情報資本主義と G7

小倉利丸
toshi@jca.apc.org

2023/4/1

G7 広島サミットの「含意」

「米国や、G7 等の国際的な枠組みが、国際社会におけるリスクを管理し、自由で開かれた国際秩序を維持・発展させることは、ますます難しくなってきている」（国家安全保障戦略文書）

- 岸田政権の思惑：核廃絶のシンボルとしての広島と核廃絶の意思をもたない保有国
- 核兵器と核の商業利用の正当化
- ロシア・ウクライナ戦争への関与
    - 外交・軍事安全保障
    - ハイブリッド戦争
    - 司法警察と軍との一体化
- 環境（気候変動と原発）
- ジェンダー

G7 広島サミットの「含意」

G7 は戦争放棄とは相容れない

- 広島サミットの主要議題のひとつは、ウクライナへのロシア侵略戦争
- 2022 年に何度か開催された G7 の首脳会談の常套句

「我々は、ウクライナの軍事及び防衛装備に関する緊急の要求を満たすための取組を引き続き調整する」

- 日本には 9 条による制約があるはずだが、 G7 加盟国として日本が「戦争放棄」を主張したことはない。
- 他のサミット諸国と同様「軍事及び防衛装備に関する緊急の要求」に応じることを約束
- 防衛 3 文書により G7/NATO との足並みが揃う。日本は、議長国として、戦争に加担する。

G7 とサイバー / デジタル

2022 年ドイツ・エルマウの首脳宣言

「サイバー・セキュリティ、不正資金及び法執行の分野において、**ロシア及び他の権威主義体制によってもたらされるものを含む**、国境を越えた脅威に照らして、我々の**国内治安を更に強化**することにコミットする。我々の市民の安全を更に確保するため、我々は、**市民社会**並びに**インターポール及び国連薬物・犯罪事務所**といった国際的主体と緊密に協力し、特に脆弱な状況において、**サイバー犯罪**及び環境犯罪を含む国際組織犯罪に対する我々の闘いを強化する。」

G7 とサイバー / デジタル

2022 年ドイツ・エルマウの首脳宣言

- ロシアを明示することによって、軍事安全保障と司法・警察の領域が事実上融合
- 行為主体として、各国政府、国連、そして市民社会組織 (いわゆる NGO) を取り込む
- 国際と国内の取り組みの融合
- サイバー領域と実空間の融合

2023 広島サミットでもこの認識が継承されるだろう。

G7 とサイバー / デジタル

2022 年ドイツ・エルマウの首脳宣言（続）

ロシアのウクライナに対する侵略は、我々の重要なインフラに対するものを含め、広範な脅威をもたらしている。したがって、我々は、各国国内及び国境を越えて、**デジタルインフラのサイバー・レジリエンス**を高めるための措置をとっている。我々は、これに関して、「ウクライナに対するロシアの戦争への対応におけるデジタルインフラのサイバー・レジリエンスに関する共同宣言」を支持する。

G7 とサイバー / デジタル

2022 年ドイツ・エルマウの首脳宣言（続）

サイバー・レジリエンス

- 情報通信インフラへの攻撃に防御体制を確立してネットワークの維持が可能な能力をもつこと。
- 「敵」からのサイバー攻撃を想定し、これを阻止するために、政府はネットワークへの**常時監視を強化することになる。このことが私たちの言論表現の自由への監視や規制**につながる。

一般に国家が強固な安全保障を確立しようとすればするほど、国家権力への異議申し立てを抑制する力が強くなり、民衆の異議申し立てを含む自由の権利が阻害される。

戦争とサイバー / デジタル

2022 年エルマウサミット 「強じんな民主主義声明」

https://www.mofa.go.jp/mofaj/files/100364065.pdf

- ハイブリッドな脅威、特に**偽情報を含む情報操作及び干渉**に対抗する。
- 情報操作に対抗し、正確な情報を促進し、**我々の共通の価値を世界に提唱する**ために協力する。
- マルチステークホルダー・アプローチを通じたものや、デジタル・スキル及びデジタル・リテラシーを強化することによるものを含め、オンライン及びオフラインでの信頼・信用できる多様な情報源及びデータ源への入手可能な価格でのアクセスを促進する。
- クライストチャーチ・コール宣言に沿って、**オンライン上の暴力的、過激主義的及び扇動的なコンテンツ**と闘うためのオンライン・プラットフォームの行動に関する透明性を強化する。

戦争とサイバー / デジタル

2022 年エルマウサミット 「強じんな民主主義声明」

https://www.mofa.go.jp/mofaj/files/100364065.pdf

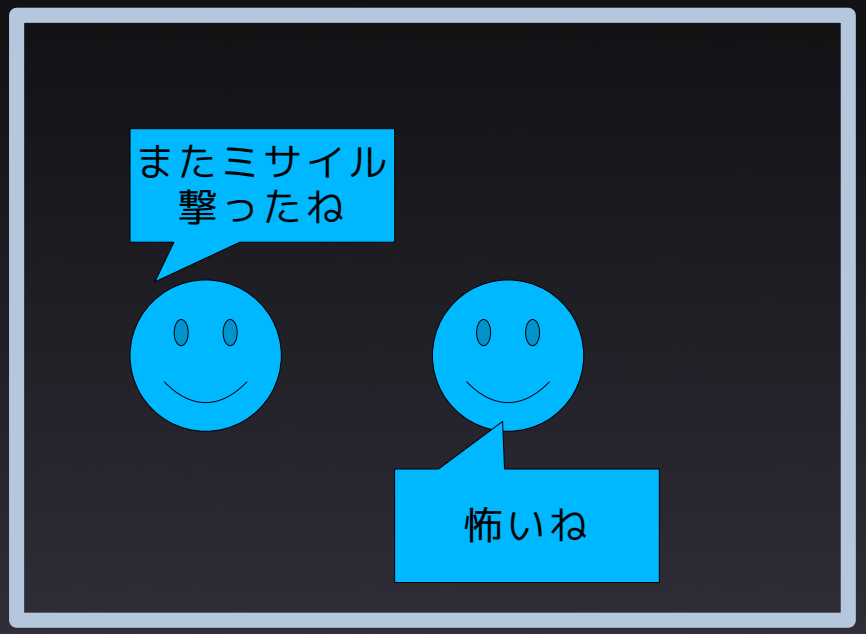
- 「我々の共通の価値を世界に提唱する」とは、G7 の側もまた、「敵」からみれば偽情報にあたるような情報発信を展開する、ということを提起。
- G7 と価値を共有しない国内の人々もまた敵扱いにされる。
- 「デジタル・スキル及びデジタル・リテラシーを強化」国策に沿った情報発信の技術や「リテラシー」の体制を整える。
- これらに、民間や NGO なども巻き込む。

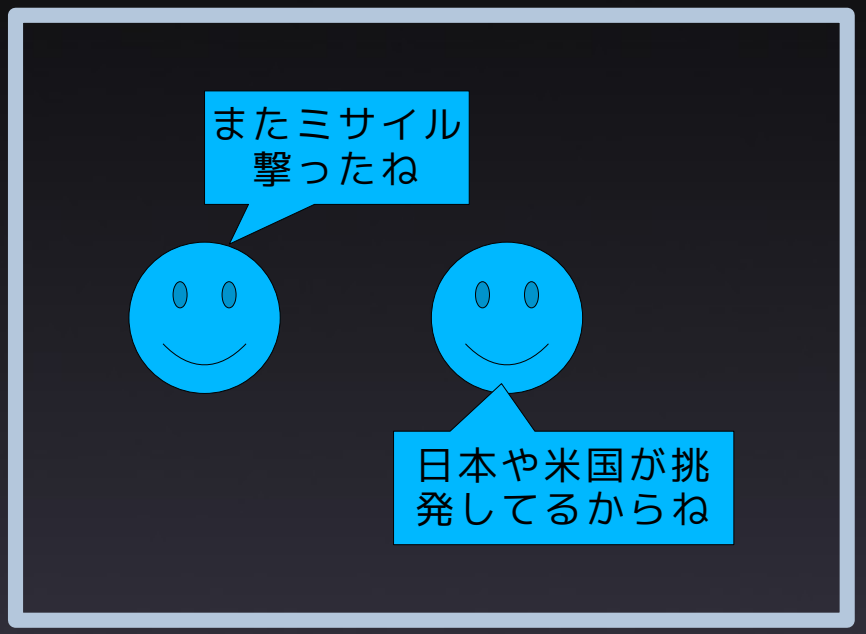
戦争とサイバー／デジタル

2022年国家安全保障戦略

「相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は 急速に高まっている。サイバー攻撃による重要インフラの機能停止や 破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、**武力攻撃の前から偽情報の拡散等を通じた情報戦が展開される**など、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせる**ハイブリッド戦**が、今後更に洗練された形で実施される可能性が高い。」

戦争とサイバー / デジタル





SNS などでの拡散
を促す

SNS などでの拡散
を抑制する

世論の動向を誘導する
国内の反政府言論を監視対象に

戦争とサイバー／デジタル
（事例）ノルドストリーム爆破事件

- 9月26日 海面下80メートルにあるノルド・ストリームの爆発
- ウクライナ、27日にロシアによる「テロ攻撃」と非難
- 欧州連合（EU）、アメリカ、北大西洋条約機構（NATO）は、同パイプラインが故意に損傷されたと示唆しつつ、ロシアを直接非難せず。
- ロシアはアメリカが関わっている可能性を指摘

欧米主要メディアは以後沈黙

戦争とサイバー／デジタル
（事例）ノルドストリーム爆破事件

バイデン政権がドイツの同意も知識もなく、ガスパイプラインのノルドストリーム２を意図的に爆破したと主張する詳細なレポートを、米国の著名なジャーナリスト、シーモア・ハーシュが発表。 https://seymourhersh.substack.com/p/how-america-took-out-the-nord-stream

日本語訳

https://iwj.co.jp/wj/open/archives/514010

［メディアの］関心の低さは、この報告書が不適切であったからということでは説明できない。もしバイデン政権が本当にノルウェー政府と密接に協力してノルドストリーム２を爆破し、何十億ドルもの損害を直接与え、世界の全地域を十分なエネルギーのない凍える冬に突入させたとしたら、それは史上最悪のテロ攻撃の１つに数えられるもので、同盟国とされている国に対する明白な侵略行為である。

したがって、もしバイデンが本当にこの攻撃を命じたのなら、これほど重大なニュースはないだろう。実際、ハーシュによれば、バイデン、ビクトリア・ヌーランド国務次官、アントニー・ブリンケン国務長官からジェイク・サリバン国家安全保障顧問まで、関係者全員が自分たちのしていることが ＂戦争行為 ＂であることを理解していたというのである。

戦争とサイバー / デジタル

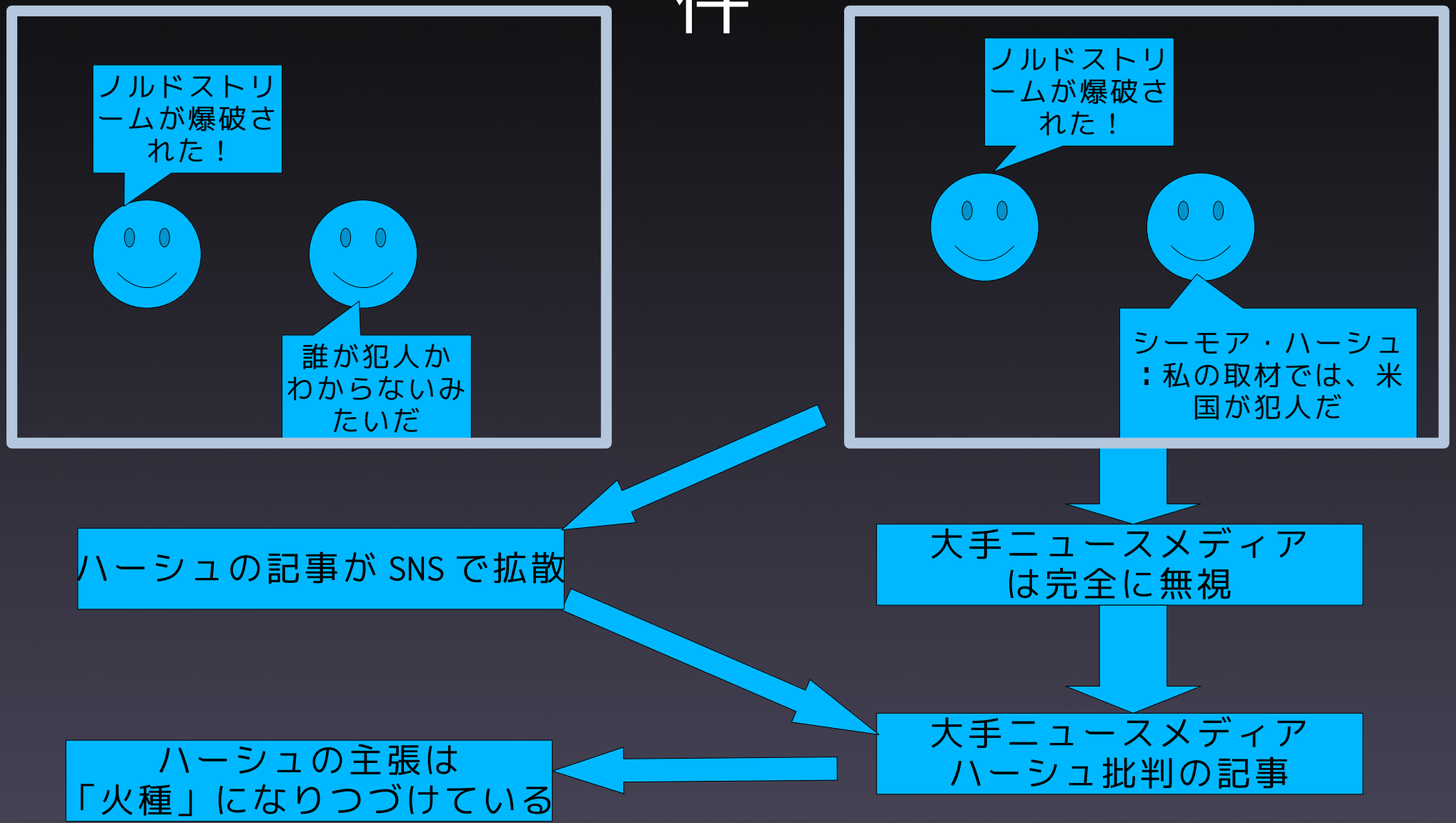
ノルドストリーム事件は世論操作の転換点

ネットを使った世論の誘導方法

- 検索順位の上位に政府、大手マスメディア報道が来るように「アルゴリズム」の設計がなされている。
- SNS で拡散しやすくしたり拡散しにくくするなどの操作をプラットフォーマーが行なう。
- 「偽情報サイト」や「偽情報発信アカウント」を規制する

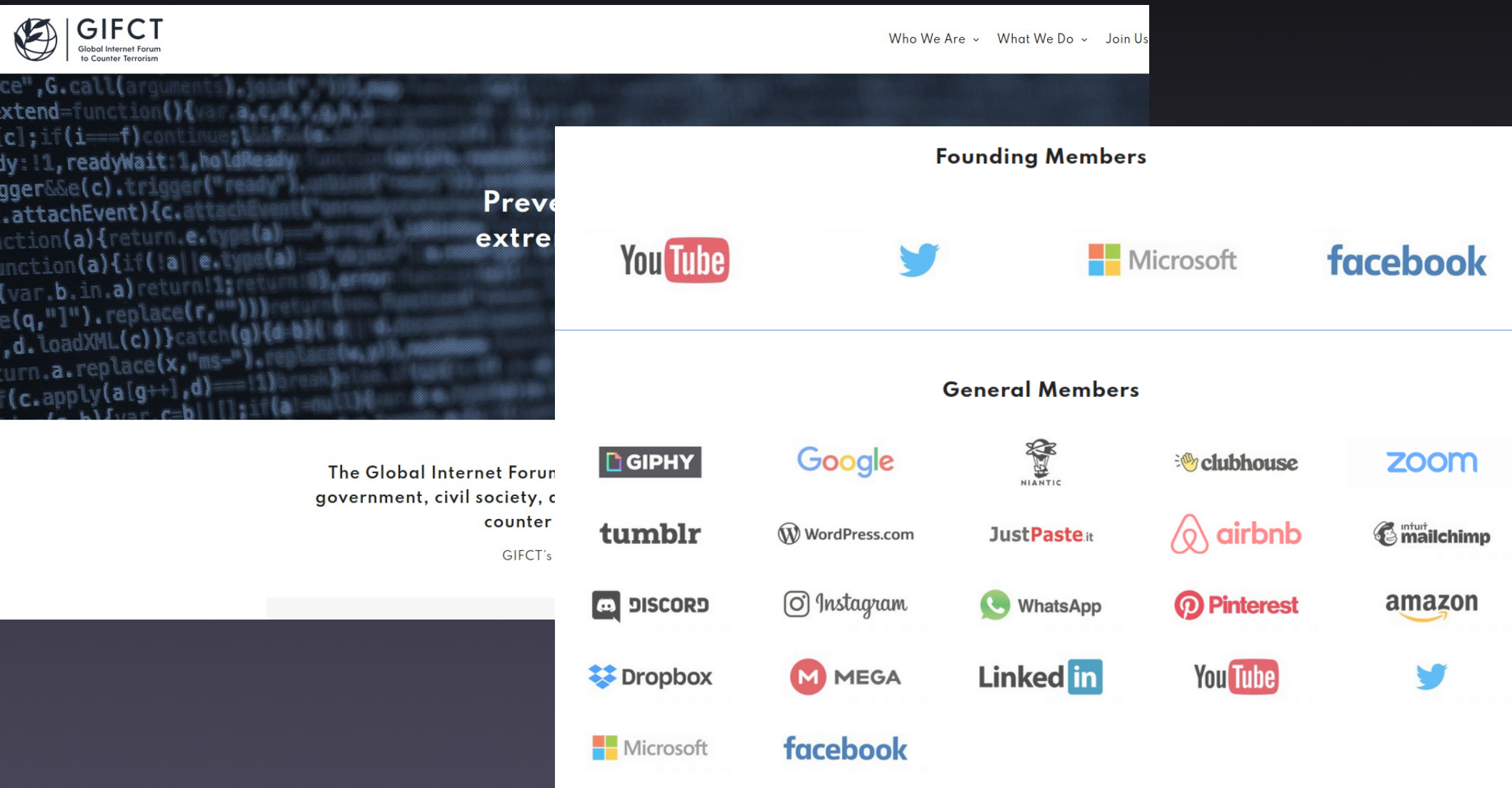
情報流通にプラットフォーマーや政府が介入はしても、私たちには実感できないので、警戒心を持つことが非常に難しい。

（事例）ノルドストリーム爆破事件



「ハイブリッド戦」の構造

2017年 Global Internet Forum to Counter Terrorism：GIFCT設置



「ハイブリッド戦」の構造

GIFCT の関連団体

- The Global Network on Extremism and Technology（GNET） テロリストの技術利用の調査研究と対抗のための IT 産業界が資金を提供する研究プロジェクト。ロンドンの King's College の Department of War Studies が事務局を担う。

  https://gnet-research.org/

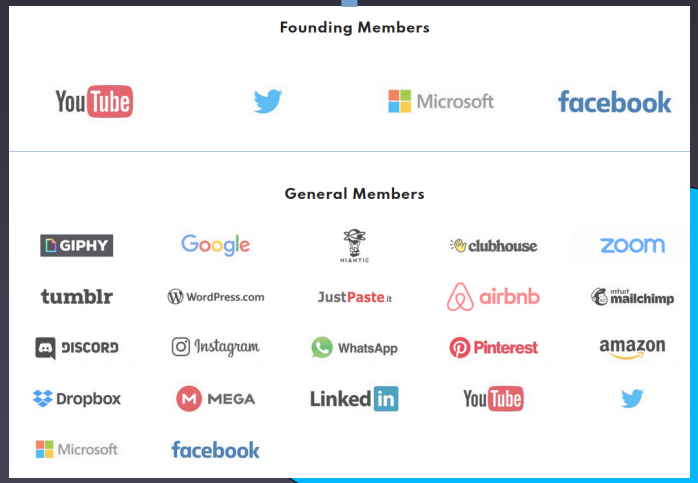
- Tech Against Terrorismは、国連テロ対策執行理事会（UN CTED）が支援するイニシアチブ。GIFCT を通じたハイテク産業と各国政府の両方が資金提供。 https://www.deepl.com/translator

「ハイブリッド戦」の構造

各国政府

関連情報の収集と分析
(GIFCT など)

取り締まり、情報操作、サイバー攻撃など



インターネット
ビッグデータ

ハイブリッド戦の構図

ハイブリッド戦の構図

従来の「反戦運動」の射程外にある問題として

- 私たちの日常生活の基盤をなす情報通信領域がそのまま戦争の道具になり、かつ戦場にもなる。
- 情報戦の核心にあるのは、憎悪と愛国心の扇動である。
- 私たちは、ハイブリッド戦において自国政府から「敵」とみなされる。(911 同時多発テロ以降、米国愛国者法が国内市民に対する監視を強化して以降、国内外の境界はあいまいになっている)

ハイブリッド戦の構図

従来の「反戦運動」の射程外にある問題として

システムの機能変容：教育、住民管理から経済、教育、文化まで

- 国境を越えた軍警一体化
- マイナンバー（カード）
- 防災関連の政策
- 原子力発電所やプルトニウムの保有
- 経済安全保障
- 家族政策
- 移民・難民政策

NGOや学会、人権団体などが政府のハイブリッド戦に加担

「正義の戦争」を支援するために、侵略者へのサイバー領域での攻撃に加担する。

ハイブリッド戦争に抗するには

Founding Members

YouTube　Microsoft　facebook

General Members

GIPHY　Google　NIANTIC　clubhouse　zoom

tumblr　WordPress.com　JustPaste.it　airbnb

DISCORD　Instagram　WhatsApp　Pinterest

Dropbox　MEGA　LinkedIn　YouTube

Microsoft　facebook

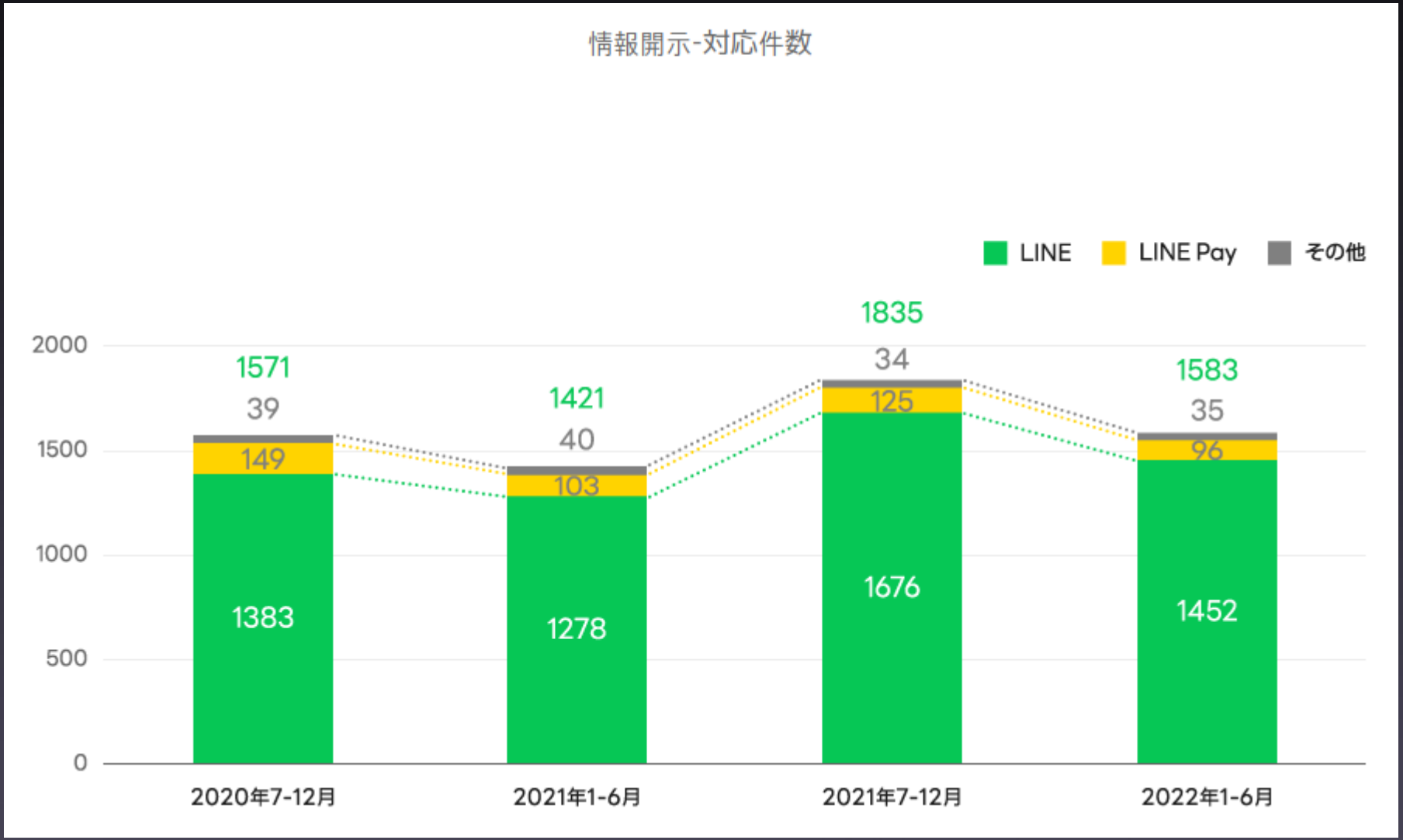
私たちの情報発信がすでに、 GIFCT のメンバー企業などに大きく依存している。

マイクロソフト社は安倍政権の働き方改革を全面的に支援した。平野拓也と安倍のツーショットが今でもウエッブに

https://news.microsoft.com/ja-jp/2017/06/08/170608-information/

ハイブリッド戦争に抗するには

Line1 社だけで年間 3000 件の情報を捜査機関に提供している



https://linecorp.com/ja/security/transparency/2022h1

能動的サイバー防御

「戦略」文書の記述

武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する。

そのために、サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備する

能動的サイバー防御

「戦略」文書の記述

「重大なサイバー攻撃のおそれがある場合、これを未然に排除」

相手の攻撃がなくても、先制攻撃を行なうことを明記

サイバー領域における先制攻撃は、どのような事態なのかがわかりにくい。

真珠湾攻撃のように通常兵器による先制攻撃はイメージしやすいが ...

能動的サイバー防御

サイバー領域における「能動的防御」（アクティブディフェンス）

- 攻撃元のサーバーに対してハックバックや破壊行為を仕掛けるなど
- 「防御」といっても行なわれることは、サイバー攻撃そのもの

https://cybersecurity-jp.com/security-measures/30860

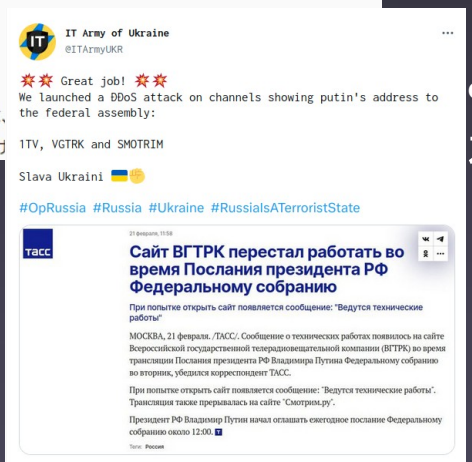
サイバー攻撃の手法は、不正アクセス禁止法、電子計算機使用詐欺罪、電子計算機損壊等業務妨害罪などに該当。

https://keiji-pro.com/columns/114/

サイバー領域での「能動的防御」は、自衛隊だけでなく、**一般の市民ボランティアを巻き込んで展開することが可能な領域**である。サイバー攻撃の武器はネットに接続されたパソコンやスマホ。攻撃のターゲットは、ネットに接続された「敵」のインフラなどになる。

能動的サイバー防御
ウクライナ IT 軍

ウクライナ IT 軍に日本からの参加実績がある



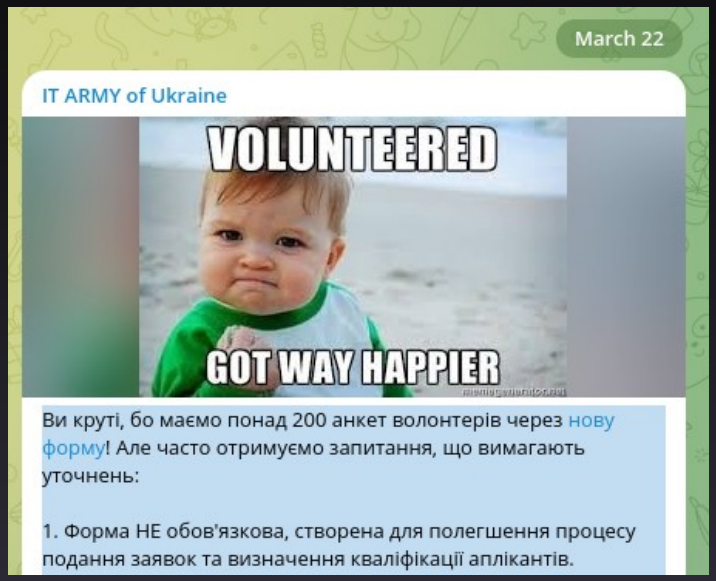
サイバー防御であれ攻撃であれ、これらは、私たちが日常使用しているパソコンなどを用いて「参加」が可能だ。
サイバー領域は、より簡単に私たちを戦争に巻き込むことができる。

https://www.nhk.jp/p/gendai/ts/R7Y6NGLJ6G/blog/bl/pkEldmVQ6R/bp/pM2ajWz5zZ/

- プーチン大統領が毎年行っている「国家代表演説」の際に、ロシアの国営メディアのウェブサイトをオフラインにする
- ロシアの銀行、食品配達サービス、動画共有サイトなど民間人を標的にした攻撃

能動的サイバー防御

ウクライナ IT 軍



ウクライナ IT 軍は現在も精力的にボランティアを世界中から募集している。ウクライナ IT 軍の Telegram チャンネルより。 3 月 22 日の告知

https://t.me/itarmyofukraine2022/1111

ボランティアとして、あなたはソフトウェア開発、サイバーセキュリティ、ペンテストの分野であなたのスキルや専門知識に貢献する機会を得ることができます。

この数週間で、すでに 200 人以上のボランティアの応募がありました！

このフォームには、個人的な質問は含まれていません。このフォームに記入する際は、あなた自身を特定できないようなメールアドレスを使用していることを確認してください。また、 Telegram のプライバシー設定も確認してください。

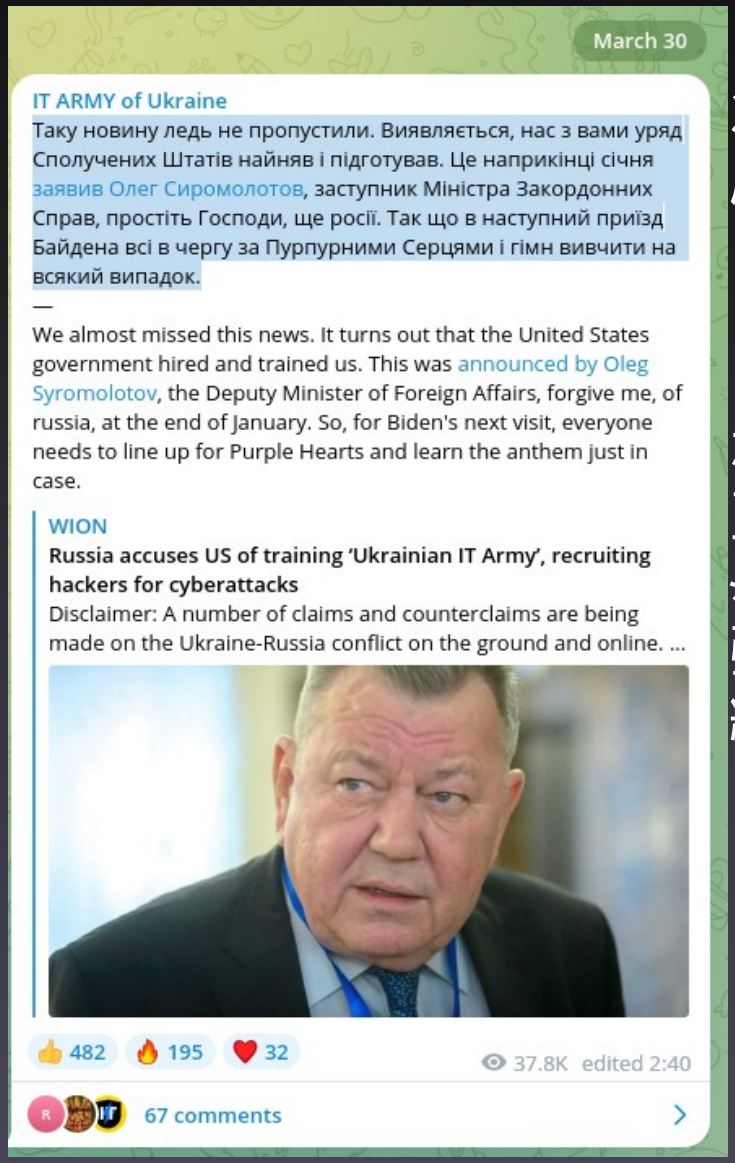
端末に複数の Google プロフィールがある場合、フォームではどのアカウントを使用するか尋ねられます。プロファイルが 1 つしかない場合は、自動的に入力されます。

このフォームはウクライナの IT 軍関係者のみが見ることができ、 Google アカウント情報は共有されません。ただし、情報は Google のサーバーに保存されるため、あなたを追跡できないアカウントを使用することをお勧めします。

「いつ連絡が来るのか」という質問について：応募をしたからといって、すぐに受理されるわけではありません。私たちは、興味のあるボランティアのリストを管理し、必要に応じて連絡を取ります。

https://docs.google.com/forms/d/e/1FAIpQLSfdSnn52XhhkFPc3dQ-QKpifYyJU0Td8n0h9oYPeFHg2CM-vw/viewform

能動的サイバー防御
ウクライナ IT 軍



ウクライナ IT 軍の Telegram チャンネル
3/30 日：米国が「ウクライナ IT 軍」を育成し、サイバー攻撃用のハッカーを募集、これをロシアが批判、という記事を紹介。

ウクライナ IT 軍は、正式の「軍」ではなく、ボランティアの位置づけだったが、これを正式の軍に編入するための法改正が審議中。
* ボランティア軍を正規軍に編入して統制強化する手法はアゾフ大隊のウクライナ軍編入の前例がある。

能動的サイバー防御
日本の NATO のサイバー防衛への参加

- 2018 年、安倍政権　NATO サイバー防衛協力センター (CCĐCOE) の Contributing Participant として参加 https://ccdcoe.org/news/2018/japan-to-join-the-nato-cooperative-cyber-defence-centre-of-excellence-in-tallinn/
- サイバー防衛演習「**ロックド・シールズ**」に、 2021 、 2022 年に参加
- 2022 年 11 月 CCĐCOE に正式加盟。

能動的サイバー防御
日本の NATO のサイバー防衛への参加

ロックシールズ演習：軍官民一体となって参加

防衛省から、内部部局、統合幕僚監部、陸上自衛隊システム通信団、海上自衛隊システム通信隊群、航空自衛隊作戦システム運用隊、航空自衛隊航空システム通信隊、自衛隊サイバー防衛隊。他府省から**内閣官房内閣サイバーセキュリティセンター（ NISC ）、総務省、警察庁、情報処理推進機構（ IPA ）、 JPCERT コーディネーションセンター（ JPCERT/CC ）、重要インフラ事業者**等が参加

演習の想定

- 攻撃により、政府や軍のネットワーク、通信、浄水システム、電力網の運用に深刻な混乱が生じ、最終的には国民の不安や抗議行動に発展
- 中央銀行の準備金管理および金融メッセージングシステムのシミュレーション（Mastercard Inc. や Banco Santander SA など大手金融機関 5 ～ 10 社が参加 ）
- 重要インフラの一部として 5G スタンドアローン移動通信プラットフォームが配備

ハイブリッド戦争に抗するには

- コンピュータ・テクノロジーが支配的な社会では、サイバー戦争はそれ自体が直ちに総力戦にならざるをえない
- 私たちの手元にあるコンピュータデバイスは、戦争状態では、武器にもなるから、武器と非武器の境界はあいまいになる。
- 私たちのネットでの情報発信は、いかに私的な通信であっても、ビッグデータとして解析されることによって、世論を操作し、敵に対する効果的なプロパガンダを展開するための重要なデータになる。
- 私たちの日常行動は二重の意味で、戦争とむすびつけられる。
    - 自国の政府にとっては、戦争動員に不可欠なデータ収集のターゲットとして
    - また、サイバー攻撃の「兵士」として
    - 敵にとっては、世論のターゲットとして、またサイバー攻撃のターゲットになる。

ハイブリッド戦争に抗するには

従来の反戦運動に加えて私たちには多くの取り組みが必要になる。

- サイバー戦争に巻き込まれず加担しない
  - 政府、マスメディアに対抗する情報発信
  - サイバー戦争に参戦しない、させないこと
  - 反監視技術の構築
- 反戦運動の弾圧に対抗すること
  - 弾圧に抵抗しうる民衆のサイバーセキュリティ構築
- 国際的な連帯の構築
  - 草の根の国際連帯。言語の壁を越える

ハイブリッド戦争に抗するには

危機感をもつことが大切

- 9条の枠組では「情報戦争」を阻止できない
- 兵器だけが戦争の「武器」ではない。
- 私たちの行動やコミュニケーションを戦争に利用させない意識的な取り組みが喫緊の課題。そのためにできることは沢山ある。

いかなる国家による戦争も私たちの戦争ではない。

サイバー戦争の放棄へ!!

昨年の G7 デジタル大臣会合の声明では

「我々は、戦場としてのデジタル領域の使用に対抗することを決意する」

として、「戦場としてのデジタル領域」を明記した。

私たちは、これに対抗して、デジタル領域を戦場にさせないことが重要な課題になっている。しかし、９条の枠組や従来の平和運動の戦争概念ではサイバー戦争を総体として拒否し、非協力の運動を支えることができていないのではないか？私たちは、これまでの経験を越えた領域での反戦運動、平和運動の構築を問われていると思う。