民間企業による自力救済手段としてのActive Cyber Defenseの検討

Consideration of Active Cyber Defense as Self-Help Measure by Private Sector

笠原大空・湯淺研究室・情報セキュリティ大学院大学

〈Abstract〉

In cyberspace, due to the asymmetry that the attacker has overwhelming advantage, the cyberspace is in a natural state where a malicious users are unleashed. In the natural state, the victims have no choice but to resort to self-help that regains their rights and property on their own hands because the they can not hope for legal remedies. Accordingly, in recent years “Active Cyber Defense” has been considered as a means of self-help against cyber attack.

サイバー空間は攻撃側が優位となる非対称性問題の結果、サイバー空間は自然状態、つまり悪意あるユーザが野放しになっている．自然状態では被害者の法的救済が望めないため、被害者自身の手で権利を保護・回復する自力救済に訴えざるを得ない。こうした状況により、近年では積極的サイバー防御(ACD: Active Cyber Defense)と呼ばれるサイバー攻撃対策が検討されている。

しかしながら、ACDはHoney PotやDeception等の攻撃側を欺く技術だけでなく、Hack BackやLegal Malware等のサイバー攻撃の転用を含める場合があるため、その効果を検証する以前に合法性が問題となる。ACDは国家・非国家問わずサイバー攻撃への能動的な対抗手段であるが、国家は自衛権を行使することで実施可能である一方、国家に帰属しない行為主体は法的根拠がなく、民間企業のACDは違法行為となる。

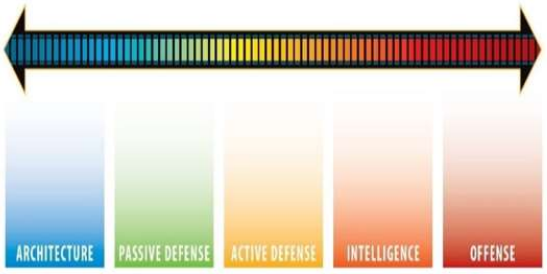
法的救済が難しい現状から、民間企業の自力救済を実現する手段としてのACDについて、その概念等を分析した後、民間企業が実施した場合どのような法律に抵触するのかについて検討していく。

サイバー空間の非対称性(林・田川[2018])

評価基準	攻撃側	防御側
①実行者の特定	ツールによる秘匿が容易	Attributionが困難
②攻撃の隠密性	検知されずに侵入することが可能	・容易に判断することが困難 ・原因究明に時間を要する
③攻防の活動	・成功するまで繰り返し攻撃可能 ・一点突破が可能	・全面防御できなければ失敗 ・合法的対処に制限
④コスト	低コストで大きな利益	対策ツール等の導入に大きなコスト
⑤人材・組織	・様々な素性を持つ ・緩やかな国際連携	・正規の採用後選抜 ・国内組織が中心
⑥国家の関与	・違法行為の黙認や暗黙の支援 ・国家機関による実施	・民営のインフラは民間企業主導 ・国家は国際秩序を遵守
⑦計算資源	膨大な計算資源の利用が可能	限られた計算資源

The Sliding Scale of Cyber Security (Lee[2015])

・SANS Instituteのインストラクター Robert M. Lee によるWhitepaper
・Cyber Securityを可変的な概念で解釈で捉えた



ACDとCyber Attackの対応関係(CCHS[2016])

ANATOMY OF EXPLOIT AND ATTACK		Active Defense Measure		
Attack Category	Attack Stage	Measures	Network Area	Impact/Risk
Stage1: External Preparation of the Attacker	①Reconnaissance	・Tarpits ・Sandboxes ・Honeypots	Internal	Low
	②Malware Creation & Weaponization	Denial & Deception	Internal	Low
	③Decision to Target a Victim	・Coordinated Sanctions, ・Indictments & Trade Remedies	External	High
Stage2: The Intrusion	④Delivery	Information Sharing	Internal	Low
	⑤Gain a Foothold	Intelligence Gathering (Deep Web/Dark Net)	External	High
Stage3: The Active Breach	⑥Establish C & C	Botnet Takedowns	External	High
	⑦Expansion & Preparation	Hunting	Internal	Low
	⑧Action on Objectives	Notification Beacons	Internal	Low
		Information Beacons	External	Low
		White-hat Ransomware	External	High
		Rescue Missions	External	High

サイバー活動と行為主体の法的根拠

サイバー活動		合法性	
ネットワーク領域	サイバー防御	民間企業	国家機関
外部	サイバー攻撃	違法行為	違法行為
	サイバー反撃		自衛権行使可能
	積極的サイバー防御 (攻撃側のネットワーク外部)		
内部	積極的サイバー防御 (攻撃側のネットワーク内部)	違法の場合有	違法性無
	・Firewall ・マルウェア対策ソフト ・フォレンジック etc…	違法性無	