『サイバー革命論』は本当なのか？

宮岡研究会8期生共同研究
2017年12月学生シンポジウム

*“Cyber, in my modest opinion, will soon be revealed to the **biggest revolution in warfare**, more than gunpowder and the utilization of airpower in the last century.”*

-イスラエル軍事情報機関長官Aviv KOCHAVI（2014）

☆まずは語句の定義を確認しましょう！

・「サイバー戦争」とは…

政治的利益のために物理的インフラを破壊するコンピューター攻撃
(例：スタックスネット事件)

・「サイバー革命論」とは…

サイバーが戦争の性質を革命的に変えているという説
戦争形態に新たな選択肢を提示した3つの柱から成り立つ

目次

導入：サイバー戦争、サイバー革命論とは

第1部：サイバー空間における**非対称性**について

第2部：サイバー空間における**攻撃・防御バランス**について

第3部：サイバー空間における**抑止**について

- 各部の構成

1)サイバー革命論について

2)サイバー革命論に対する反対の意見

3私たちの結論

第1部：サイバー空間におけるアクターの非対称性

1-1　非対称性：サイバー革命論①

革命論①：サイバー空間は軍事的弱者の武器になりうる

1)サイバー兵器は弱者にとって使いやすい

a)サイバー空間は他の物理領域と違って参入コストが低い

b)敵の特定が困難なため、攻撃側への報復や抑止が難しい

2)サイバー空間において強国は脆弱である

強国の軍事力はネットなどのIT技術に依存

→サイバー攻撃の影響を受けやすい

1-2　非対称性：サイバー革命論①への反論

反論：サイバー空間は弱者の武器になりえない

1)匿名性と有効性創出の為には甚大な労力を要する
　（高度な専門知識、人材、設備等）
2)強国はリスクの対応や軽減をする能力がある
3)強国は軍事的後ろ盾を持っている
　→容易に攻撃不可能＝抑止

1–3　非対称性：私たちの結論

結論：サイバー空間は弱者の武器になりえない

1)弱者には知的資源が乏しい

2)サイバー攻撃は軍事力と組み合わせた方がより強力になる

★原則的に強国優位だが、状況によっては弱者優位になることもある

例１：今後の技術進歩に伴う強国のさらなるIT依存度の上昇。

例２：サイバー空間と物理的空間を上手く組み合わせた攻撃が行われた場合。

第2部：サイバー空間における攻撃・防御バランス

2-1　攻撃優位論：サイバー革命論②

革命論②：サイバー空間は攻撃優位である

1)サイバー攻撃への参入コストの低さ
2)帰属特定の難しさがサイバー攻撃を容易にする
3)防御は常に成功する必要があるが、攻撃は一度成功すればよい
4)スタックスネットの事例における防御側のコスト
　a)核開発施設への攻撃を防ぐ対策
　b)核開発施設の即時的な生産力喪失
　c)遠心分離機の取替費用

2-2　攻撃優位論：サイバー革命論②への反論

反論：サイバー空間は常に攻撃優位となるわけではない

1)ソフトウェアは攻撃側に脆弱性を与える恣意的な複雑性を持つ

2)攻撃では物理的な損害を与える為には多大なコストがかかる

3)攻撃目標の複雑性や防御側の能力の程度に依存する

　→攻撃優位は目標の単純さや不十分な防御の結果

4)欺瞞戦略によって直接攻撃を防ぐ　例)ハニーポッド

2–3　攻撃優位論：私たちの結論

結論：攻撃と防御のどちらが優位に立つかということは様々な条件に依存する

- **攻撃が有利になる条件**
  1)ソフトウェアの恣意的な複雑性を管理する適切な**組織的能力**
  2)**攻撃目標の単純さ**、防御側の**不十分な組織的能力**
- **防御が有利になる条件**
  1)高水準のソフトウェアの存在
  2)**攻撃に対する技術者の高度な能力**

第3部：サイバー空間における抑止

3-1　抑止無効論：サイバー革命論③

革命論③：<u>サイバー空間では抑止は無効である</u>

☆サイバー空間においては、懲罰的抑止は効力がない

<u>**抑止**を妨げる要素</u>

1)攻撃してくる相手が不明確
2)非国家主体の介入が可能

} 報復の対象が絞れない

3-2　抑止無効論：サイバー革命論③への反論

反論：サイバー空間での抑止は不可能ではない

懲罰的抑止（サイバー革命論の焦点）

1)相手を特定する方法を確立できれば抑止が可能になる

a)攻撃パターンを分析する

b)罠を仕掛ける

拒否的抑止（サイバー革命論で着目されていない点）

1)防御力を上げる事ができれば相手の目的を無効化できる

3-3　抑止無効論：私たちの結論

主張：将来的に抑止の可能性が高まる

現在：抑止を妨げるサイバー空間の要素が多い
　→現在の技術では抑止は困難、効果は薄い

将来：サイバー空間内の技術の向上により相手の特定が可能に
　→懲罰的・拒否的抑止が将来的に効力を持つ可能性がある

1部、2部、3部のまとめ

1部：現在のサイバー空間は、原則的に強国優位である

※強国のIT依存度の上昇などによって弱者が優位になる可能性有

2部：サイバー空間において常に攻撃が防御より優位に立つとは限らない

※高水準のソフトウェアや技術者能力により防御優位になる可能性有

3部：将来的に技術の向上などによって抑止が効力を持つ可能性

※現在のサイバー空間では抑止を妨げる要素が多い

現在の防衛省の施策

1)強国優位

→米国との協力（情報共有体制の構築・重要インフラの防護）＆軍事的後ろ盾

→脅威情報の共有・共同の演習も行う

2)攻撃と防御

→「サイバー防衛隊」の規模と能力を強化し、サイバー攻撃の方法を研究

→敵に攻撃する能力の育成を図るが、憲法との関係で課題は多い

3)抑止困難

→情報収集・分析機能の強化による多様性・匿名性への対処

→拒否的抑止力の強化：技術の向上による抗たん性の向上

→防衛省通信基盤（DII）の整備やサイバー攻撃対処技術の研究による防御力強化

※2016年9月頃にDIIへのサイバー攻撃を感知

防衛省に対する政策提案

主張：防御中心にサイバー専門部隊の増員・育成に注力すべき

憲法9条との兼ね合いは未だはっきりしていない

→攻撃に積極的な姿勢は示しにくい

サイバー空間では前述の理由から懲罰的抑止が難しい

→防御に力を入れ、相手の目的を消滅させることで拒否的抑止を働かせる

→攻撃の優位性に立つべきではない

→相手の目的を消滅させるためには技術優位に立つしかない


Thank you
for
listening!