black hat®
USA 2019

AUGUST 3-8, 2019
MANDALAY BAY / LAS VEGAS

Rough and Ready: Frameworks to Measure Persistent Engagement and Deterrence

SIPA

Jason Healey and Neil Jenkins

CYBER THREAT ALLIANCE

Columbia University SIPA
Cyber Threat Alliance

@Jason_Healey @NEJenkins

Structure of This Talk

- Understanding “Persistent Engagement” and Deterrence
- Frameworks for Answering the Question if US Policy Makes Things Better or Worse
- Describing Transgressions to be Measured
- Next Steps

UNDERSTANDING PERSISTENT ENGAGEMENT AND DETERRENCE

SIPA

CYBER THREAT ALLIANCE

National Security Advisor John Bolton

Intent of Administration on Cyber Deterrence

We have authorized offensive cyber operations […] not because we want more offensive operations in cyberspace, but precisely to create the structures of deterrence that will demonstrate to adversaries that the cost of their engaging in operations against us is higher than they want to bear

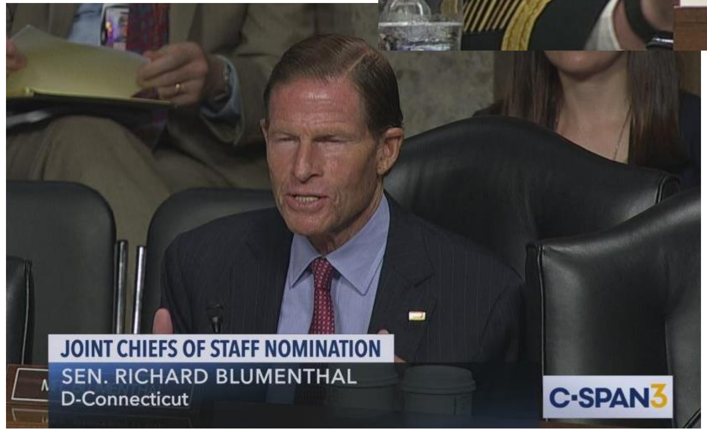
The hacking of [OPM] by China … that's the kind of threat to privacy from hostile foreign actors that we're determined to deter

https://news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg

New CJCS Sums It Up

"… A good offense is critical and that is the best defense.

"…If [adversaries] know that we have incredible offensive capability, then that should deter them from conducting attacks on us in cyber"



https://www.armed-services.senate.gov/imo/media/doc/19-58_07-11-19.pdf

But Not Just Possession But *Use* of Cyber Capabilities

"Unlike the nuclear realm … in cyberspace it's the use of cyber capabilities that is strategically consequential. The threat of using something in cyberspace is not as powerful as actually using it.

"…[I]f we're going to have an impact on an adversary, we have to persistently engage with that adversary … we have to be able to impose cumulative costs…

"…[W]e must take this fight to the enemy, just as we do in other aspects of conflict. A persistence force has a much higher chance of disrupting adversary plots and protecting Americans, compared with a force that is confined to sporadic reconnaissance."

JFQ Joint Force Quarterly
Defending Forward
An Interview with Paul M. Nakasone
Malign Actors and Cryptocurrency

An Interview with Paul M. Nakasone

https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-92/jfq-92.pdf

The Debate

- **Hawkish view**: A more forceful approach will lead to deterrence and tamer adversaries

The Debate

- **Hawkish view**: A more forceful approach will lead to deterrence and tamer adversaries

- **Owlish view**: More cautious and worried it backfire, leading to yet more attacks

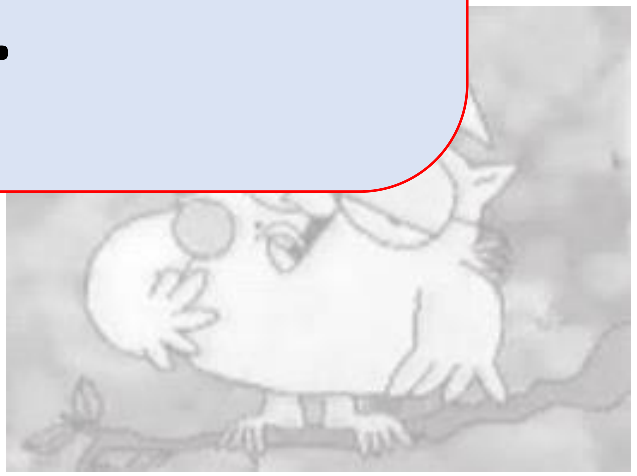
The Debate

- **Hawkish view**: A more forceful approach will lead to
a

Little evidence either way!

Let’s fix that…

- C
cautious and worried it backfire, leading to yet more attacks



Not Just Hacking Metrics

- This is a policy question
- Rooted to
  - Goals of US policymakers;
  - Understanding of adversary geopolitical goals and action (not just their hacking teams); and
  - Statistics of security incidents

Not Just Science, But *Political* Science!

Negative or Positive Feedback

- If negative feedback, then US counter-offensives will shepherd adversaries back to previous, more stable norms
  - Decrease in extreme, dangerous, de-stabilizing incidents
  - Adversary behavior is less destabilizing next year than this year

- If positive feedback, then US counter-offensives amplify current trends, moving farther from previous norms
  - Increase in aggressive/reckless, brazen incidents

Implied Hypothesis Of USG Argument

Problem

1. Adversaries are conducting free-for-all attacks to **destabilize the United States** (and its allies) and **erode sources of national power**;

Method

2. U.S. cyber forces must **defend forward** against these threats, maneuvering to positions of advantage in foreign cyberspace to maintain persistent presence so “as the adversary tries to maneuver, we can actually stay with the adversary;”
3. To achieve this advantage, the U.S. cyber forces must operate with **reduced operational constraints**, “to act as we see emerging threats and opportunities in this space;”
4. With persistent presence, the United States can “**intercept and halt cyber threats**,” enter “an adversary’s network to learn what they are doing as a means of improving defenses,” and “degrade the infrastructure and other resources that enable our adversaries to fight in cyberspace”
5. Persistent presence will **improve U.S. defenses**, as DoD observes adversary behavior and warns targets of the facts and methods of coming (or ongoing) attacks,;
6. Together, these actions **impose friction** to, in the short term, directly disrupt specific adversary operations;
7. Friction will also, in the medium term, tie up adversaries forcing them to spend more resources responding to U.S. actions and rebuilding degraded infrastructure, **reducing their *ability* to attack**;
8. Also in the medium term, there will be a stabilizing process of **tacit bargaining** between adversaries as they mutually discover the upper and lower bounds of conflict through repeated interactions;
9. U.S. cyber forces will simultaneously use more purely offensive cyber capabilities for **deterrence** purposes, to threaten targets that adversaries value, making clear the strategic costs of attacking the United States and reducing their *willingness* to attack;

Result

10. Adversaries will, over the long term, moderate their behavior in response to U.S. actions, creating a more **stable environment and continued U.S superiority**.

US actions impose **negative feedback**: stimulus to revert to previous norm

FRAMEWORKS TO ANSWER THE QUESTION

SIPA

CYBER THREAT ALLIANCE

Three Basic Frameworks

- US Government Incident Severity Score
  - **Strengths**: Already used by DHS, White House including non-public incidents, best at ability to be correlated with USG actions or policy
  - **Weakness**: Not tied to context, will miss unknown incidents, may be classified
- Tracking of Significant Incidents
  - **Strengths**: Simple to use and can largely be done with open sources, can be transparent and public to allow analytical discourse
  - **Weaknesses**: Cannot correlate directly with USG actions or policy, not tied to context, and will miss unknown incidents
- Deep Dive on Particular Adversary/Goal Pairings
  - **Strengths**: Best at measuring context, can be transparent and public to allow analytical discourse
  - **Weaknesses**: Cannot correlate directly with USG actions or policy

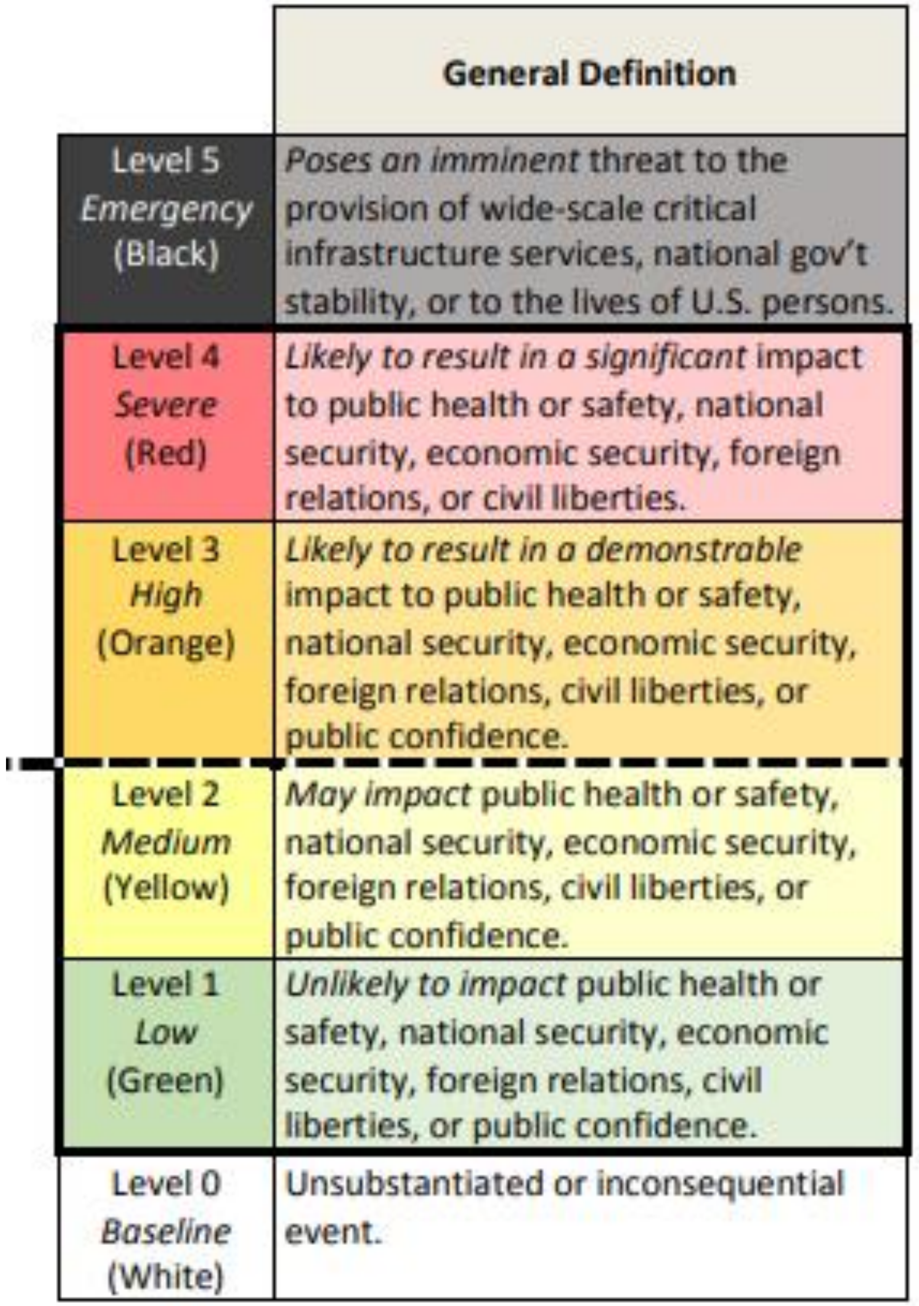
(1) USG Incident Severity System

Simple Count of Serious Incidents

If cyber_level = {3,4,5} then count = count+1

Plotted as time series

Very messy but simple and integrates with existing government response process

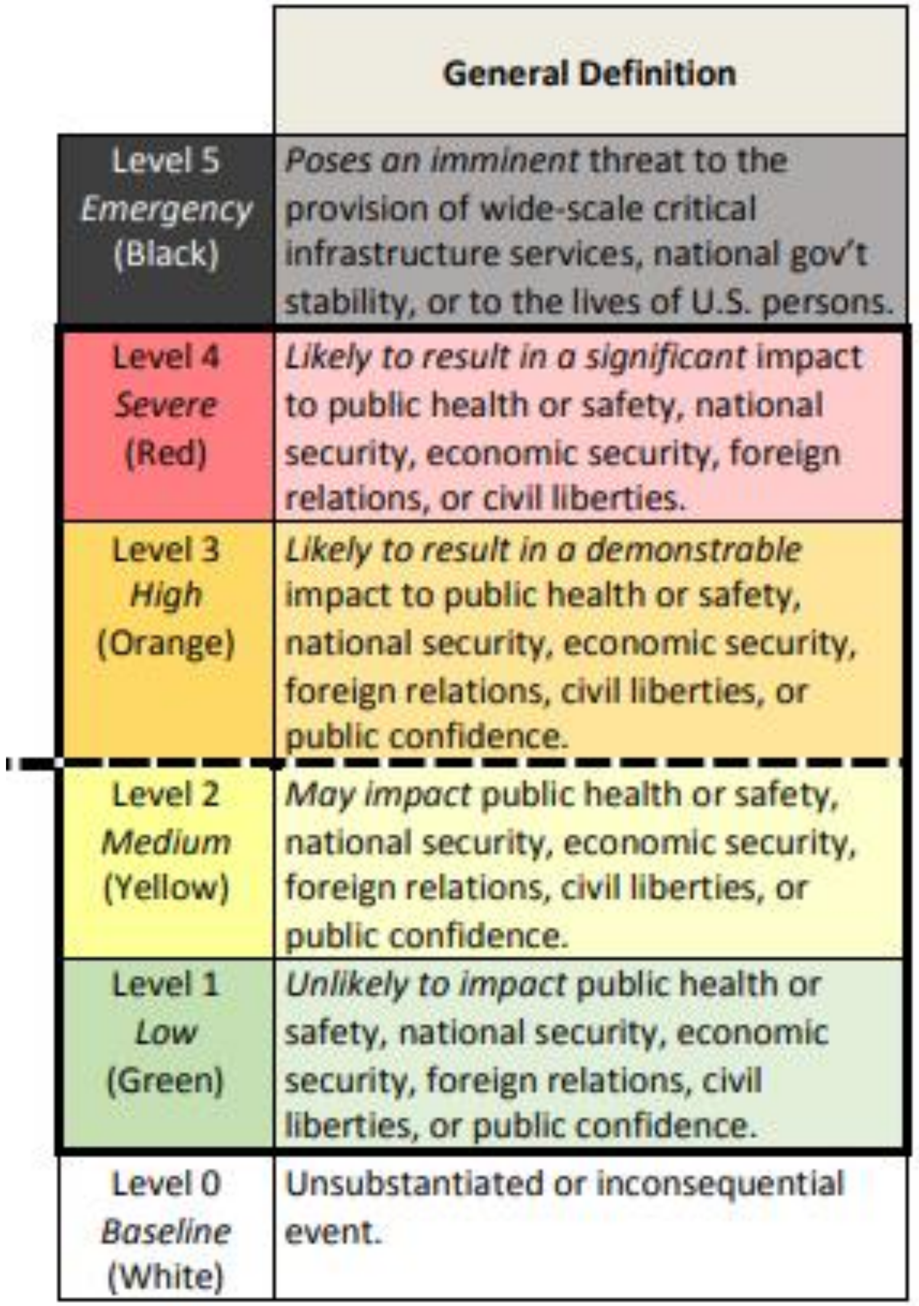


	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

(1) USG Incident Severity System

Simple Count of Serious Incidents

1. Messy data
2. Simple
3. Integrates with existing government response process
4. Can't get close to causation



	General Definition
Level 5 *Emergency* (Black)	*Poses an imminent* threat to the provision of wide-scale critical infrastructure services, national gov't stability, or to the lives of U.S. persons.
Level 4 *Severe* (Red)	*Likely to result in a significant* impact to public health or safety, national security, economic security, foreign relations, or civil liberties.
Level 3 *High* (Orange)	*Likely to result in a demonstrable* impact to public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 2 *Medium* (Yellow)	*May impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 1 *Low* (Green)	*Unlikely to impact* public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence.
Level 0 *Baseline* (White)	Unsubstantiated or inconsequential event.

(2) National Security Advisor John Bolton

Intent of Administration on Cyber Deterrence

The hacking of [OPM] by China …
that's the kind of threat to privacy from hostile foreign actors that we're determined to deter

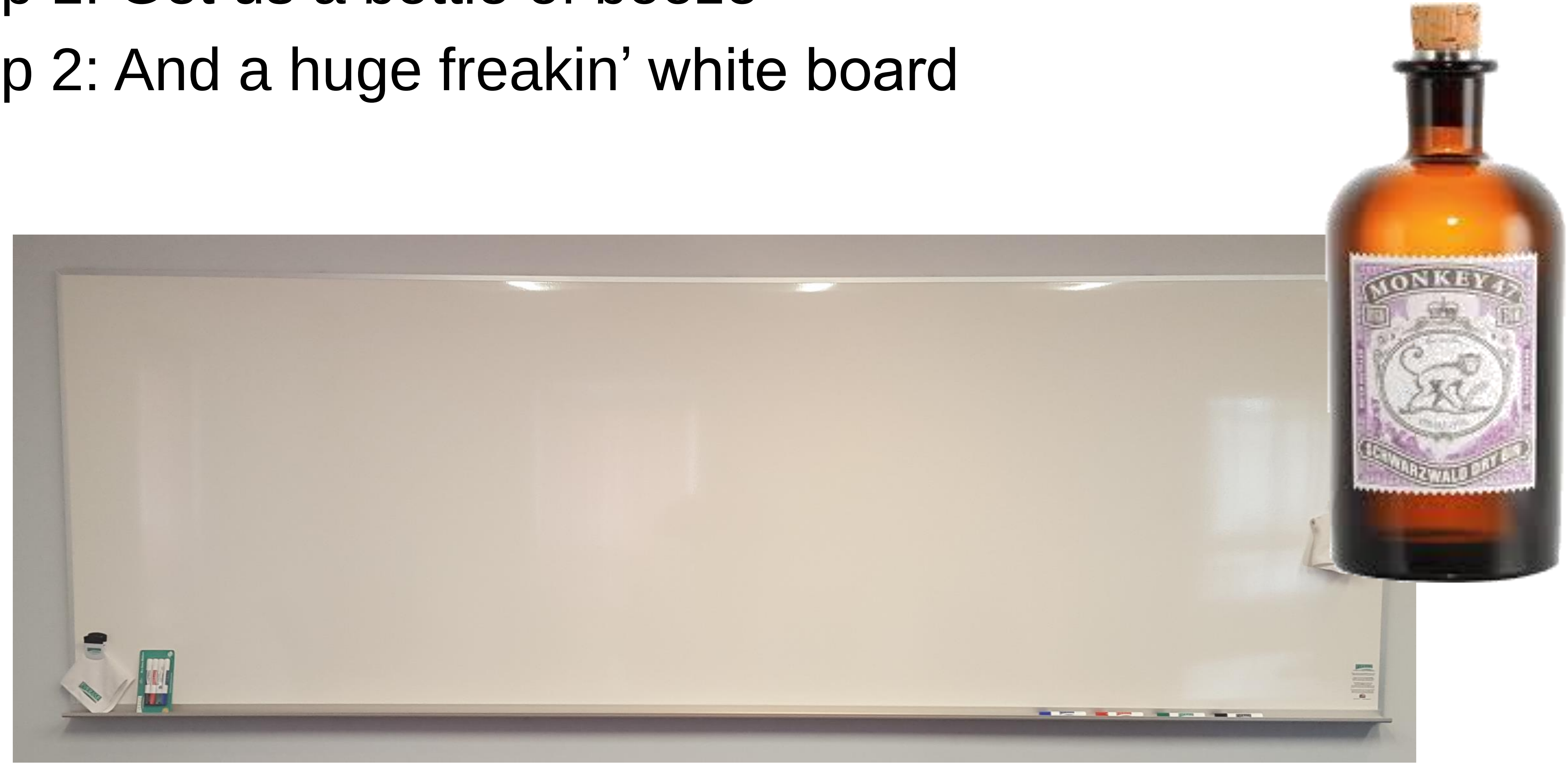
https://news.grabien.com/making-transcript-white-house-press-briefing-national-cyber-strateg

(2) Bolton Wanted to Deter Incidents Like OPM

- Step 1: Get us a bottle of booze

(2) Bolton Wanted to Deter Incidents Like OPM

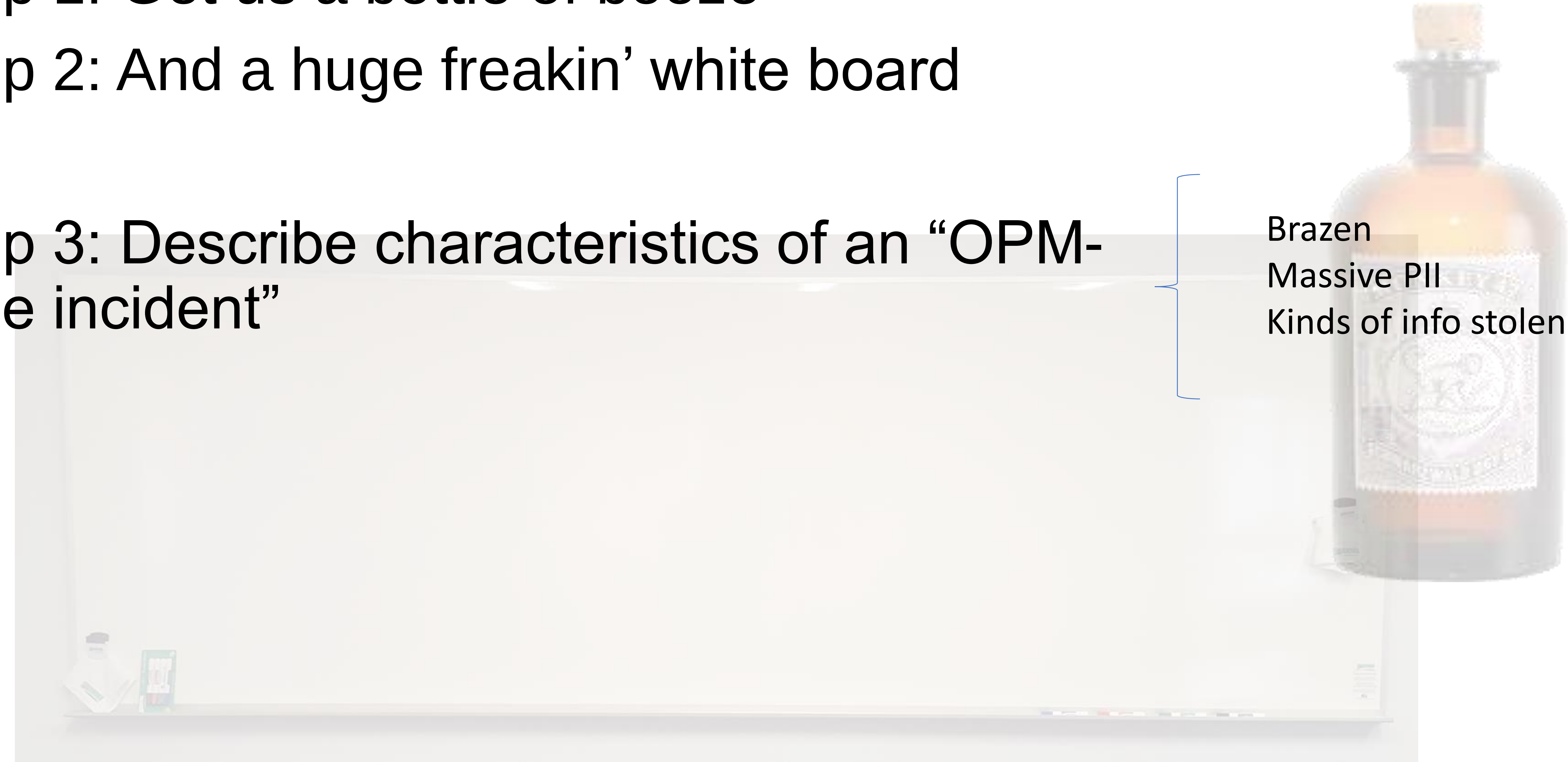
- Step 1: Get us a bottle of booze
- Step 2: And a huge freakin' white board



(2) Bolton Wanted to Deter Incidents Like OPM

- Step 1: Get us a bottle of booze
- Step 2: And a huge freakin' white board
- Step 3: Describe characteristics of an "OPM-style incident"

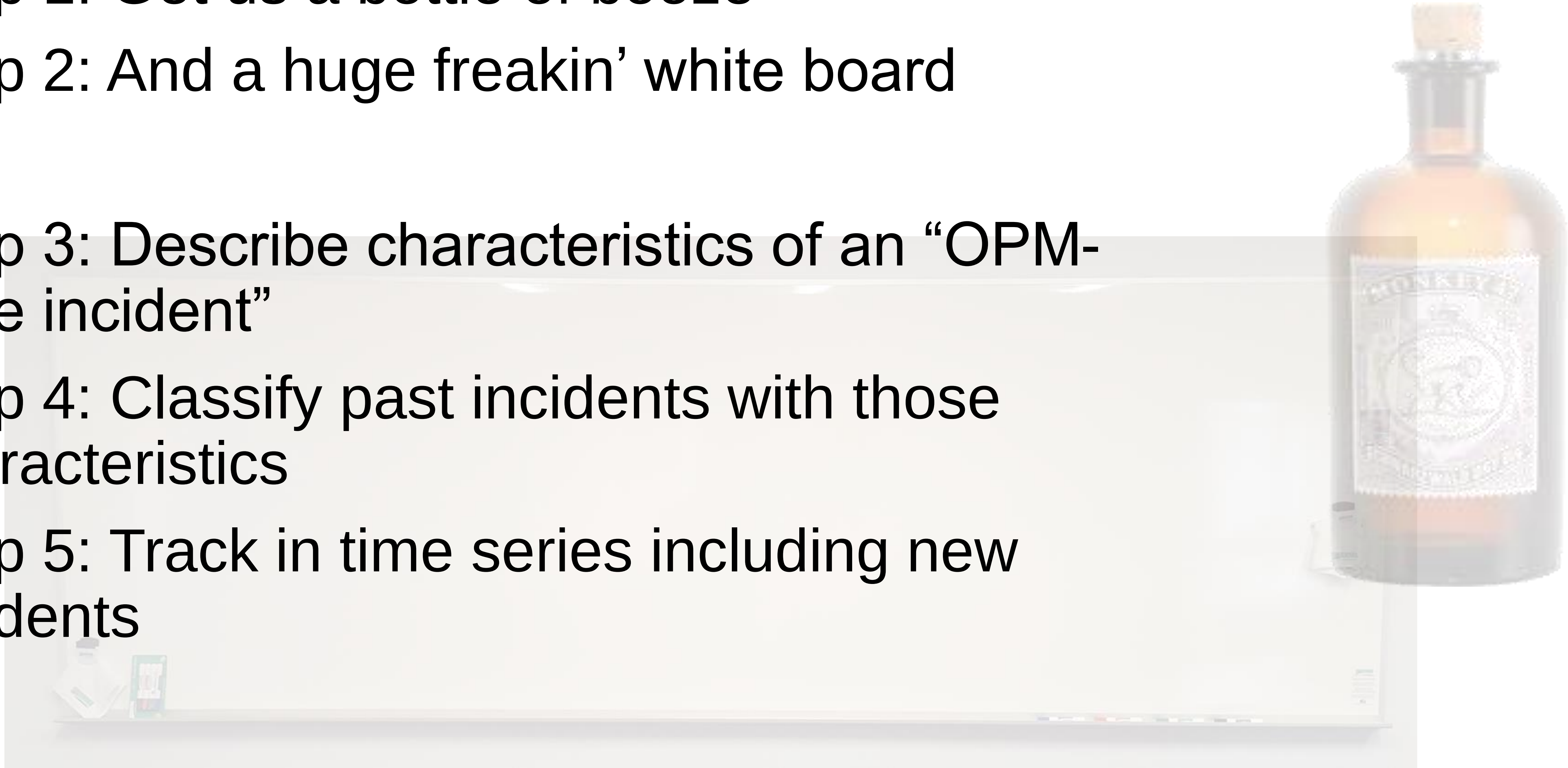
Brazen
Massive PII
Kinds of info stolen



(2) Bolton Wanted to Deter Incidents Like OPM

- Step 1: Get us a bottle of booze
- Step 2: And a huge freakin’ white board

- Step 3: Describe characteristics of an “OPM-style incident”
- Step 4: Classify past incidents with those characteristics
- Step 5: Track in time series including new incidents

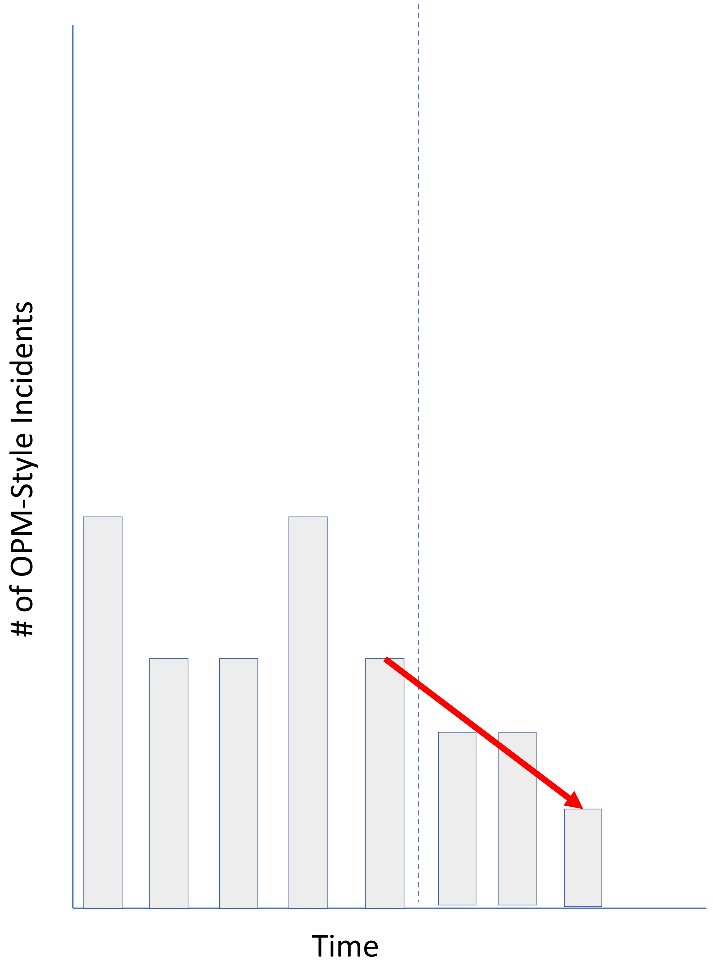


(2) Tracking of Significant Incidents

Incidence of "OPM-Style Incidents"

Case 1: Bolton's Intent

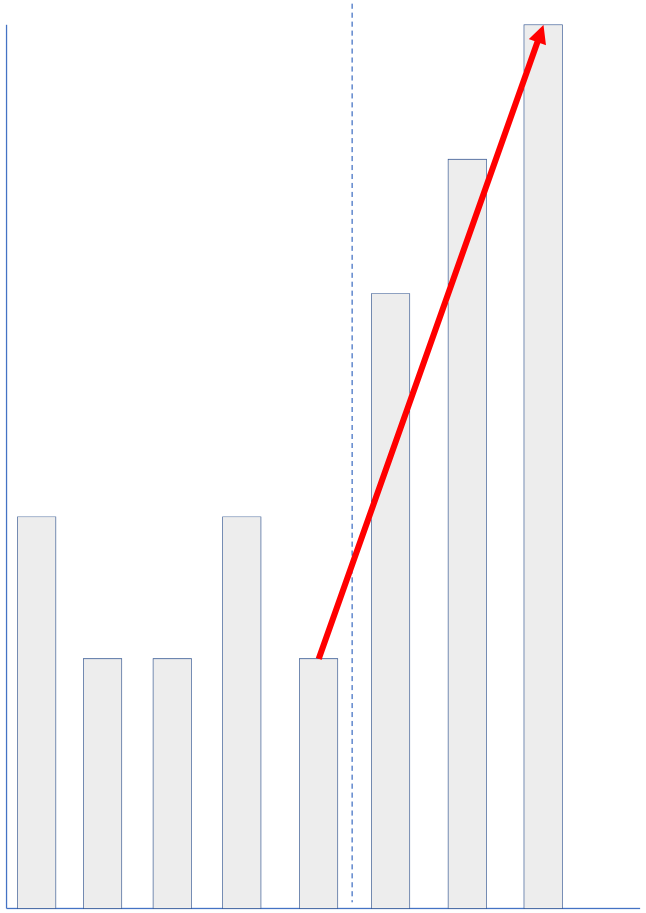
After the new policy enacted, reduction in significant events



OR

Case 2: Critic's Fear

After the new policy enacted, increase in significant events

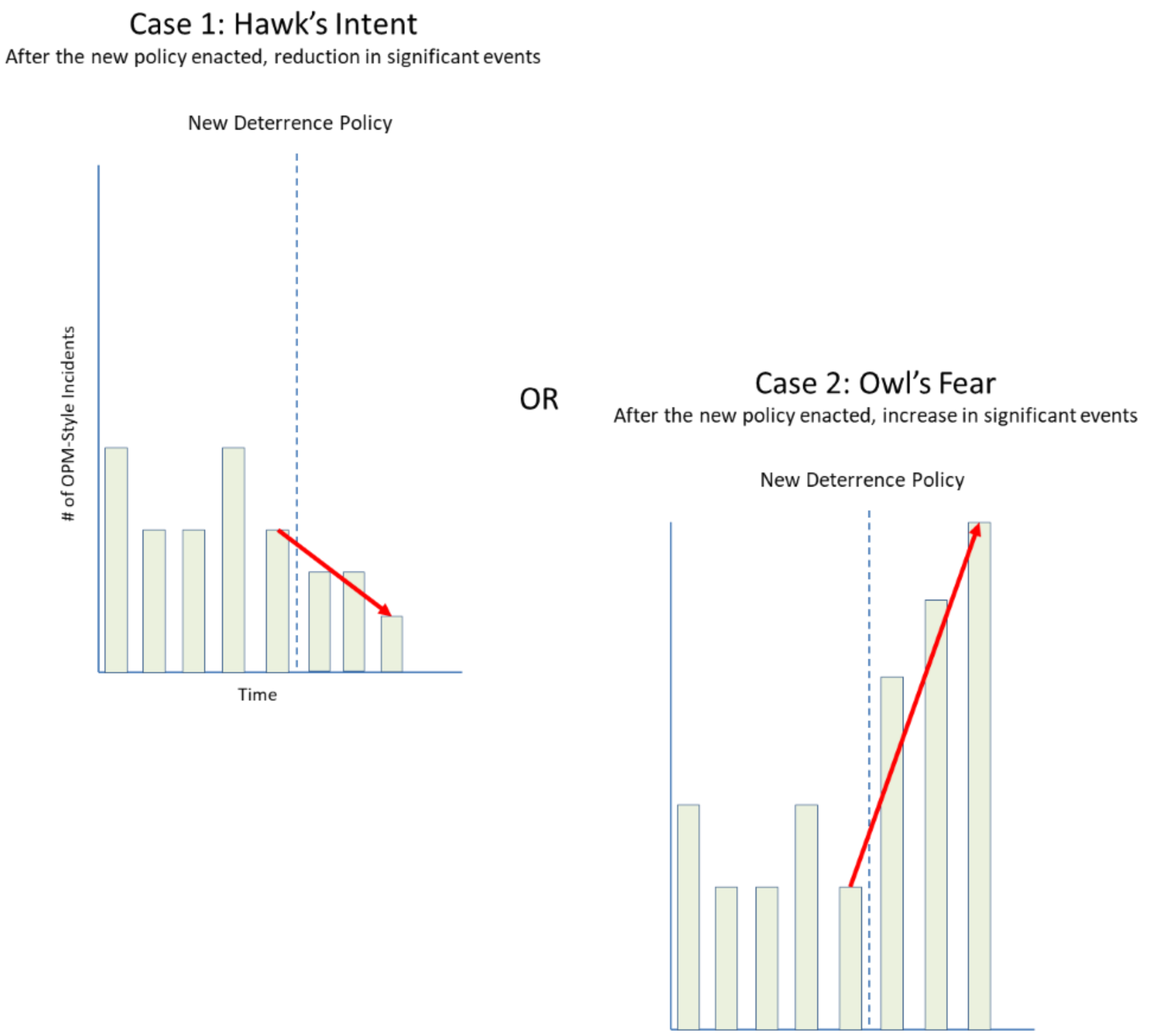


(2) Tracking of Significant Incidents

Incidence of “OPM-Style Incidents”

- Case wouldn’t be “proven” or “disproven” either way, but evidence is suggestive…

- Failure is louder than success



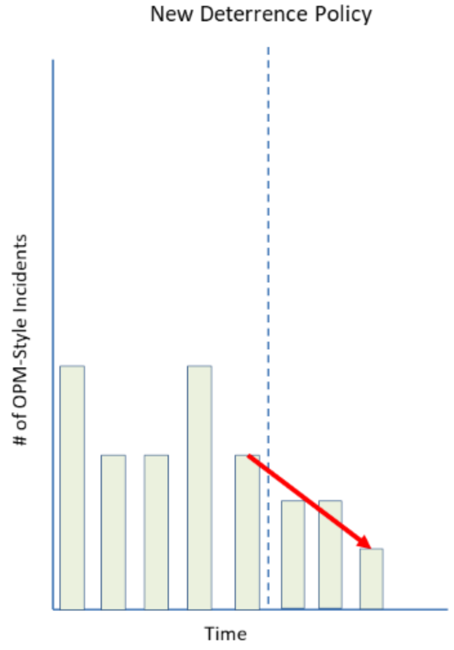
(2) Tracking of Significant Incidents

Incidence of “OPM-Style Incidents”

1. Still messy but maybe less so
2. Tied more directly to policymaker goals
3. Not correlated to specific US cyber actions
4. Many (most?) “OPM-style incidents” are widespread/disruptive and can be found in open source
5. Allows more analytical transparency

Case 1: Hawk’s Intent

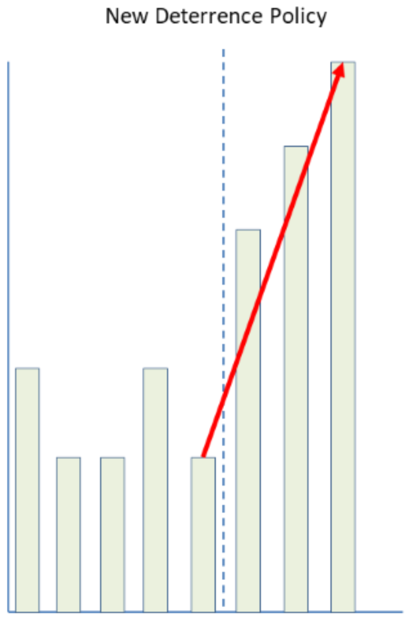
After the new policy enacted, reduction in significant events



OR

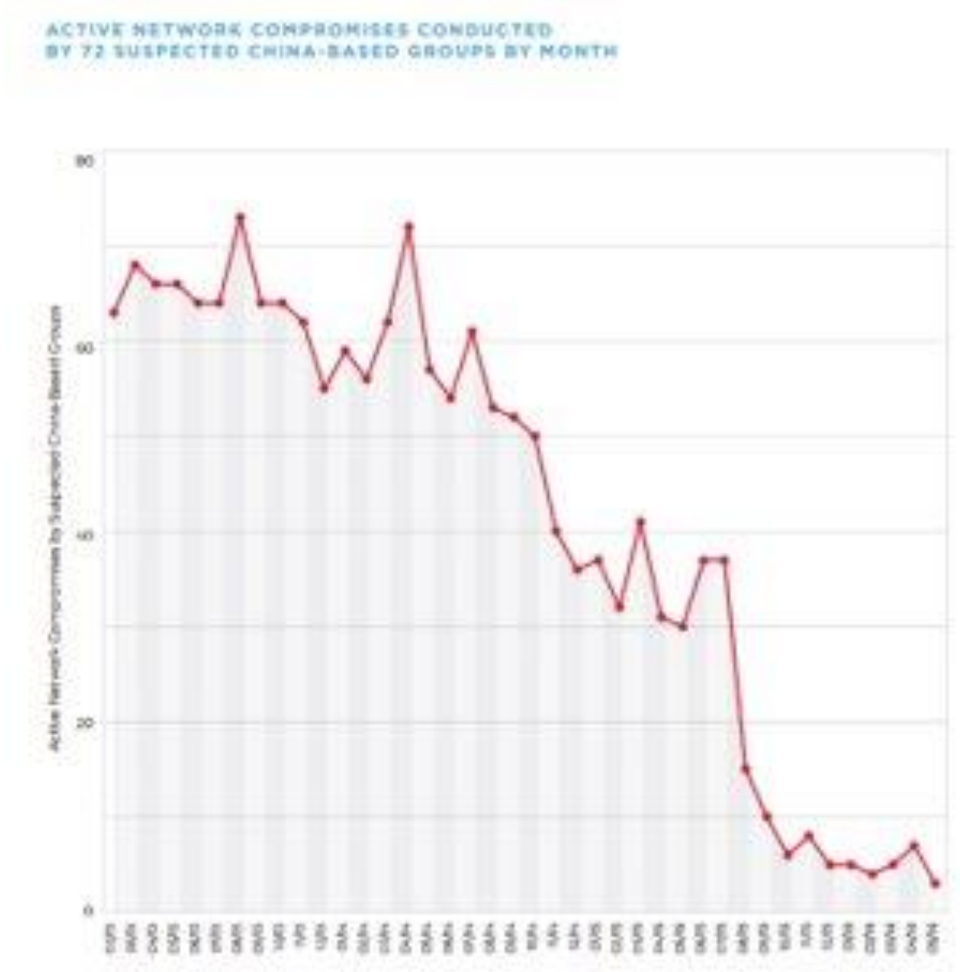
Case 2: Owl’s Fear

After the new policy enacted, increase in significant events



(3) Deep Dives on Particular Adversary/Goal Pairings

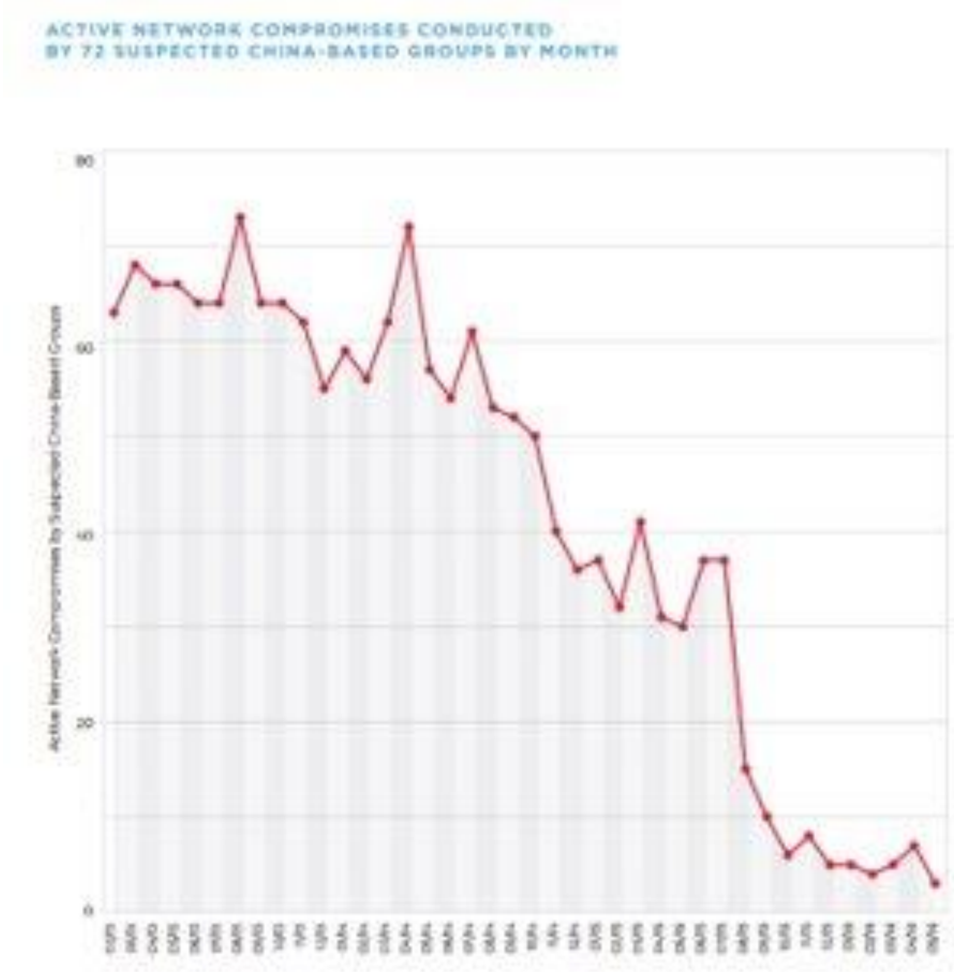
- Best example so far:
- FireEye, “Red Line Drawn” report



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

(3) Deep Dives on Particular Adversary/Goal Pairings

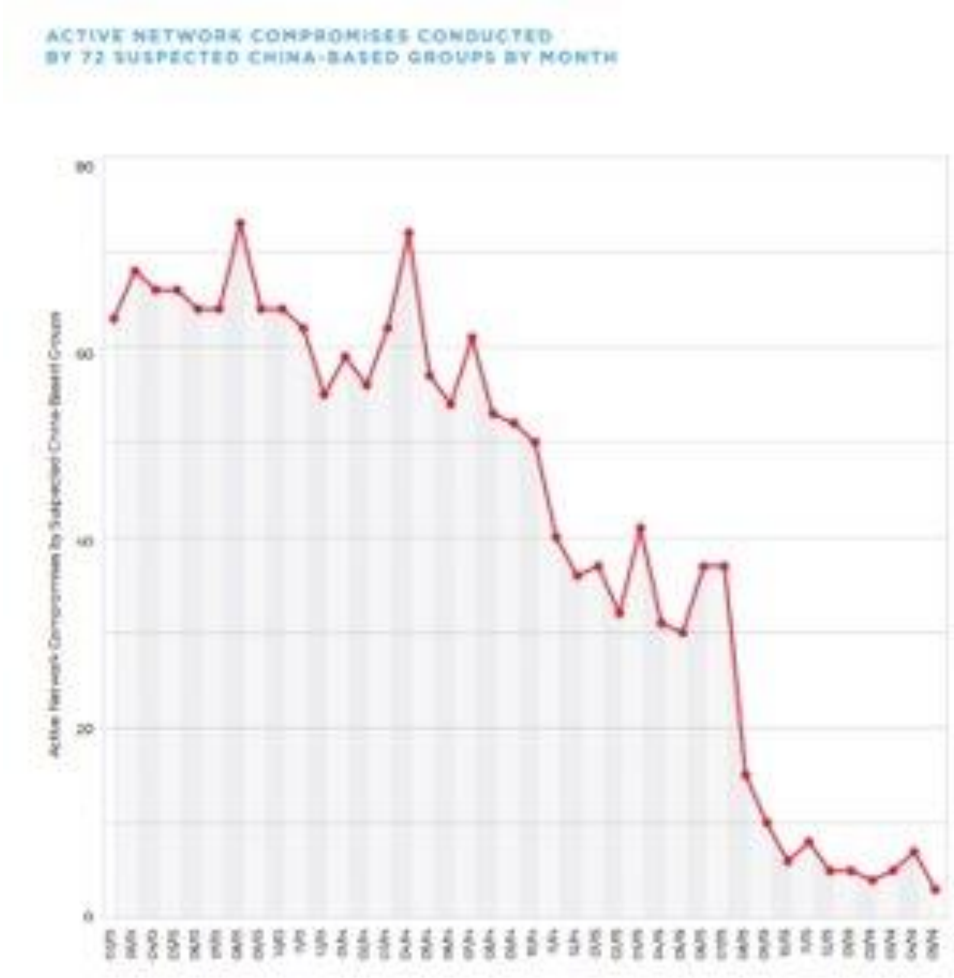
- **Was there was an actual decrease in Chinese espionage operations for commercial purposes?**
  - Perhaps the number of incidents held steady, but the bulk were not detected due to improved Chinese stealthiness.
  - This is generally a question for cyber threat analysts.
- How much of any Chinese response was the result of the U.S. policy?
  - Perhaps the Chinese primarily acted for their own reasons, in response to domestic Chinese pressures, and U.S. policies had little additional impact.
  - This is a question best answered by China experts.
- Did the decrease matter?
  - Perhaps the few networks still being compromised were those most critical to national security, so the overall impact was not meaningfully diminished.
  - This is a question best answered by the policymakers themselves.



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

(3) Deep Dives on Particular Adversary/Goal Pairings

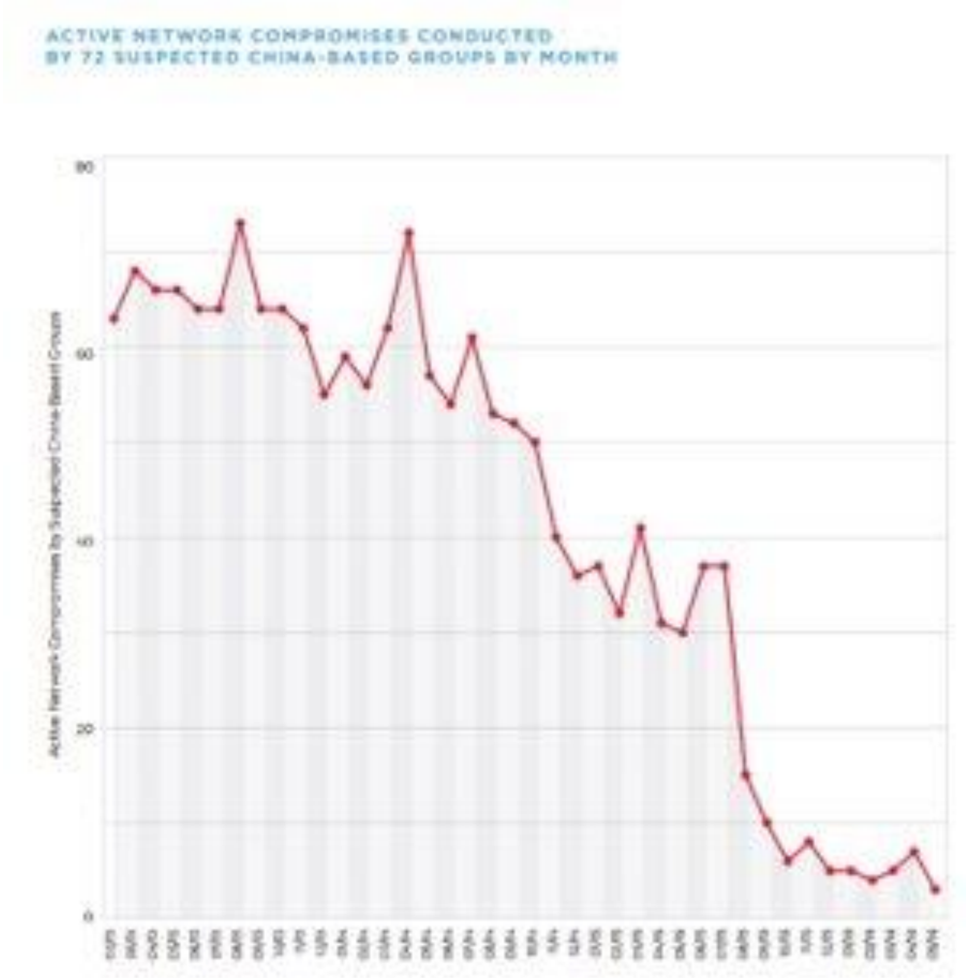
- Was there was an actual decrease in Chinese espionage operations for commercial purposes?
  - Perhaps the number of incidents held steady, but the bulk were not detected due to improved Chinese stealthiness.
  - This is generally a question for cyber threat analysts.
- **How much of any Chinese response was the result of the U.S. policy?**
  - Perhaps the Chinese primarily acted for their own reasons, in response to domestic Chinese pressures, and U.S. policies had little additional impact.
  - This is a question best answered by China experts.
- Did the decrease matter?
  - Perhaps the few networks still being compromised were those most critical to national security, so the overall impact was not meaningfully diminished.
  - This is a question best answered by the policymakers themselves.



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

(3) Deep Dives on Particular Adversary/Goal Pairings

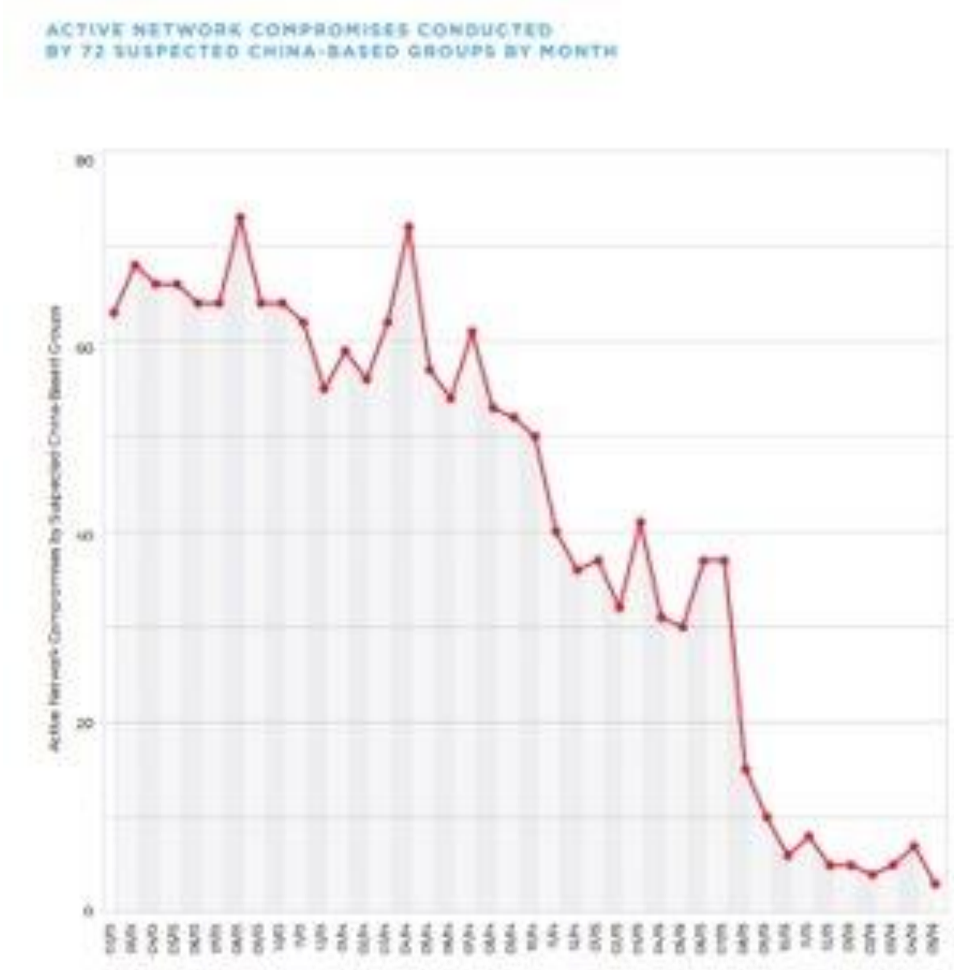
- Was there was an actual decrease in Chinese espionage operations for commercial purposes?
  - Perhaps the number of incidents held steady, but the bulk were not detected due to improved Chinese stealthiness.
  - This is generally a question for cyber threat analysts.
- How much of any Chinese response was the result of the U.S. policy?
  - Perhaps the Chinese primarily acted for their own reasons, in response to domestic Chinese pressures, and U.S. policies had little additional impact.
  - This is a question best answered by China experts.
- **Did the decrease matter?**
  - Perhaps the few networks still being compromised were those most critical to national security, so the overall impact was not meaningfully diminished.
  - This is a question best answered by the policymakers themselves.



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

(3) Deep Dives on Particular Adversary/Goal Pairings

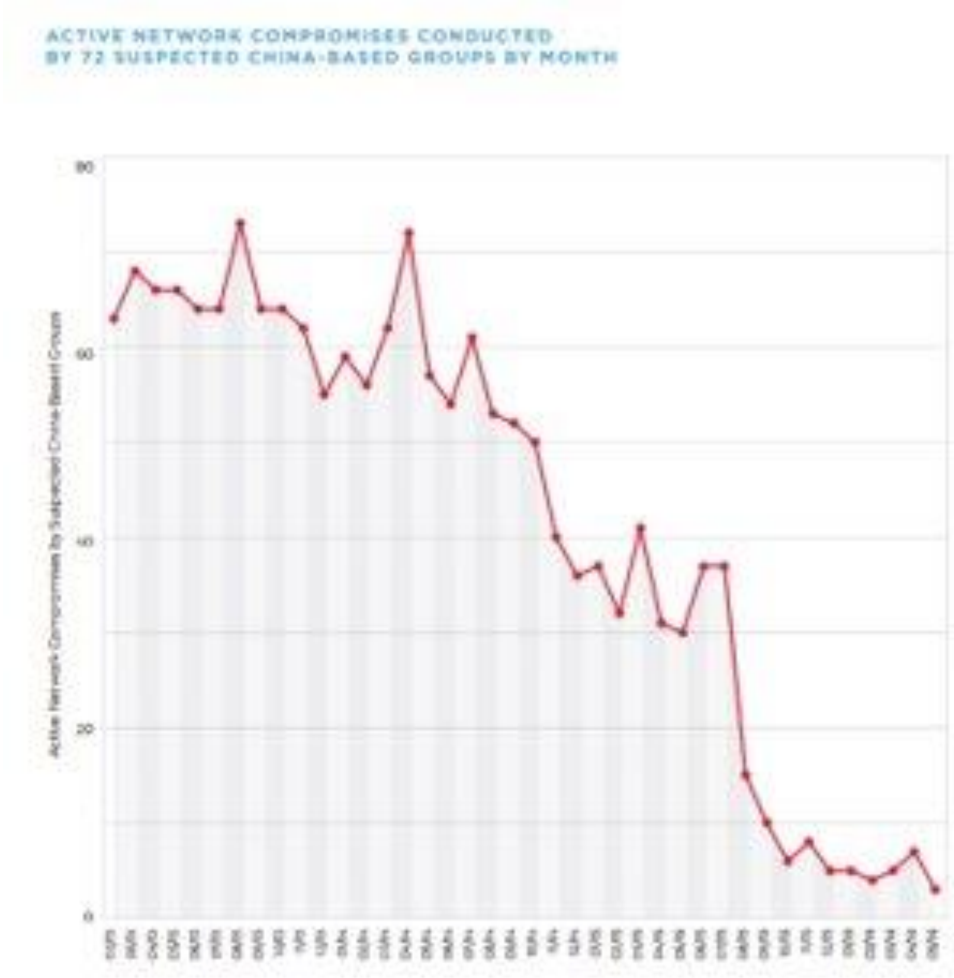
- Was there was an actual decrease in Chinese espionage operations for commercial purposes?
  - Perhaps the number of incidents held steady, but the bulk were not detected due to improved Chinese stealthiness.
  - This is generally a question for cyber threat analysts.
- How much of any Chinese response was the result of the U.S. policy?
  - Perhaps the Chinese primarily acted for their own reasons, in response to domestic Chinese pressures, and U.S. policies had little additional impact.
  - This is a question best answered by China experts.
- **Did the decrease matter?**
  - Perhaps the few networks still being compromised were those most critical to national security, so the overall impact was not meaningfully diminished.
  - This is a question best answered by the policymakers themselves.



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

(3) Deep Dives on Particular Adversary/Goal Pairings

1. Far less messy
2. Tied more directly to policymaker goals
3. Not correlated to specific US cyber actions
4. Allows more analytical transparency and specificity
5. Significant effort
6. Still can’t prove cause and effect



FireEye, Red Line Drawn: China Recalculates Its Use of Cyber Espionage, June 2016

Three Basic Frameworks

- US Government Incident Severity Score
  - **Strengths**: Already used by DHS, White House including non-public incidences, best at ability to be correlated with USG actions or policy
  - **Weakness**: Not tied to context, will miss unknown incidents, likely to be classified
- Tracking of Significant Incidents
  - **Strengths**: Simple to use and can largely be done with open sources, can be transparent and public to allow analytical discourse
  - **Weaknesses**: Cannot correlate directly with USG actions or policy, not tied to context, and will miss unknown incidents
- Deep Dive on Particular Adversary/Goal Pairings
  - **Strengths**: Best at measuring context, can be transparent and public to allow analytical discourse
  - **Weaknesses**: Cannot correlate directly with USG actions or policy

Shortcomings 1/3

- Effect of U.S. actions may be swamped by technical developments
    - An increase in the number of reported incidents could be due to new classes of vulnerabilities, a flood of new and insecure Internet-of-things devices, or improvements in detection and defense
    - The deployment of more secure infrastructure would lead to fewer attacks as would an increase in adversary use of “living off the land” and obfuscation techniques
- Control:
    - Check competing hypotheses by comparing trendlines between adversaries, especially “deep-dive”

Shortcomings 2/3

- Many attacks (and adversary motivations) are hidden and data can be hard to come by and analyze
- Geopolitical events could cause adversaries to decrease or increase their use of cyber capabilities for strategic ends regardless of U.S. counter-offensive operations
- Controls:
  - Having an exact enumeration of the events in each category matters less than the direction and magnitude of the trends
    - Advocates of persistent engagement suggest it should have a substantial, perhaps unprecedented impact on adversary behavior.
    - **Anything other than a correspondingly strong reduction suggests the policy may not be working as intended**
  - Have multiple analytical teams with different data sources: USG, academia, cyber threat analysts

Shortcomings 3/3

- Significant methodological factors will hinder any direct assessment of correlation or causation
  - Timescale to discover cyber incidents hampers assessment as incidents are often not known until well after they are conducted
  - May be so few truly dangerous attacks that an increase or decrease of a small number of incidents leads to an enormous percentage increase or decrease
  - System is chaotic so that cause and effect are often indistinguishable
- Control:
  - Appropriate structuring of the framework and coding of the data
  - Giving up, because no strategy can have any measurable effect

DESCRIBING TRANSGRESSIONS TO BE MEASURED

SIPA

CYBER THREAT ALLIANCE

Norms from the Paris Call

- Prevent and recover from malicious cyber activities that threaten or cause **significant, indiscriminate or systemic harm to individuals and critical infrastructure**;
- Prevent activity that intentionally and substantially **damages the general availability or integrity of the public core of the Internet**;
- Strengthen our capacity to prevent malign interference by foreign actors aimed at **undermining electoral processes** through malicious cyber activities;
- Prevent **ICT-enabled theft of intellectual property**, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector;
- Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm;
- Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain;
- Support efforts to strengthen an advanced cyber hygiene for all actors;
- Take steps to **prevent non-State actors, including the private sector, from hacking-back**, for their own purposes or those of other non-State actors;
- Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

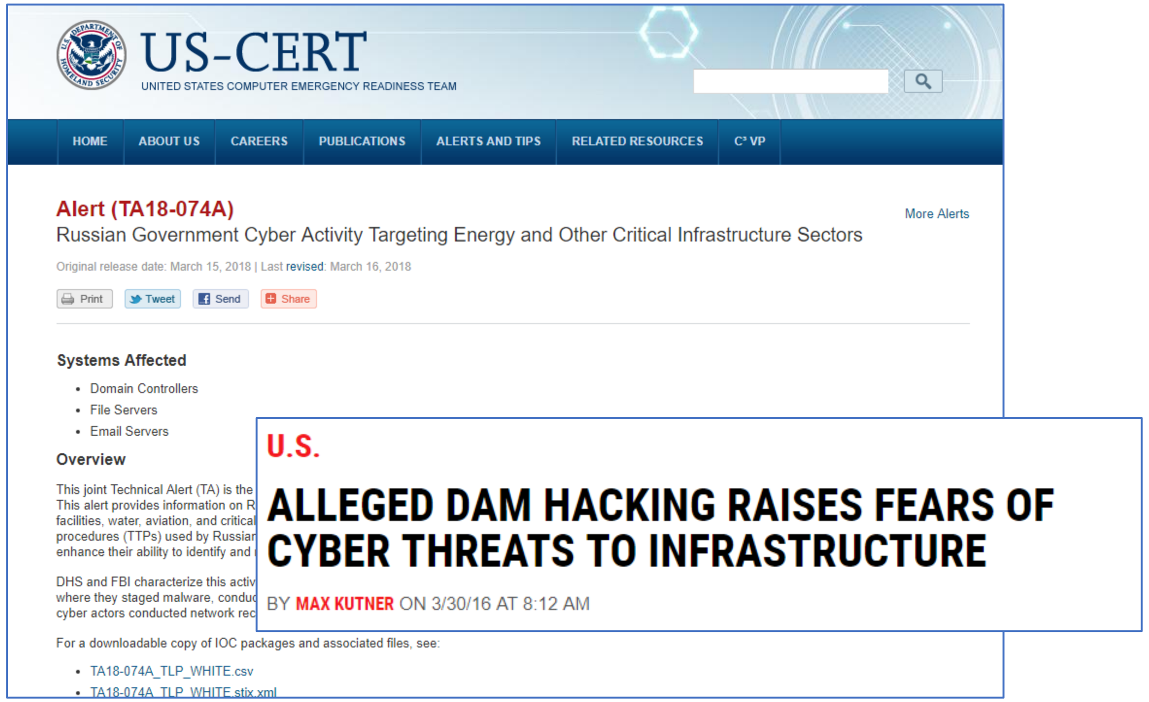
https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Categories of Adversary-Focused Metrics

- **Statements by Adversary Leadership**
  - Public and non-public statements
  - Statements may not match actions, but can be useful

Categories of Adversary-Focused Metrics

- **Presence in Specific Target Sets**
  - Any intrusions into particular targets might themselves be considered dangerous or destabilizing
  - Especially so if specifically warned to avoid those targets
  - Simplest metrics can be binary
    - Definitely in / Not definitely in
- **Potential Metrics**
  - Track instances of indicators associated with targeted critical infrastructure sectors



Alert (TA18-074A)

Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors

Original release date: March 15, 2018 | Last revised: March 16, 2018

Systems Affected

- Domain Controllers
- File Servers
- Email Servers

Overview

This joint Technical Alert (TA) is the
This alert provides information on R
facilities, water, aviation, and critical
procedures (TTPs) used by Russian
enhance their ability to identify and

DHS and FBI characterize this activ
where they staged malware, conduc
cyber actors conducted network rec

For a downloadable copy of IOC packages and associated files, see:

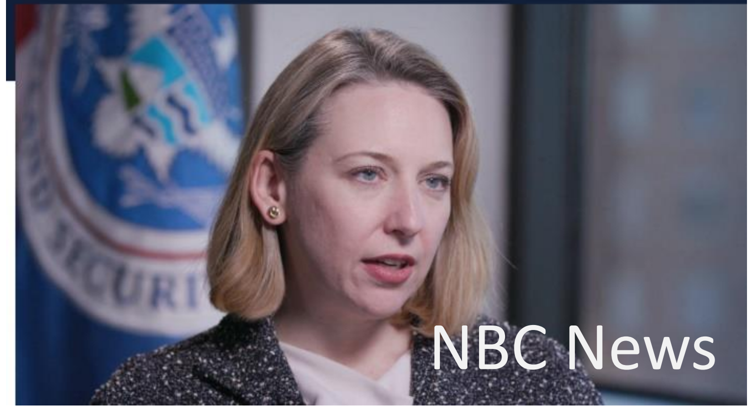
- TA18-074A_TLP_WHITE.csv
- TA18-074A_TLP_WHITE.stix.xml

U.S.

ALLEGED DAM HACKING RAISES FEARS OF CYBER THREATS TO INFRASTRUCTURE

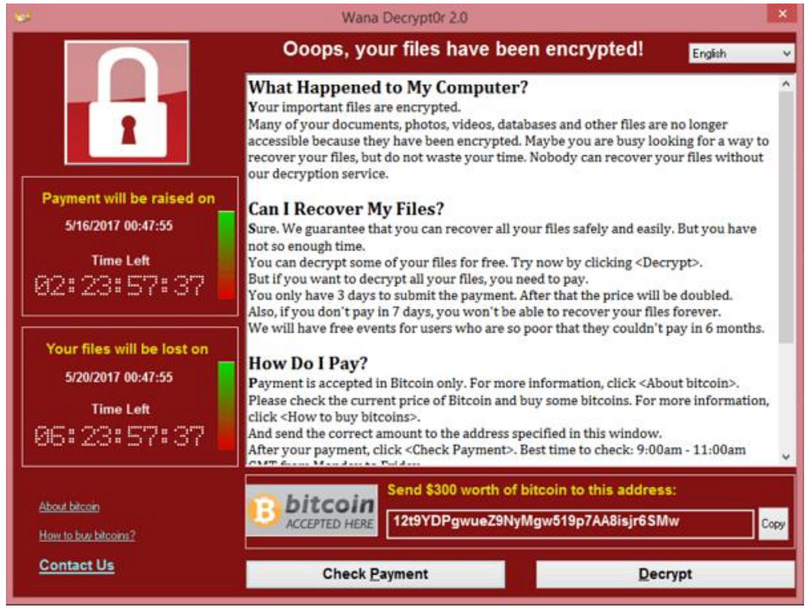
BY MAX KUTNER ON 3/30/16 AT 8:12 AM

Russians penetrated U.S. voter systems, top U.S. official says



Categories of Adversary-Focused Metrics

- **Reckless Attacks**
  - Attacks well beyond norms especially mass effects on civilians
  - Attacks with potential systemic effects
  - Potential metrics
    - Number and severity, per adversary



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

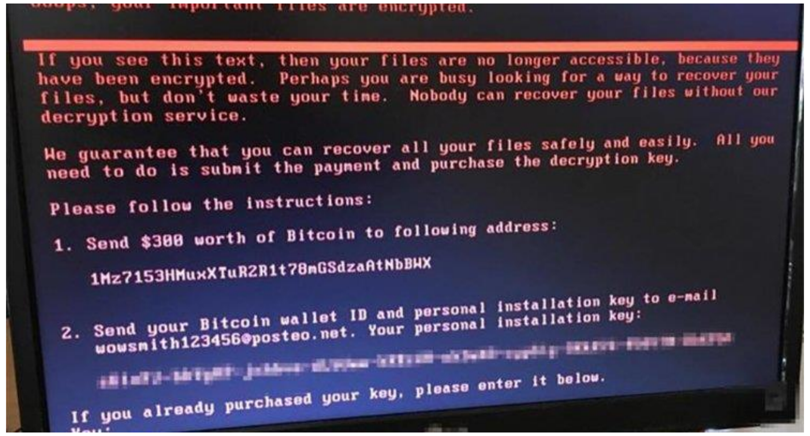
And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

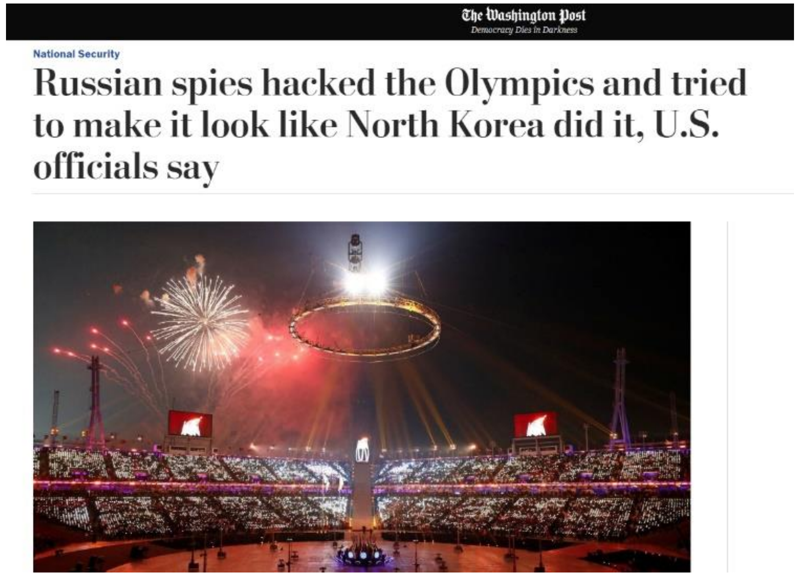
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   [redacted]

If you already purchased your key, please enter it below.
```

Categories of Adversary-Focused Metrics

- **Brazen Attacks**
  - Crossing specific threshold
  - Causing death and destruction especially outside of armed conflict
  - False flag attacks
  - Potential metrics
    - Number and severity, per adversary



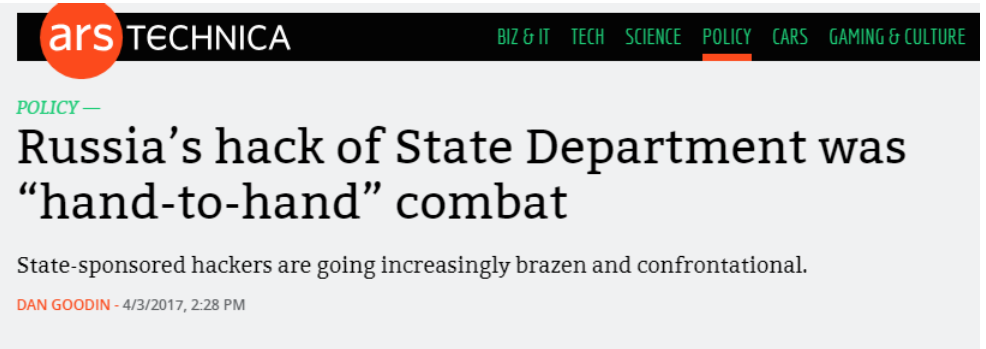
The Washington Post
Democracy Dies in Darkness

National Security

Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say

Categories of Adversary-Focused Metrics

- **Aggressive Attacks**
  - Track behavior and TTPs of adversaries
  - May not be measurable directly
  - Potential metrics
    - Five-point qualitative assessment by analysts



POLICY —

Russia's hack of State Department was "hand-to-hand" combat

State-sponsored hackers are going increasingly brazen and confrontational.

DAN GOODIN - 4/3/2017, 2:28 PM

Other Categories

Metrics of US Actions

- Outbound US operations
- Statements by US leadership
- Rationale:
  - Can help to determine causation, to determine effects are due to US actions

Metrics of Overall Relationship

- Can be simple metric on whether US relationship with each adversary country is improving, stable, or deteriorating
- Think US-North Korea changes from 2017-2018
- Rationale
  - Help determine causation

FUTURE WORK

Future Work

- Further refine framework
  - Explain or define “reckless, brazen, aggressive”
  - Explore quantity metrics
- Possible CTA analytical processes
  - Track metrics
- Process tracing of particular case studies
  - Who did what to whom, over time
- Game theoretic modeling

Future Work

- Research historical antecedents of persistent engagement.
- Similarities to other examples of where military and intelligence forces of the two blocs during the Cold War were in routine belligerent contact:
  - Anti-submarine warfare
  - Espionage-counterespionage
  - Freedom-of-navigation operations, and
  - Surveillance, and “exciter” flights against each other’s homelands

Indicators for “Cyber Peace Index”

- What observable indicators of fewer or less serious transgressions? Of more and more serious transgressions?
  - Frequency of incidents targeted at/disrupting core infrastructure (DNS, BGP)
  - Increase or decrease in DDoS severity (peak intensity, number of high-intensity attacks)
  - Fewer active nation-state groups

Call to Action

- If you believe this new offensive posture is going to make it more difficult to protect the entities you are being paid to defend, then let us know
  - Talk about it, blog about it, tweet about it
  - And if you include data along with your opinion, policymakers are much more likely to listen to you

- How can the network defense community help?
  - Help us pick the best frameworks, develop them, and – most importantly – use them!
  - Share your results with the community, whether in a trust group or publicly via blogs and reports
  - If we don't start measuring now, we'll just be that much further behind

QUESTIONS?

@Jason_Healey

@NEJenkins

SIPA

CYBER THREAT ALLIANCE