WEBCAST SERIES

Quantifying Threat Actor Assessments

HOSTED BY
Katie Nickels

GUEST SPEAKER
Andy Piazza

Welcome to the SANS Threat Analysis Rundown

Our goal is to bring you the **inside scoop** on what you need to know about cyber threats. We'll bring you **different voices** from around the community to ensure you're **up-to-date** on what's happening in the threat landscape so you can **take action**.

Today's Agenda

- Rundown
- Deep-Dive
- Wrap-Up


SANS THREAT ANALYSIS RUNDOWN
Rundown

Rundown: January 28, 2021

- Emotet takedown
- NetWalker ransomware operation disrupted
- North Korean actors targeting security researchers
- SolarWinds hits keep on coming


SANS THREAT ANALYSIS RUNDOWN
Deep-Dive
Andy Piazza
phia LLC

phia
Cyber | Intelligence | Technology

Quantifying Threat Actor Assessments

Andy Piazza | @klrgrz | /in/andypiazza/
Chief Evangelist & Cyber Threat Analyst
GSEC, GCIH, GCIA, GCFA (Gold), GCTI (Gold), GCCC, GCPM
Master's Degree Candidate at the SANS Technology Institute

phia
Cyber | Intelligence | Technology

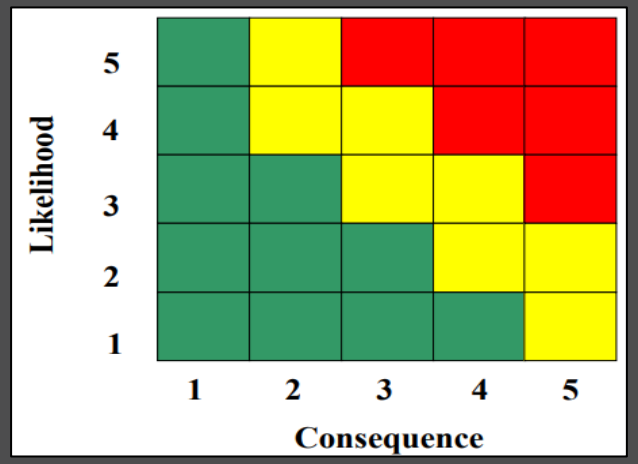
A Gap in Methodologies

- Current models attempt to quantify risks to organizations
- Risk models do not offer visibility into the human elements that many executives seek to understand
- The CHALLENGE: Develop a threat actor assessment methodology
- How do we address questions like:
  - Who should I care about tracking for my enterprise?
  - Is China more dangerous to us than Iran?

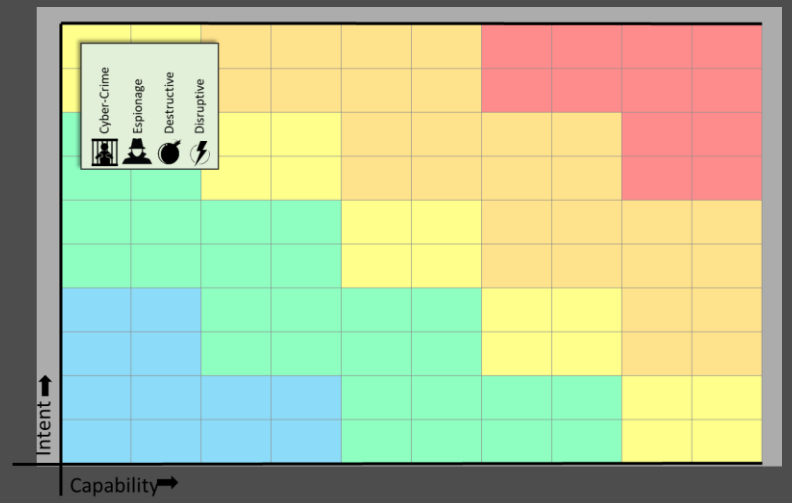
phia
Cyber | Intelligence | Technology

Quantifying Human Elements

- Target organizations have specific information that actors want
- Actors have unique intentions and capabilities
- *Intent* and *Capability* are quantifiable and mappable



Source: DOD Risk Reporting Matrix (OSD/ATL-ED, 2006)



Example Threat Box

phia
Cyber | Intelligence | Technology

Applying the Model

- Three notional organizations serve as the targets for this research
  - **American Oil (AmO)**
    - Texas-based oil company operating ICS manufacturing and operations in the US and Saudi Arabia
  - **United States Government Financial Organization (USGFO)**
    - Washington, DC-based federal agency that processes financial payments for all USG services that are provided to the public
  - **Information Technology Company (ITCO)**
    - California-based tech company that offers multiple online services, such as cloud computing and storage, and sells proprietary IT hardware

Attack Categories

- Each actor group is assessed for four attack categories
  - **Espionage** – attacks impacting the **Confidentiality** of data or systems
  - **Destructive** – attacks impacting the **Integrity** of data or systems
  - **Disruptive** – attacks impacting the **Availability** of data or systems
  - **Cyber-Crime** – attacks intended for **near-term financial profit**

phia
Cyber | Intelligence | Technology

Intent & Willingness

- Each actor is assessed for their intentions to carry out a specific attack type against the targeted organization
  - Attempts to answer, “Why would this actor target this organization with this type of attack?”
  - Analysts make this assessment based on existing threat intelligence
- The Intent score is balanced by the Willingness Modifier
  - Attempts to answer, “What constraints may impact the actor's intent?”
  - Considers existing legal, political, and economic dependencies

phia
Cyber | Intelligence | Technology

Intent & Willingness

	Intent: Why would this actor target this organization with this type of attack?	
5	Target-Specific Data	$ACTOR targets $ORG based on an objective that can only be achieved within $ORG's network
4	Ideology Association	$ACTOR targets $ORG based on its association with a specific ideology (e.g., USG, war, ...)
3	Sector Association	$ACTOR targets $ORG based on its association with a business sector (e.g., finance, energy,...)
2	Regional Association	$ACTOR targets $ORG based on its regional area of operations (e.g., N. America, Europe, ...)
1	Target of Opportunity	$ACTOR targets $ORG simply as a target of opportunity

	Willingness modifier: What constraints may impact the actor's intent?
-0	Strained diplomatic relations/previous hostilities/significant economic disruption perceived by $ACTOR from $ORG's operations
-1	Moderate relations with the U.S. and moderate economic dependencies between $ACTOR interests and $ORG's operations
-2	Strong diplomatic, economic, and security ties with the US

phia
Cyber | Intelligence | Technology

Capabilities & Novelty

- Each actor is assessed for their known capabilities by attack type
  - Attempts to answer, “What evidence is available that this actor is capable of this attack type?
  - Analysts make this assessment based on existing threat intelligence
- The *Capability* score is balanced by the *Novelty Modifier*
  - Attempts to answer, “What indication of advanced skills are evident?”

phia
Cyber | Intelligence | Technology

Capabilities & Novelty

	Capability: What evidence is available that this actor is capable of this attack type?	
5	Significant Capability	Significant evidence that $ACTOR previously conducted this type of activity; multiple trusted sources confirmed
4	Credible Capability	Credible evidence of operational capability; moderately confirmed
3	Limited Capability	Some evidence of operational capability; limited sources
2	Possible Capability	Very limited evidence of operational capability; feasibility confirmed
1	Not Capable	No evidence of operational capability; feasibility unconfirmed

	Novelty modifier: What indication of advanced skills are evident?
-0	Custom toolset per campaign with demonstrated living off the land capability
-1	Limited availability/high-cost toolset used in multiple campaigns
-2	Toolset generally available

phia
Cyber | Intelligence | Technology

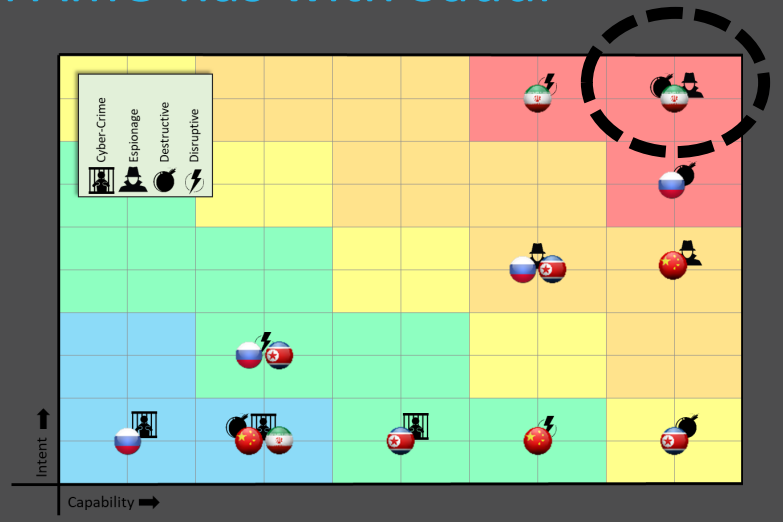
Sourcing the Model

- Evidence-based analysis prevents the “if I was a bad guy” approach
  - Historical threat reporting is foundational to the Threat Box
- Depth-of-knowledge was replicated using the following sources:
  - APT Groups and Operations Google Sheet
  - MITRE ATT&CK’s Groups pages
  - Malpedia’s Actors Page

Translating What You Read

- American Oil Threat Assessment
  - FireEye's "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware"
  - …"Iran's desire to expand its own petrochemical production and improve its competitiveness in the region."
  - Indicates at least an Intent-4, region association
  - Indicates Iran targets based on partnerships, which AmO has with Saudi

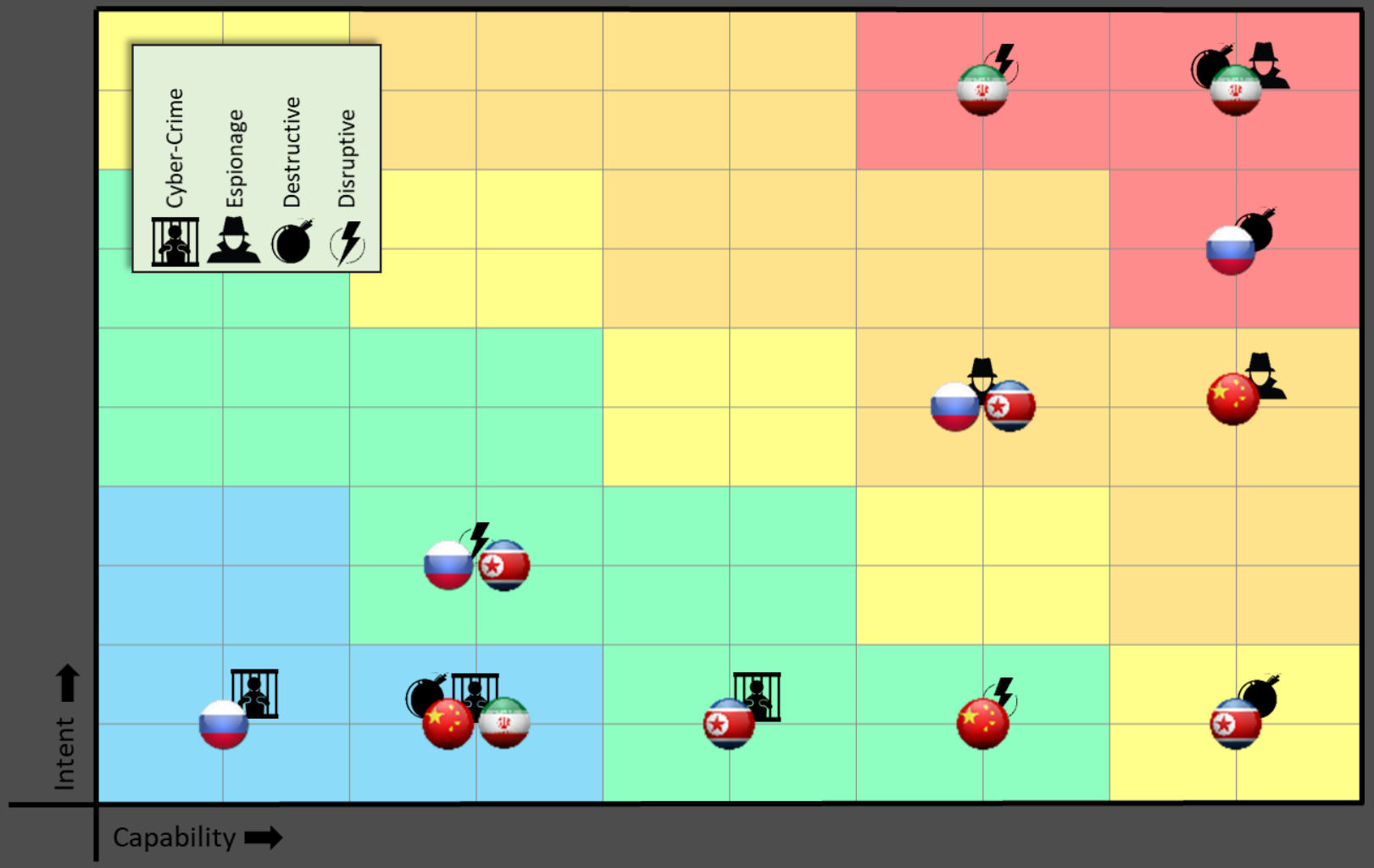
> We believe the targeting of the Saudi organization may have been an attempt to gain insight into regional rivals, while the targeting of South Korean companies may be due to South Korea's recent partnerships with Iran's petrochemical industry as well as South Korea's relationships with Saudi petrochemical companies. Iran has expressed interest in growing their petrochemical industry and often posited this expansion in competition to Saudi petrochemical companies. APT33 may have targeted these organizations as a result of Iran's desire to expand its own petrochemical production and improve its competitiveness within the region.



https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

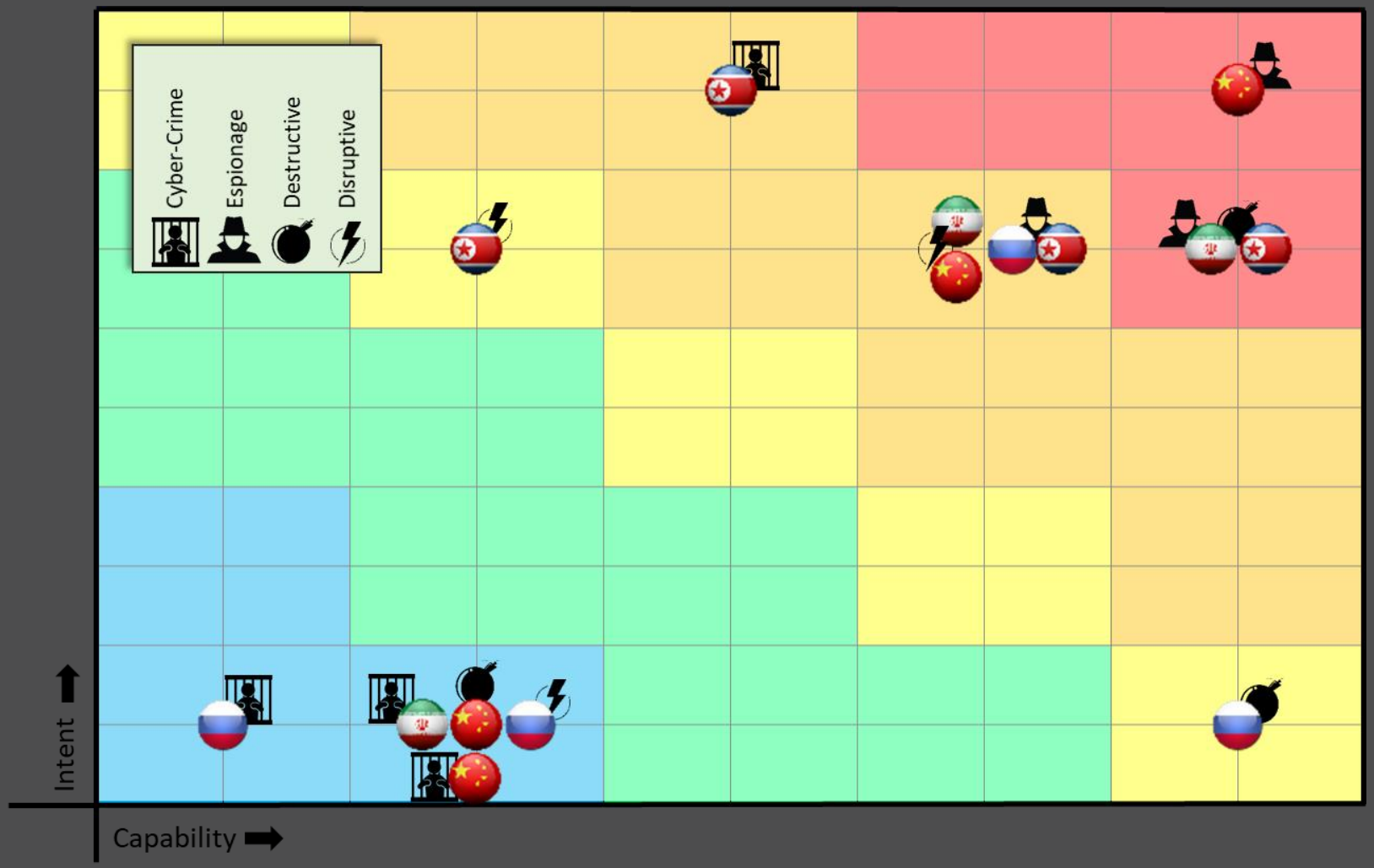
phia
Cyber | Intelligence | Technology

AmO's Threat Box



phia
Cyber | Intelligence | Technology

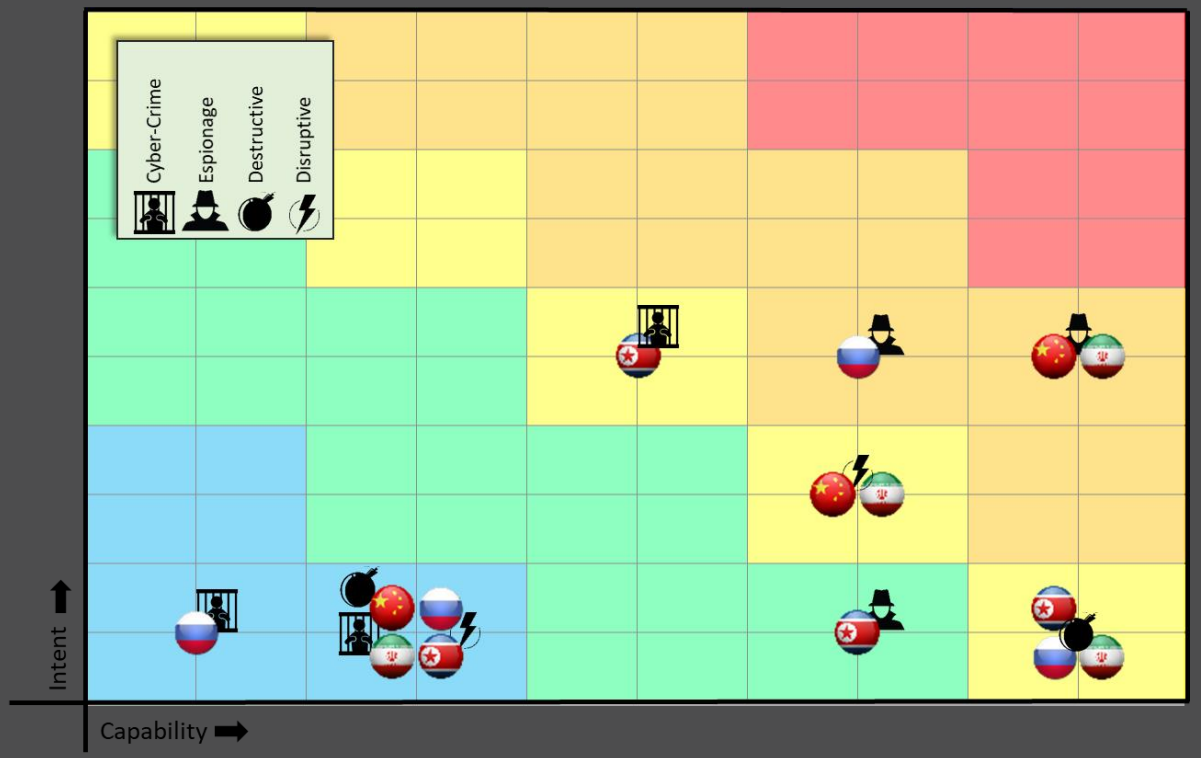
USGFO's Threat Box



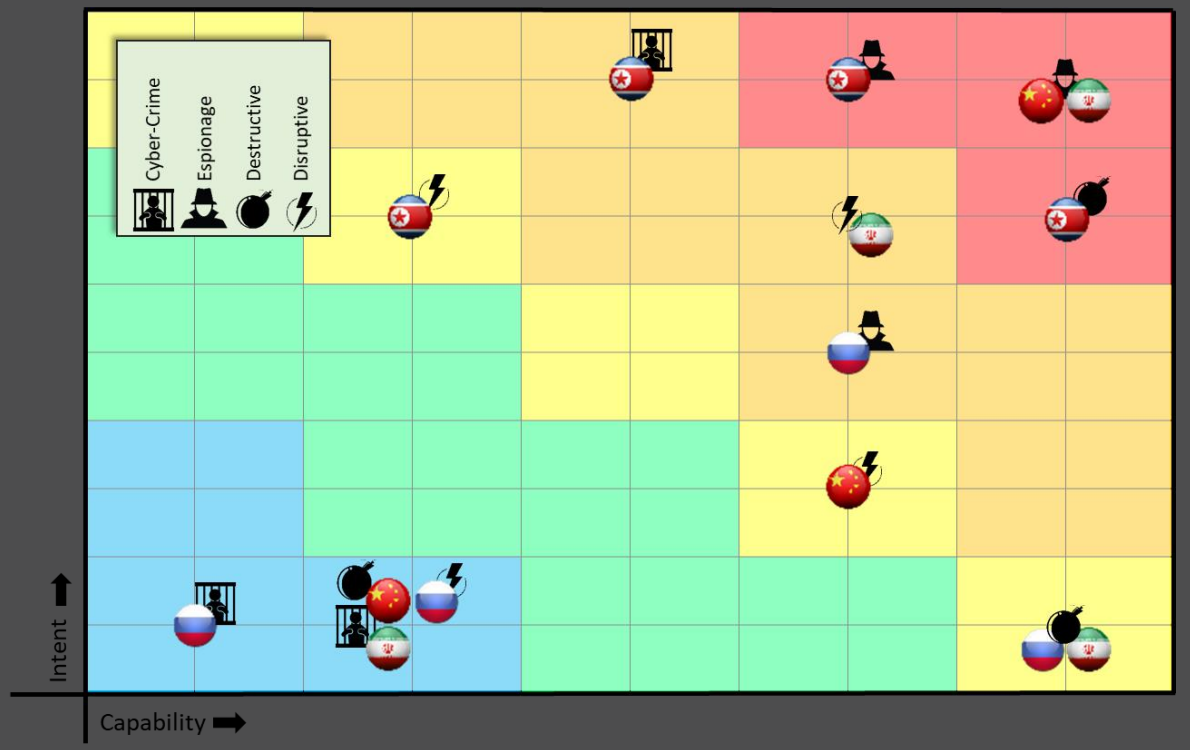
phia
Cyber | Intelligence | Technology

ITCO's Enterprise & Services Threat Box

Enterprise Threat Box

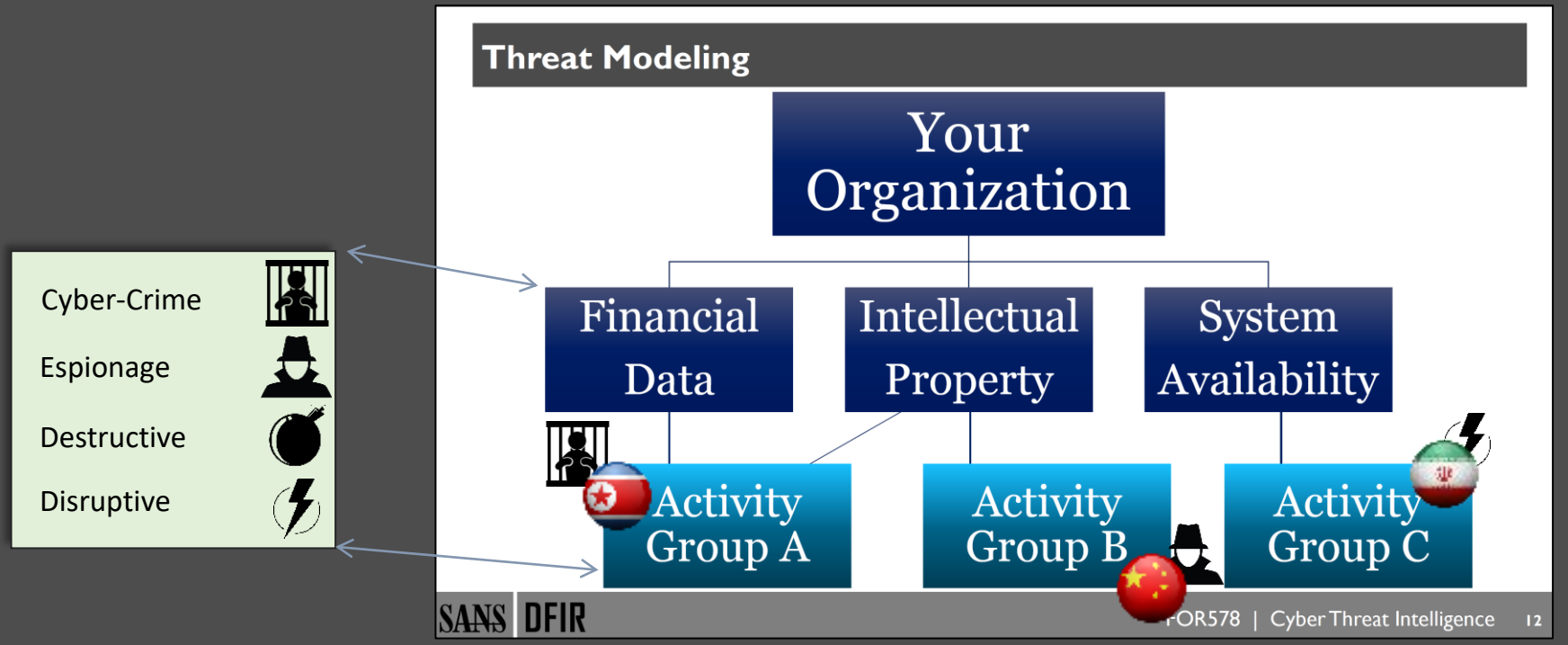


Services Threat Box



Pushing the Research Further

- Combining the Threat Box with an organization's threat model



Source: SANS Cyber Threat Intelligence course (FOR578)

phia
Cyber | Intelligence | Technology

Summary

- Risk models do not account for human intentions and capabilities
- Threat Box fills this gap by quantitatively assessing actors
  - It is data driven and target focused
  - Historical reporting is a foundational requirement for success
  - Provides analysts and executives with a graphical representation of threat actors' intentions and capabilities to carry out attacks

phia

Cyber | Intelligence | Technology


SANS THREAT ANALYSIS RUNDOWN
Questions
and discussion

Action Items

- Consider how you assess the threat actors that matter most to your org
- Think about if you could use some kind of quantifiable assessment methodology
- Remember the limitations of any assessment methodology

References

- Andy's work
  - https://klrgrz.medium.com/quantifying-threat-actors-with-threat-box-e6b641109b11
  - https://www.sans.org/reading-room/whitepapers/threatintelligence/paper/39585

References

- Emotet
  - https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
  - https://www.youtube.com/watch?v=_BLOmClsSpc
  - https://team-cymru.com/blog/2021/01/27/taking-down-emotet/
- NetWalker
  - https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

References

- North Korean actors targeting security researchers
  - https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/
- SolarWinds
  - https://www.microsoft.com/security/blog/2021/01/20/deep-dive-into-the-solorigate-second-stage-activation-from-sunburst-to-teardrop-and-raindrop/
  - https://www.fireeye.com/content/dam/collateral/en/wp-m-unc2452.pdf
  - https://www.splunk.com/en_us/blog/security/a-golden-saml-journey-solarwinds-continued.html


SANS THREAT ANALYSIS RUNDOWN
Thank you for coming!
For the recording and slides, please visit
https://www.sans.org/webcasts/archive/