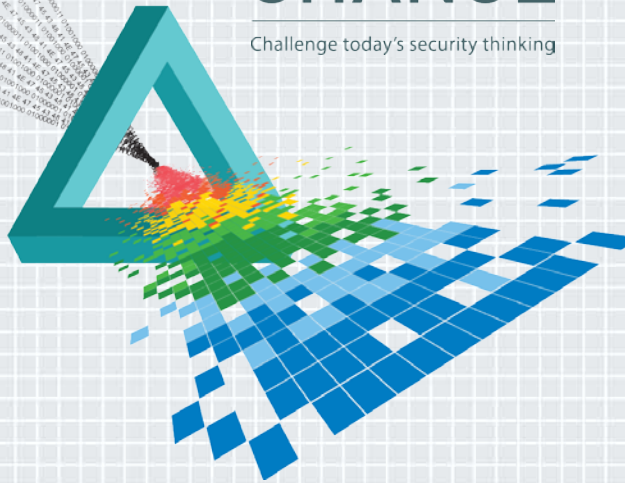
RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking



SESSION ID: HT-T10

Hacktivism: It's Not Just for the Lulz Anymore

Joe Gallop

Strategic Lead, Hacktivism Threat Intelligence, iSIGHT Partners

iSIGHTPARTNERS

"One cannot legitimately hope to improve a nation's free access to information by working to disable its data networks."

- cDc, CCC, 2600, Phrack

July 1, 1999

Anonymous is Dead

Nothing New Under the Sun

We - the undersigned - strongly oppose any attempt to use the power of hacking to threaten or destroy the information infrastructure of a country, for any reason. This has nothing to do with hacktivism or hacker ethics and is nothing a hacker could be proud of.

What happens when someone in another country decides that the United States needs to be punished for its human rights record? This is one door that will be very hard to close if we allow it to be opened.

Governments worldwide are seeking to establish cyberspace as a new battleground for their artificial conflicts. If hackers solicit recognition as paramilitary factions then hacking in general will be seen as an act of war.

Strategic combat planning in the United States and among other nations has reached the point where real-world cases are needed to justify assigned budgets. The LoU is providing this real-world case now.

How Can They Not?

RSAConference2015

San Francisco | April 20-24 | Moscone Center

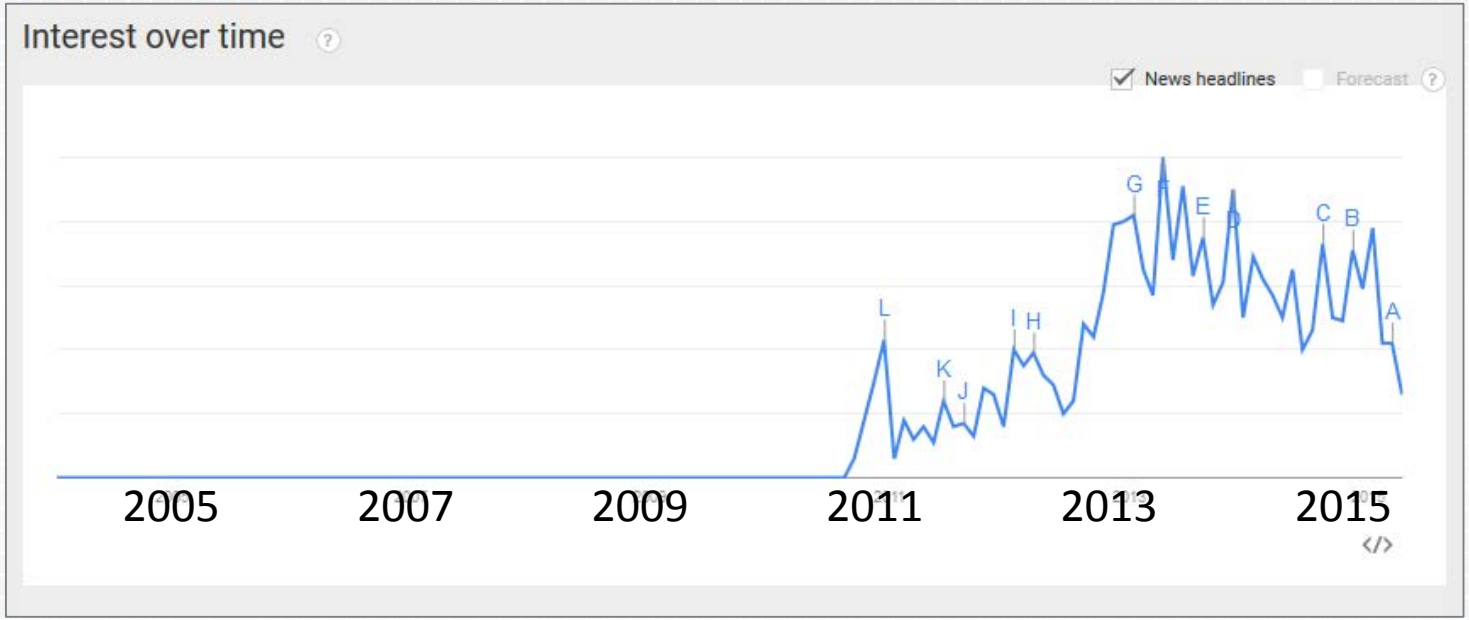
Plausible Deniability

What is Hacktivism?

"Using technology to improve human rights across electronic media."

Anonymous Made Hacktivism What It Is

"Hacktivist"



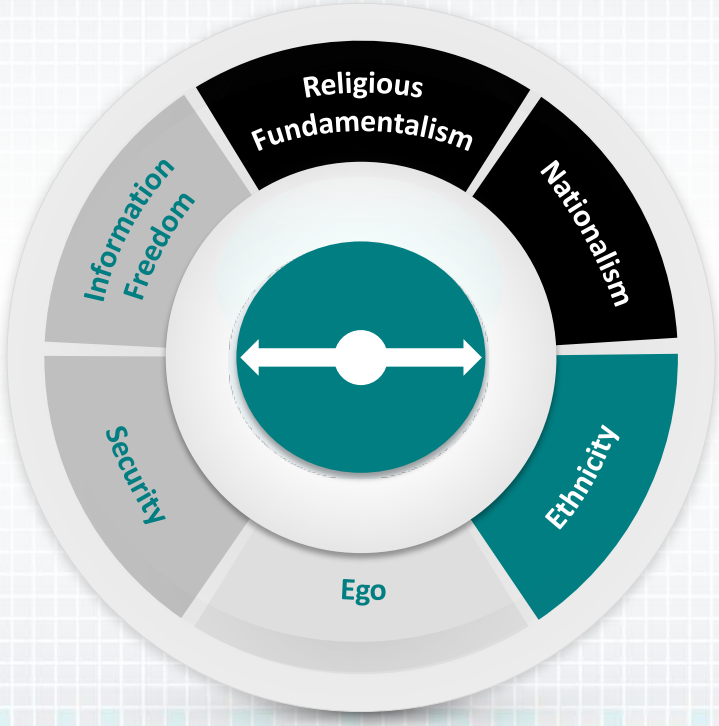
Google Trends

Web Definitions

- Hacktivism is the act of breaking into a computer system or disrupting services for a politically or socially motivated purpose.
- Hacking as an intimidation tactic, or “hacktivism,” is an emerging threat to the online world, involving the use of embarrassment to coerce action.
- The cornerstone of hacktivism is the recruitment of common people through social media to engage in participatory action to produce a loud noise.

Defining Hacktivism

MOTIVATIONS



OBJECTIVES


Actions


Opinion


Justice

UNIQUE FACTORS


Publicity


Disruption

Hacktivism:

Cyber threat activity that is motivated by ideology or rationale, with the objective of either enacting justice or of directly altering the actions or opinions of an audience.

Grassroots vs. State-sponsored

“We believe that the LoU should carefully investigate the idea of declaring "war" against China and Iraq. Was it planted with them by someone with different interests in mind other than advancing human rights considerations?”

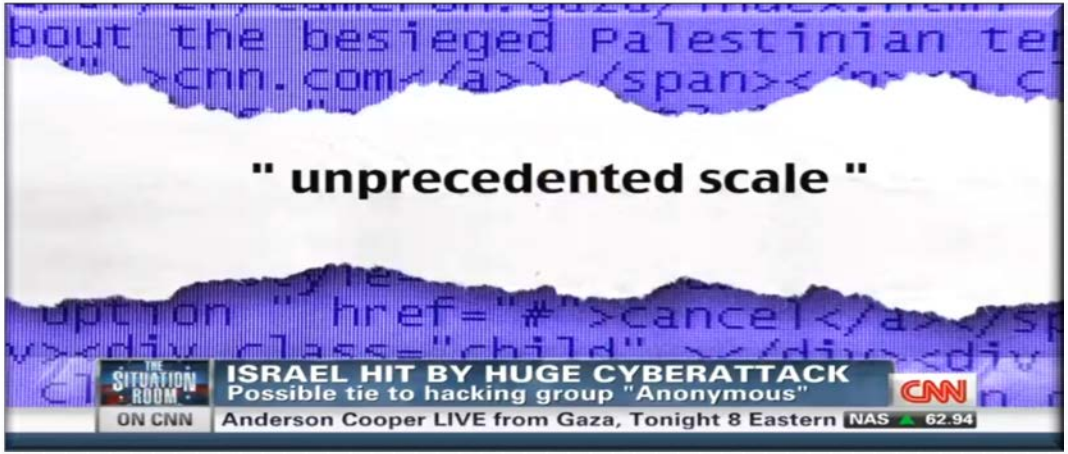
Who Made Hacktivism Fakeable?

State-Sponsored Hacktivism

- Institutional use of Cyber Espionage methodology is assumed.
- State linked hacktivist groups are growing in number and impact.

Media Misinformation

- 24-hour news cycle turns out large numbers of speculative reports.



- Hacktivists seek out this type of coverage, and make unsubstantiated claims in attempts to publicize their cause or their build their ego.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

Impact and Effectiveness

Perception is Reality

Inauthentic Attacks

Attacks are unsuccessful or do not occur.

Hacktivists claim, media promulgates.

Public perception is public reality.

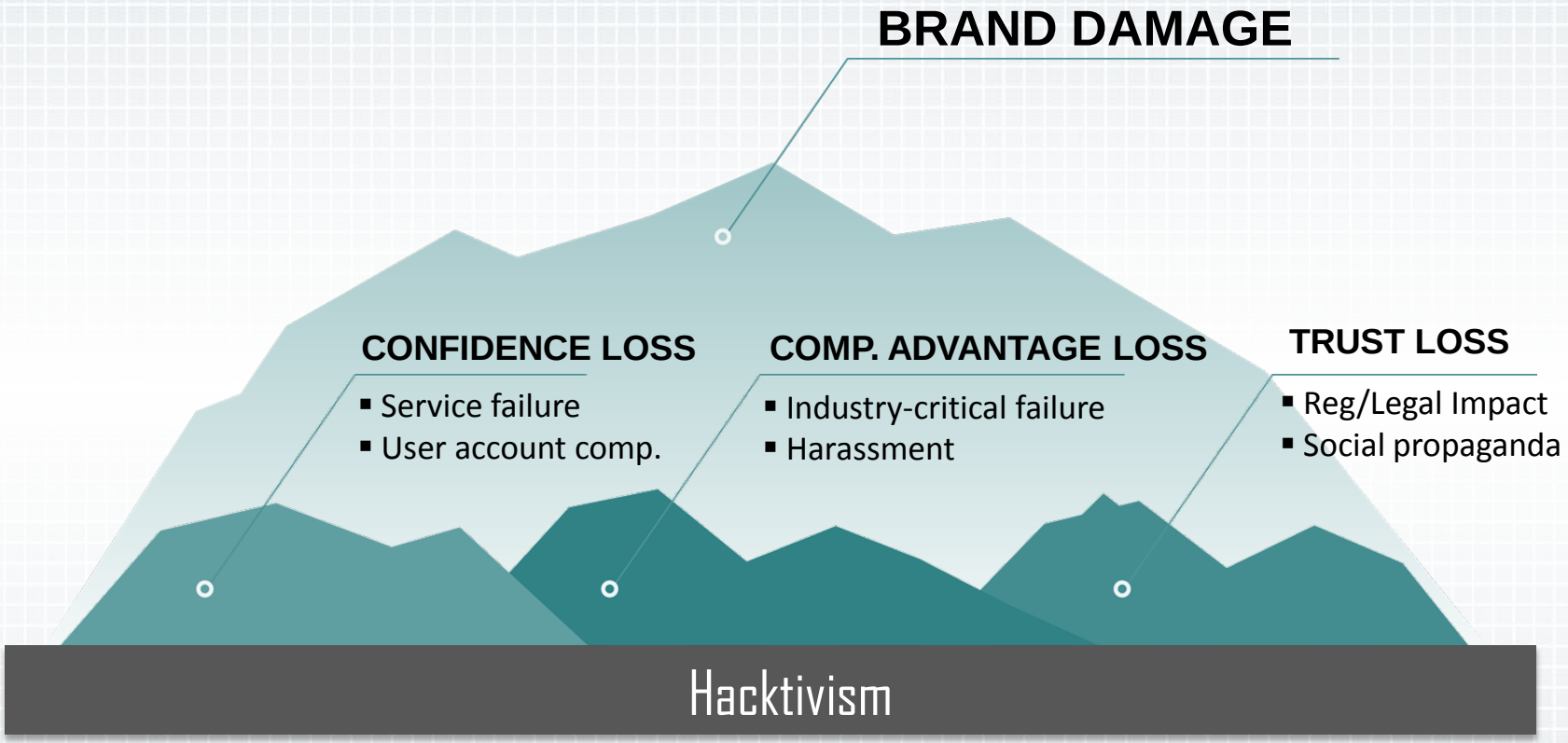
Damage by Association

Association may be real, fake, or insignificant.

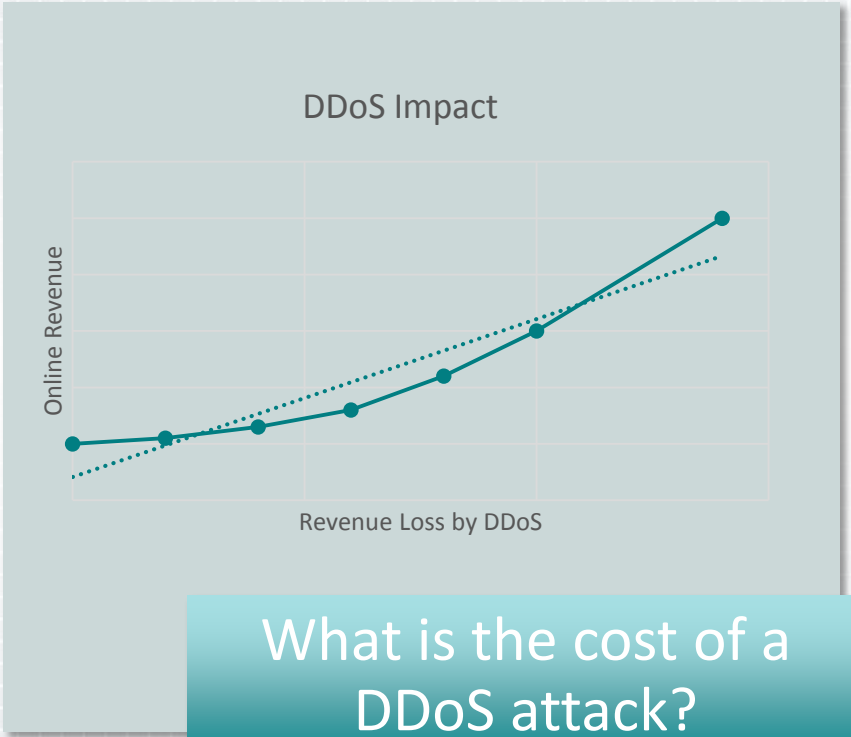
Propaganda implies or claims association.

Public perception is public reality.

Mountains and Molehills



Online Revenue



What is the cost of a DDoS attack?

Operation Ababil

$40,000 - $400,000/hr

iSIGHTPARTNERS

Production

Aramco Says Cyberattack Was Aimed at Production

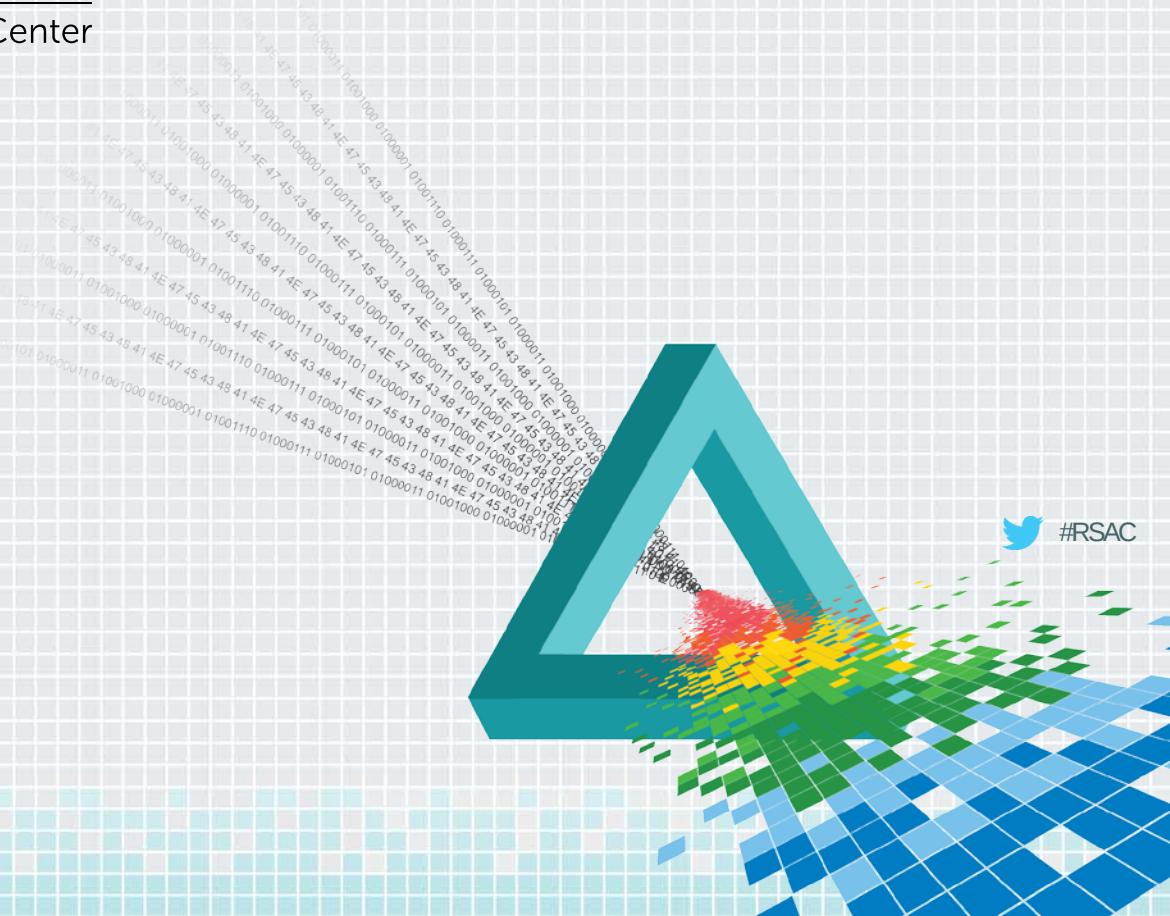
By REUTERS DEC. 9, 2012

"The main target in this attack was to stop the flow of oil and gas to local and international markets."

We, behalf of an anti-oppression hacker group that have been fed up of crimes and atrocities taking place in various countries around the world, especially in the neighboring countries such as Syria, Bahrain, Yemen, Lebanon, Egypt and ..., and also of dual approach of the world community to these nations, want to hit the main supporters of these disasters by this action.
One of the main supporters of this disasters is Al-Saud corrupt regime that sponsors such oppressive measures by using Muslims oil resources. Al-Saud is a partner in committing these crimes. It's hands are infected with the blood of innocent children and people.
In the first step, an action was performed against Aramco company, as the largest financial source for Al-Saud regime. In this step, we penetrated a system of Aramco company by using the hacked systems in several countries and then sended a malicious virus to destroy thirty thousand computers networked in this company. The destruction operations began on Wednesday, Aug 15, 2012 at 11:08 AM (Local time in Saudi Arabia) and will be completed within a few hours.
This is a warning to the tyrants of this country and other countries that support such criminal disasters with injustice and oppression. We invite all anti-tyranny hacker groups all over the world to join this movement. We want them to support this movement by designing and performing such operations, if they are against tyranny and oppression.

Cutting Sword of Justice

Efficiency



Lack of Recourse

Small or rogue nations:

- Faced with debilitating sanctions.
- There is no opportunity cost.
- There is no alternative for retaliation.

OPERATION ABABIL

BB&T
PNC
Bank of America
WELLS FARGO
REGIONS
BMO Harris Bank
citibank

Simple Cost of Alternatives

Diplomatic:

$200,000/hr

Kinetic:

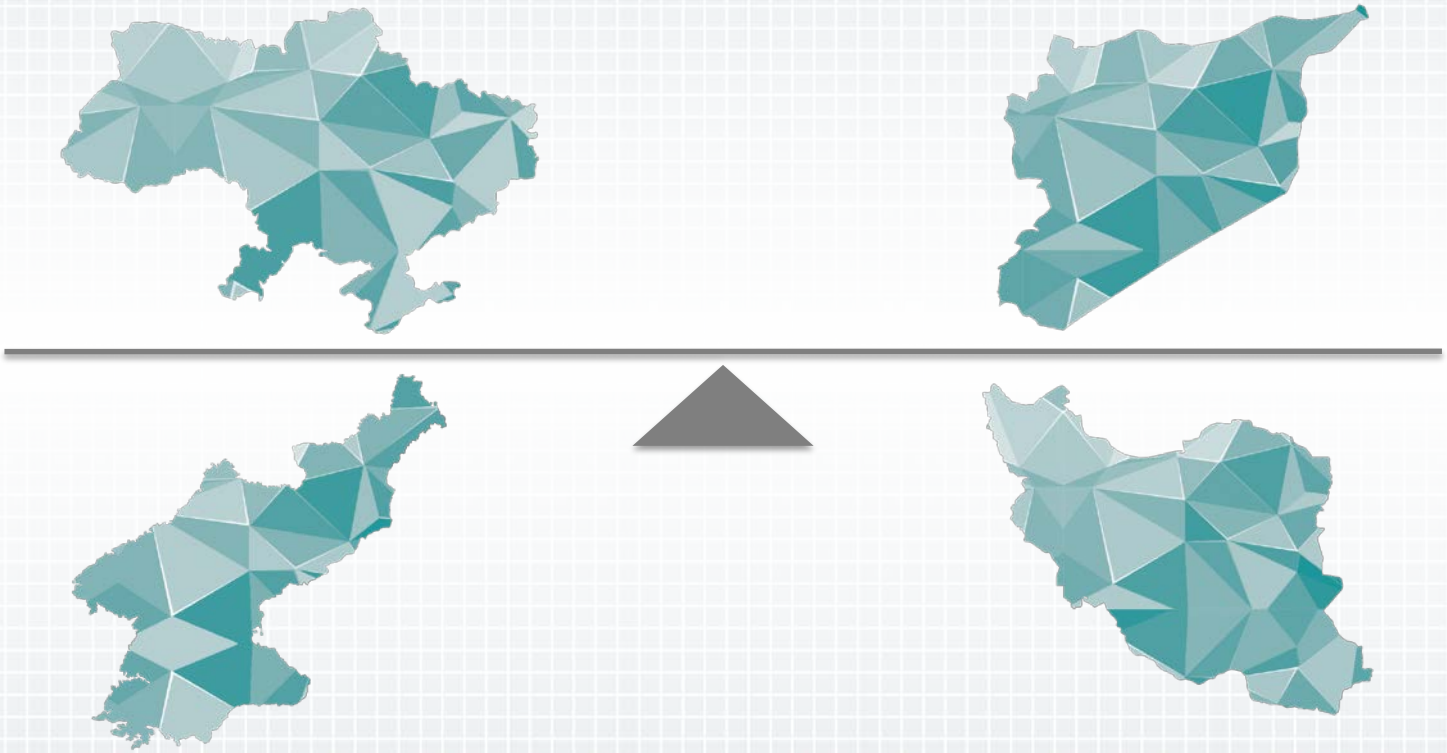
$1 million

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Triggers and Tipping Points

What is the tipping point?



Should We Treat Them Separately?

Attribution

- Levels of attribution:
  - Specific technical identifiers – allows blocking from identical source
  - General category of actors – allows you to understand likely targets and objectives, direct public relations, policy
  - Team or actor persona – allows detection of other methods in use by actor
  - True name attribution – allows direct law enforcement engagement

As a security professional or intelligence analyst, attribution to a category of individuals is critical for affecting business.

RSAConference2015

San Francisco | April 20-24 | Moscone Center

What Else Will Change?

Attacks From all Corners

What is the tipping point for terrorists?

- Capability
- Motivation

What is the tipping point commercial institutions?

- Creativity
- Low risk/fear of reprisal

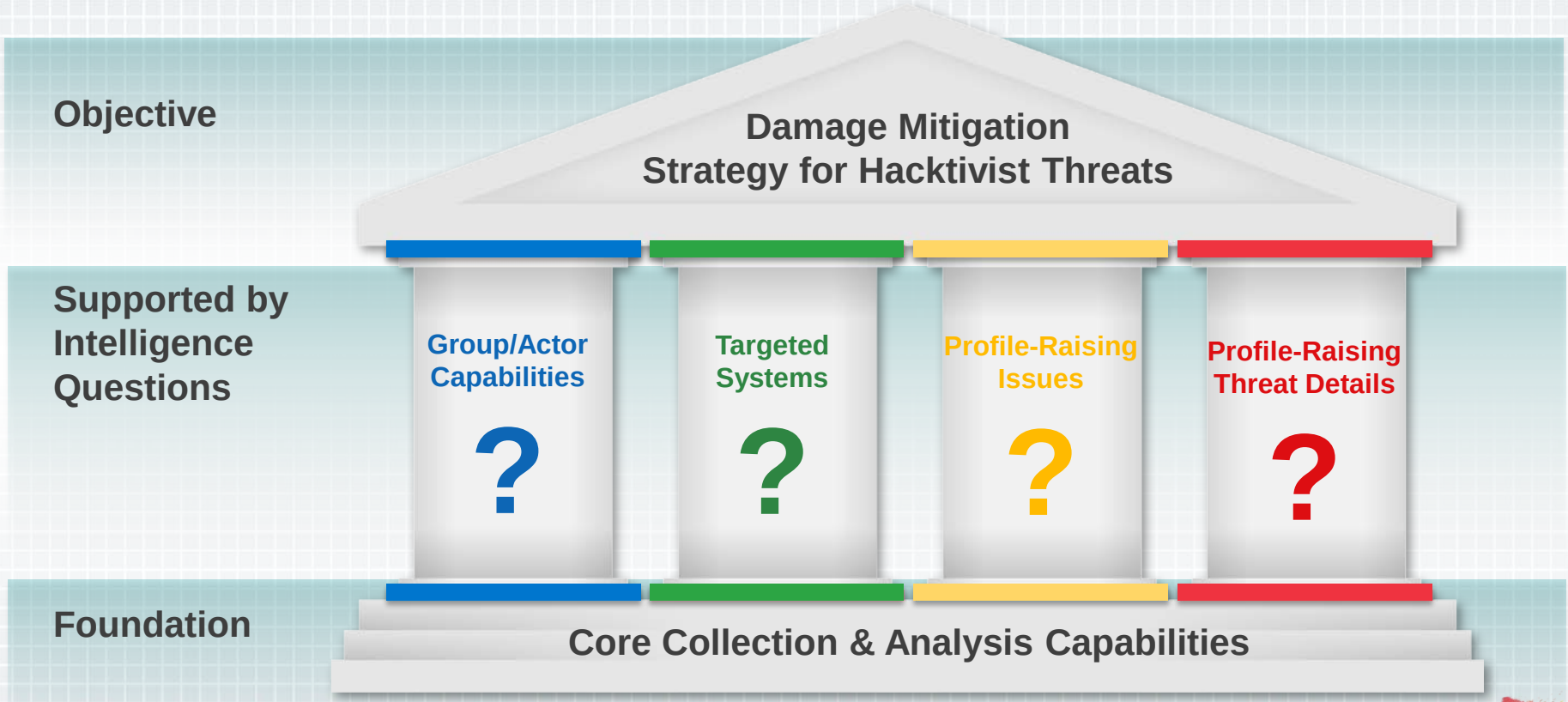
The Ubiquitous Mask

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Application

CTI to Mitigation Strategy



Apply

- If you are in the news media sector, be skeptical.
- Do not simply react to public hacktivist pronouncements. Be informed as to the true capabilities of the different groups that are likely to impact your organization.
- Understand “trigger actions” for your organization. Educate business executives to be aware of possible triggering risks and establish a communications process that facilitates risk discussions (integrate IT security and public relations).
- Understand business risks and mitigation strategies for extended outages of critical systems. There is a difference between systems being degraded and being destroyed.

"Strategic combat planning in the United States and among other nations has reached the point where real-world cases are needed to justify assigned budgets."