First Step to Active Cyber Defence: The Significance of Profiling Attackers

JPCERT Coordination Center
Early Warning Group Manager
Threat Analyst
Hayato Sasaki

Before start

Current status (November 2022)

As the government is considering revisions to the three key national security documents, the concept of "active cyber defense" is mentioned.

While there is a lot of talk about whether to include or not to include "counterattacks," there is no concrete explanation of the "definition," what kind of operations are involved, or the advantages or disadvantages of such operations.

Actually, there is no definition of such a term, and no one knows the specific theory!

Issue

In general, in this kind of issue, various “means” newly considered may become activity traps.

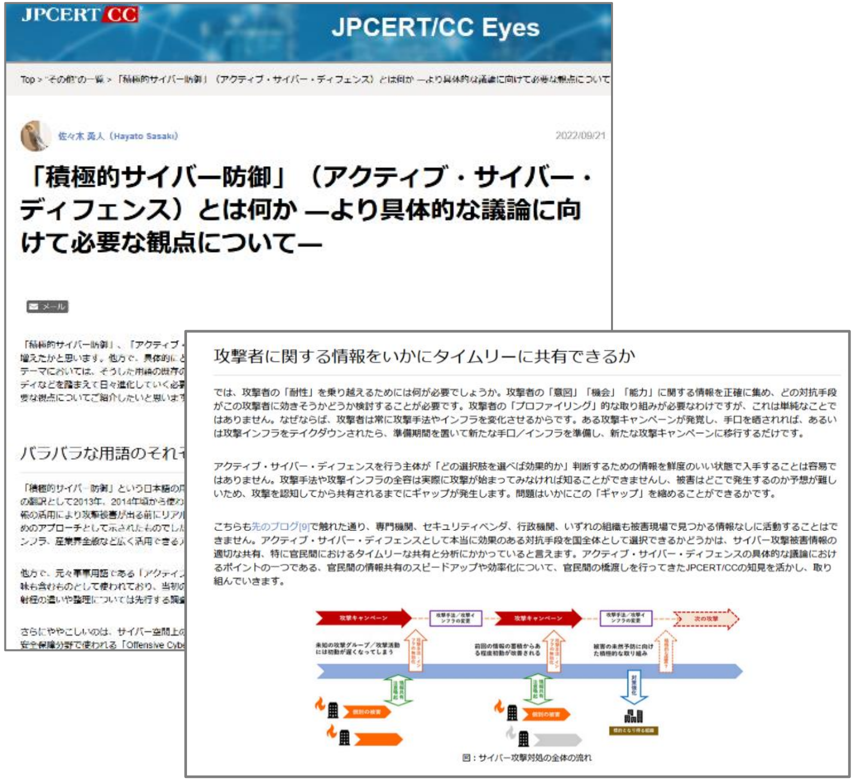
The "who's going to do it?" argument can essentially lead to a false means.

Will there be any "divergence" or "conflict" with existing incident response sites?

Profiling* of attackers is important to determine specific operations and which threats to counter.

*While "criminal profiling" is well known for inferring criminals based on crime types and characteristics of crimes committed, this presentation will use it as an analysis of attacker groupings and attack characteristics and trends.

Preliminary Research



Top > "その他"の一覧 > 「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か —より具体的な議論に向けて必要な観点について

佐々木 勇人（Hayato Sasaki） 2022/09/21

「積極的サイバー防御」（アクティブ・サイバー・ディフェンス）とは何か —より具体的な議論に向けて必要な観点について—

「積極的サイバー防御」、「アクティブ・
増えたかと思います。他方で、具体的にど
テーマにおいては、そうした用語の既存の
ディなどを踏まえて日々進化していく必要
要な視点についてご紹介したいと思います

バラバラな用語のそれぞ

「積極的サイバー防御」という日本語の用
の翻訳として2013年、2014年頃から使わ
術の活用により攻撃被害が出る前にリアル
めのアプローチとして示されたものでした
ンフラ、産業界全般など広く活用できる人

他方で、元々軍事用語である「アクティブ
味も含むものとして使われており、当初の
射程の違いや整理については先行する調査

さらにややこしいのは、サイバー空間上の
安全保障分野で使われる「Offensive Cybe

攻撃者に関する情報をいかにタイムリーに共有できるか

では、攻撃者の「耐性」を乗り越えるためには何が必要でしょうか。攻撃者の「意図」「機会」「能力」に関する情報を正確に集め、どの対抗手段がこの攻撃者に効きそうかどうか検討することが必要です。攻撃者の「プロファイリング」的な取り組みが必要なわけですが、これは単純なことではありません。なぜならば、攻撃者は常に攻撃手法やインフラを変化させるからです。ある攻撃キャンペーンが発覚し、手口を晒されれば、あるいは攻撃インフラをテイクダウンされたら、準備期間を置いて新たな手口／インフラを準備し、新たな攻撃キャンペーンに移行するだけです。

アクティブ・サイバー・ディフェンスを行う主体が「どの選択肢を選べば効果的か」判断するための情報を鮮度のいい状態で入手することは容易ではありません。攻撃手法や攻撃インフラの全容は実際に攻撃が始まってみなければ知ることができませんし、被害はどこで発生するのか予想が難しいため、攻撃を認知してから共有されるまでにギャップが発生します。問題はいかにこの「ギャップ」を縮めることができるかです。

こちらも先のブログ[9]で触れた通り、専門機関、セキュリティベンダ、行政機関、いずれの組織も被害現場で見つかる情報なしに活動することはできません。アクティブ・サイバー・ディフェンスとして本当に効果のある対抗手段を国全体として選択できるかどうかは、サイバー攻撃被害情報の適切な共有、特に官民間におけるタイムリーな共有と分析にかかっていると言えます。アクティブ・サイバー・ディフェンスの具体的な議論におけるポイントの一つである、官民間の情報共有のスピードアップや効率化について、官民間の橋渡しを行ってきたJPCERT/CCの知見を活かし、取り組んでいきます。

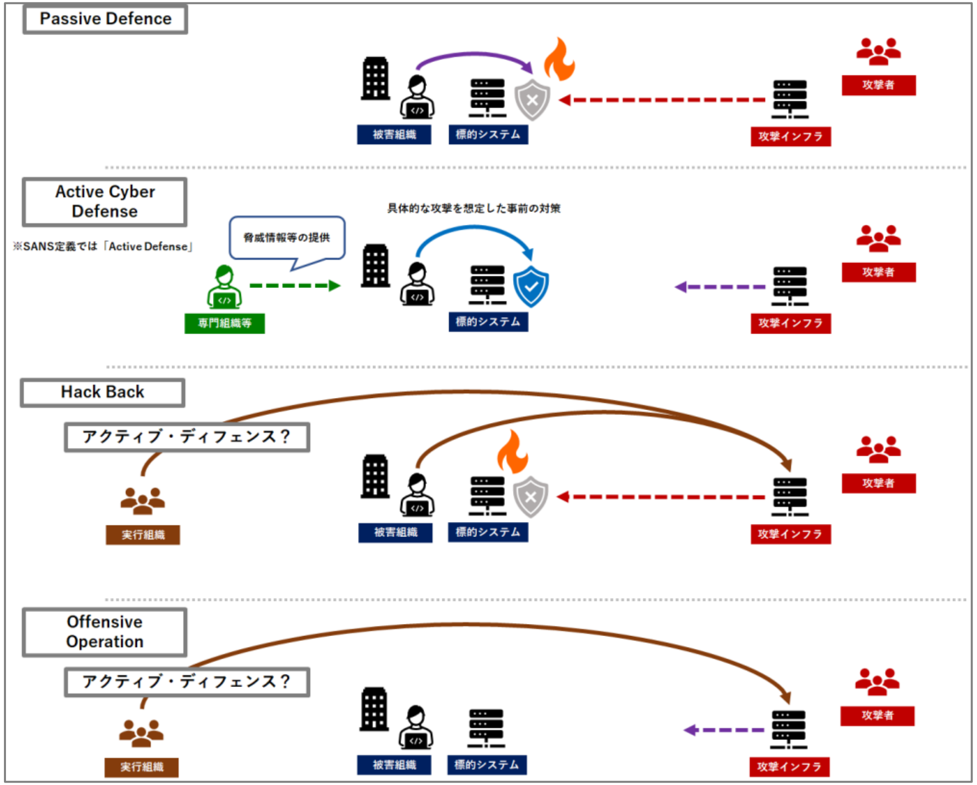
攻撃キャンペーン
攻撃手法／攻撃インフラの変更
攻撃キャンペーン
攻撃手法／攻撃インフラの変更
次の攻撃
未知の攻撃グループ／攻撃活動には初動が遅くなってしまう
攻撃手法・インフラの無効化
前回の情報の蓄積からある程度初動が改善される
攻撃手法・インフラの無効化
被害の未然予防に向けた積極的な取り組み
積極的な追跡?
情報共有注意喚起
情報共有注意喚起
対策強化
個別の被害
個別の被害
標的となり得る組織

図：サイバー攻撃対処の全体の流れ

https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

- September 21, 2022 JPCERT/CC Blog (Japanese only)
- explains how the term "active cyber defense" came to be used, how it has evolved, and how the "definition" of the term has become blurred.
- points out that there is a combination of different options for countering proactive cyber attacks

From the research: The evolution of the terminology



https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

[Hypothesis]

With various entities using the terminology, the mix of terms that have flowed in from industries other than cybersecurity may have confused/diversified the concept.

[Background].

- People rephrased the terms more "positive sounding expressions" at the time.

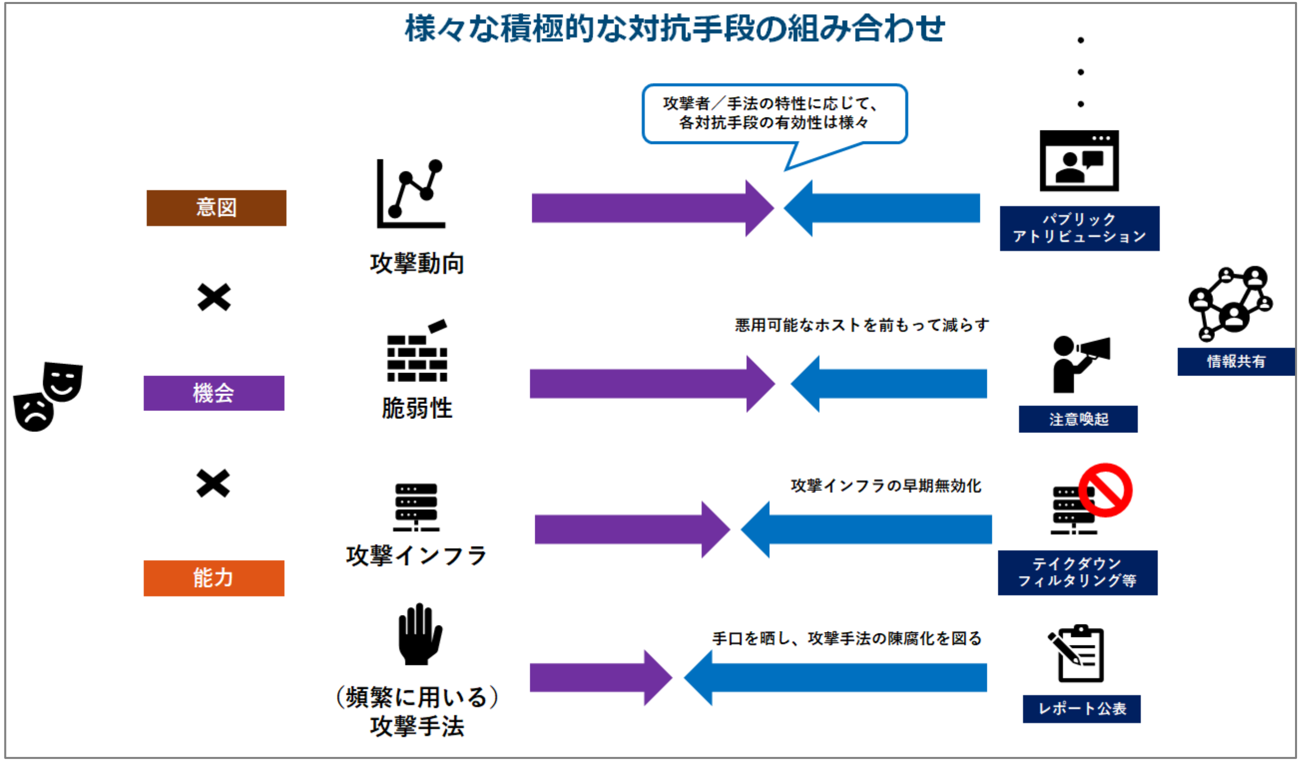
  Example: defensive combat doctrine → "active defense" (1976)

- Terminology imported from the military/intelligence industry to the cybersecurity industry.

  E.g., kill chain, threat intelligence, etc.

From the research: Proactive countermeasure options

- Various proactive countermeasures exist in addition to offensive methods.



様々な積極的な対抗手段の組み合わせ

意図 × 機会 × 能力

攻撃動向

脆弱性

攻撃インフラ

（頻繁に用いる）攻撃手法

攻撃者／手法の特性に応じて、各対抗手段の有効性は様々

悪用可能なホストを前もって減らす

攻撃インフラの早期無効化

手口を晒し、攻撃手法の陳腐化を図る

パブリック アトリビューション

注意喚起

テイクダウン フィルタリング等

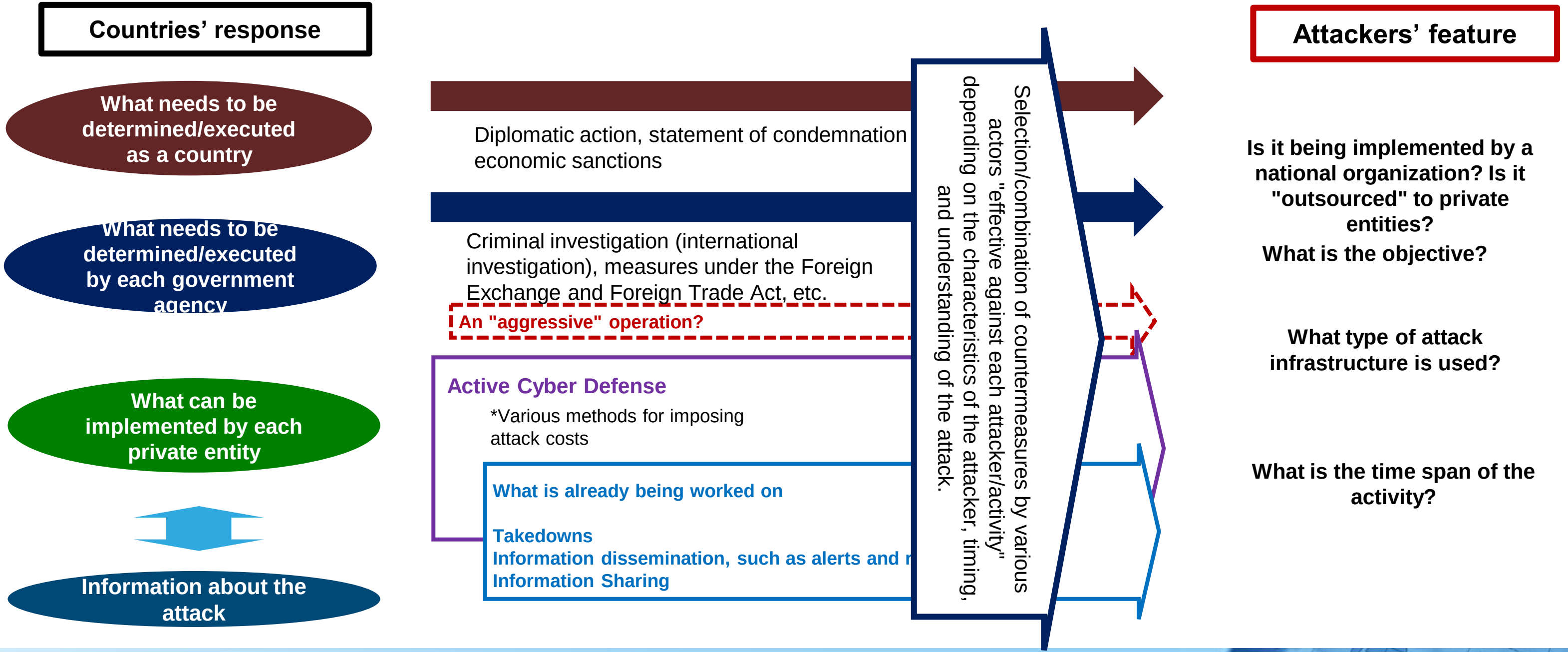
レポート公表

情報共有

https://blogs.jpcert.or.jp/ja/2022/09/active-cyber-defense.html

Consider flexible and dynamic countermeasures

- Of the various options for dealing with attackers, "active cyber defense" or "offensive" operations are only a small part of the equation.
- Nevertheless, as we consider "active cyber defense," **isn't it useful to try something that hasn't been done before?**



Countries' response

What needs to be determined/executed as a country

Diplomatic action, statement of condemnation economic sanctions

What needs to be determined/executed by each government agency

Criminal investigation (international investigation), measures under the Foreign Exchange and Foreign Trade Act, etc.

An "aggressive" operation?

What can be implemented by each private entity

Active Cyber Defense

*Various methods for imposing attack costs

What is already being worked on

Takedowns
Information dissemination, such as alerts and r
Information Sharing

Information about the attack

Selection/combination of countermeasures by various actors "effective against each attacker/activity" depending on the characteristics of the attacker, timing, and understanding of the attack.

Attackers' feature

Is it being implemented by a national organization? Is it "outsourced" to private entities?

What is the objective?

What type of attack infrastructure is used?

What is the time span of the activity?

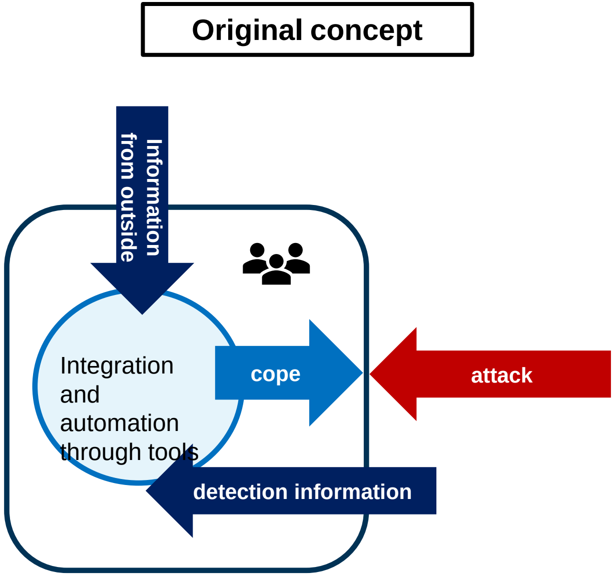
...but in the end, we don‘t know about it yet.

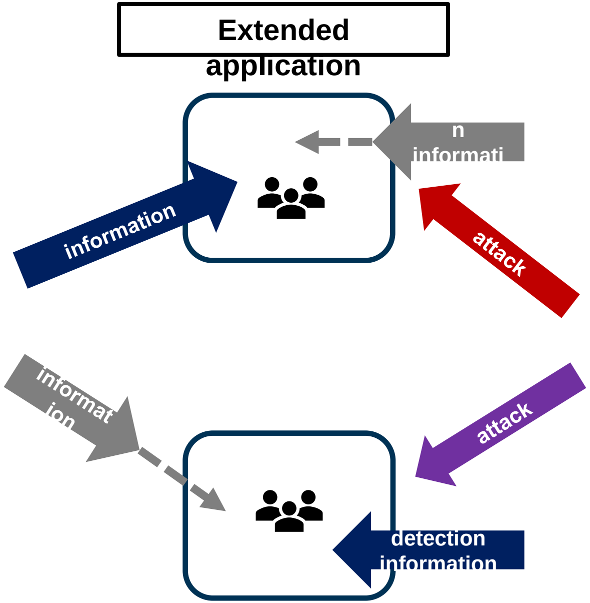
- Are we talking about responding to individual cases or the country as a whole?
- Should we respond before or after an attack?
- Is it to stop or interrupt offensive activity?

Let’s look back at the “definition” of the word a bit

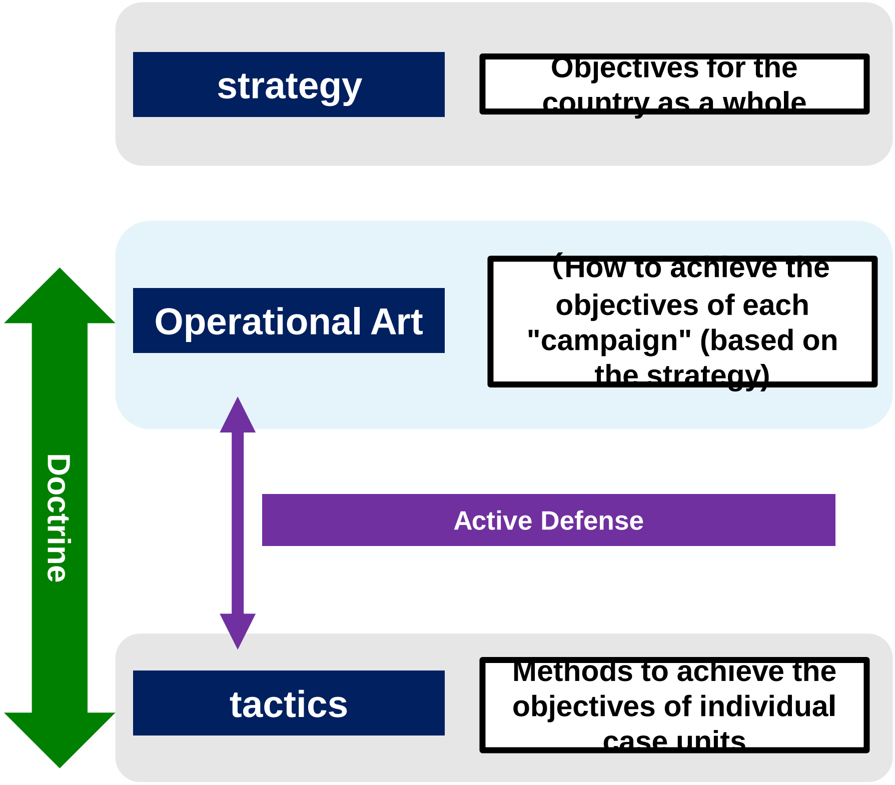
Limitations in expanding application of the original "active cyber defense"

- A proactive attack response concept originally intended for implementation in individual organizational units
- When collaborating by industry/sector or region, the larger the scale, the more difficult it becomes to collaborate between organizations, and the different types of attacks they are subjected to make it difficult to respond proactively in a logical manner.





Origins of the ambiguity in "active cyber defense"



strategy

Objectives for the country as a whole

Operational Art

(How to achieve the objectives of each "campaign" (based on the strategy)

Active Defense

tactics

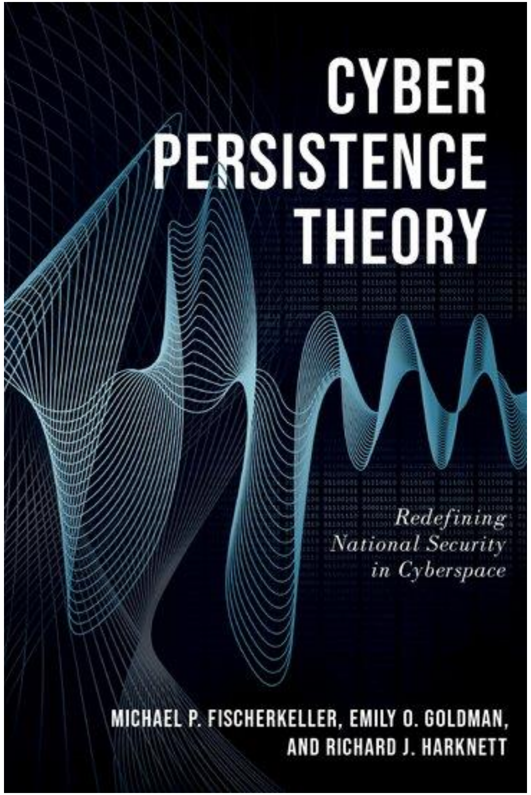
Methods to achieve the objectives of individual case units

Doctrine

- The concept of "**active defense" as it** appears in U.S. Army Combat Doctrine FM 100-5 (1976 edition)
- Operational Art
  - - Operational art is the art of **campaign"** (John English, 1996).
  - - Operational art is the link between tactical success and strategic achievement points (British Integration Doctrine).
- The concept of "active defence" was criticized for being focused on the tactical level and was subsequently revised to overcome this at the operational level
- Improvements are needed to extend "active (cyber) defense," originally at the "tactical" level, to the "operational" level.

References: Keizo Kitagawa, "Intellectual Innovation in Military Organizations: Doctrine and the Imagination of Operational Art," David M. Glantz, "Soviet Military <Operational Art>: The Pursuit of Vertical Deep Battle," etc.

Point to consider a definition: Campaign

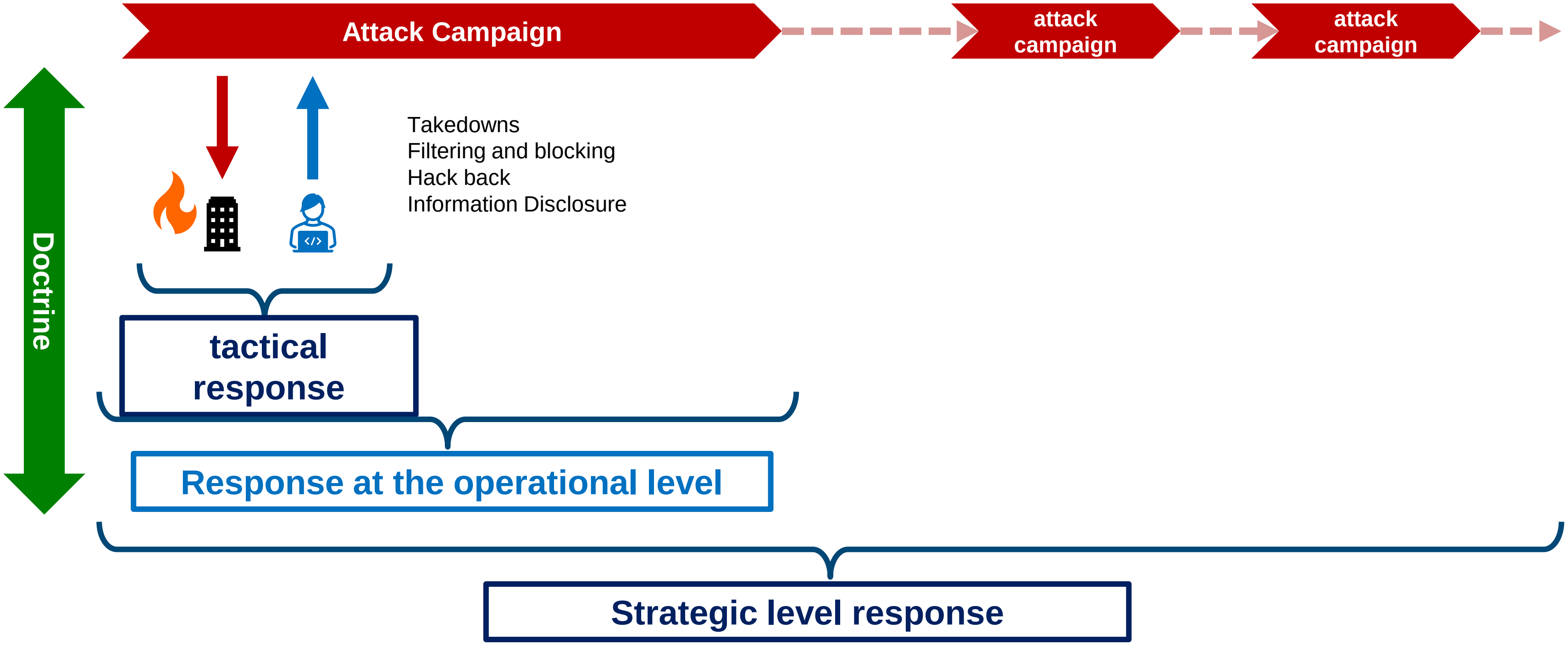

CYBER PERSISTENCE THEORY
Redefining National Security in Cyberspace
MICHAEL P. FISCHERKELLER, EMILY O. GOLDMAN, AND RICHARD J. HARKNETT

https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&

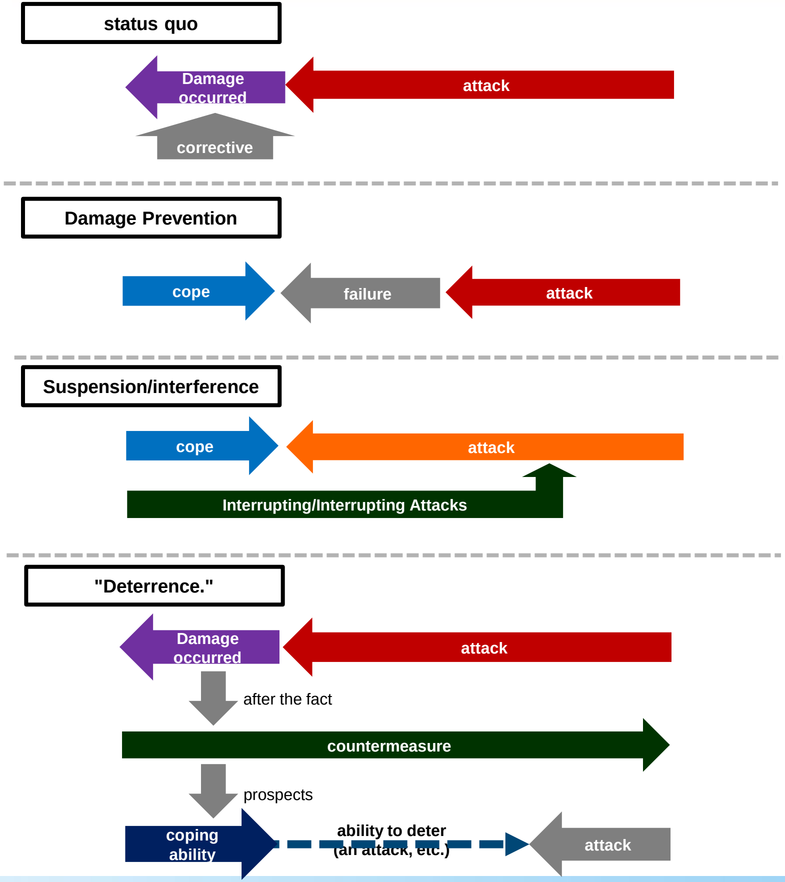
- Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, "CYBER PERSITENCE THEORY," 2022
- He pointed out that most cyber attacks backed by state actors are not "coercion" but "exploitation" and "fait accompli.
- Evaluates and analyzes the history of countermeasure implementation in the U.S. to date, including the ineffectiveness of countermeasures such as public attribution based on existing deterrence theory.
- Focusing on the attack "**campaign"** unit, we propose the "Cyber Persistence Theory," an approach to maintaining superiority through sustained "Direct Cyber Engagement" in response.

Active Cyber Defense as Doctrine

- Vertical axis: What are we going to do
- Horizontal axis: What is a purpose and when to do



Point to consider a definition: timing and cost

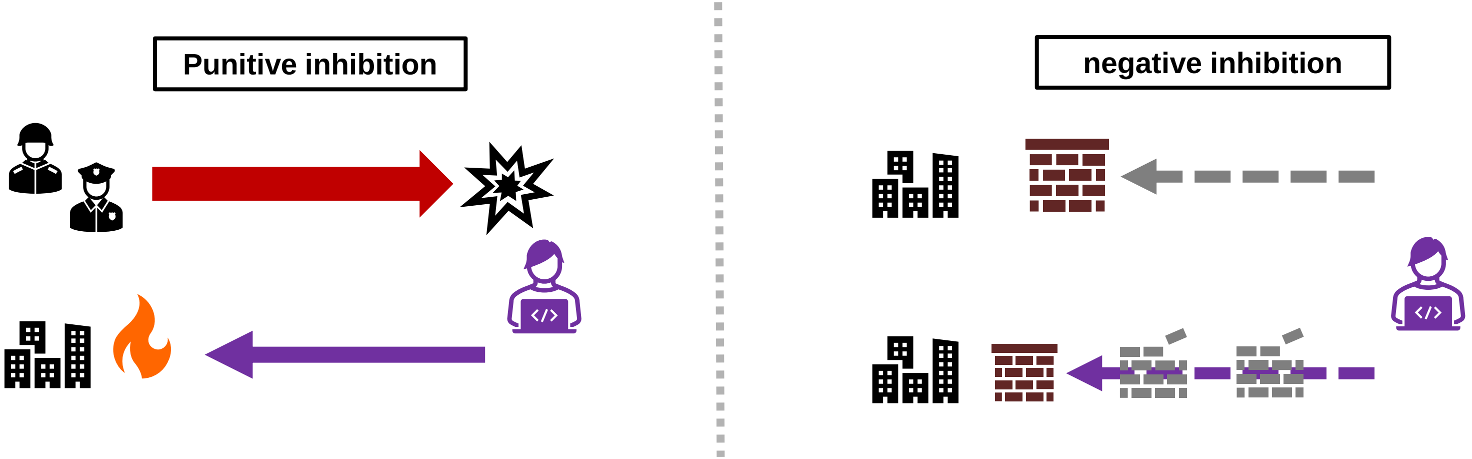


- If the objective is "damage prevention," when and what kind of attack "damage" is to be prevented?
  - APT attacks are difficult to capture early. Need information from the first "hit" organization
  - For example, if an unauthorized access is received, isn't it "damage prevention" to catch it early and stop the attack before the information is leaked?
- Imposing "cost" on attackers.
  - Raising the cost of launching/successfully launching an attack (denial deterrence?)
  - To suspend the attack
  - - Sanctions as punitive deterrence

What does it mean to "impose a cost" on an attacker?

- The term "imposing costs" is increasingly used by Western governments and others.
- It is a double-meaning.

- Punitive deterrence: "cost" in the sense of "making them pay the price". It is only intended to aim at subsequent deterrence through measures taken after the attack.
- Denial deterrence: "cost" in the sense that it is difficult for an attack to succeed/takes a great deal of effort to succeed.

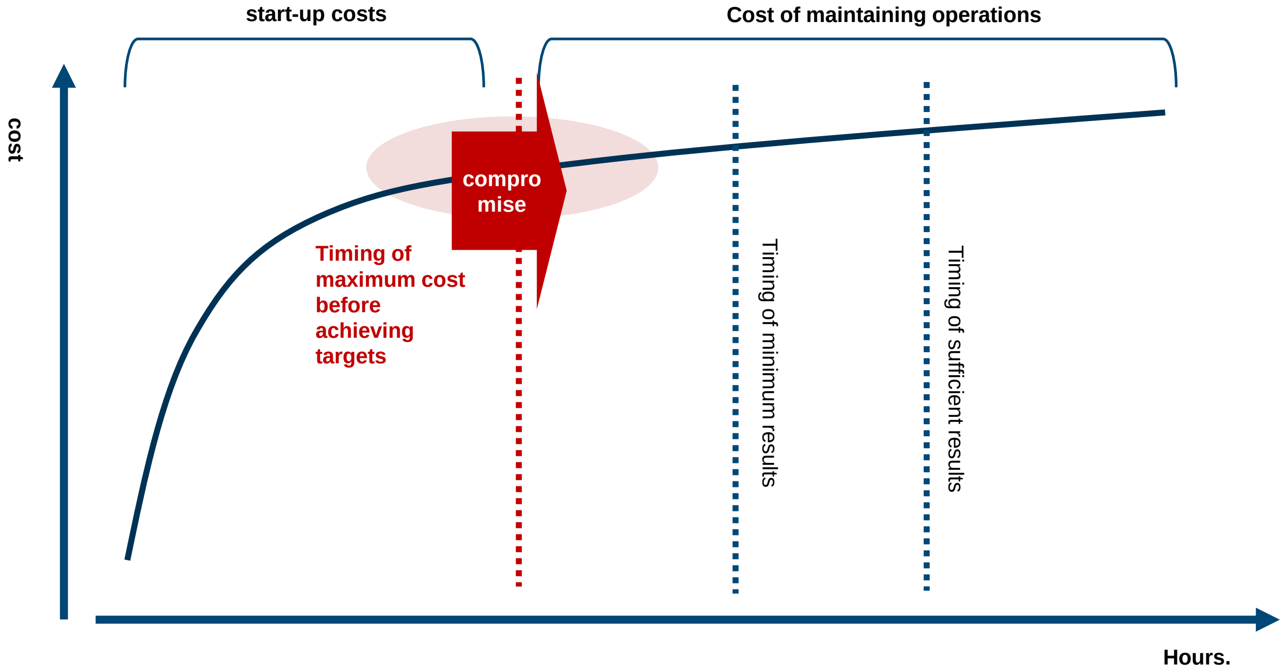


Punitive inhibition

negative inhibition

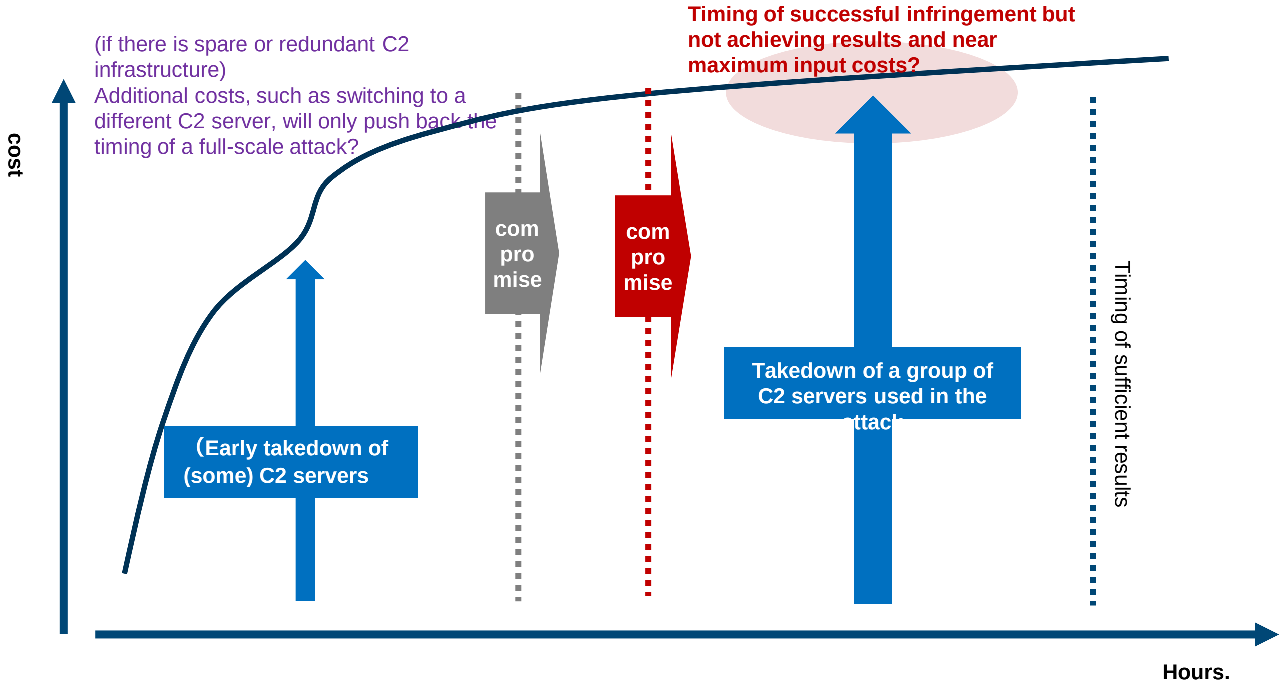
Rethink Attacker's Cost

- Isn't the phase immediately prior to a breach of the target organization the most costly phase, including preparation of human resources, malware development, preparation of attack infrastructure, target selection, and initial penetration route development?
- Could there be an approach that not only "imposes costs" but also generates/increases lost profits or sunk costs on the part of the attacker?


start-up costs
Cost of maintaining operations
cost
compro mise
Timing of maximum cost before achieving targets
Timing of minimum results
Timing of sufficient results
Hours.

Rethink Attacker's Cost

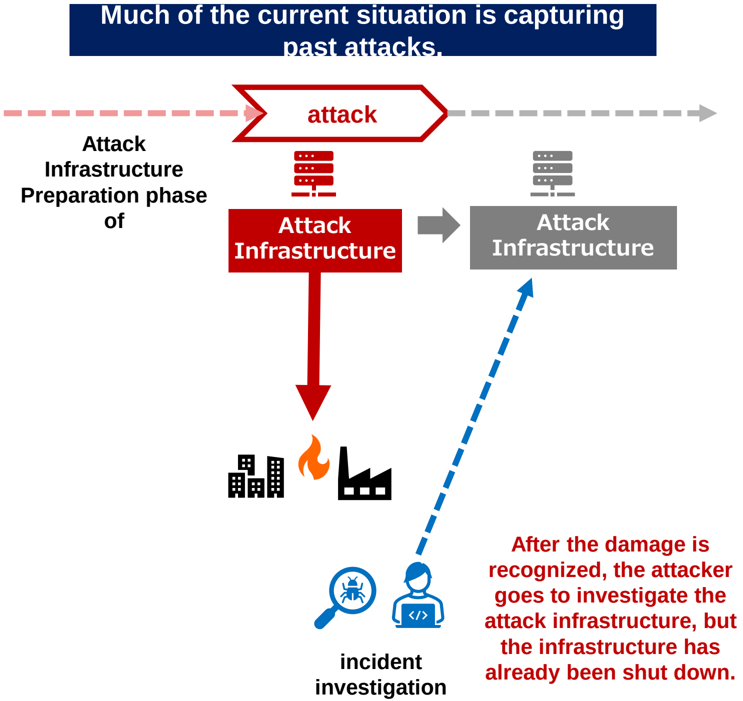
- Rather than capturing and taking down a portion of the C2 server population before full-scale attack activity, wouldn't it be more "costly" to abort the attack at a time when the attack has begun but the C2 server population can generally be captured and the sunk cost to the attacker is at its maximum?
- <u>**Accurate profiling of attackers is essential.**</u>


Timing of successful infringement but not achieving results and near maximum input costs?
(if there is spare or redundant C2 infrastructure)
Additional costs, such as switching to a different C2 server, will only push back the timing of a full-scale attack?
cost
com pro mise
com pro mise
Takedown of a group of C2 servers used in the attack
（Early takedown of (some) C2 servers
Timing of sufficient results
Hours.

Individual tactics

Block Communication

- Even if legal and technical problems are solved, proactive measures cannot be taken unless the source of the unauthorized communication can be identified at an early stage.



Much of the current situation is capturing past attacks.

attack

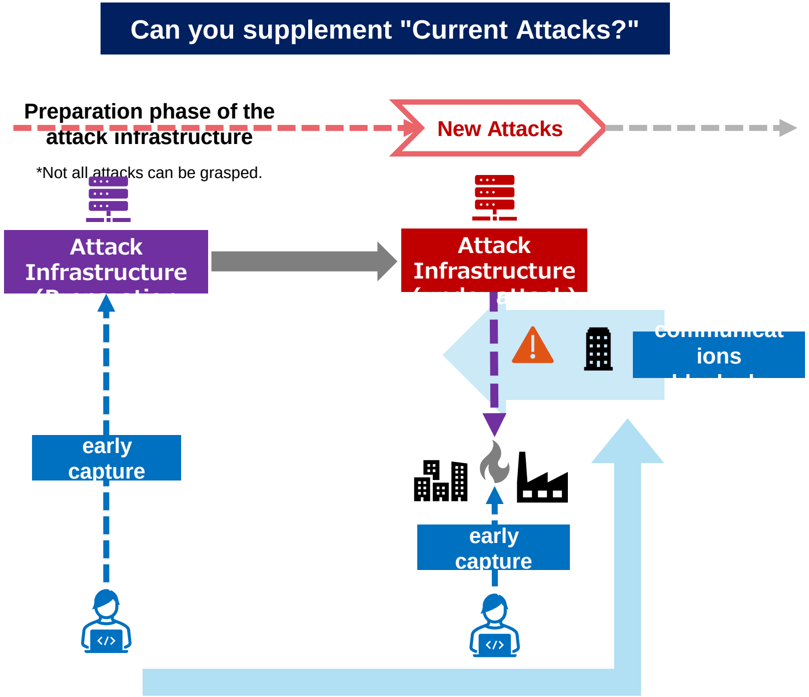
Attack Infrastructure Preparation phase of

Attack Infrastructure

Attack Infrastructure

incident investigation

After the damage is recognized, the attacker goes to investigate the attack infrastructure, but the infrastructure has already been shut down.



Can you supplement "Current Attacks?"

Preparation phase of the attack infrastructure

New Attacks

*Not all attacks can be grasped.

Attack Infrastructure (Preparation

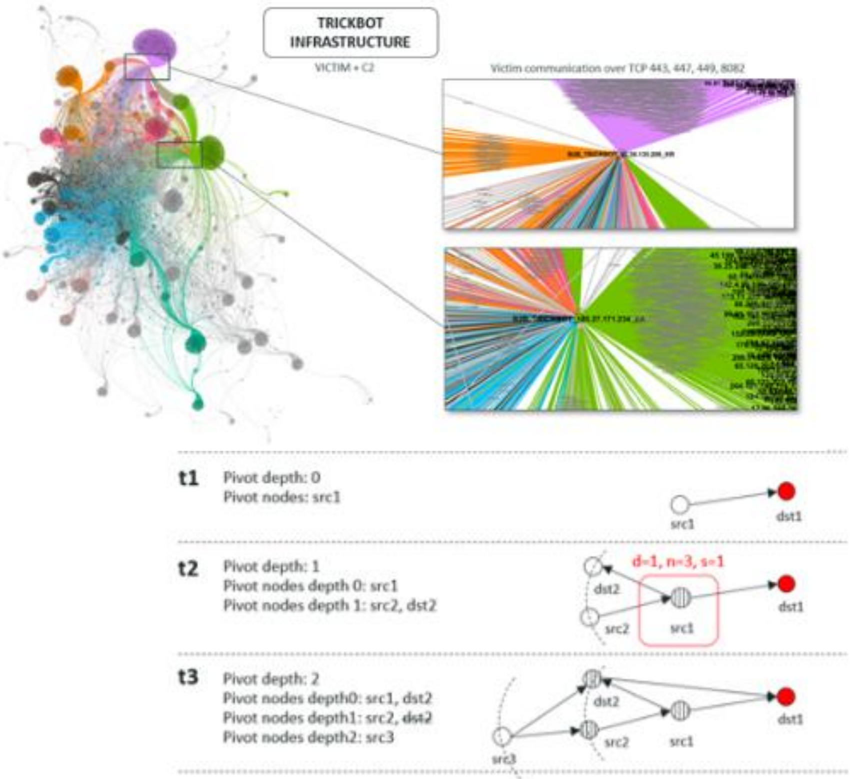
Attack Infrastructure (under attack)

Communications blocked

early capture

early capture

Example: Investigate infrastructure used for an attack



https://insight-jp.nttsecurity.com/post/102fvek/12-5-soc-trickbot

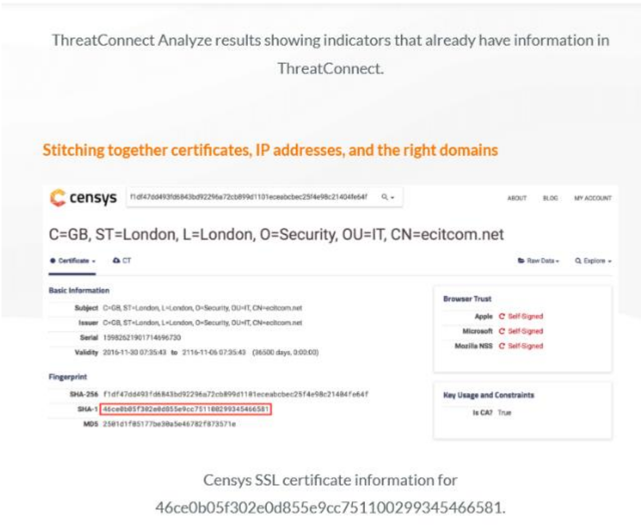
- Investigation of Trickbot's attack infrastructure configuration by analyzing Netflow data
- Verification of a method to locate the C2 server configuration that constitutes the attack infrastructure based on the characteristics of the botnet network connectivity.
- Extract communications from Netflow data that have characteristics that match the botnet infrastructure configuration and communication patterns.

Note that the take-down of Trickbot itself (October 2020) failed (*explains later).

Can we investigate infrastructure used for an attack (C2 hunting)?

- Past investigations by ThreatConnect
- Investigate non-known C2 servers based on characteristics of SSL certificates commonly used by APT28 (Sofacy) C2 servers.

ThreatConnect



ThreatConnect Analyze results showing indicators that already have information in ThreatConnect.

Stitching together certificates, IP addresses, and the right domains

censys
f1df47dd493fd6843bd92296a72cb899d1101eceabcbec25f4e98c21404fe64f
ABOUT
BLOG
MY ACCOUNT
Certificate
CT
Raw Data
Explore

C=GB, ST=London, L=London, O=Security, OU=IT, CN=ecitcom.net

Basic Information

Subject	C=GB, ST=London, L=London, O=Security, OU=IT, CN=ecitcom.net
Issuer	C=GB, ST=London, L=London, O=Security, OU=IT, CN=ecitcom.net
Serial	15982621901714696730
Validity	2016-11-30 07:35:43 to 2116-11-06 07:35:43 (36500 days, 0:00:00)

Fingerprint

SHA-256	f1df47dd493fd6843bd92296a72cb899d1101eceabcbec25f4e98c21404fe64f
SHA-1	46ce0b05f302e0d855e9cc751100299345466581
MD5	2501d1f05177be30a5e46782f873571e

Browser Trust

Apple	Self-Signed
Microsoft	Self-Signed
Mozilla NSS	Self-Signed

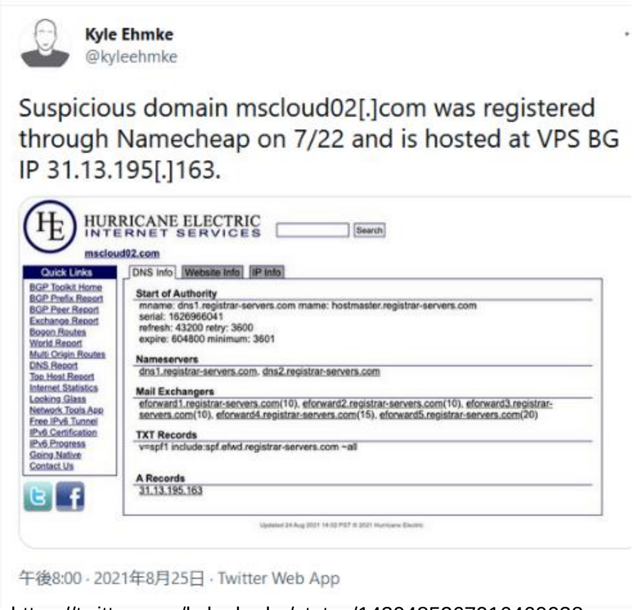
Key Usage and Constraints

Is CA?	True

Censys SSL certificate information for 46ce0b05f302e0d855e9cc751100299345466581.

https://threatconnect.com/blog/using-fancy-bear-ssl-certificate-information-to-identify-their-infrastructure/

- Search for suspicious domains based on the characteristics of the registrar, name server, acquisition date, and IP address/hosting service associated with the domain, which are frequently used by the attacker.



Kyle Ehmke
@kyleehmke

Suspicious domain mscloud02[.]com was registered through Namecheap on 7/22 and is hosted at VPS BG IP 31.13.195[.]163.

mscloud02.com

Start of Authority
mname: dns1.registrar-servers.com rname: hostmaster.registrar-servers.com
serial: 1626966041
refresh: 43200 retry: 3600
expire: 604800 minimum: 3601

Nameservers
dns1.registrar-servers.com, dns2.registrar-servers.com

Mail Exchangers
eforward1.registrar-servers.com(10), eforward2.registrar-servers.com(10), eforward3.registrar-servers.com(10), eforward4.registrar-servers.com(15), eforward5.registrar-servers.com(20)

TXT Records
v=spf1 include:spf.efwd.registrar-servers.com ~all

A Records
31.13.195.163

Updated 24 Aug 2021 14:02 PST © 2021 Hurricane Electric

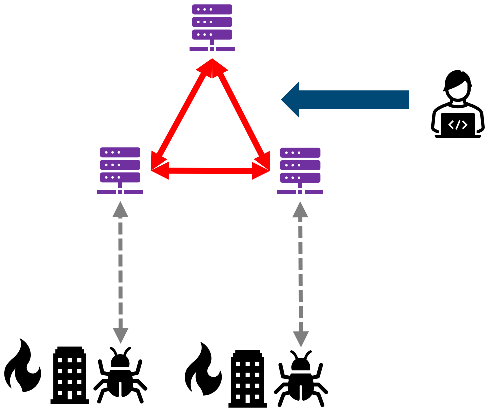
午後8:00 · 2021年8月25日 · Twitter Web App

https://twitter.com/kyleehmke/status/1430485267916460038

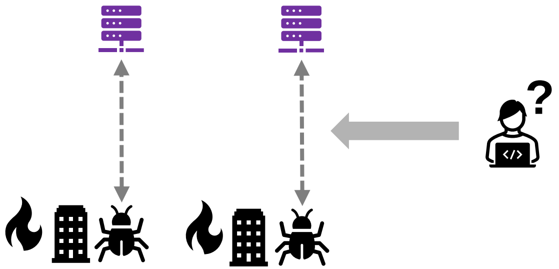
Can we do a proactive C2 search?

- Revision of the Guidelines
  - Allow investigation and identification of C2 using Net Flow information
  - Immediate shutdown is not envisioned at this time.
- By using Net Flow information, we can search attack infrastructures, such as botnets, that have characteristic intercommunication between C2s, but we cannot search C2 servers that exist on their own.

Search by the known infrastructure configurations



How do we search a single attack infrastructure?



Effectiveness of Blocking Communication

*Assuming this measure as a counter to APT.

- Advantages over other countermeasures
  - Can be implemented before damage occurs
  - Low response cost burden on an affected organization
  - Can be implemented at the time of maximum cost to attackers

- Limitations of effectiveness as a countermeasure

  Can only be performed on attack activities that have some accumulated information on known attackers/infrastructure (e.g., large botnets that have been in operation for some time).

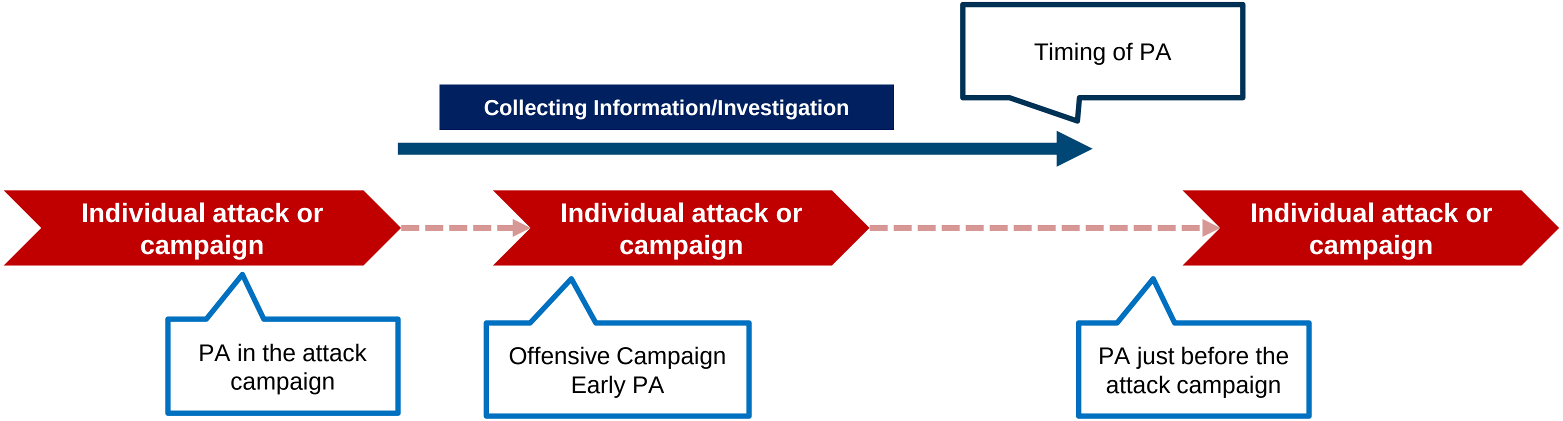
  - Attacker can switch to another C2 server after blocking
  - Attacker can take a redundancy measure based on the assumption that communication is blocked.
  - May become an endless battle (continually increasing the burden on telecommunications carriers)

- Issue
  - Only a limited number of attack communications can be captured by NetFlow information alone
  - Need to comprehensively capture unidentified attack infrastructures based not only on observed attack infrastructures at the damage site, but also on the features of each attack group

  ⇒Profiling of attackers is important

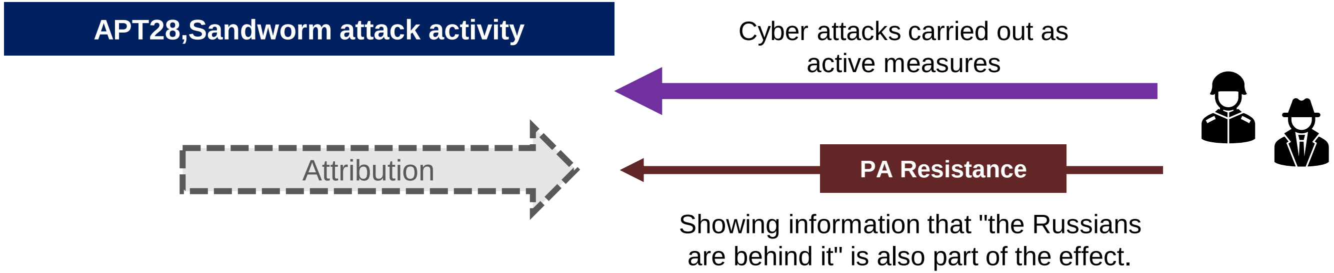
"Public Attribution" issue

- Content, granularity, and timing of public attribution (PA) depends on who the "audience" is
  - To contain attackers?
  - To contain the background entity?
  - To draw attention?
  - To appeal to the relations with allies?
  - To appeal to the international community?


Timing of PA
Collecting Information/Investigation
Individual attack or campaign
Individual attack or campaign
Individual attack or campaign
PA in the attack campaign
Offensive Campaign Early PA
PA just before the attack campaign

Public Attribution "tolerance" issue

- Myth of Public Attribution
- There are many attack activities/groups that are highly attribution "resistant".
- **<u>Accurate profiling of attackers is critical.</u>**



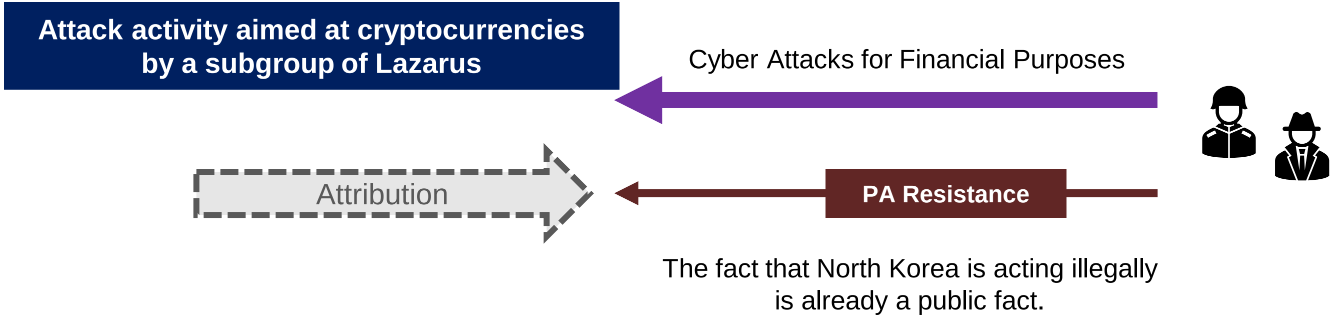
APT28,Sandworm attack activity

Cyber attacks carried out as active measures

Attribution

PA Resistance

Showing information that "the Russians are behind it" is also part of the effect.



Attack activity aimed at cryptocurrencies by a subgroup of Lazarus

Cyber Attacks for Financial Purposes

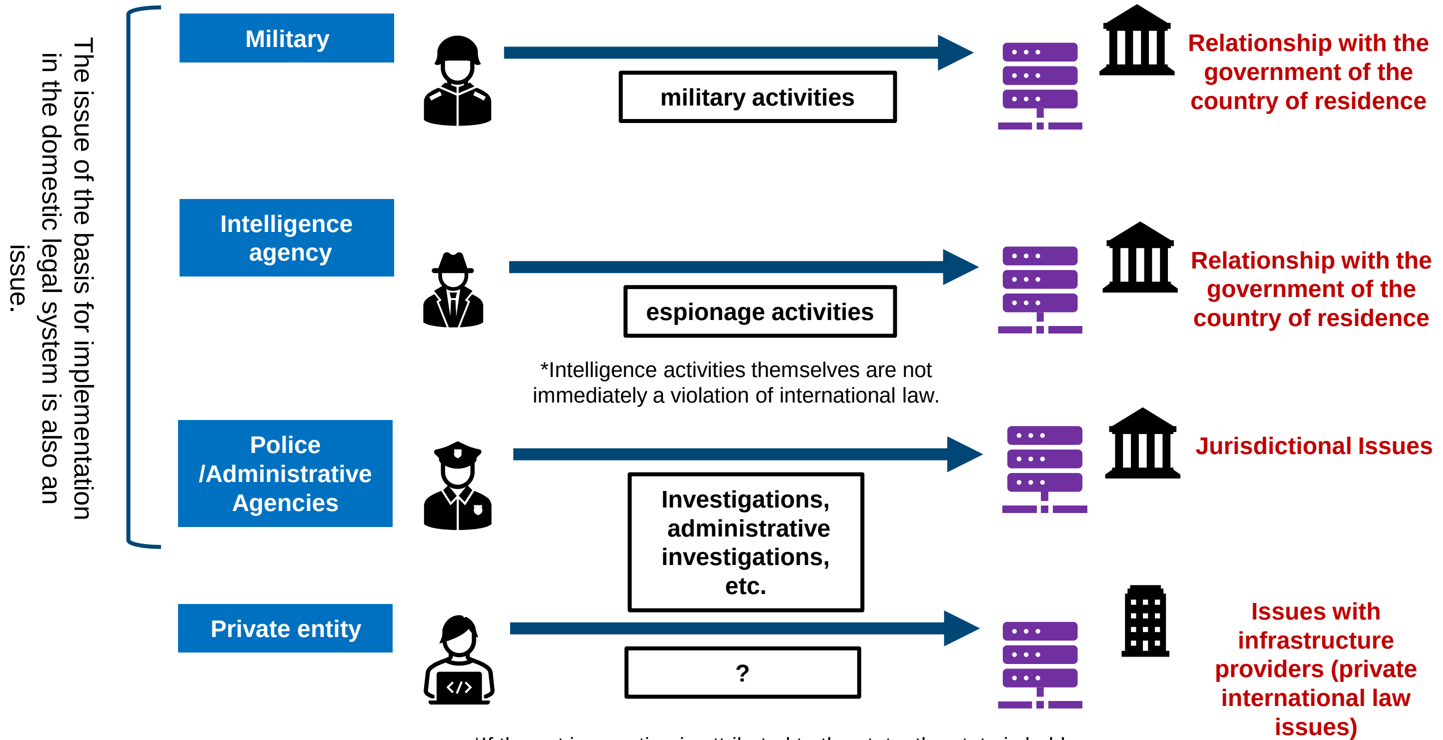
Attribution

PA Resistance

The fact that North Korea is acting illegally is already a public fact.

"Active" cross-border access - who will do it?

- The same access may have different purposes and legal characteristics depending on the entity.



The issue of the basis for implementation in the domestic legal system is also an issue.

Military

military activities

Relationship with the government of the country of residence

Intelligence agency

espionage activities

Relationship with the government of the country of residence

*Intelligence activities themselves are not immediately a violation of international law.

Police /Administrative Agencies

Investigations, administrative investigations, etc.

Jurisdictional Issues

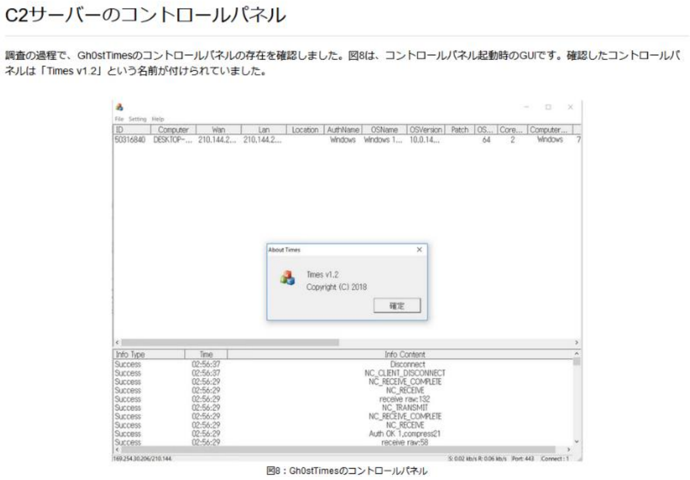
Private entity

?

Issues with infrastructure providers (private international law issues)

*If the act in question is attributed to the state, the state is held responsible.

Case Study: BlackTech's C2 Server Survey



C2サーバーのコントロールパネル

調査の過程で、Gh0stTimesのコントロールパネルの存在を確認しました。図8は、コントロールパネル起動時のGUIです。確認したコントロールパネルは「Times v1.2」という名前が付けられていました。

ID	Computer	Wan	Lan	Location	AuthName	OSName	OSVersion	Patch	OS...	Core...	Computer...	
50316840	DESKTOP-...	210.144.2...	210.144.2...		Windows	Windows 1...	10.0.14...		64	2	Windows	7

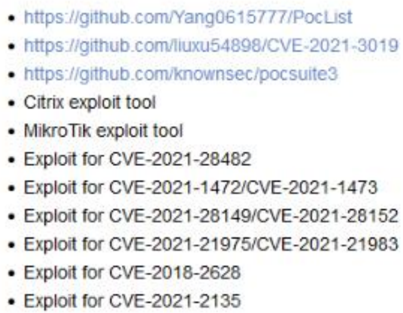
About Times

Times v1.2
Copyright (C) 2018

Info Type	Time	Info Content
Success	02:56:37	Disconnect
Success	02:56:37	NC_CLIENT_DISCONNECT
Success	02:56:29	NC_RECEIVE_COMPLETE
Success	02:56:29	NC_RECEIVE
Success	02:56:29	receive raw:132
Success	02:56:29	NC_TRANSMIT
Success	02:56:29	NC_RECEIVE_COMPLETE
Success	02:56:29	NC_RECEIVE
Success	02:56:29	Auth OK 1,compress21
Success	02:56:29	receive raw:58

```
169.254.30.206/210.144          S: 0.02 kb/s R: 0.06 kb/s   Port: 443   Connect : 1
```

図8：Gh0stTimesのコントロールパネル



- https://github.com/Yang0615777/PocList
- https://github.com/liuxu54898/CVE-2021-3019
- https://github.com/knownsec/pocsuite3
- Citrix exploit tool
- MikroTik exploit tool
- Exploit for CVE-2021-28482
- Exploit for CVE-2021-1472/CVE-2021-1473
- Exploit for CVE-2021-28149/CVE-2021-28152
- Exploit for CVE-2021-21975/CVE-2021-21983
- Exploit for CVE-2018-2628
- Exploit for CVE-2021-2135

- JPCERT/CC’s blog post on September 2021
- The possibility of a distraction on the part of the attacker or a "trap" for the investigator was also assumed.
- Information from closer proximity to the attacker, such as the attack infrastructure or the attacker's "arsenal," increases the accuracy of attacker profiling

Malware Gh0stTimes used by JPCERT/CC attack group BlackTech
https://blogs.jpcert.or.jp/ja/2021/09/gh0sttimes.html

"Active" Cross-border Access - Where to "Fight Back"

- Not only is it a matter of information acquisition and timing, but it is forgotten that the "counterattack" is basically on the (foreign) civilian infrastructure.

Problem of not finding a counterattack "destination" due to time constraints.

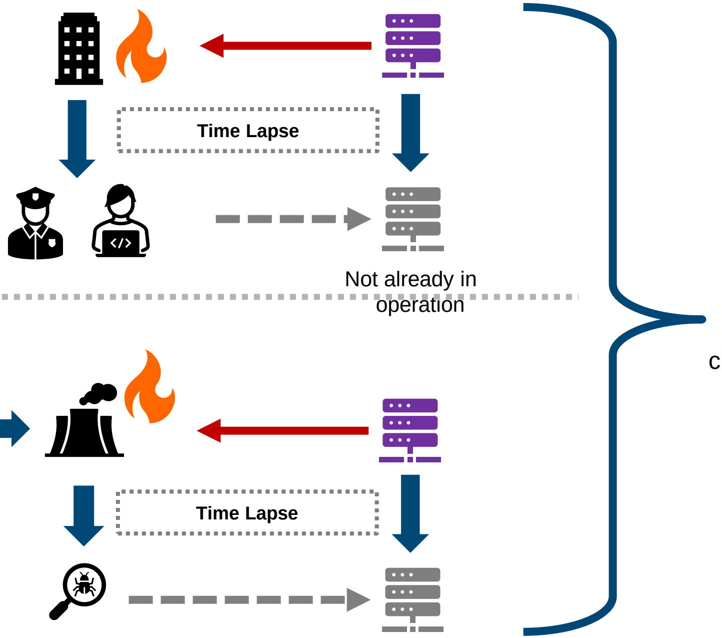
General Unauthorized Access Cases

In many cases, the attack is over by the time it is recognized).

Slow intervention by a third party

Large-Scale Cyber Incidents

It is difficult for a third party to intervene to investigate a security incident when the priority is on restoration, etc.



The question of whether counterattack is appropriate.

Attack infrastructure is basically running on private servers.

Even if it is due to fraudulent contracts, there is a problem of damage to the infrastructure provider itself or other subscribers due to counterattacks.

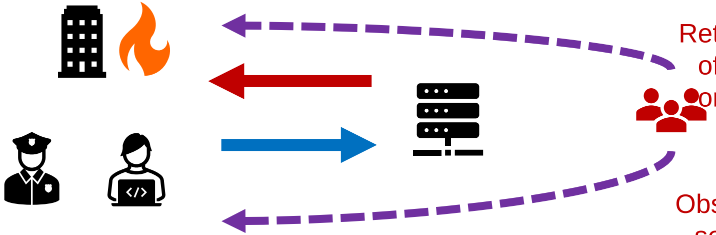
cloud computing provider
hosting company
ISP, etc.

"Active" Cross-border Access - What Happens After "Fighting Back"?

- Need to discuss technically/operationally realistic assumptions for each attacker
- In particular, there is no preliminary knowledge of how to prepare for countermeasures or "counterattacks" on the part of the attacker against countermeasures

If an ongoing attack is recognizable

In addition to takedown, C2 servers can be shut down by direct manipulation.
Conduct cyber attack to attackers



What will the attacker do?

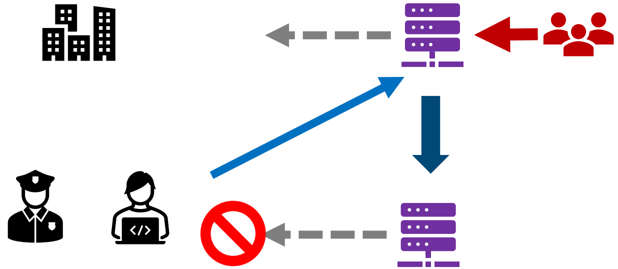
Retaliation/disturbance/destruction of evidence against the victim organization

Obstructing investigations, retaliating, setting "traps"

If the preparation of attack is captured

. It is unclear if the attack is targeting domestic organizations. However, assumingly it is prepared by the actor who has attacked in the past.

Domain takedown
Prepare for (immediate) communication blocking and filtering
Disable by direct operation



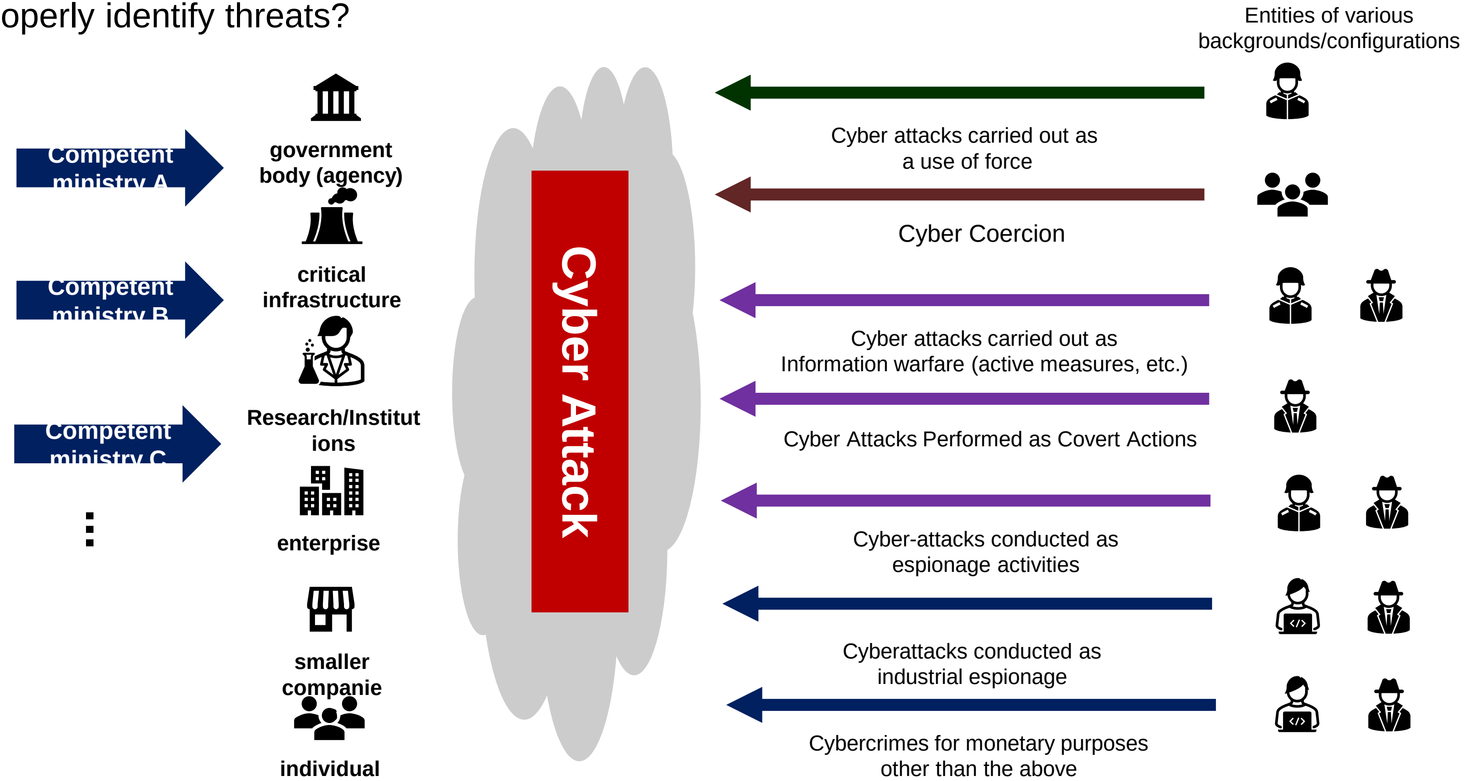
What will the attacker do?

Extensive use of legitimate server tampering and botnets
Takeover/abuse of legitimate infrastructure within the target country
Leading to "decoy" attack infrastructure

The Importance of Profiling

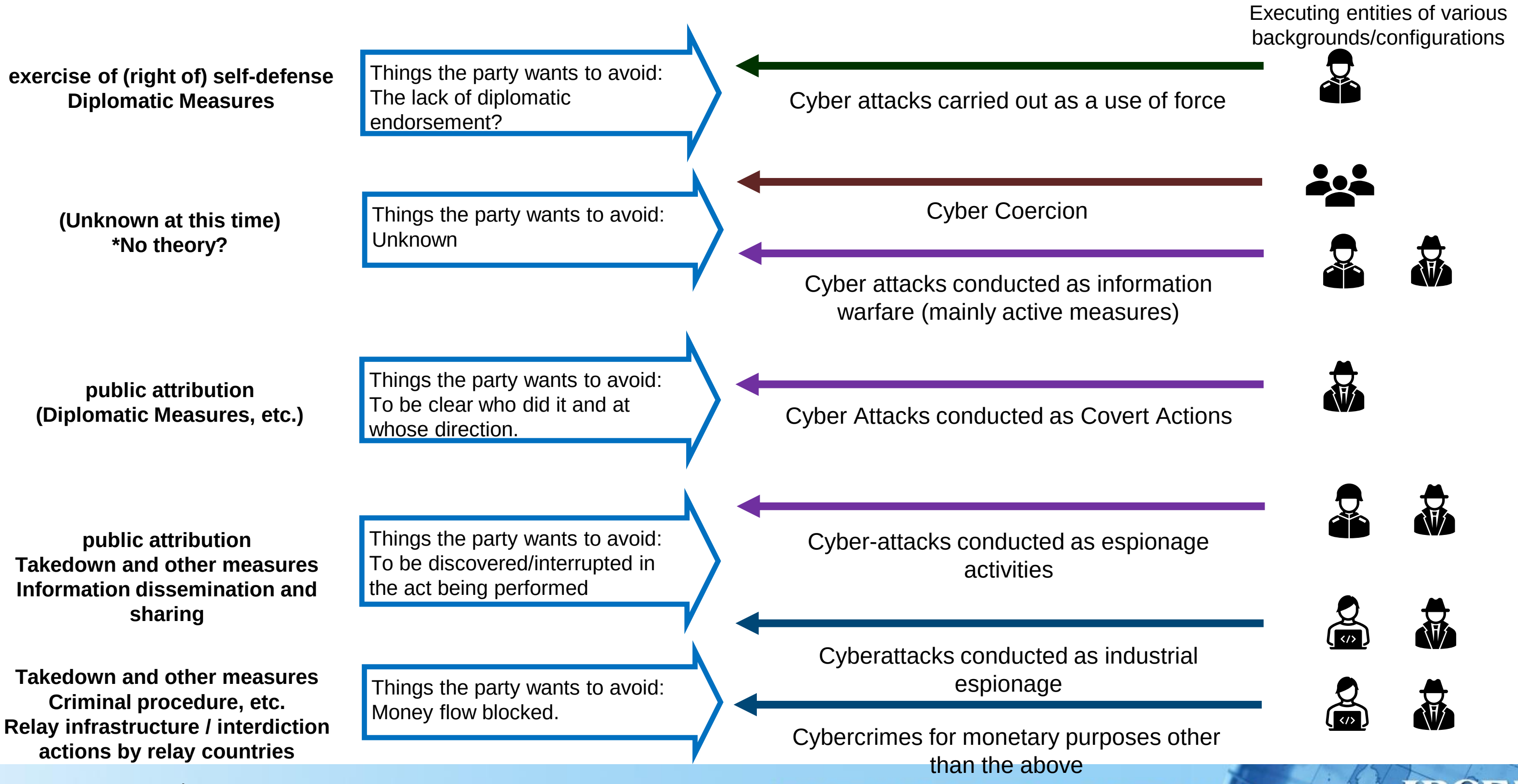
Identify threats correctly

- Various attack activities with completely different objectives/entities are all described as "cyber-attacks“ and are basically handled by the affected industry/sector.
- Do we properly identify threats?


Entities of various backgrounds/configurations
Competent ministry A
Competent ministry B
Competent ministry C
⋮
government body (agency)
critical infrastructure
Research/Institutions
enterprise
smaller companie
individual
Cyber Attack
Cyber attacks carried out as a use of force
Cyber Coercion
Cyber attacks carried out as Information warfare (active measures, etc.)
Cyber Attacks Performed as Covert Actions
Cyber-attacks conducted as espionage activities
Cyberattacks conducted as industrial espionage
Cybercrimes for monetary purposes other than the above

Effective countermeasures according to threat characteristics

- Effective countermeasures vary depending on the purpose of the attack/the entity carrying out the attack
- **Profiling of attackers is critical.**



Executing entities of various backgrounds/configurations

exercise of (right of) self-defense
Diplomatic Measures

Things the party wants to avoid: The lack of diplomatic endorsement?

Cyber attacks carried out as a use of force

(Unknown at this time)
***No theory?**

Things the party wants to avoid: Unknown

Cyber Coercion

Cyber attacks conducted as information warfare (mainly active measures)

public attribution
(Diplomatic Measures, etc.)

Things the party wants to avoid: To be clear who did it and at whose direction.

Cyber Attacks conducted as Covert Actions

public attribution
Takedown and other measures
Information dissemination and sharing

Things the party wants to avoid: To be discovered/interrupted in the act being performed

Cyber-attacks conducted as espionage activities

Cyberattacks conducted as industrial espionage

Takedown and other measures
Criminal procedure, etc.
Relay infrastructure / interdiction actions by relay countries

Things the party wants to avoid: Money flow blocked.

Cybercrimes for monetary purposes other than the above

From the past cases

Overseas examples of (pro)active operations

- **Soft**

  - Prompt sharing/publication of information in the 2014 Sony Picture Entertainment case
  - Early information sharing/publication on multiple wiper prior to the 2022 invasion of Ukraine

- **(Relatively) soft**

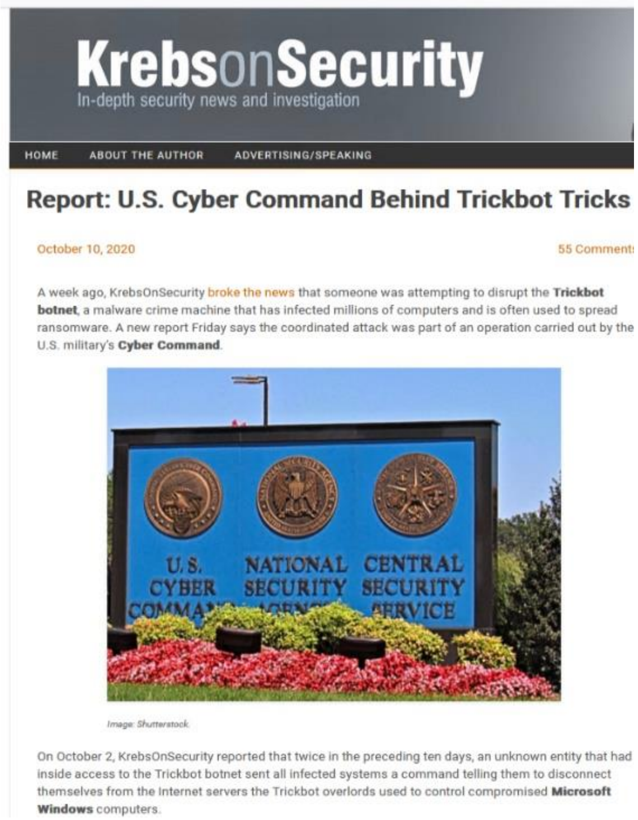
  - Takedown using civil injunctive proceedings against APT28-related domains in Microsoft Corporation prior to the 2018 U.S. midterm elections.

- **Hard**

  *Technical effectiveness is unknown.

  - Cyber operations by U.S. Cyber Command against Russian IRA infrastructure prior to 2018 midterm elections (details unknown)
  - 2019 Operation by the U.S. Cyber Command against the infrastructure of a cyber attack group that claims to have been involved in the attack in retaliation for the Strait of Hormuz tanker attack (details unknown).
  - 2020 Trickbot takedown operations and operations by U.S. Cyber Command (details unknown)

Assessment of Operations Against Trickbot on October 2020



KrebsonSecurity

In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Report: U.S. Cyber Command Behind Trickbot Tricks

October 10, 2020 55 Comment

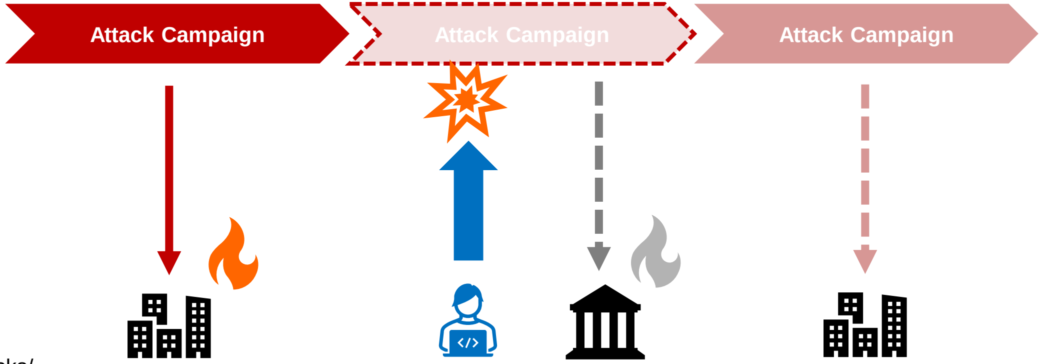
A week ago, KrebsOnSecurity broke the news that someone was attempting to disrupt the **Trickbot botnet**, a malware crime machine that has infected millions of computers and is often used to spread ransomware. A new report Friday says the coordinated attack was part of an operation carried out by the U.S. military's **Cyber Command**.

Image: Shutterstock

On October 2, KrebsOnSecurity reported that twice in the preceding ten days, an unknown entity that had inside access to the Trickbot botnet sent all infected systems a command telling them to disconnect themselves from the Internet servers the Trickbot overlords used to control compromised **Microsoft Windows** computers.

https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/

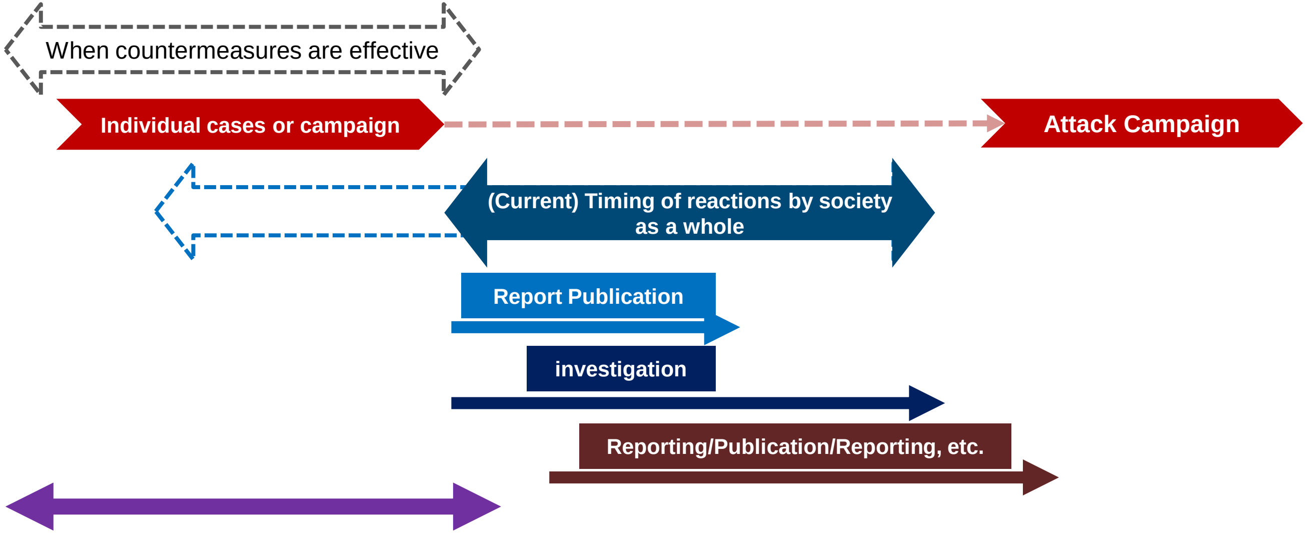
- Domain Injunction Proceedings by Microsoft
- In addition, the possibility of a "disruption" operation by U.S. cyber forces
- The fact that Trickbot did not completely cease its activities after a series of responses led to a series of negative views of the U.S. Cyber Command's operations.
- On the other hand, the response was made in advance of the U.S. presidential election in November 2020, and some believe that it was not exploited in a large-scale attack that could have affected the presidential election during the period in question.



Further Issues to Consider

Rethink how to obtain information on the edge

- The earlier it is, the more options for countermeasures
- No single organization (security vendor, specialized agency, police, etc.) can consider and implement countermeasures alone
- Even if recognized early by individual organizational units, if it takes time/coordination costs to be shared among the organizations involved, the time needed to consider countermeasures will be consumed.
- Limitations of detailed information on the affected organization

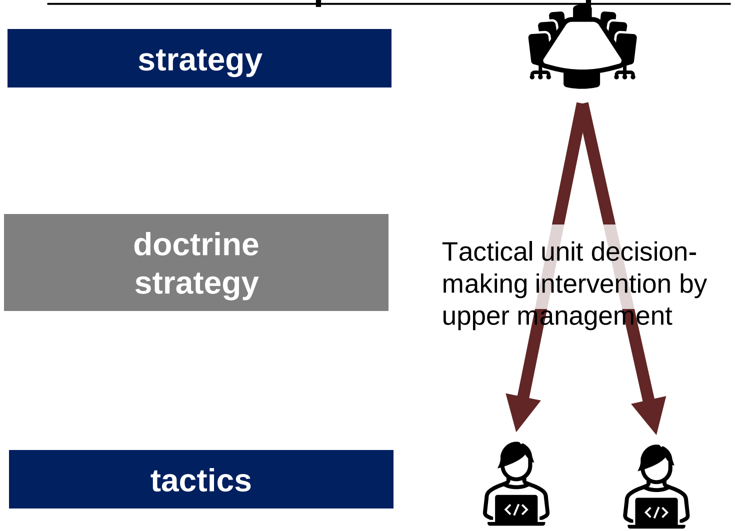

When countermeasures are effective
Individual cases or campaign
Attack Campaign
(Current) Timing of reactions by society as a whole
Report Publication
investigation
Reporting/Publication/Reporting, etc.

Delayed communication of information to third parties
Delayed sharing among organizations that intervened in the case
Conflict between information sharing/dissemination/tracking

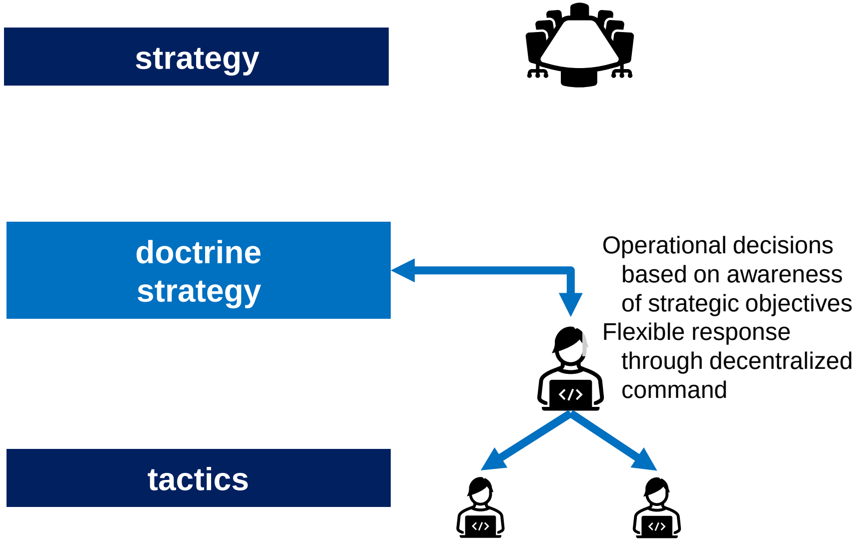
Who will make the decision to do this?

- Strategic decision-making layers should not interfere with detailed tactical unit decision-making in the field.
- Each unit/commander chooses the tactics necessary for its objectives based on doctrine
- Decentralized command will be necessary to ensure mobility ← Need to secure sufficient human resources to withstand this

A classic example of a failed operation


strategy
doctrine
strategy
tactics
Tactical unit decision-making intervention by upper management

What the "Art of Operation" is all about


strategy
doctrine
strategy
tactics
Operational decisions based on awareness of strategic objectives
Flexible response through decentralized command

Impact of professional organizations and analysts

The activities of professional organizations and analysts
will become even more important.

Relationship to previous activities

- How can we respond to retaliation or interference from the attacker after an "offensive" countermeasure has been taken? How can we assume this?
- How to accept that the APT group will be less traceable after a disruptive operation
- Will there be any restrictions on the dissemination of information by individual analysts, security companies, and researchers with autonomy?

Newly required roles

- Response to the issue of who will do the evaluation after a positive operation has taken place.
- Role of Analysts in External Evaluations Other Than Active Operations Performers
- Role as one of the parties involved in constantly evaluating the ethics of countermeasures

Summary

Building a "doctrine" of countermeasures

- Assemble countermeasures (selection) targeting the attack campaign ⇒ "5W1H" of countermeasures
- Theoretical organization is needed to determine when and for what purpose countermeasures should be implemented (not from existing deterrence theory, but from new perspectives such as attacker cost)

Importance of Public-Private Partnerships

- New approaches to understanding information are needed for early recognition of attacks, not relying too heavily on "information provided by the victim organization.
- The more powerful countermeasures that require legal authority and the more the role of state institutions increases, the more the issue of response "timing" becomes a bottleneck, so that a close collaboration between state institutions that take (procedural) time but can initiate powerful measures, and soft but highly mobile private actors' activities Close coordination will be necessary.

Reevaluation of prior cases, case studies

- Even in the U.S., which is ahead of other countries, there is trial and error, and even the evaluation of past cases (measurement of effectiveness) has not yet been established. In addition, the actors/background entities to be confronted are also different. ⇒Simply trying to imitate "the same thing as overseas" is meaningless.
- Need to examine each technical/operational issue based on specific past case studies

Profiling, tracking and evaluation

- Accurate profiling of actors targeting their countries is necessary first, and the role of analysts becomes even more important.
- In order to evaluate the results of proactive operations, especially mid- to long-term impacts, it may be necessary to track/evaluate analysts from "outside" the organization conducting the operations.

There’s just on more thing…

https://www.hanmoto.com/bd/isbn/9784890634309#

- DWIGHT D. EISENHOWER, “Plans are useless, but planning is indispensable”
- When formulating strategic documents, it is often the case that participants are limited from the standpoint of preserving confidentiality.
- If the subordinate organizations that make up the organization do not have a sense of ownership, they will not have a sense that the strategy document prepared by a limited number of members is "their strategy”.
- Example of a higher-level strategy being shared as tacit knowledge
  - The policy of “containment” of the U.S. during the Cold War was not defined as an official strategy document, although George Kennan's "Long Telegram" and "X Article" existed.

Thank you