アクティブサイバーディフェンスの法律的側面

弁護士 高橋郁夫

「国家安全保障戦略」

- 令和４年１２月１６日
  - 国家安全保障会議及び閣議
  - 安全保障関連3文書の決定
    - 国家安全保障戦略
    - 国家防衛戦略
    - 防衛力整備計画
- 「能動的サイバー防御を導入」
  - 武力攻撃に至らないものの（even if they do not amount to an armed attack）、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
  - 目的
    - これを未然に排除し（eliminating in advance the　possibility of serious cyberattacks）/または
    - 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（preventing the spread of damage in case　of such attack）
  - 能動的サイバー防御（active cyber defense）を導入

能動的サイバー防御(active cyber defense)の概念

- 三つの概念
  - （ｱ）（日本は、）重要インフラ分野を含め、民間事業者等がサイバー攻撃を受けた場合等の政府への情報共有や、政府から民間事業者等への対処調整、支援等の取組を強化するなどの取組を進める。
  - (ｲ)（日本は、）国内の通信事業者が役務提供する通信に係る情報（information on communications services provided by　domestic telecommunications providers.）を活用し、攻撃者による悪用が疑われるサーバ等を検知（detect servers and others suspected of being abused by attackers）するために、所要の取組を進める。
  - (ｳ) 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について、可能な限り未然に攻撃者のサーバ等への侵入・無害化（penetrate and neutralize attacker's servers and others ）ができるよう、政府に対し必要な権限が付与されるようにする。

攻撃者への影響を必要としない/
日本的な「通信の秘密」問題が記載されている

(イ)悪用が疑われるサーバ等を検知

- （日本は）国内の通信事業者が役務提供する通信に係る情報（information on communications services provided by domestic telecommunications providers.）を活用
- (高橋コメント)

1. これは、(武力攻撃に至る場合、いたらない場合とも（even if they do not amount to an armed attack）)どのような仕組みを準備しようというのか
2. ISPがトラフィックの状況を分析するのは、当然だろう。そして、それが、通信秩序を侵害する場合に対応するのは当然/国家と共有できるのは当然だろう-憲法違反という学者/メディアはでるだろう。
3. 海外の事業者の取扱中にかかる通信についても検知できるはず-それが除かれているのはなぜか？

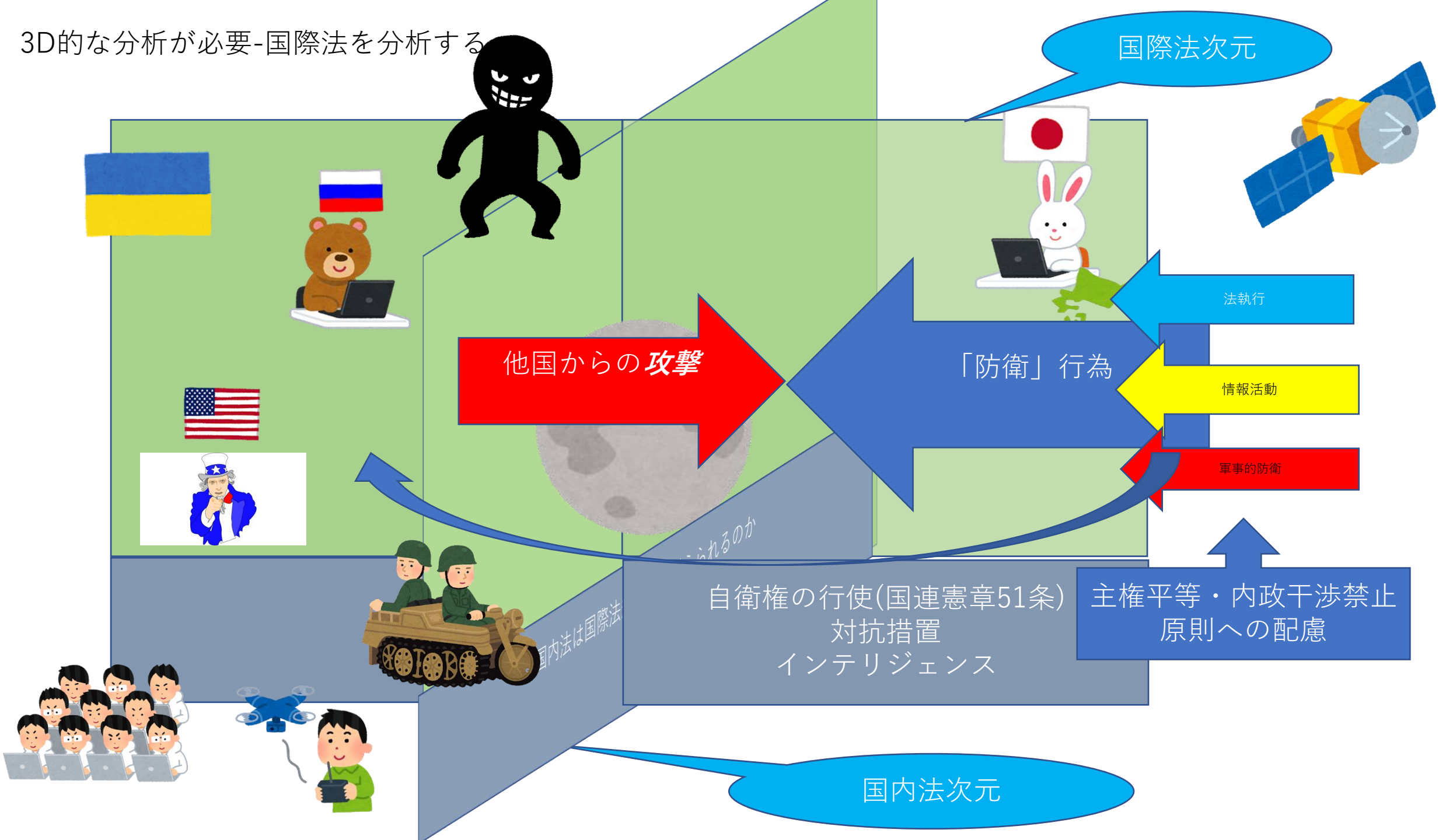
(ウ)未然に攻撃者のサーバ等への侵入・無害化

- 概念要素
  - 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
  - 攻撃者のサーバ等
  - 政府に対し必要な権限が付与される
- コメント
  - 政府は誰だ/手続は？
    - 令状によるボットネットテイクダウン
    - 自衛隊のオペレーションとしてありうるのか？
  - サーバ等-感染しているクライアント？
    - HAFNIUM(ハフニウム)に対するFBIのweb shell

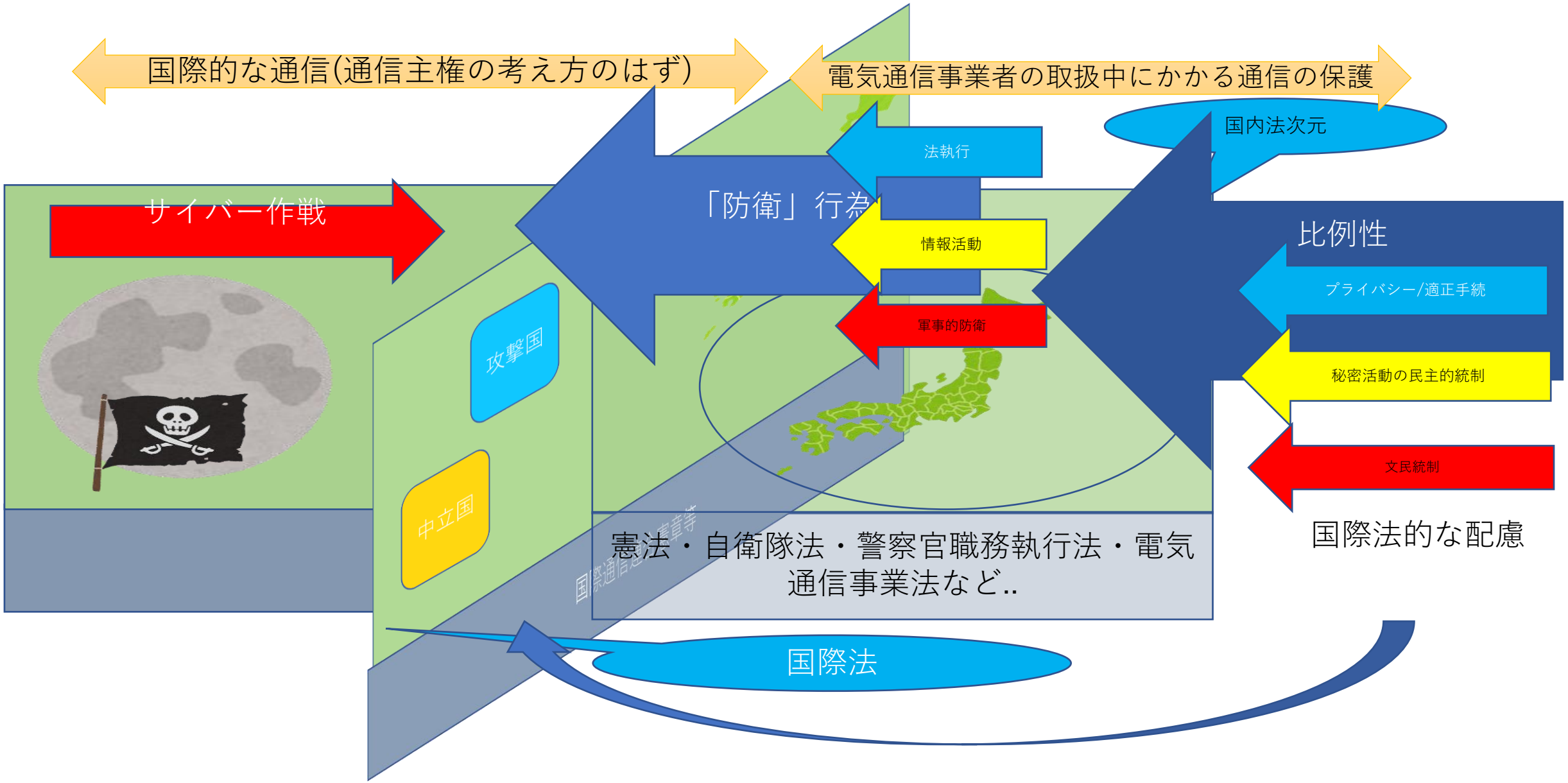
傘としての能動的サイバー防御の概念

- 唯一の「能動的サイバー防御」の概念規定は困難である
- ある程度の要素
  1. 特定の進行中の悪意あるサイバー作戦やキャンペーンに関して
  2. 技術的に無力化し、その影響を緩和し、かつ/または技術的に帰属させることを目的
  3. 個々の国家によって、または集団で
  4. 政府機関によって実施または義務付けられた
  5. 一つまたは複数の技術的措置
  6. 攻撃者に直接的に影響を与えうる行為(？)
- 許容性は、上の要素がそれぞれもつ「法的な」意味を考える

3D的な分析が必要-国際法を分析する



3D的な分析が必要-国内法を分析する



論点の全体像

広範囲な
グレーゾーンの存在

烈度	国際法		国内法		
	武力紛争時	自衛権の行使	自衛隊による防衛出動		
	平時	サイバー力の行使による攻撃者への損害等	自衛隊/軍	？	米国の継続的関与
			法執行機関	警察官職務執行法/令状による	裁判所の関与による措置
		情報インフラへの業務阻害	自衛隊/情報機関/法執行機関	？	ソニーピクチャアエンターテイメント事件後のDos（？）
		中立化（攻撃能力の阻害）	自衛隊/情報機関/法執行機関	法執行機関による場合->裁判所の令状？ 情報機関の活動 ->民主的統制	ボットのテイクダウン ホワイトワーム 継続的な関与
		情報の取得	法執行機関/情報機関	刑事訴訟法/警察官職務執行法	米国における共同作戦/プロバイダー例外

パネル用資料

警察官職務執行法の限界

- 職務執行法の警察官の権限
  - 質問（2条）
  - 保護（3条）
  - 避難等の措置（4条）
  - 犯罪の予防および制止（5条）
    - ボットネットの解毒は、制止として論じることができないのか。透明性はどうか。
    - 第三者がしらないで、犯罪を助力しているのを強制解毒という場合もある
  - 立入（6条）
  - 武器の使用（7条）
    - サイバー的手法は、「武器」ではないし、予防および制止措置でもない。当然使えるという解釈はありうるのか？
- なしたい行為は、証拠の取得・分析・弱点(脆弱性を含む)情報の取得ではないか？
  - 適する規定がない？
  - 「予防および制止」のほうに近いのではないか
    - 警察官の行う実力行使の問題になるだろう。

サイバー領域における令状による捜査

- 刑事訴訟法218条
  - 検察官、検察事務官又は司法警察職員は、犯罪の捜査をするについて必要があるときは、裁判官の発する令状により、差押え、記録命令付差押え、捜索又は検証をすることができる。
- 捜査と進行中の犯罪の防止の機能の流用？
- 防衛行為によって生じる被害をどのように考えるのか・その程度のメルクマールは、何か？
  - 強制？ 生命身体？ 日本におけるGPS判決最高裁平成29年3月15日大法廷判決の示唆
- 米国におけるプロバイダー特権と法執行機関の積極的な情報取得の可能性
- 国際的な法執行作用と国際法の衝突

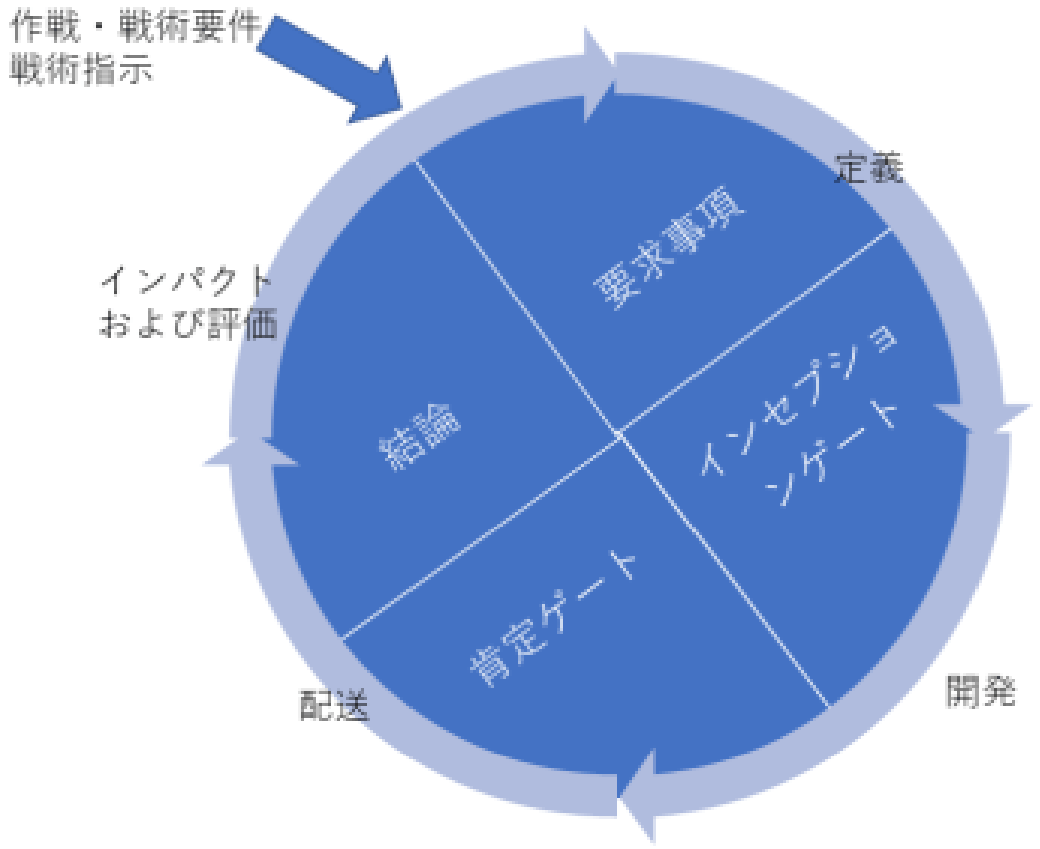
ドラマ GCHQに戻ってみよう

- サイバー攻撃を未然に防ぐ目的で相手のシステムへアクセスする「能動的サイバー防御」の導入
  - オフェンシブ・サイバーの導入を意味しているのか？
  - 実際のオペレーション
    - NCF(国家サイバー部隊)-ユニフォームが、GCHQ にやってきて、キーボードを叩く
    - 自動的に作戦が行われる

なぜ、NCFがキーボードを叩くのか

- 戦闘員の定義
- NCFの活動に対する法的な規制

  - 強固な法的・倫理的枠組みの厳格な遵守
  - 強固な監視と説明責任
  - 明確な戦略、ドクトリン、必要な基本方針
  - 権限付与を含む作戦を管理するための徹底的で確立されたプロセス
  - 効果的にコントロールでき、予測可能なサイバー能力
  - 説明責任を果たし、正確で調整された作戦の原則が維持されるようにするための洗練された計画プロセス



まとめ

- 能動的サイバー防御という概念自体から何か有益なものを導くことはできない
- 攻撃側に影響があるか、どうかだけでも論点を導きうる
- 影響のある場合でも、攻撃と反撃の烈度によって、法的な位置づけは非常に異なる
- 法的な位置づけは、国内法と国際法との3D分析をなすことが必要
- 主体と行為で分析する場合に、従来の国内法と国際法の分析枠組はきわめて有効である(地勢的な一般論は、有害無益である)
- 「国家安全保障戦略」が、法的にどのような意味を含んでいるのかというのは、サイバーセキュリティの法専門家でないと分析できないだろう
- 具体的な論点については、国際法／国内法、具体的な行為に応じて種々の論点が存在しており、広大な法的なグレイゾーンが存在している。
- 通信事業者への負担を前提に、その合理的な規制、また、技術的なツールを前提に、そのツールの技術評価、効果・コラテラルな影響を評価しうることが重要であるが、我が国では論点の指摘もなされていない