RSAConference2020
San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: HT-W02

Alice Ain't Home: Detecting and Countering Foreign Hackers on Social Media

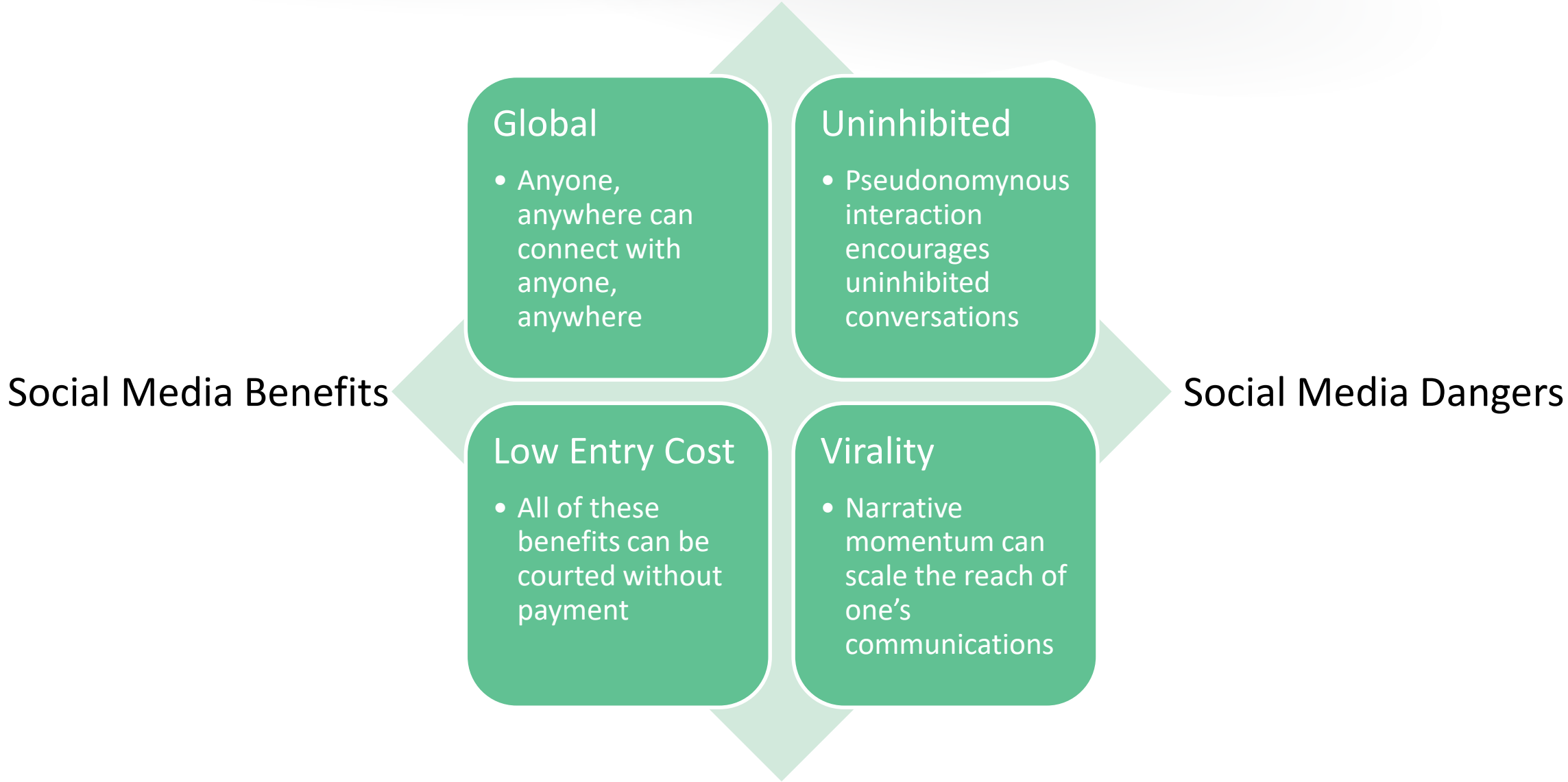
Chris Ott

Technology, Data Security, and Privacy Litigator
Rothwell Figg

Alex Kobzanets

Special Agent
Federal Bureau of Investigation

Part One: The Tyranny of Eggs



Part One: The Tyranny of Eggs

- Partial History of Social Media in Geopolitical Conflict Before 2016

Viral Protests and Social Movements

- "Arab Spring" 2011-2012
- Viral Protests throughout the former Soviet Bloc 2013-2014
- L'Affaire Magnitsky 2012 +

Putin Described Social Media as a CIA Invention Designed to Destabilize Russia

Part One: The Tyranny of Eggs

- Partial History of Social Media in Geopolitical Conflict Before 2016

Initial Reactions

- Total Shutdown (Ukraine BGP/IP Hijacking)
- Media/News
- Disinformation

2016 Election

Part One: The Tyranny of Eggs

- Social Media and the 2016 Election

Weaponizing Social Media Accounts

- Internet Research Agency
- “Troll Farms”

Different Types of False Social Media Personae

- The “Journalist”
- The “Leaker”
- The “Agitator”
- The “Victim”

All weaponizing the global reach, uninhibited discourse, and cheap virality

RSAConference2020

Alice Ain't Home - Part Two

Alice Donovan Case Study

Part Two: Alice Donovan

- Alice Donovan
  - Self Described - “Freelance writer and journalist”
    - Thirty Articles
      - “Does America Need Such Friends?”
      - “Russia to Destroy Terrorists in Aleppo”
      - “Blacks against Hillary Clinton”
    - DC Leaks and Guccifer 2.0
      - Stolen Emails
      - Synergies between articles and doxing
  - Not a single person but, rather, a valuable online persona

Part Two: Alice Donovan

Civil War in Venezuela: a US Joint Operation with Colombia?

By Alice Donovan

counterpunch.org — This July, the people of Venezuela elected the National Constituent Assembly that, as expected, would be aimed at preparing amendments to the Constitution. The convocation of this body was initiated by President Maduro. The opposition condemned and failed to recognize the elections stating the National Constituent Assembly convocation should be held by the referendum.

9 MONTHS AGO | Who shared? | Wrong byline?

US-Led Air Strikes Killed Record Number of Civilians in Syria

By Rob Seimetz, Alice Donovan

counterpunch.org — Air strikes carried out by the US and its coalition partners in Syria have killed the highest number of civilians on record since the bombing campaign began, a war monitor has said. The Syrian Observatory for Human Rights, a group mostly advocating anti-government forces in the war in Syria, said on Tuesday that the US-led coalition killed a total of 225 civilians between April 23 and May 23, the highest 30-day toll since the campaign began in 2014.

ABOUT A YEAR AGO | Who shared? | Wrong byline?

Escalation in Syria

By Alice Donovan

counterpunch.org — According to the Syrian media sources, the Russian government has taken measures to guarantee more security for its forces in case of possible attack regarding the recent U.S. Tomahawk air strikes on the Shayrat air base on April 7. At this moment, two Russian all-purpose jets capable of spotting and intercepting cruise missiles are barraging in the Eastern Mediterranean.

ABOUT A YEAR AGO | Who shared? | Wrong byline?

Dramatic Escalation in Syria - Russia Prepared to Strike Back

By Alice Donovan, Luke Rudkowski

wearechange.org — According to the Syrian media sources, the Russian government to guarantee more security for its forces in case of possible attack regarding the recent U.S. Tomahawk air strikes on the Shayrat air base on April 7. At this moment, two Russian all-purpose jets capable of spotting and intercepting cruise missiles are barraging in the Eastern Mediterranean.

ABOUT A YEAR AGO | Who shared? | Wrong byline?

Beginning in 2016, "Alice" Began Posting Widely Across the Political Spectrum

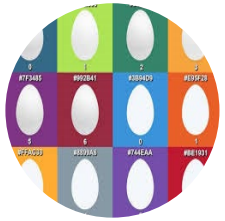
- Counterpunch
- GlobalResearch
- The ActivistPost
- Veterans Today
- Op-Ed News
  Popular Resistance
- Restoring Liberty
- WeAreChange

Part Two: Alice Donovan

Shallow Online Presence

Heavy on Political Memes

No podcast, radio, or YouTube interviews



Primarily Bot Followers

No personal details at all

Part Two: Alice Donovan

Valuable Online Persona

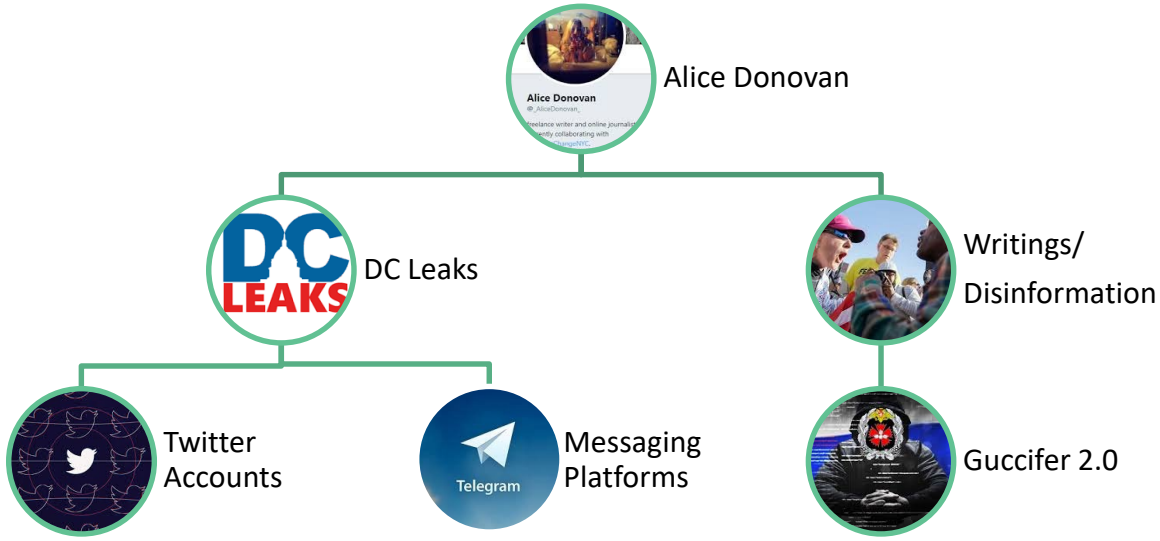
Hack Mouthpiece

Doxxing Infrastructure

Built-In "News" Coverage

Part Two: Alice Donovan

- Alice Donovan as an Online Persona
  - Web of Connections
  - Technical characteristics
    - Many people touching one account
      - Varied logins to a single account
      - Heavy VPN use
    - One person touching many accounts
    - Team management
  - Goofs
    - Doxxing contains Russian language settings in the PDFs
    - Linguistic goofs



Part Two: Alice Donovan

- Virality

RSAConference2020

Alice Ain't Home - Part Three

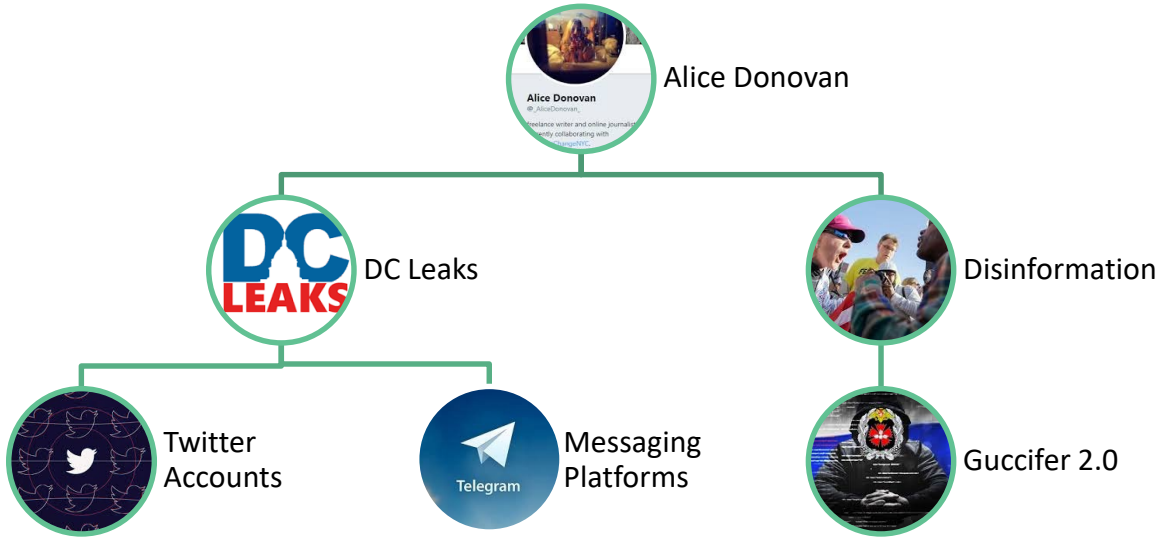
Sniffing Out the Bad Guys

Part Three: Sniffing Out the Bad Guys

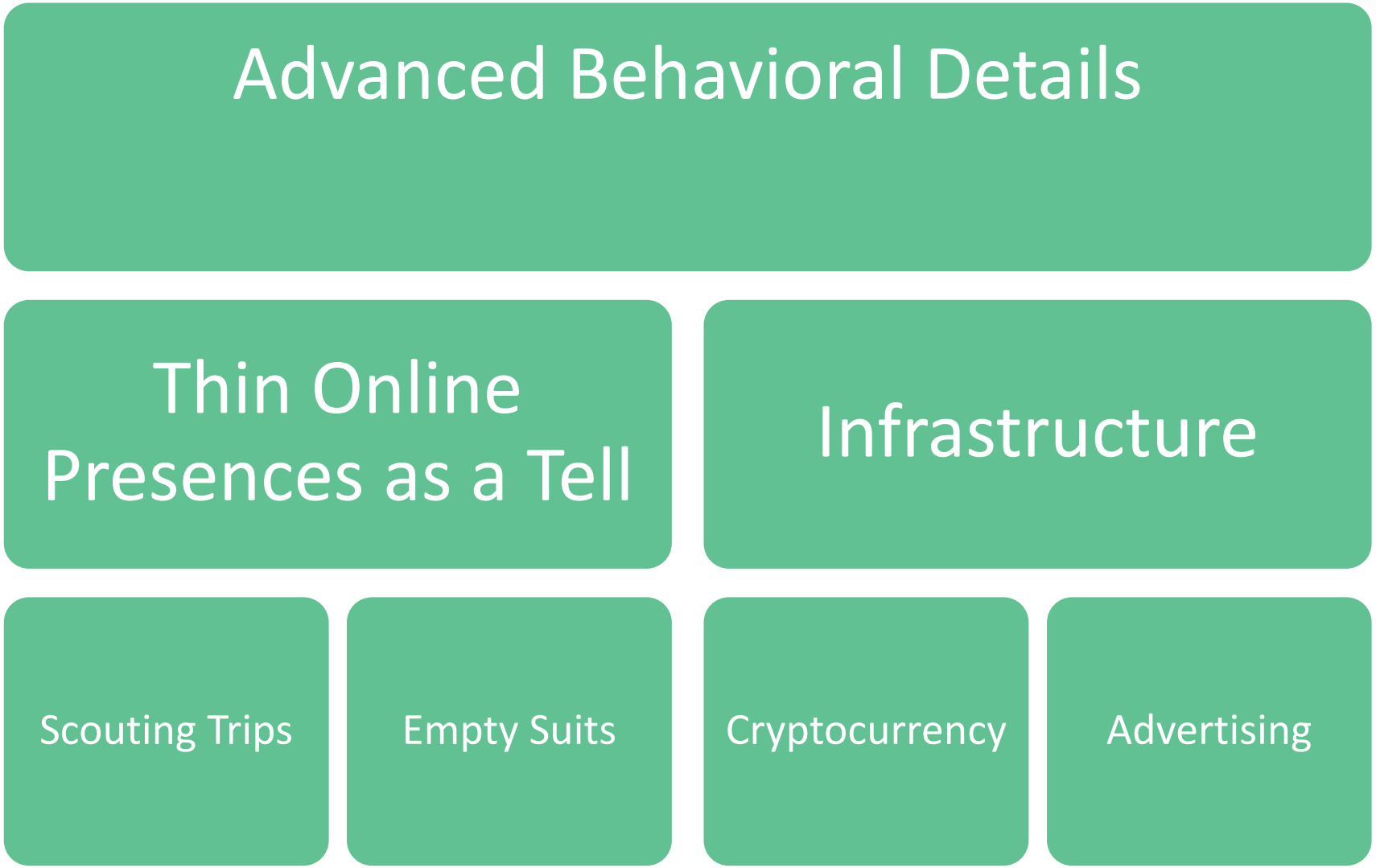
38. On or about June 8, 2016, and at approximately the same time that the dcleaks.com website was launched, the Conspirators created a DCLeaks Facebook page using a preexisting social media account under the fictitious name "Alice Donovan." In addition to the DCLeaks Facebook page, the Conspirators used other social media accounts in the names of fictitious U.S. persons such as "Jason Scott" and "Richard Gingrey" to promote the DCLeaks website. The Conspirators accessed these accounts from computers managed by POTEMKIN and his co-conspirators.

Part Three: Sniffing Out the Bad Guys

- Tendencies Described by the Internet Research Agency Indictment
  - Giveaways
    - Fixations
    - Payment
    - Online Infrastructure
    - Agitating on Both Sides



Part Three: Sniffing Out the Bad Guys



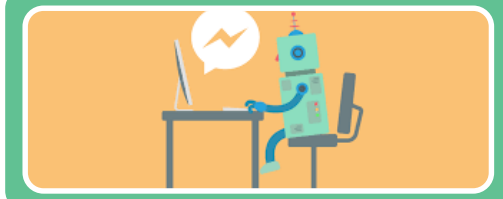
Part Three: Sniffing Out the Bad Guys

RSAConference2020

Alice Ain't Home - Part Four

Emergent Threats

Part Four: Emergent Threats



Automation

- Chat Bots
- AI maintentance
- Agitation AI

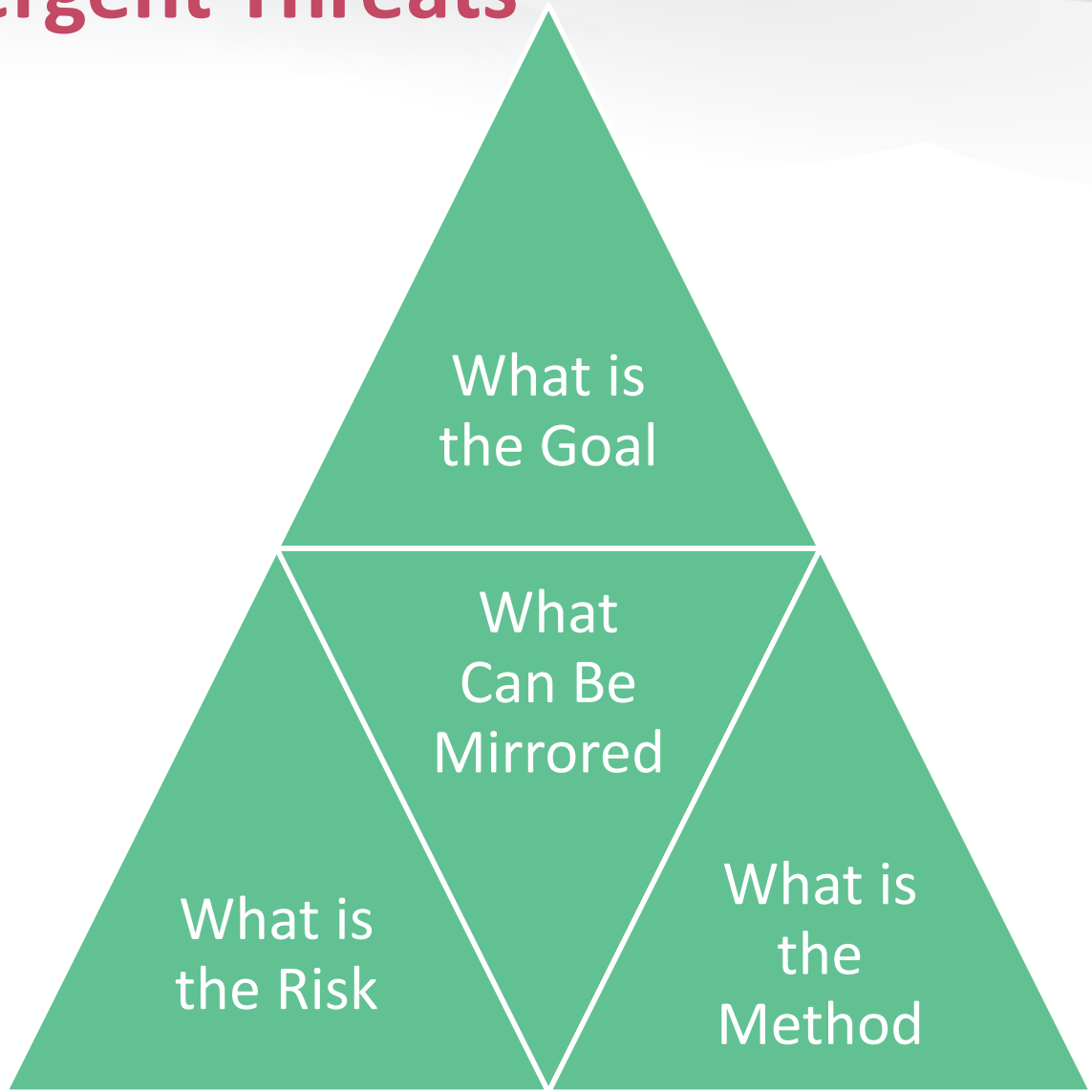
Iceberg Formations

DeepFake Audio and Video

- Real time?

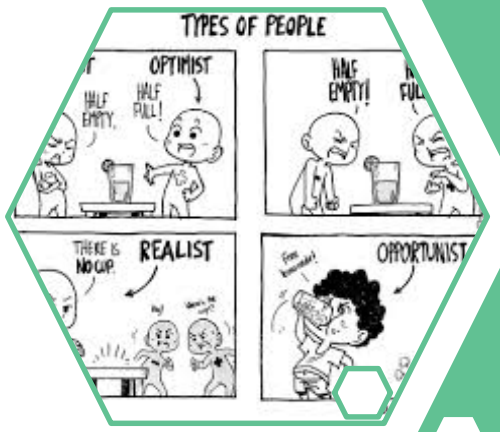
AI-Constructed Pictures

Part Four: Emergent Threats



What Have We Learned

Thin



Interconnected

Opportunisitic