

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.

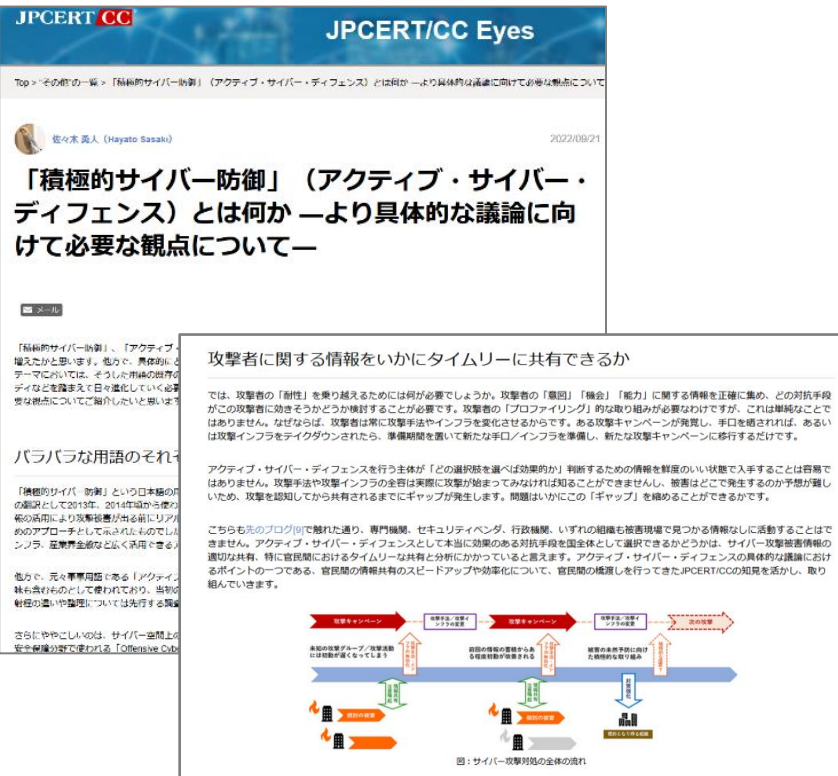
The "who's going to do it?" argument can essentially lead to a false means.

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.

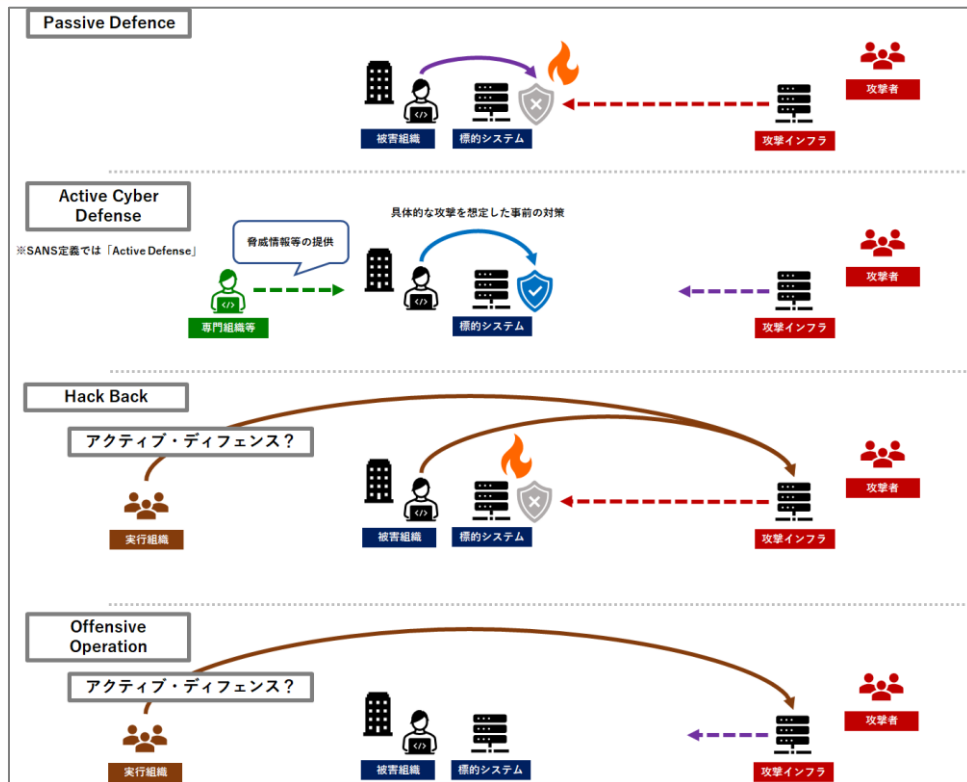
*While "criminal profiling" is well known for inferring criminals based on crime types and characteristics of crimes committed, this presentation will use it as an analysis of attacker groupings and attack characteristics and trends.



<https://blogs.ipcert.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



[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.

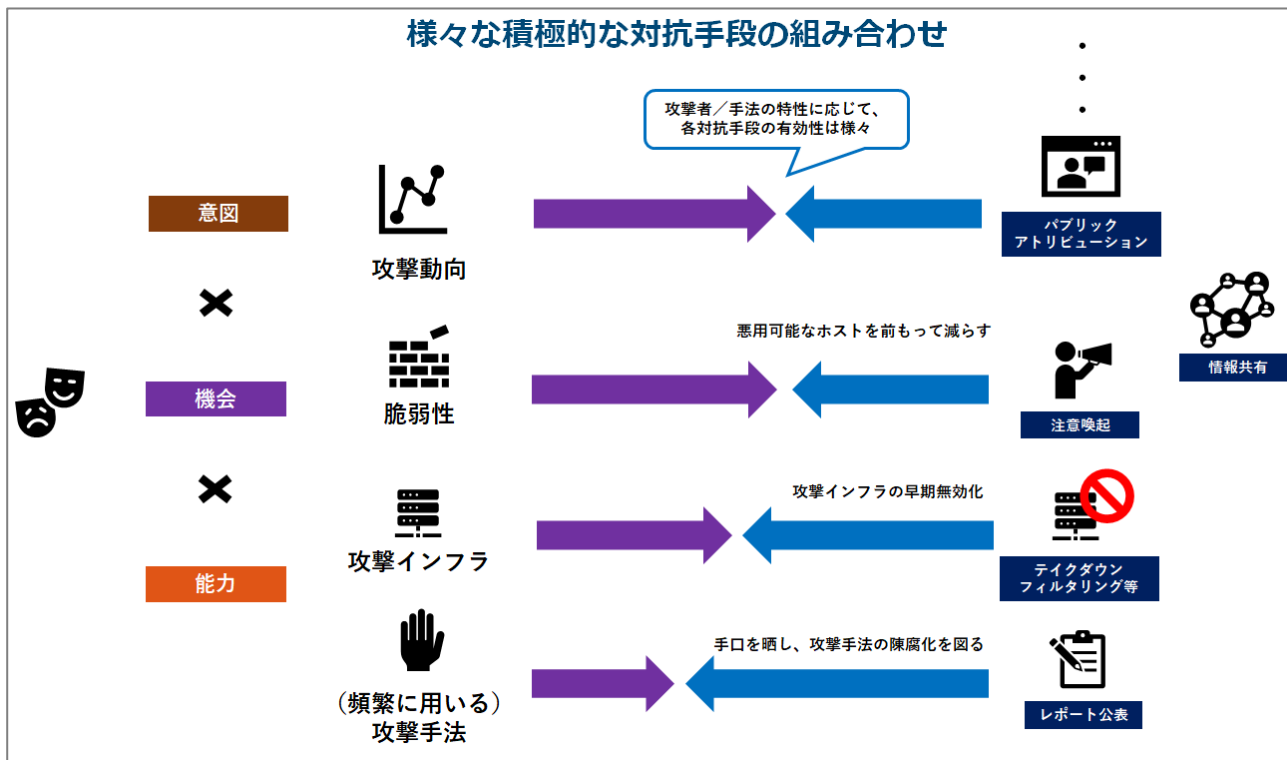
[Background].

- 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.

<https://blogs.jpccert.or.jp/ja/2022/09/active-cyber-defense.html>

From the research: Proactive countermeasure options

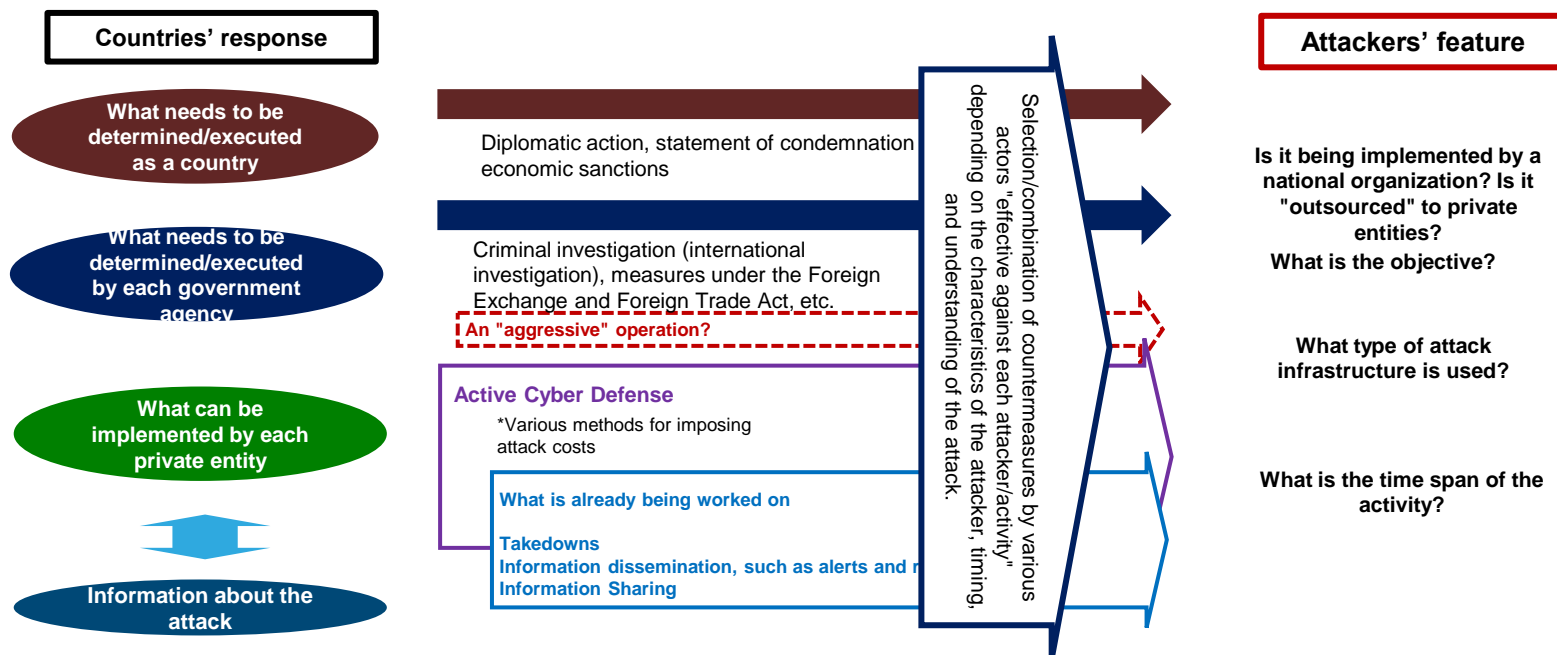
- Various proactive countermeasures exist in addition to offensive methods.



<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?**



...but in the end, we don't know about it yet.

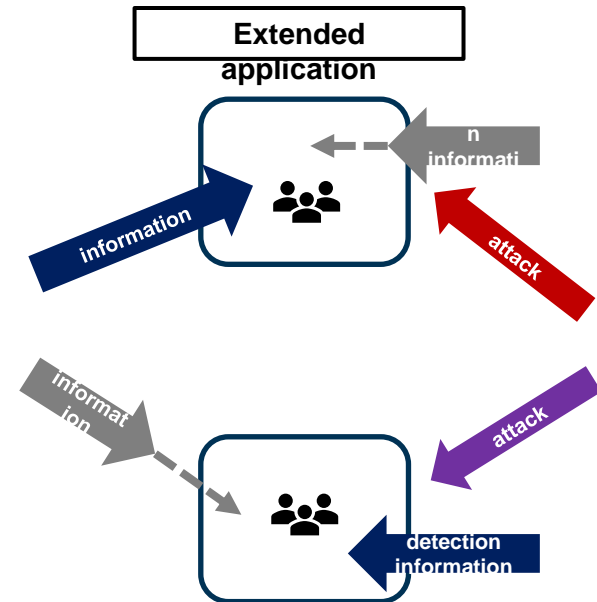
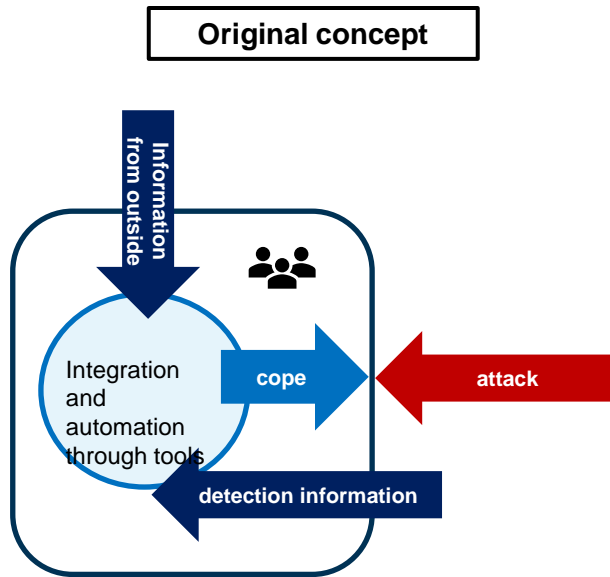
- Are we talking about responding to individual cases or the country as a whole?
- Should we respond before or after an attack?
- Is it to stop or interrupt offensive activity?



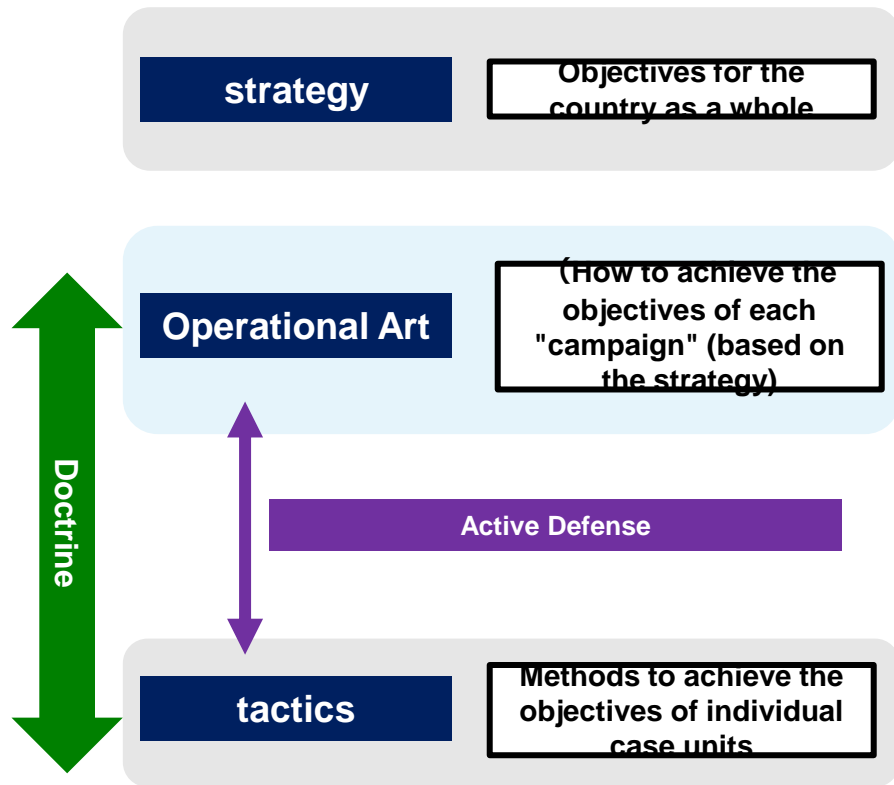
Let's look back at the “definition” of the word a bit

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.



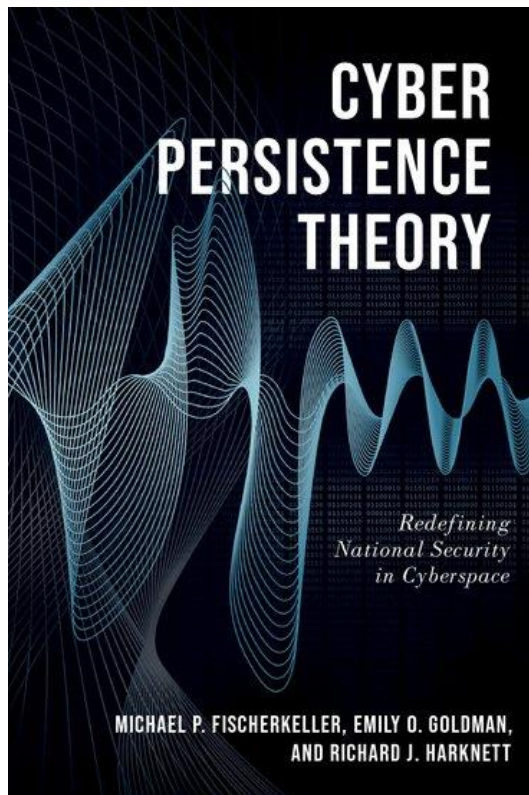
Origins of the ambiguity in "active cyber defense"



- 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

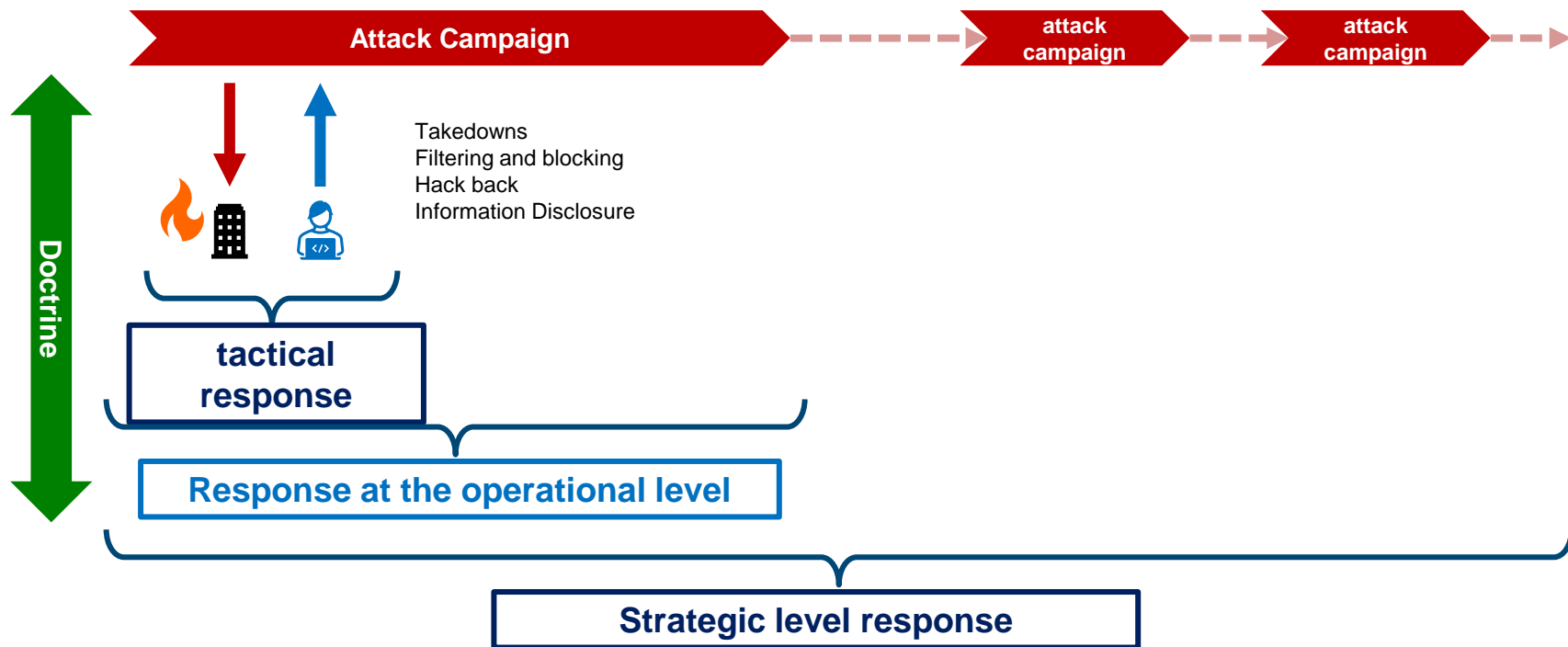


- Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, "CYBER PERSISTENCE THEORY," 2022
- He pointed out that most cyber attacks backed by state actors are not "coercion" but "exploitation" and "fait accompli."
- Evaluates and analyzes the history of countermeasure implementation in the U.S. 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.

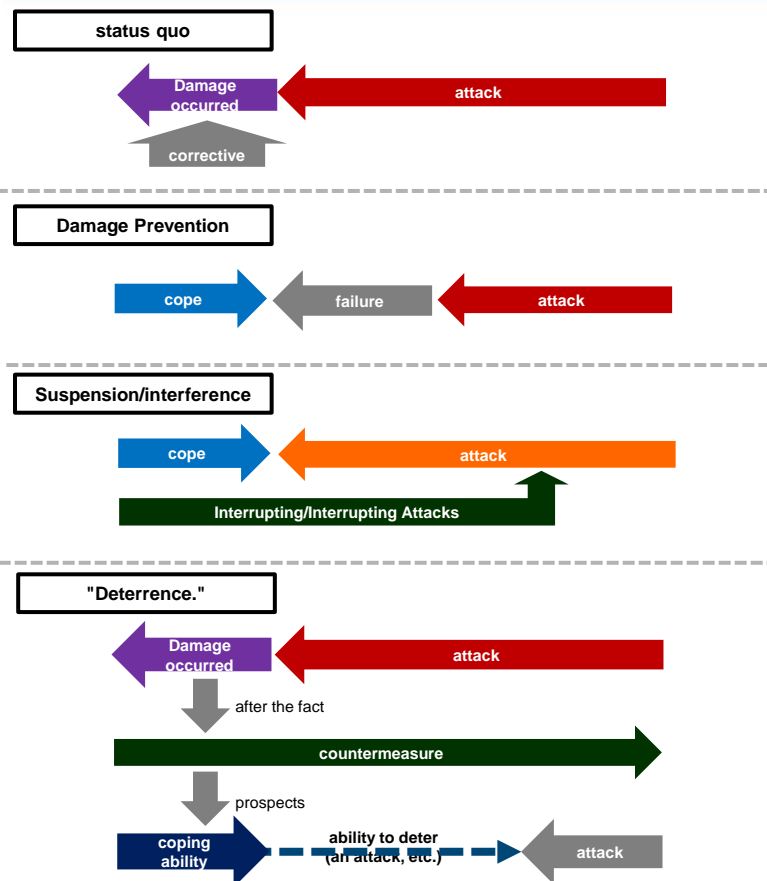
<https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&>

Active Cyber Defense as Doctrine

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



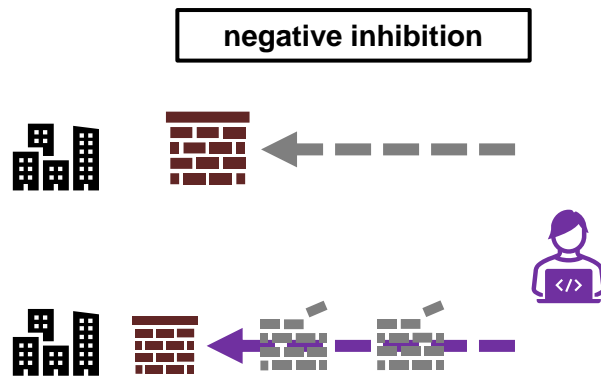
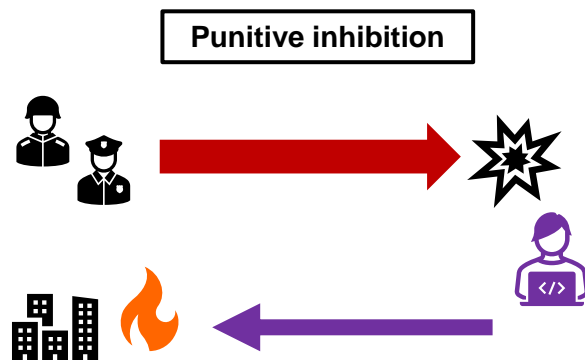
Point to consider a definition: timing and cost



- 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

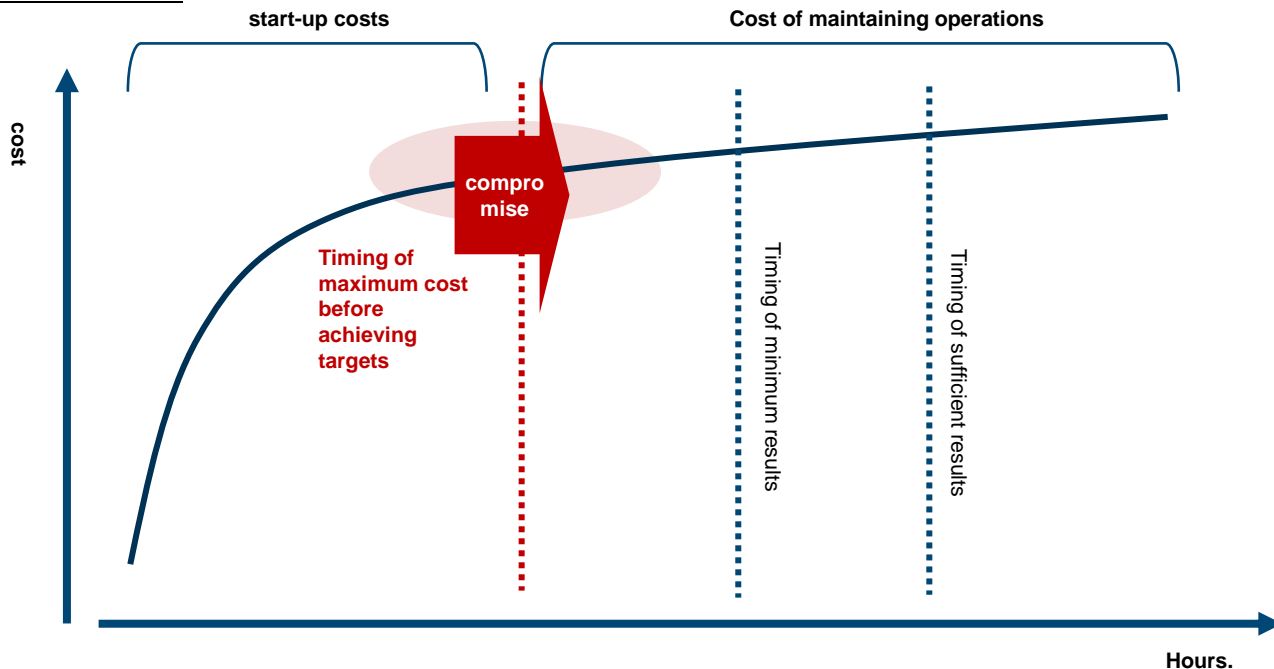
What does it mean to "impose a cost" on an attacker?

- 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.



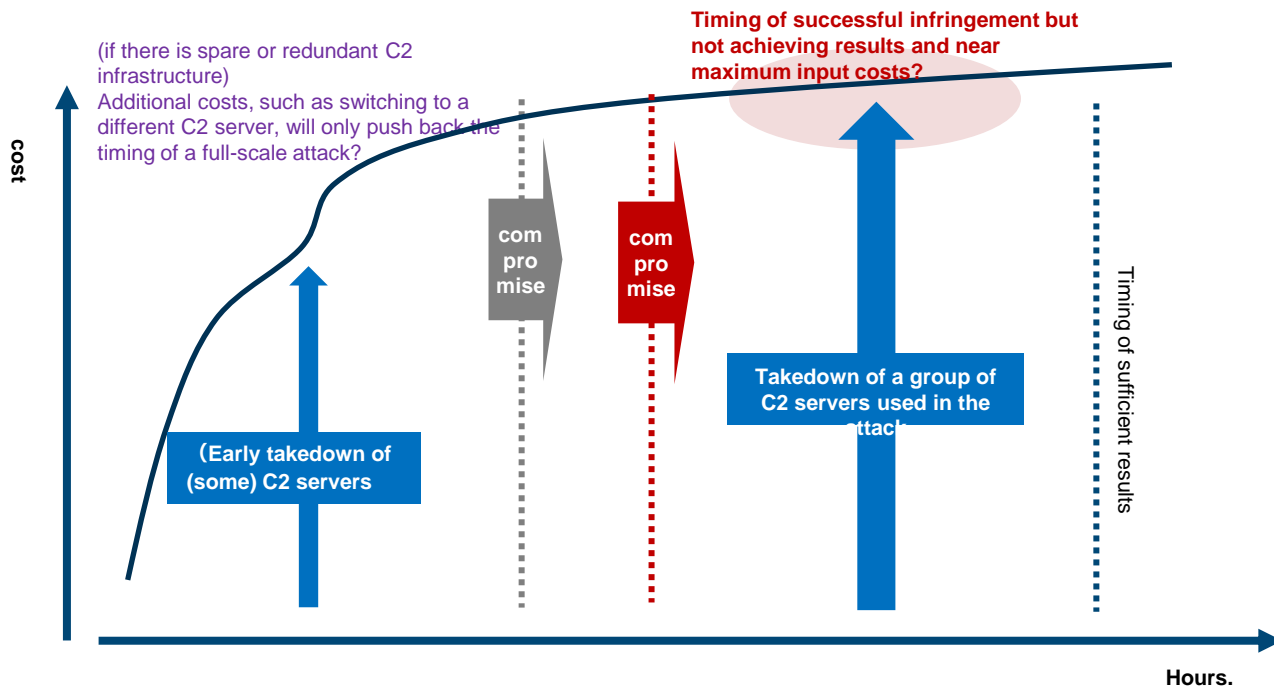
Rethink Attacker's Cost

- 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?



Rethink Attacker's Cost

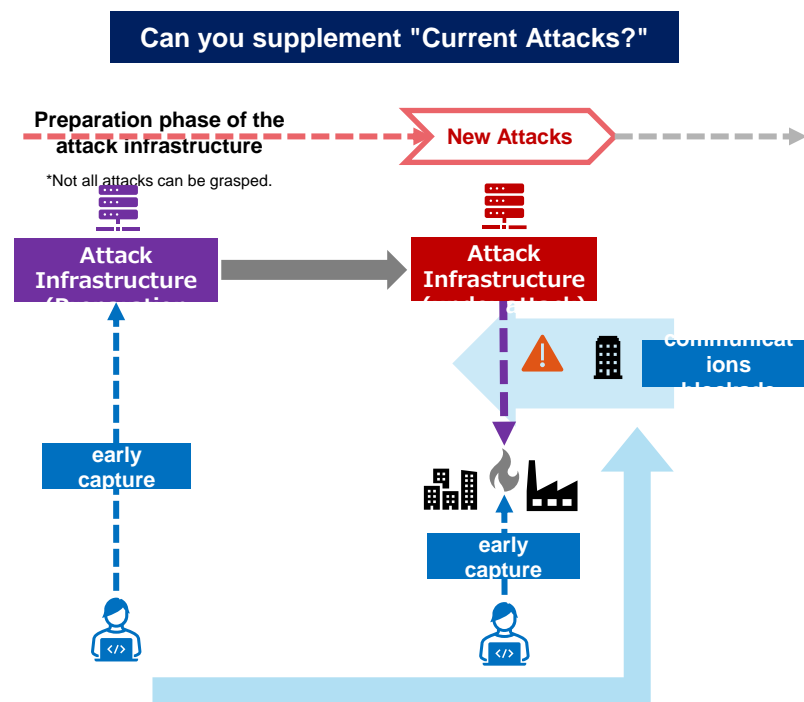
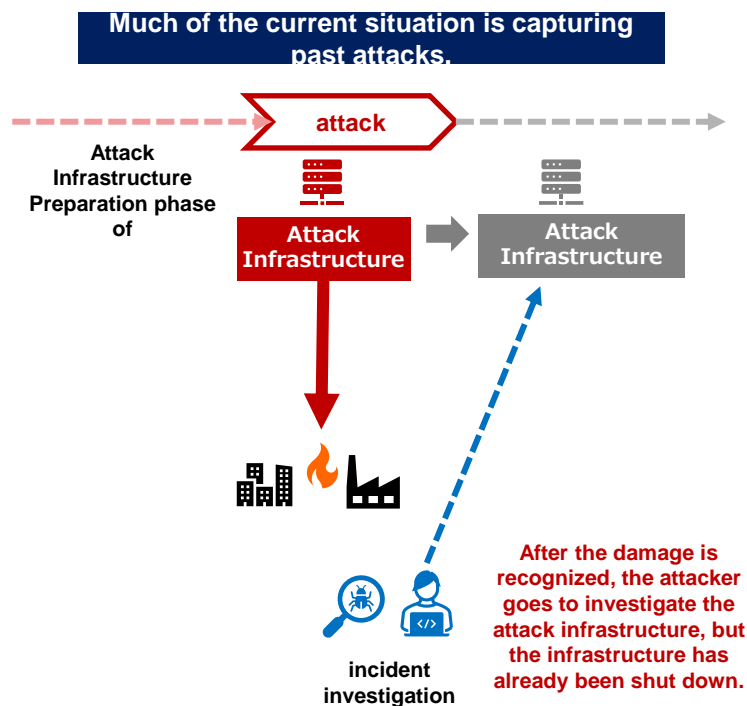
- Rather than capturing and taking down a portion of the C2 server population before full-scale attack activity, wouldn't it be more "costly" to abort the attack at a time when the attack has begun but the C2 server population can generally be captured and the sunk cost to the attacker is at its maximum?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



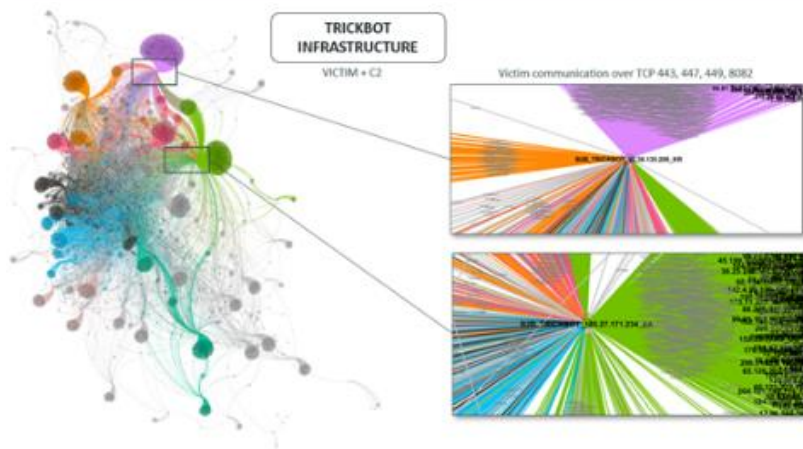
Individual tactics

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.



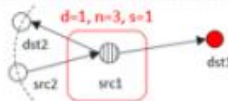
Example: Investigate infrastructure used for an attack



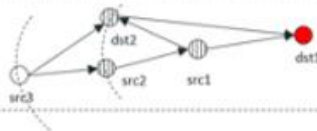
t1 Pivot depth: 0
Pivot nodes: src1



t2 Pivot depth: 1
Pivot nodes depth 0: src1
Pivot nodes depth 1: src2, dst2



t3 Pivot depth: 2
Pivot nodes depth0: src1, dst2
Pivot nodes depth1: src2, dst2
Pivot nodes depth2: src3



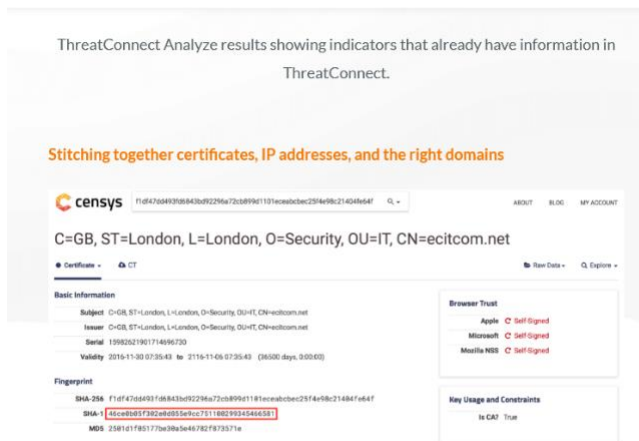
<https://insight-jp.nttsecurity.com/post/102fvek/12-5-soc-trickbot>

- 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)?

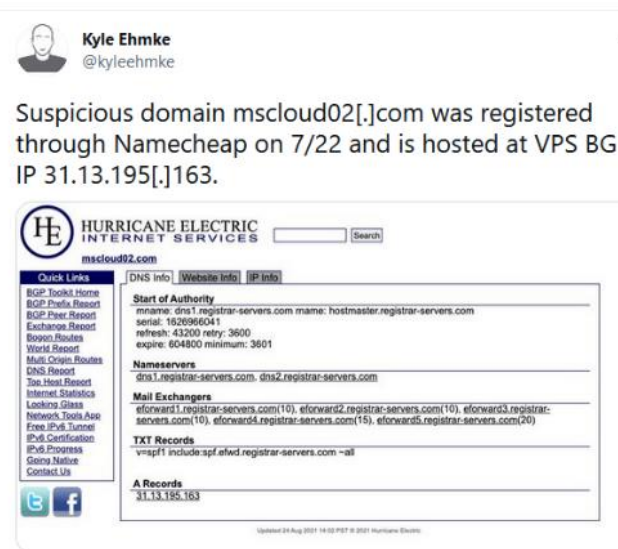
- Past investigations by ThreatConnect
- Investigate non-known C2 servers based on characteristics of SSL certificates commonly used by APT28 (Sofacy) C2 servers.



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.



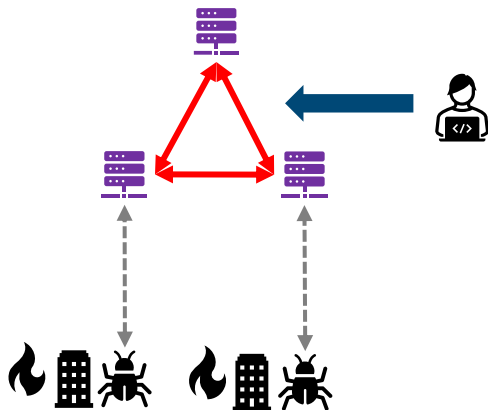
午後8:00 · 2021年8月25日 · Twitter Web App

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

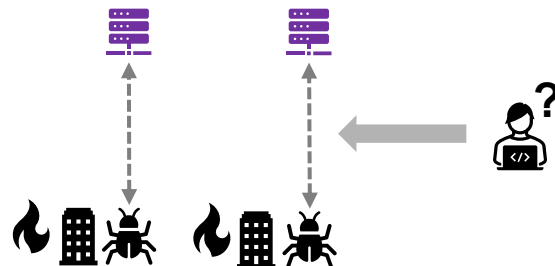
Can we do a proactive C2 search?

- 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)

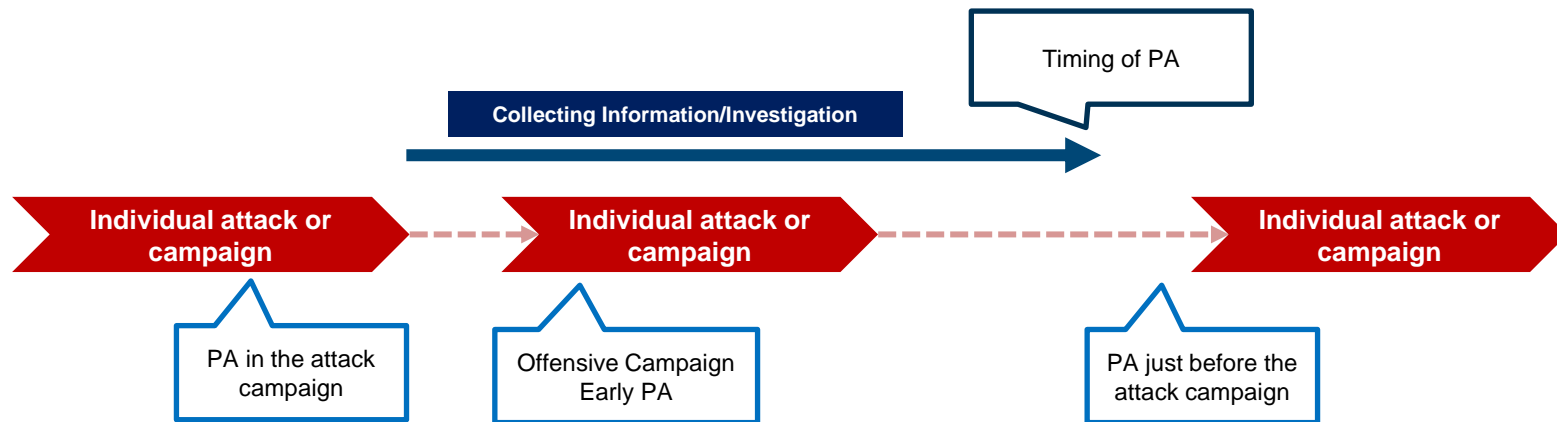
■ Issue

- 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

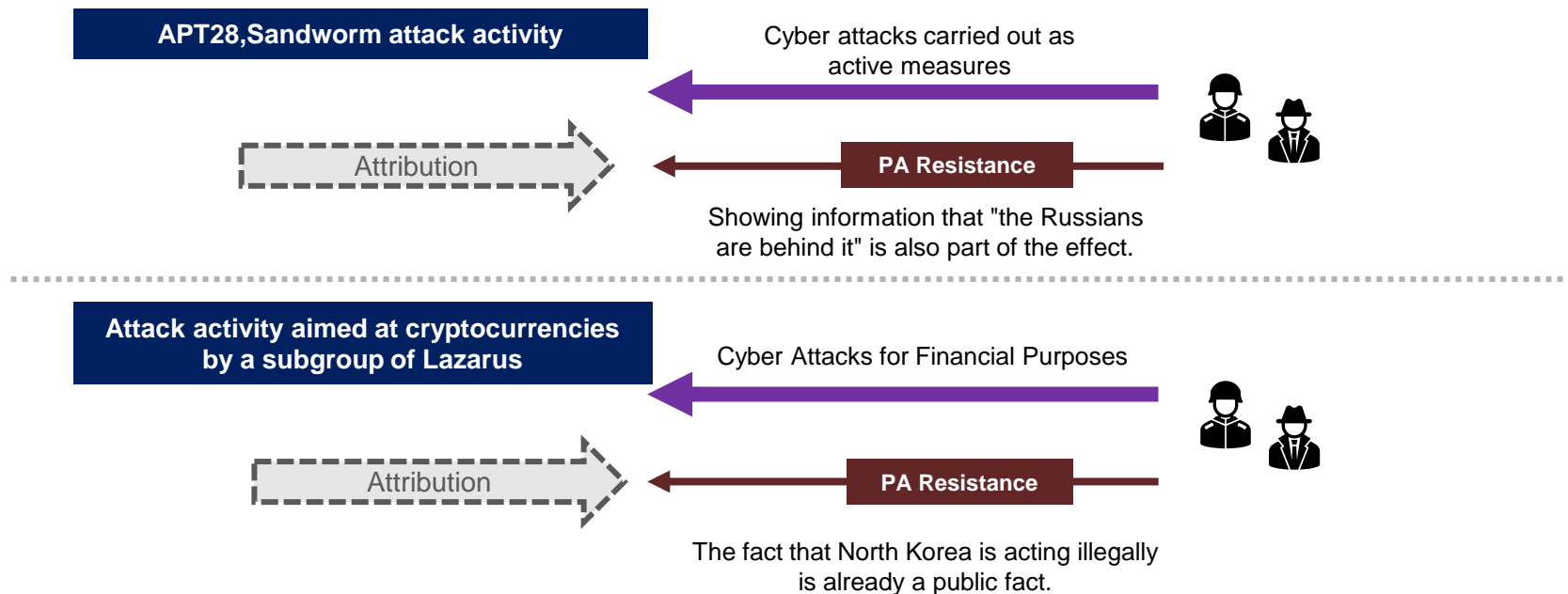
"Public Attribution" issue

- 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?



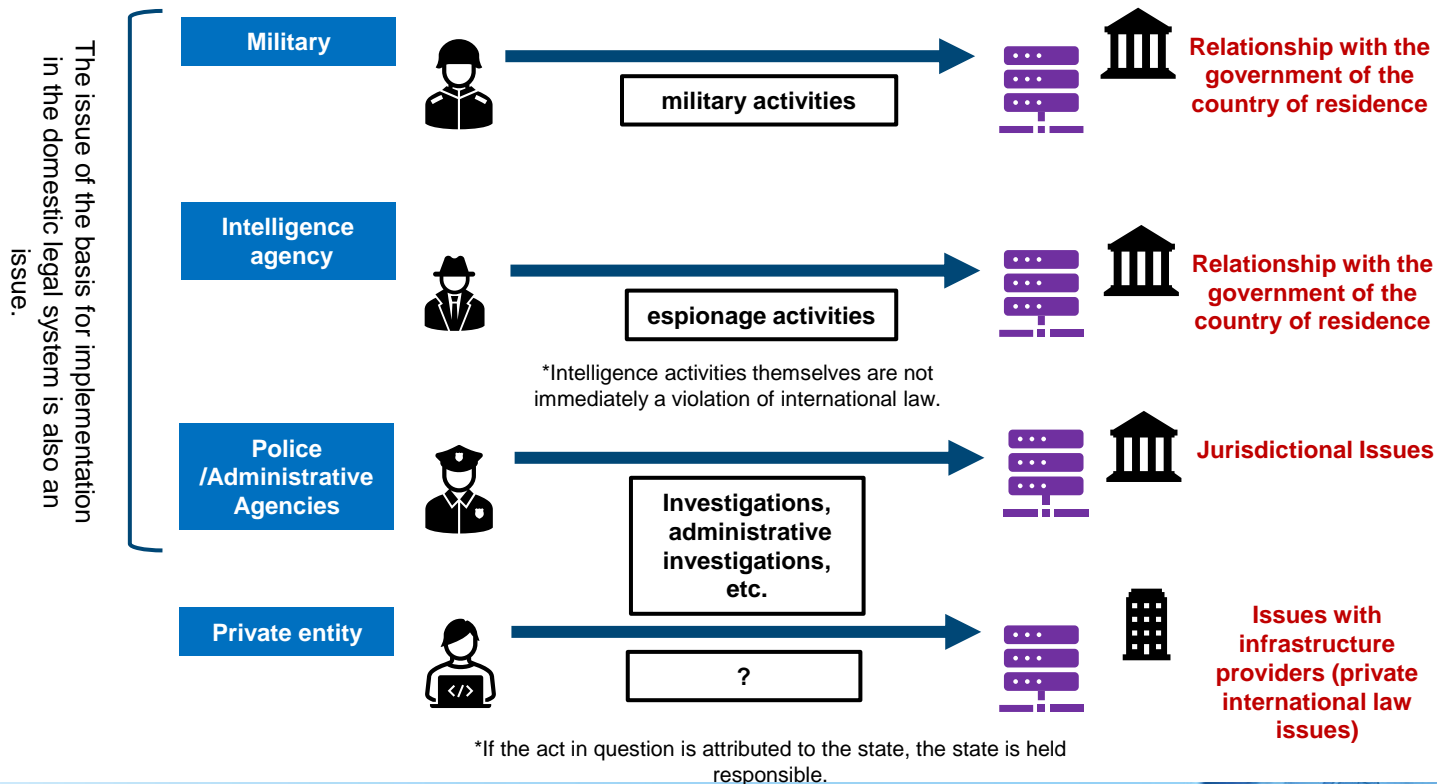
Public Attribution "tolerance" issue

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



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

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



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。

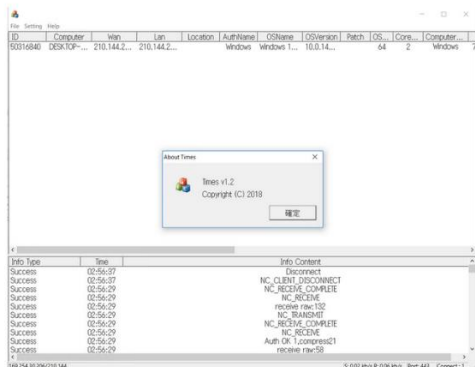


図8 : Gh0stTimesのコントロールパネル

- <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"

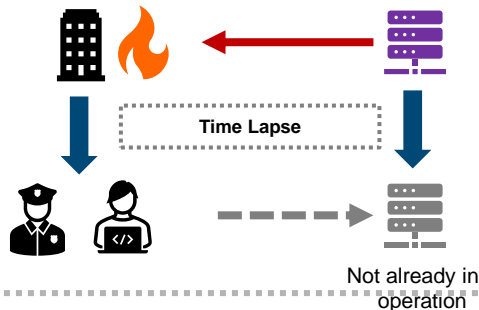
- Not only is it a matter of information acquisition and timing, but it is forgotten that the "counterattack" is basically on the (foreign) civilian infrastructure.

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

The question of whether counterattack is appropriate.

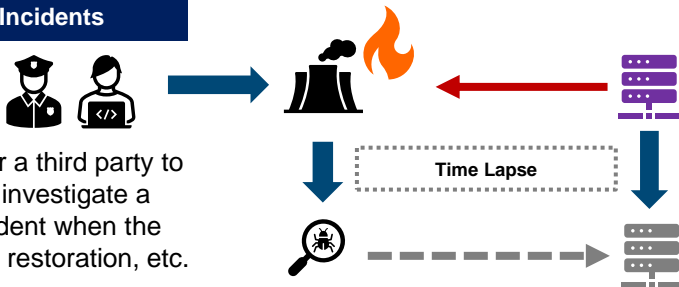
General Unauthorized Access Cases

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.



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.



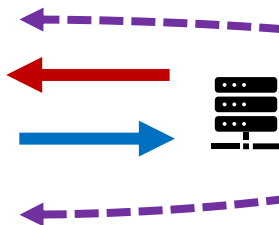
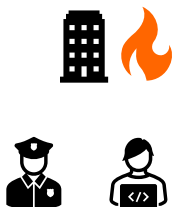
cloud computing provider
hosting company
ISP, etc.

"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?

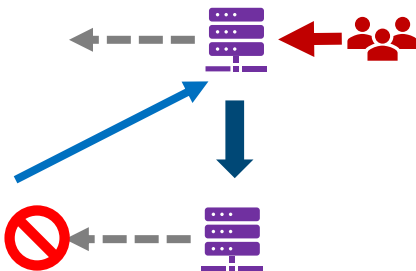
Retaliation/disturbance/destruction of evidence against the victim organization

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



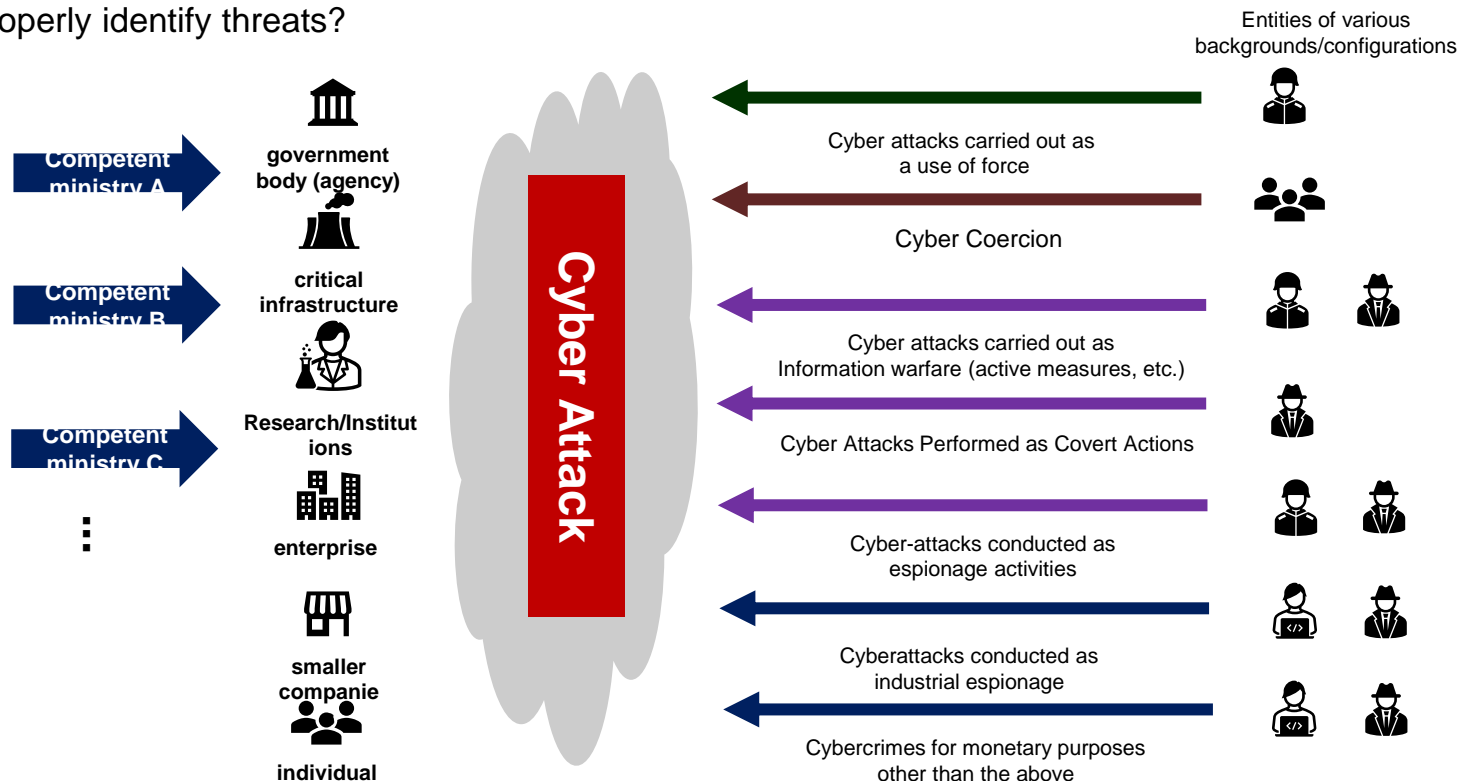
What will the attacker do?

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

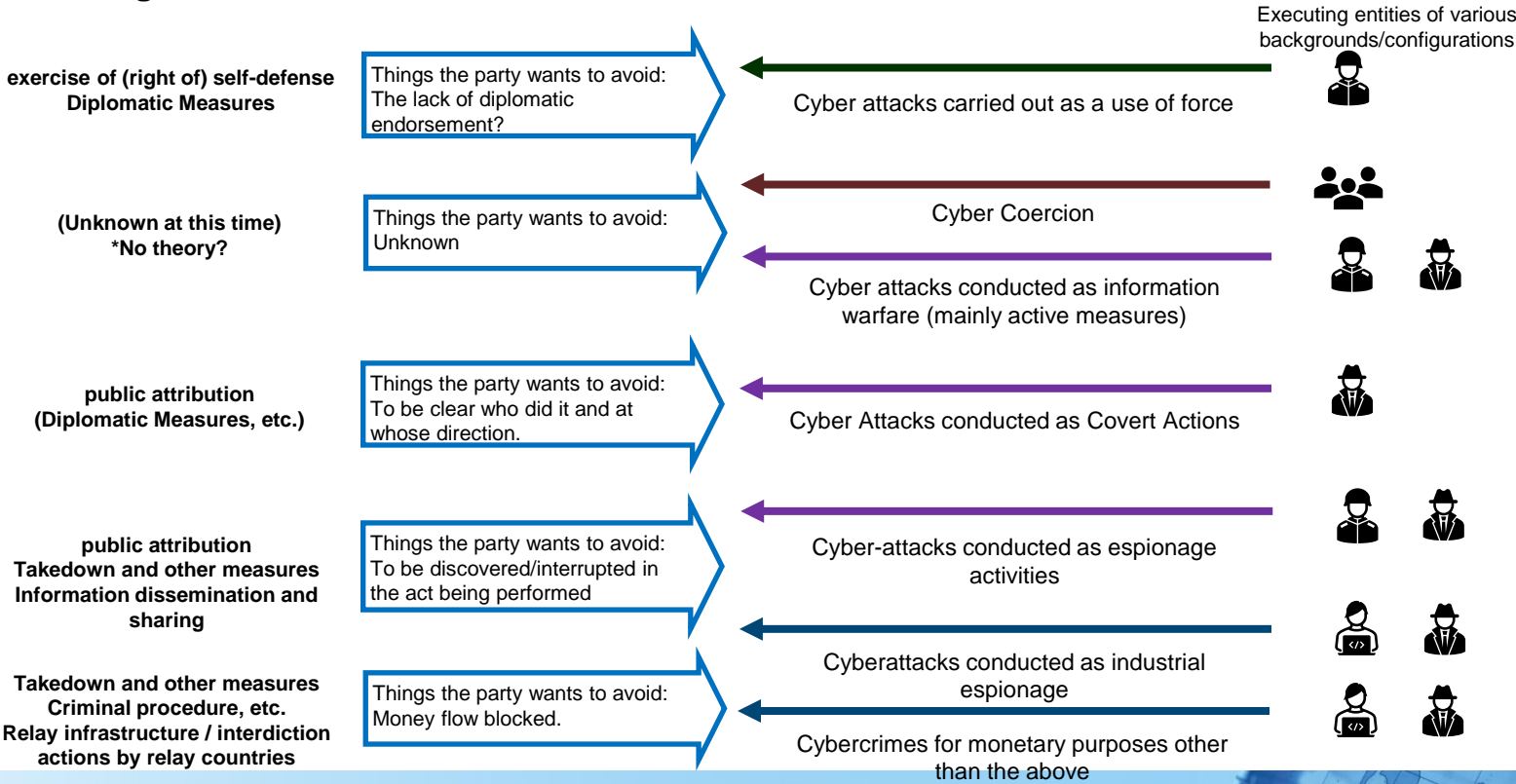
Identify threats correctly

- 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?



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.



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.

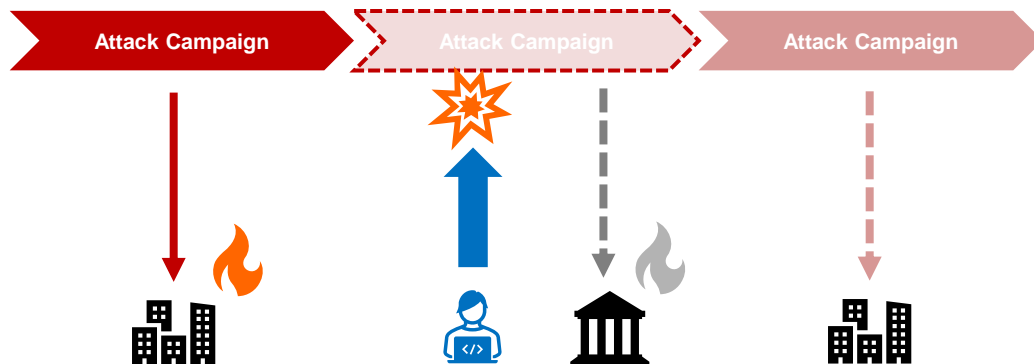
■ Hard

- *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



- 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.

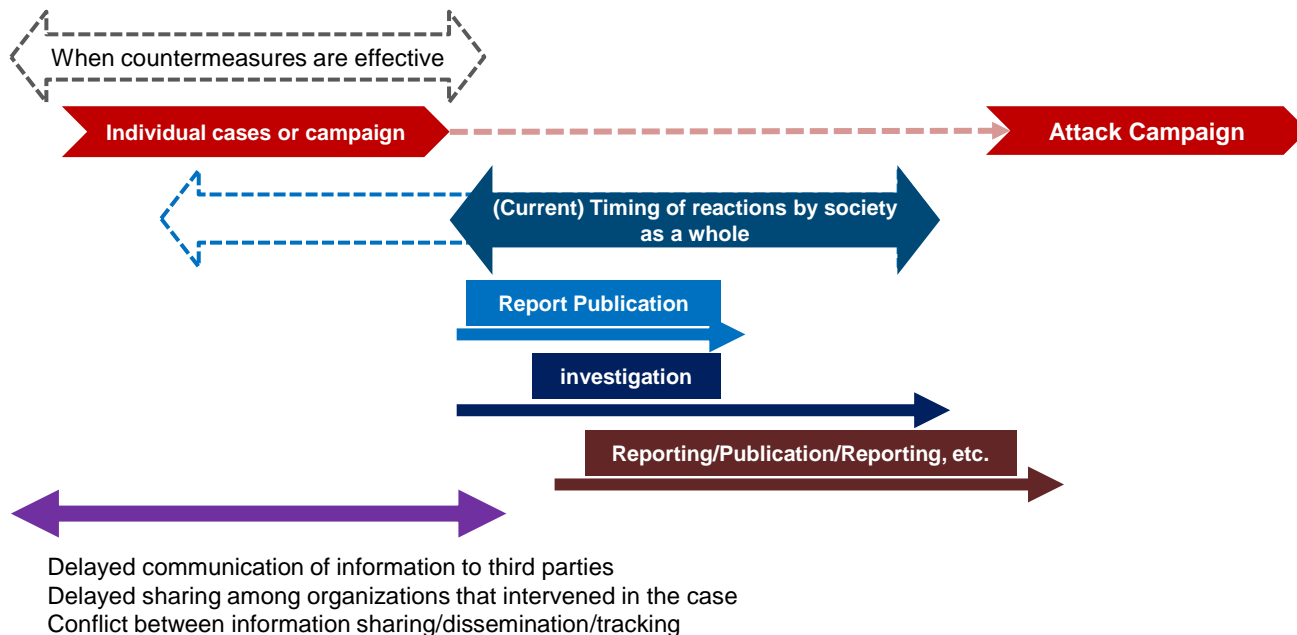


<https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/>

Further Issues to Consider

Rethink how to obtain information on the edge

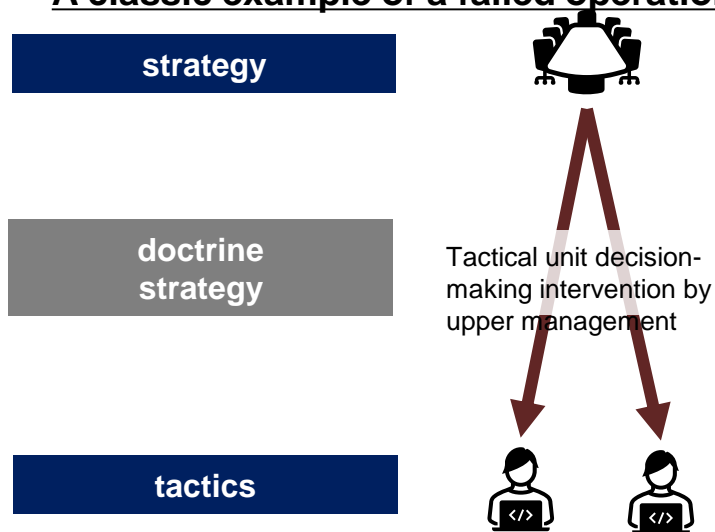
- The earlier it is, the more options for countermeasures
- No single organization (security vendor, specialized agency, police, etc.) can consider and implement countermeasures alone
- Even if recognized early by individual organizational units, if it takes time/coordination costs to be shared among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



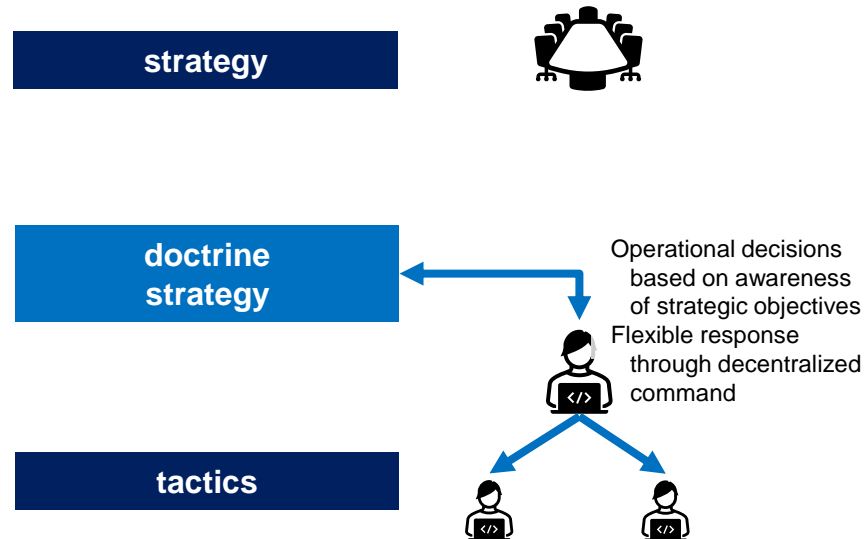
Who will make the decision to do this?

- 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



What the "Art of Operation" is all about



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

