至るか。

小括：今般のPA研究の視角（議論の前提）と研究関心

(1) 「公表(認)しない」誘引(※)が強いなか、国家をPAに踏み切らせる動機は何か？

(※情報源喪失リスク+対応の裁量低下 / 民間によるPAや非公然(covert)な反撃等の選択肢など)

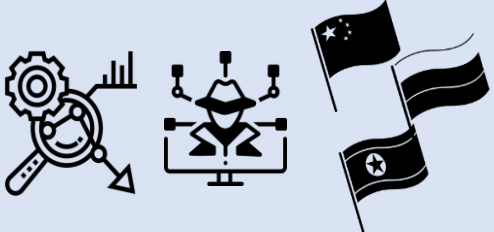


- 国家の「政策手段」 (PA as a 'means') [Egloff & Smeets 2021]たる固有(独自)の機能に関心。

(2) PAのあり方を左右する前後の政策過程（の論点）に対する関心

- 実施形式、証拠水準/法理、非国家主体との協調/競合関係、非難/証拠の政治化問題 など。

小括：PA研究の「射程/視角」（理念型としてのPAプロセスからの整理）

- 近年のPA研究：アトリビューションの過程の一部の細分化と解像度の増加の試み。
- 視座・関心として、(1) **A ≠ (B) ≠ C (≠ D)** (2) **B・Cのそれ自体の機能** (3) **C(B) → Aへの影響** など

	A. 特定 (attribution)	B. 暴露/開示 (exposure/revelation)	C. 非難 (accusation)
概要	 <ul style="list-style-type: none"> ● 使用機材、実行者、責任を負う敵対国の特定作業。 ● 技術的痕跡から地政学的文脈まで含む包括的な証拠収集と分析の過程。アトリビューションの根幹。 ● 伝統的に、情報・結果の「(非)公表」と「コミュニケーション」の論点も内包 ([Rid & Buchanan 2015] [Guiron 2017] など) 	 <ul style="list-style-type: none"> ● セキュリティ対策などの資として、各事案でのAの過程/過去に収集済の攻撃の痕跡 (IoC) や攻撃手法 (TTPs) の情報等を第三者に公表し共有する行為。 ● 国家を名指しで非難する対応(C)を伴わない実行も一部存在。 ([Baram & Sommer 2019] など) 	 <ul style="list-style-type: none"> ● 攻撃の実行者や責任国を名指しのうえ公式に非難する行為。いわゆる「名指しによる非難 (name and shame)」。 ● 後続対応 (D) と一体化する場合もあるが、非難に留まる場合も多数。 ● 非難の規範設定効果は必ずしも厳密な「特定」を必要とせず。 ([Finnemore & Hollis 2020] など)

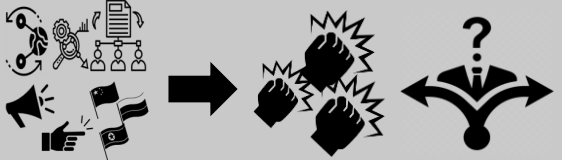
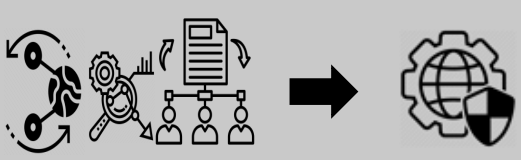
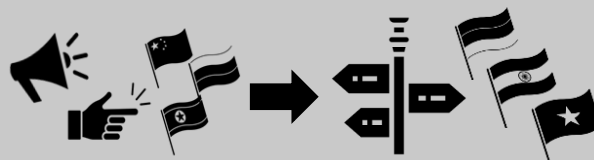
D. 後続対応 (復仇・對抗措置・自衛権行使等)

(出典) [瀬戸2021] 文末注14内の各先行研究ならびに[Egloff & Cavelti 2021]などを参照のうえで筆者作成。

- ① パブリック・アトリビューション（PA）研究の「視角/射程」 [第1節-2節]
- ② 「政策対応」としてのPA – 主要な「機能」をめぐる議論と論点 [第3節]
- ③ PA研究からみたSolarWinds事案対応 – PAの政治性の縮図？ [第4節]
- ④ むすびにかえて—今後の研究上の論点・課題[むすび+ 第1節-2節+脚注等]

「政策対応」としてのPAの「機能」を巡る論点

特に次の3つの機能は**主要先行研究**や**各国当局の議論**では指摘(ただし、データの制約上**効果は未実証**)。

	1. 抑止 (deterrence)	2. 対処(defense/counter-threats)	3. 規範設定(norm-setting)
機序を支える PAの要素	 <ol style="list-style-type: none"> 暴露/開示 (≡2.の対処の機序) 非難 (懷疑論強) 	 <p>暴露/開示 (IoC/TPPs等の公表-流通)</p> <ul style="list-style-type: none"> 情報を基にした各組織の侵入検知・セキュリティ対策向上が暗黙の前提。 (米英両国はこの作用をPAに期待する節)。 	 <p>非難</p> <ul style="list-style-type: none"> 国家の特定の活動を名指しで非難し、(国際法上)違法、(違法では無くとも) 許容し得ないとの言明。
主な 作用の機序	<ol style="list-style-type: none"> 相手への(累積的)コスト強要 ↓ 意図(intention)に作用 ↓ 対象の将来の行動変容 将来の攻撃停止/ 烈度-頻度の低減 	<ol style="list-style-type: none"> IoC/TPPs等の公表-流通 ↓ 能力(capability)の無力化(※) <ul style="list-style-type: none"> 抑止の成否/相手の行動変容は前提とせず。 能力の無力化/拒否能力向上が、累積的な相手のコストとみる場合、抑止と一体化。 ↓ 進行中の攻撃の阻害/被害軽減 	<ol style="list-style-type: none"> 非難による規範明示 ↓ 受容と内面化(選好を形成) ↓ 対象の将来の行動変容 <ul style="list-style-type: none"> PA=Shape (将来環境の安定化) : 攻撃的サイバー能力拡散を念頭に、各国の将来のドクトリン・運用政策を誘導。
主な対象 (国家念頭)	直接の攻撃国 / 現在の競争国	直接の攻撃国 (現在の競争国)	同盟/同志国・将来の潜在競争国
論点	<p>コストの源泉は何か？</p> <ul style="list-style-type: none"> PAは「それ自体」がコストか。 <ul style="list-style-type: none"> ・ [YES] 「非難」か「暴露/開示」か。 ・ [No] PA単体は抑止の信頼性低下？ 「名指し(name)」が戦略目的に資す国/局面において、非難はコストとは認識されない可能性 	<p>情報の公表・流通は対処に資するか？</p> <ul style="list-style-type: none"> 既存の公開情報の部分的切り貼りを超え、かつ時宜を得たものか？ 	<p>規範の成立は各国の目標か？</p> <ul style="list-style-type: none"> 米英など現状の能力面の優位を持つ国家は、規範が未成熟・曖昧なことの優位性を享受。「安保政策上の許容する範囲」でのみ、規範設定に関与。 ∴ 政府としての公式の非難の「回避」を志向する事例存在？

3種類の「機能」のイメージ：全体概観

攻撃的サイバー能力の水準

②パブリック・アトリビューション(PA)

緑：暴露/開示
による対処機能

公表(認)

非公表(認)

※② PAを伴わない非公然(covert)な反撃でのコスト強要/シグナルも一部の国で選択肢に存在。
[Aldrich & Cormac 2018][Carson & Yarhi-Milo2017][Carson 2017] [Warner 2019]など

①特定

③悪意ある
サイバー活動

PA 自体or後続措置によるコスト強要
(コストの源泉は相手の認知依存・未知数)

行動変容
(抑止成立)

[攻撃の停止or
烈度・頻度の低減]

費用対効果
に基づく
意思決定

現状維持
(攻撃持続)

橙：抑止機能

(論点：コストの源泉は?)

青：非難による
規範設定機能

“Shape”(Shaping) (※欧米各国軍のドクトリン上の用語法)

- 軍事力で同盟国・友好国などの能力や価値観に働きかけ、将来の紛争発生を予防する作用 (cf. 防衛外交・防衛関与) [Wolfley2021]
- 現在or将来の技術拡散で「保有」に至る攻撃的サイバー「能力」を、規範に則った「運用」(例：標的限定や特定目的利用の禁止)に留めるよう、規範を内面化させ誘導[Egloff 2020][Nye 2017]など。

運用政策の無分別性 (国際法/責任ある国家の行動規範との適合度)

- ① パブリック・アトリビューション（PA）研究の「視角/射程」 [第1節-2節]
- ② 「政策対応」としてのPA－ 主要な「機能」をめぐる議論と論点 [第3節]
- ③ PA研究からみたSolarWinds事案対応－ PAの政治性の縮図？ [第4節]
- ④ むすびにかえて－今後の研究上の論点・課題[むすび＋ 第1節-2節＋脚注等]

1. アトリビューション連合方式としての継続性

- 発覚→PA(非難)までの期間は2020年12月の発覚から約5か月(前例比でも平均的期間)。
- 露政府/対外諜報庁 (SVR) の犯行を根拠付ける決定的証拠の開示は必ずしも無し (?)。
 - ・ 政治的な判断公表 + SVR系統の脅威アクターが用いるとされるTTPs等の公表のみ。
 - ・ 多国間声明・相互支持で、主張/説得の信頼性担保を試みる従来慣行を踏襲。

2. 論点1：規範設定機能を仮定した際の米英の対応の含意

- 米国や英国は、自らを拘束する**規範の充実に必ずしも安全保障上の利益を有さない**国々。
 - ・ 自国の軍・諜報機関が展開しうる活動を規範で雁字搦めにする意図は有さず。
 - ・ 先行研究：かかる事例でPAでの公式非難を回避する仮説[Egloff 2020] [Eichensehr 2020]
- **SolarWinds事案**：専門家の分析では「米英も」手を染めてきたサイバー諜報
∴ 仮に（一般的に）**規範設定機能が伴う（と認識・行動する）**ならPAを「回避」したいはずの事例
⇔にもかかわらずPA(+米国は制裁)敢行 → PAに規範設定機能を見出してないのか？（事例研究の“Most Likely Case”）
- **代替仮説**：PAの規範設定は念頭に置いたうえでの「**スタンス**」の変更
 - ・ サイバー諜報規範問題([Libicki 2017]等)：規模 + 目的の識別困難性：諜報活動を相互に許容する不文律は非合理？
 - ・ “一定の”サイバー諜報を規律する「例外」？：バイデン政権高官の言説とは（表面上は）整合的。
- 結論：**代替仮説は支持不可** ⇔ **規範設定機能一般は謎**(∵ 英国の顕著な規範への言及欠如 + 米の対応の曖昧さの解釈如何)

3. 論点2：「早期の政治的決め打ち」と「競合的な言説環境」が導く「歪み」？

- 「政権移行期」の特殊性 = 報道の過熱と党派性 → バイデン次期大統領は**20年12月時点で制裁等の強硬措置**を表明。
 - ・ (仮に) **背反する客観証拠やPA回避の動機が見つかったとして**、政治指導者のPA回避はあり得たか？
- 露の「悪意あるサイバー活動」の「捉え方」と「語られ方」
 - ・ **技術的洗練性・深刻度**に基づく報道や議論と、**安保当局の事態認識論(国際法 + 均衡性判断)**に乖離？
 - ・ 両者が深刻に乖離したとき、**均衡性ある政策対応と世論とのクライシス・コミュニケーションを両立できるか？**

- ① パブリック・アトリビューション（PA）研究の「視角/射程」 [第1節-2節]
- ② 「政策対応」としてのPA－ 主要な「機能」をめぐる議論と論点 [第3節]
- ③ PA研究からみたSolarWinds事案対応－ PAの政治性の縮図？ [第4節]
- ④ むすびにかえて—今後の研究上の論点・課題[むすび＋ 第1節-2節＋脚注等]

1. 「政策過程」としてのPA研究の視座と関心

- 「即時性」「客観性」「透明性」などの技術的/法的アトリビューションの理念を「**歪める**」政治力学
(例) 証拠水準の精緻化：法廷外のPAを困難とする：米英蘭など「PA積極国」が「消極的」[Eichensehr 2020]。
- 「国家間競争」という時代精神の落し子：サイバー空間のガバナンスへの含意は今後の研究上の課題

2. 「政策対応」としてのPA（研究）の課題

- (可否とは別に) 効果は未実証/未知数：「**過大評価**」すべからず。「**やらないこと**」も重要な選択肢。
- 「**米英筆頭に各国が4年間継続**」は「事実」：「**過小評価**」もできず (意図の把握と期待管理は別論点)。
- 積極国が本質的に求める協力は何か (&それは我々のイメージする「アトリビューション」と同じなのか?)

A. 特定 (attribution)



A ≠ (B) ≠ C (≠ D) (PA研究の視角)

- 事実に根差した特定の判断と証拠 (根拠) は、一定の政治的・戦略的動機のもとで公表(認)されず (公表/公認が好ましいとも限らず)。

Cを前提としたAへの波及問題

- A (特定) に至る過程での (分析自体の) 「政治化」

B. 暴露/開示 (exposure/revelation)



B-Cの関係/国家と非国家の機能差

- 「**国家**」への「**名指し**」は、対処機能の向上に資する意義を何か持つのか？
- 国家(政府)による情報発出行為に**特別の比較優位(劣位)・固有性**はあるのか？
- この対応は、民間企業やCSIRTとどこまで**一体化・分離**するのが好ましいのか

C. 非難 (accusation)



A(B)の伴わないCの扱いの問題

- 現状は**必ずしも厳密なA(特定)を必要とせず**に可能。
- パブリック・アトリビューション ≠ **外交的非難**
⇔ 証拠基準・法理が未成熟。
客観的・技術的証拠が開示されないなか、両者を実証的に区分が可能？

- Broeders, Dennis, Els De Busser, and Patryk Pawlak. "Three Tales of Attribution in Cyberspace." 2020 Policy Brief. Hague: The Hague Program for Cyber Norms / Leiden University., April 2020.
- Cormac, Rory, and Richard J. Aldrich. "Grey Is the New Black: Covert Action and Implausible Deniability." *International Affairs* 94, no. 3 (May 1, 2018): 477–94. <https://doi.org/10.1093/ia/iyy067>.
- Carnegie, Allison. "Secrecy in International Relations and Foreign Policy." *Annual Review of Political Science* 24, no. 1 (2021): 213–33. <https://doi.org/10.1146/annurev-polisci-041719-102430>.
- Carnegie, Allison, and Austin Carson. *Secrets in Global Governance: Disclosure Dilemmas and the Challenge of International Cooperation*. *Secrets in Global Governance*. 1st ed. Cambridge: Cambridge University Press, 2020. <https://doi.org/10.1017/9781108778114>.
- Carson, Austin. *Secret Wars: Covert Conflict in International Politics*. *Secret Wars*. 1st ed. Princeton; Oxford: Princeton University Press, 2018. <https://doi.org/10.2307/j.ctv346p45>.
- Carson, Austin. "Obama Used Covert Retaliation in Response to Russian Election Meddling. Here's Why." *Washington Post*. June 29, 2017, Online Edition edition. <https://www.washingtonpost.com/news/monkey-cage/wp/2017/06/29/obama-used-covert-retaliation-in-response-to-russian-election-meddling-heres-why/>.
- Eichensehr, Kristen. "The Law & Politics of Cyberattack Attribution." *UCLA Law Review* 67, no. 3 (July 2020): 520–99.
- Egloff, Florian J., and Max Smeets. "Publicly Attributing Cyber Attacks: A Framework." *Journal of Strategic Studies* 0, no. 0 (March 2021): 1–32. <https://doi.org/10.1080/01402390.2021.1895117>.
- Egloff, Florian J. "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* 6, no. 1 (September 14, 2020): 1–12. <https://doi.org/10.1093/cybsec/tyaa012>.
- Finnemore, Martha, and Duncan B Hollis. "Beyond Naming and Shaming: Accusations and International Law in Cybersecurity." *European Journal of International Law* 31, no. 3 (December 15, 2020): 969–1003. <https://doi.org/10.1093/ejil/chaa056>.
- Guittou, Clement. *Inside the Enemy's Computer: Identifying Cyber Attackers*. London: Hurst Publishers, 2017. <https://doi.org/10.1093/oso/9780190699994.001.0001>.
- Giles, Keir, and Kim Hartmann. "'Silent Battle' Goes Loud: Entering a New Era of State-Avowed Cyber Conflict." In *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–13. Tallinn, Estonia: IEEE, 2019. <https://doi.org/10.23919/CYCON.2019.8756713>.
- Poznansky, Michael, and Evan Perkoski. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3, no. 4 (October 2018): 402–16. <https://doi.org/10.1093/jogss/ogy022>.
- Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (January 1, 2017): 44–71. https://doi.org/10.1162/ISEC_a_00266.
- Warner, Michael. "A Matter of Trust: Covert Action Reconsidered." *Studies in Intelligence* 63, no. 4 (December 2019): 33–41.
- Soesanto, Stefan, and Max Smeets. "Cyber Deterrence: The Past, Present, and Future." In *NL ARMS (Netherlands Annual Review of Military Studies) 2020*, edited by Frans Osinga and Tim Sweijts, 385–400. NL ARMS. The Hague: T.M.C. Asser Press, 2021. https://doi.org/10.1007/978-94-6265-419-8_20.
- Romanosky, Sasha and Benjamin Boudreaux, "Private-Sector Attribution of Cyber Incidents: Benefits and Risks to the U.S. Government," *International Journal of Intelligence and Counterintelligence*, Vol 34, No. 3, pp. 463-49
- Wolfley, Kyle J. *Military Statecraft and the Rise of Shaping in World Politics*. Lanham, Maryland: Rowman & Littlefield Publishers, 2021.
- Libicki, Martin. "The Coming of Cyber Espionage Norms." In *2017 9th International Conference on Cyber Conflict (CyCon)*, 1–17. Tallinn: IEEE, 2017. <https://doi.org/10.23919/CYCON.2017.8240325>.

ご清聴ありがとうございました。