Cyber Security Defense:

From Moving Target Defense to Cyber Deception

Jie Wu

Temple University

Outline

1. Offense vs. Defense
2. Cyber Deception in Offense
3. Deep Fake
4. Cyber Deception in Defense
5. Moving Target Defense
6. Challenges of Cyber Deception
7. Conclusions

1. Offense vs. Defense

- The Art of War
  - All warfare is based on deception
- Offense vs. Defense
  - Attack is the secret of defense
  - Defense is the planning of an attack
- Cyber Deception
  - Both attacker and defender

2. Cyber Deception in Offense

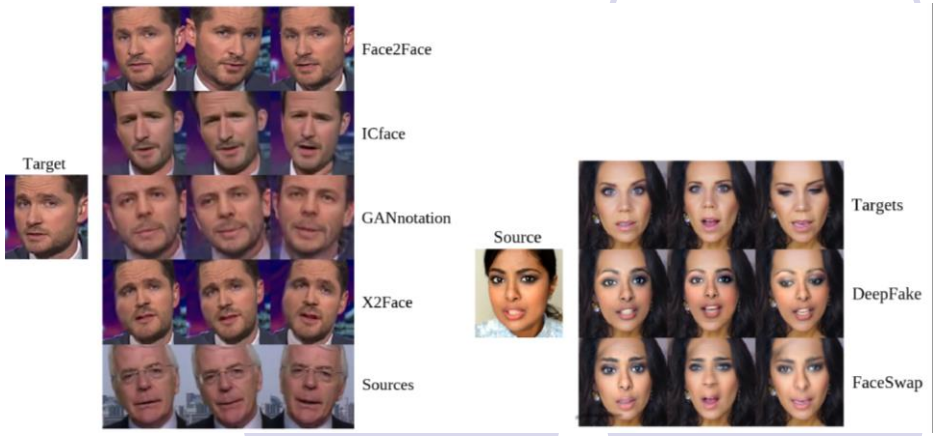
New York Times (12/28/2020)

Designed to Deceive

- Website Generated.Photos
- "unique, worry-free" fake person for $2.99

3. Deep Fake

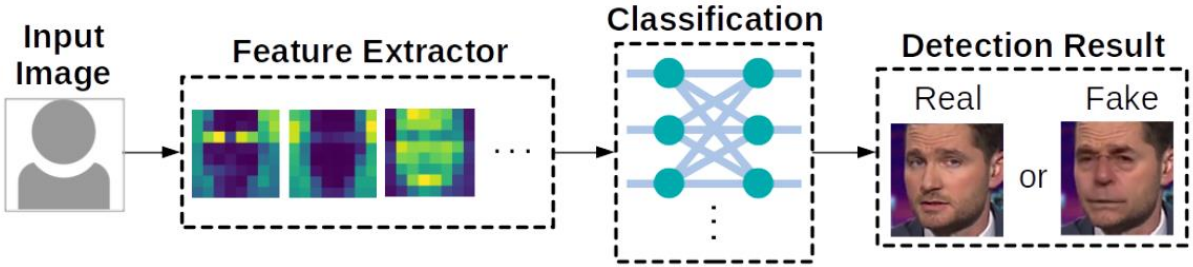
- Defend against facial forgery



Face reenactment

Face swapping

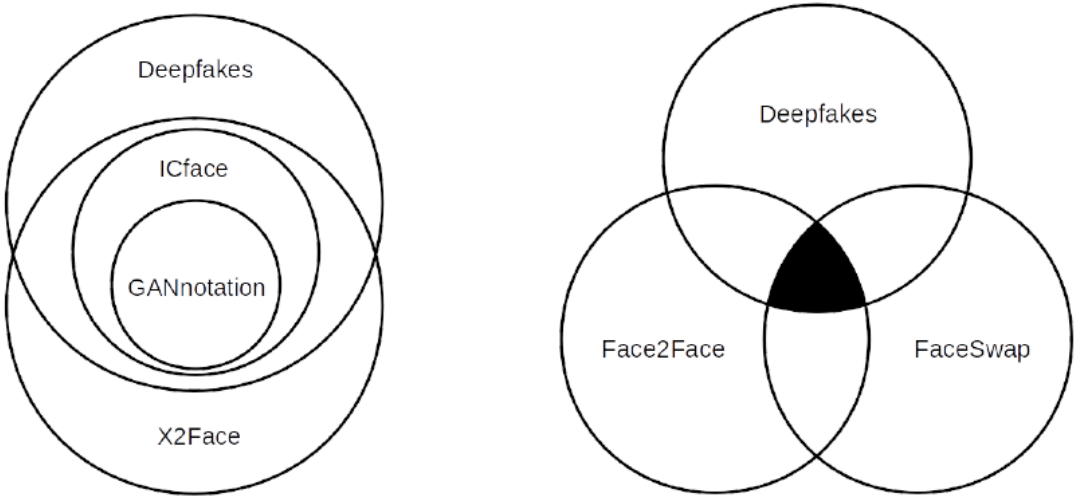
Face2Face, CVPR 2016



Architecture of deepfake defense systems

Deep Fake Detection

- Limitation of current defense systems
  - Cannot defend against unseen attack methods
  - Features of different attack methods can be independent

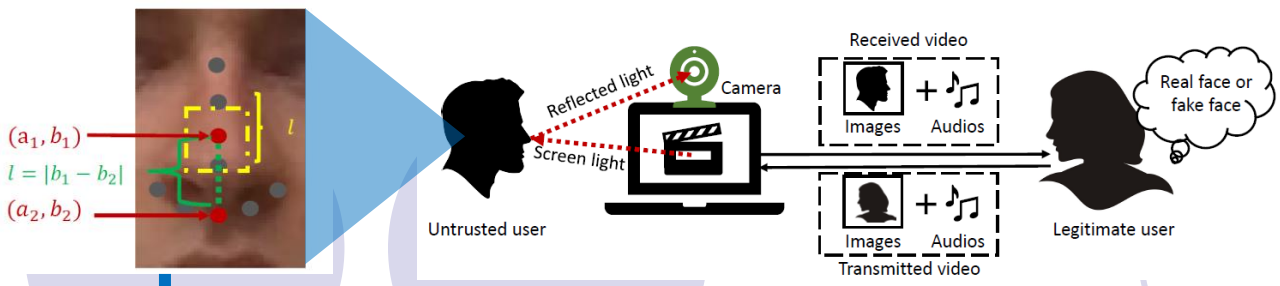


Feature overlap among existing facial forgery techniques [1] (tested on MesoNet)

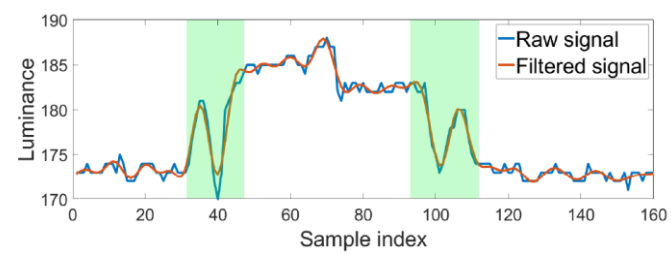
[1] J. Brockschmidt, J. Shang, and J. Wu., "On the Generality of Facial Forgery Detection", Proc of REUNS 2019 (Best Paper)

Deep Fake Detection (Cont'd)

- Detection using side-channel information [2]
  - The screen light reflected off human faces



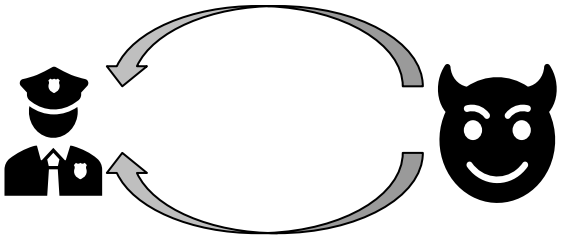
$$C = 0.2126R + 0.7152G + 0.722B$$



[2] J. Shang and J. Wu, "Protecting Real-time Video Chat against Fake Facial Videos Generated by Face Reenactment", *Proc of ICDCS 2020*

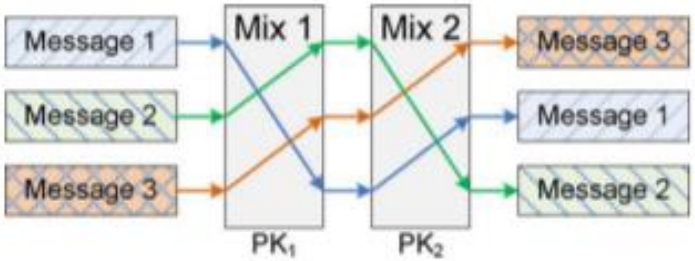
2. Cyber Deception in Defense

- Cyber deception
  - Planned actions to mislead/confuse (i.e. trap) attackers
- Goals
  - Complement detection, enhance prevention, and mitigate successful attacks
- Unit and layer
  - Parameter, file, account, profile, …
  - Network, system, application, data, …
- Life cycle of cyber deception
  - Collect knowledge of attacker
  - Implement deception schemes

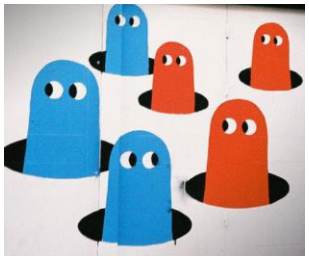


Types of Deception

- Perturbation
  - Perturb sensitive data with noises
- Mixing
  - Prevent linkability (mixing zone)



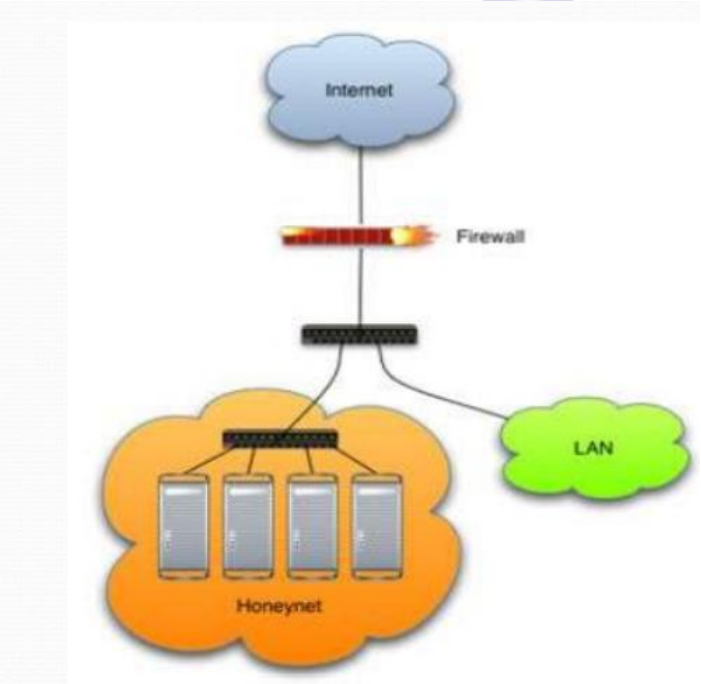
- Obfuscation
  - Decoy targets and/or reveal useless info
- Honey-X
  - Disguise honeypots as real systems
- Moving target defense (MTD)
  - Change attack surfaces to increase uncertainty and complexity for attackers



Honeypots and Honey-X

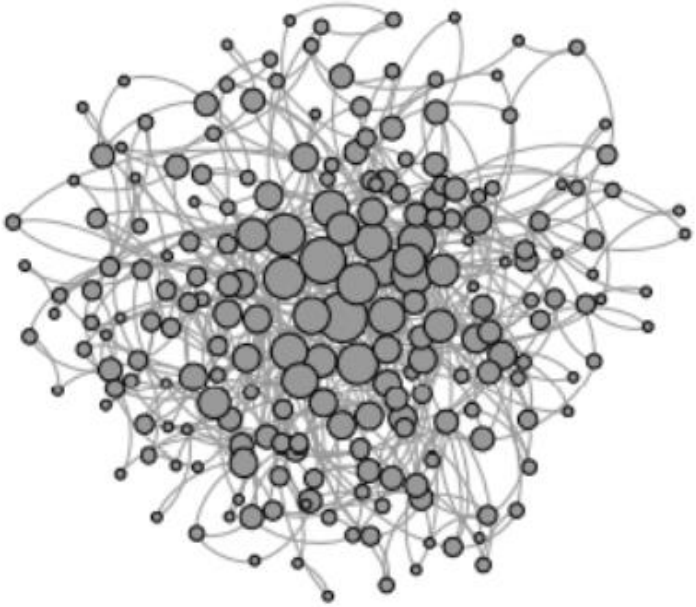
- Honeypots
  - Bears: honey eaters
  - Traps

- Honey-X
  - Honeynet: two ore more honeypots on a network
  - Honeyfile, honeyword, …



5. Moving Target Defense

- Hierarchical military command chains
- Network hierarchy
  - SDN controllers: load balance and fault tolerance



Self-Organizing Solutions

Local decision

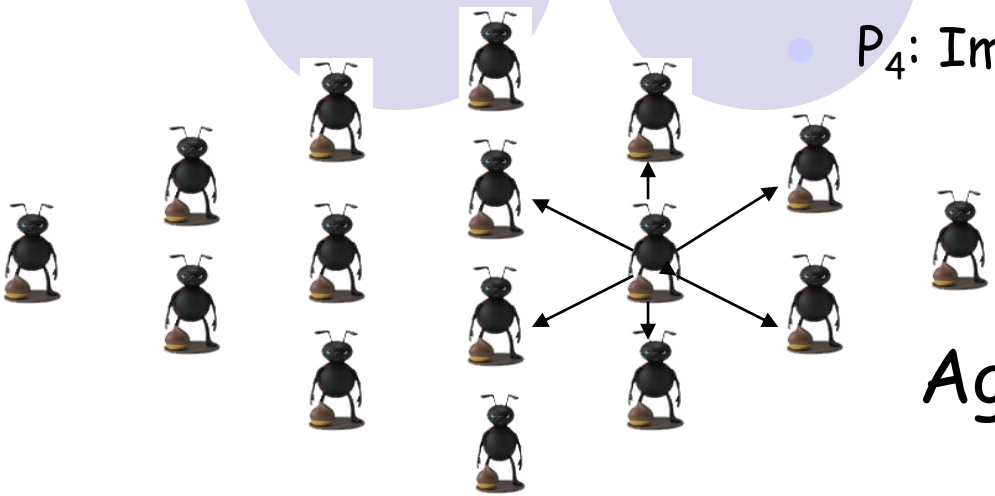
- P2P and simple interaction (mostly local and without sequential propagation)

Global functionality

- Adaptive, robust, and scalable

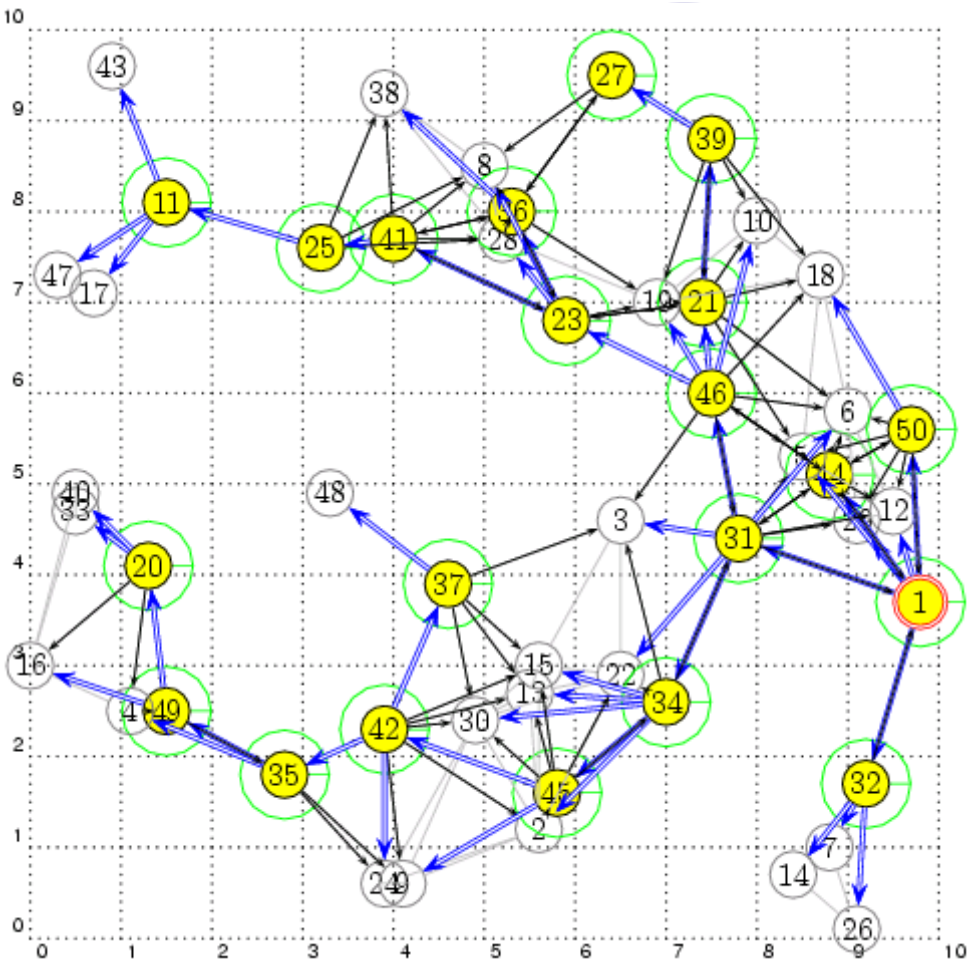
Principles

- P_1: Local interactions with global properties (scalability)
- P_2: Minimization of maintained state (usability)
- P_3: Adaptive to changes (self-healing)
- P_4: Implicit coordination (efficiency)



Agility

MTD Applications



Connected Dominating Set (CDS)

Local decision:

backbone nodes

based on node priority (ID, degree, …)

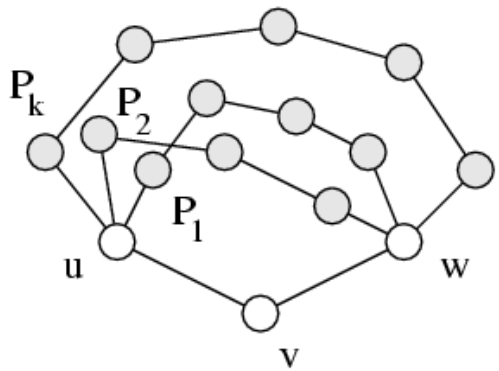
Global properties:

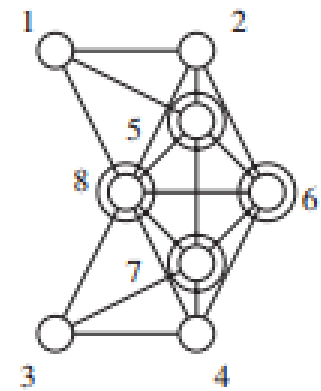
Connectivity

Coverage

Application: Resiliency and Rotation

- Redundancy: *K-connected & K-dominated*
  - Non-backbone node: K node-disjointed paths for any neighbor pairs (for multiple CDS)





- Moving target defense: CDS rotation
- *Self Healing: How can we deal with the complexity of building a structure along with a change of topology [3]?*

[3] J. Wu, "Uncovering the Useful Structures of Complex Networks in Socially-Rich and Dynamic Environments", *Proc. of IEEE ICDCS*, 2017

4. Challenges of Cyber Deceptions

- Limited Applications
  - Projected market to be $1B by 2020
- Effectiveness
  - How to measure?
- Game Theory and Learning
  - Ability of both attackers & defender

Limited Applications in Defense

- Still limited in cyber deception, why?
  - Differences: cyber deception vs. deceptions in warfare
    - Domain: cyber vs. physical, social, …
    - Time: different scales, logical clock vs. physical clock (i.e., real time)
    - Space: virtual space vs. physical space
    - Speed: speed of light vs. physical space laws (e.g., movement of a tank)
  - Do not understand the attackers well: known vs. unknown
    - Know your enemies and know yourself
  - How to attract attackers to interact with them in cyberspace?
    - It is relatively easy to engage your enemies in a battle field

Effectiveness

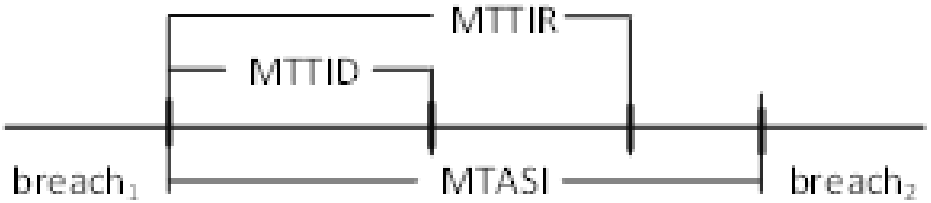
- Effectiveness measurement for attackers
  - Rate frustration in time and cost
- Effectiveness measurement for systems
  - Time and place of attacker's action
  - How much attacker's resources are wasted (e.g. num. of packets)
  - How long before attacker break the system/ stop acting
  - How much valuable data are breached
  - And more…

Measurement

Lord Kelvin: If you cannot measure it, then we cannot improve it

Extended dependability that includes security

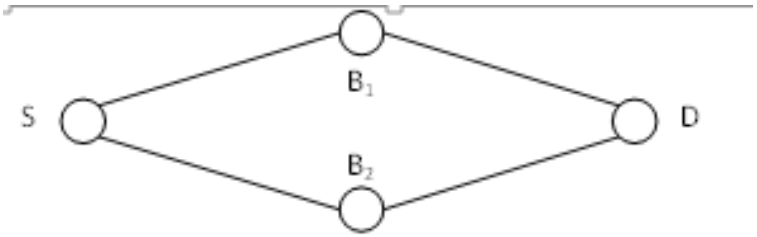
- Mean time between security incidents (MTBSI)
- Mean time to incident discovery (MTTID)
- Mean time to incident recovery (MTTIR)



Performability: work completed before the next security breach

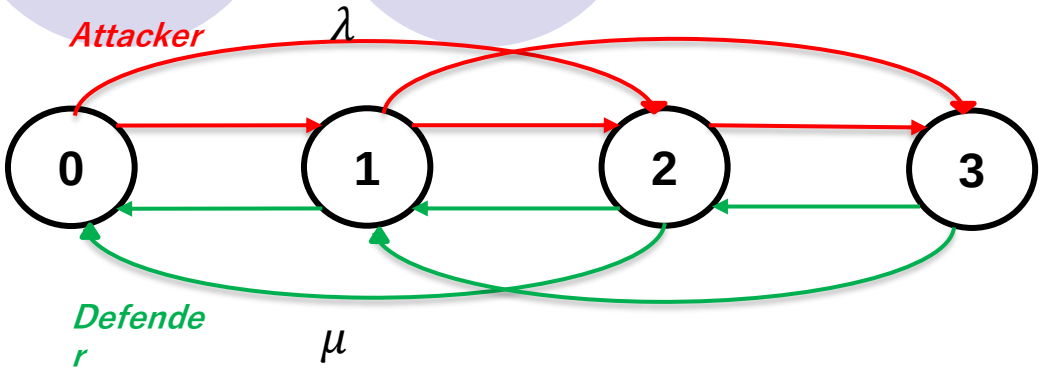
Degradation

- B_1: Level 1 breach, 1,000 hrs
- B_2: Level 4 breach, 5 hrs



Game Theory and Learning

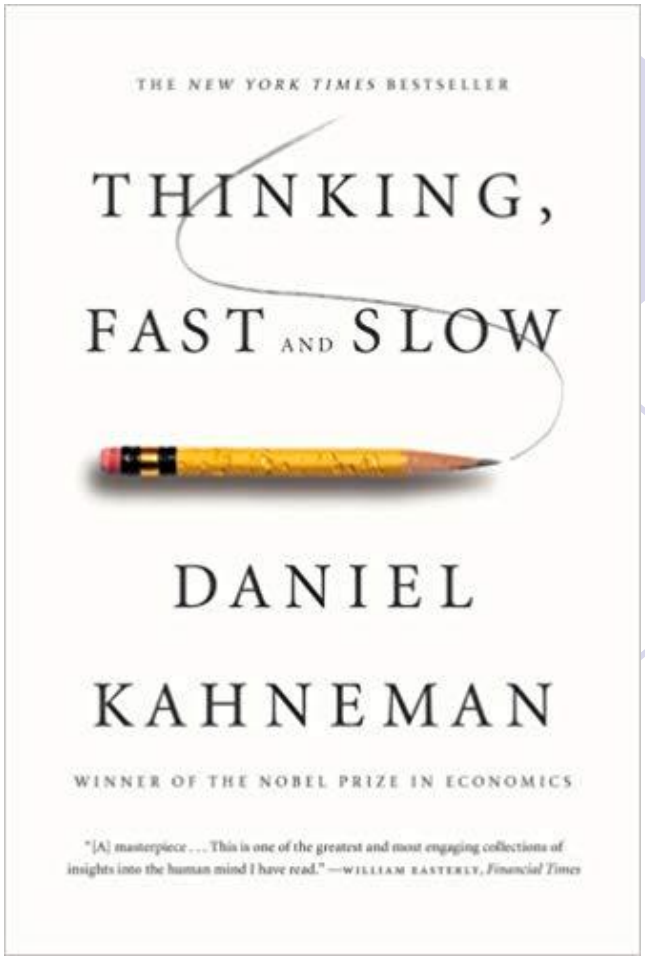
- Markov chain (MC)
  - Basic MC: transition probability
  - Semi MC: time and budget limit
  - Hidden MC: partially observable state (attacker/defense)
- Stochastic repeated game
  - Learn the behavior of the attacker: learning theory



(0: healthy, 1: slightly damaged, 2: heavily damaged, 3: disabled)

Learning: Cognitive Biases

- Deception is strongly relied on human psychology
  - Cognitive biases
- Cultural biases
  - Power Distance Index (PDI)
  - Uncertainty Avoidance (UAI)

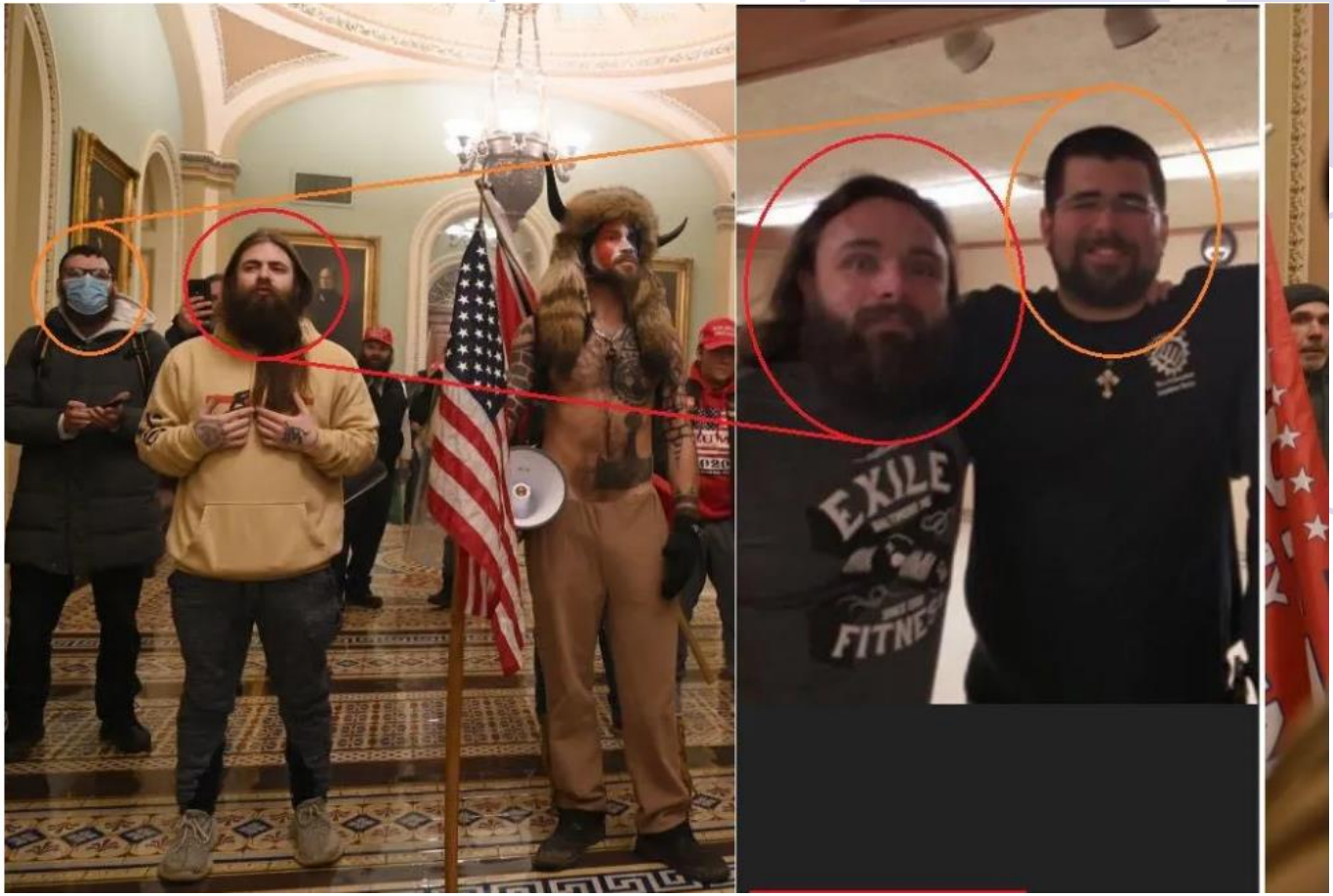


Final Thoughts

- Cyber-deception: friend or foe?
- Misinformation vs. disinformation
  - Disinformation is information that is deliberately false or misleading
  - Recent events in the world
- Challenges
  - Identifying disinformation is not merely about the truth, but about referring the intent (to mislead)

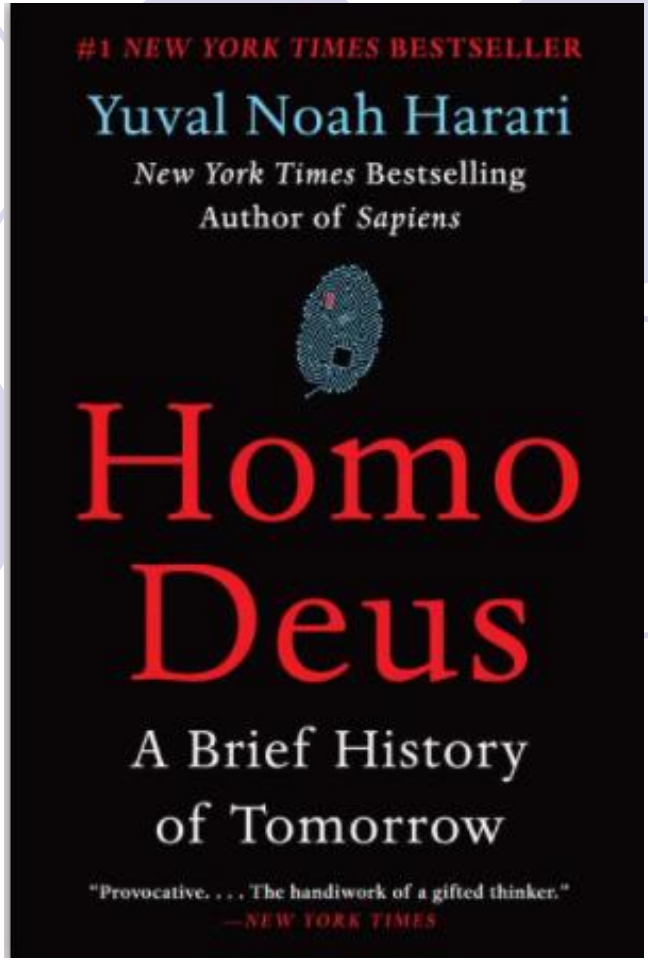
QAnon or Antifa?

- An article in WeChat
  - US Capital Hill, 01/06/2021



Smarter Than You Think

- Who is Smarter
  - Human or Computer?
- Homo Dues: Man God
  - AI-designed software/media
  - Controls Homo Sapiens
  - Replaces human beings



5. Conclusions

- Importance of cyber deception
  - Compliment to the existing security methods
- Self-organized design for agility
  - Basic principles and challenges
- Future
  - A better learning model for attackers/defenders
    - Security vs. ML
    - Game theoretical models
  - Science of security (S & P 2017)