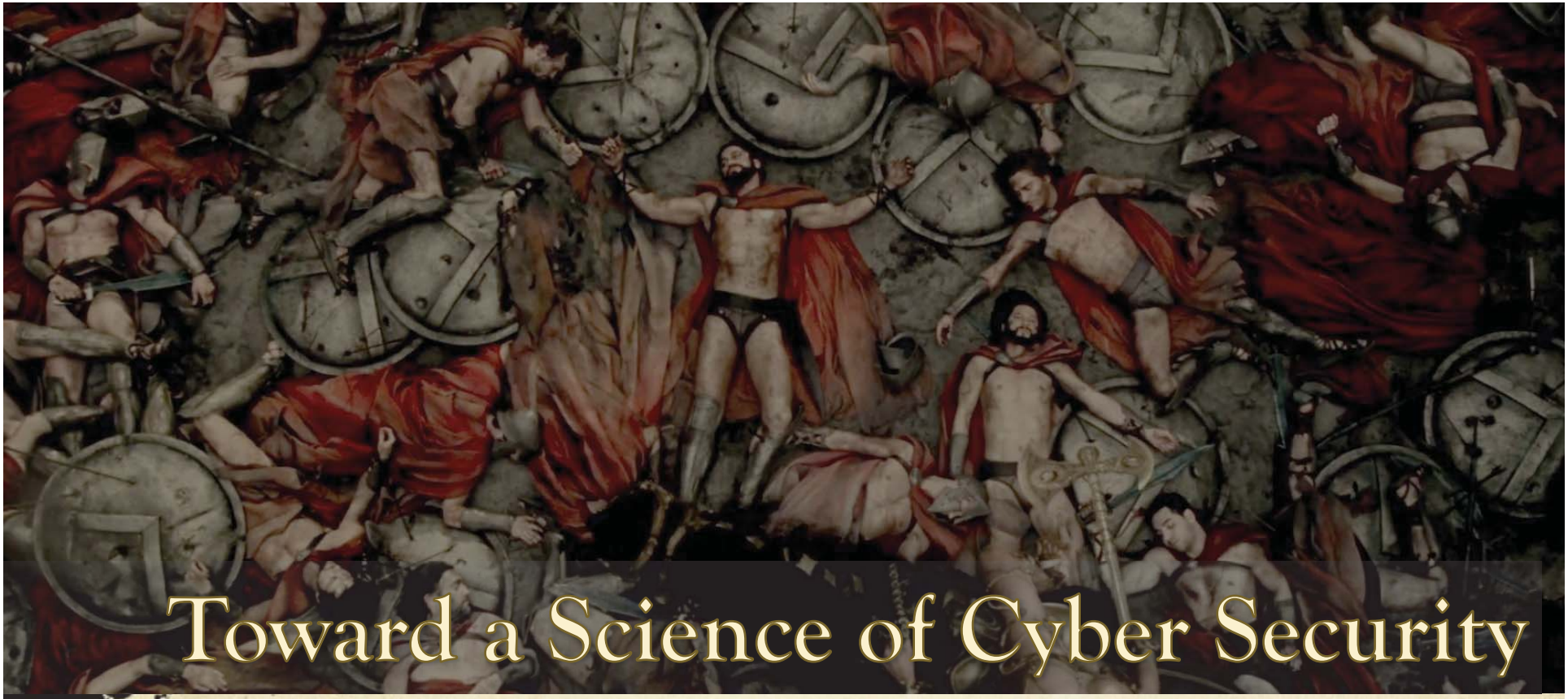


Toward a Science of Cyber Security

A War Like No Other

Bud Mishra
Professor of Computer Science, Mathematics, Human Genetics and Cell Biology
Courant Inst, NYU SoM, MSSM, CSHL, TIFR...

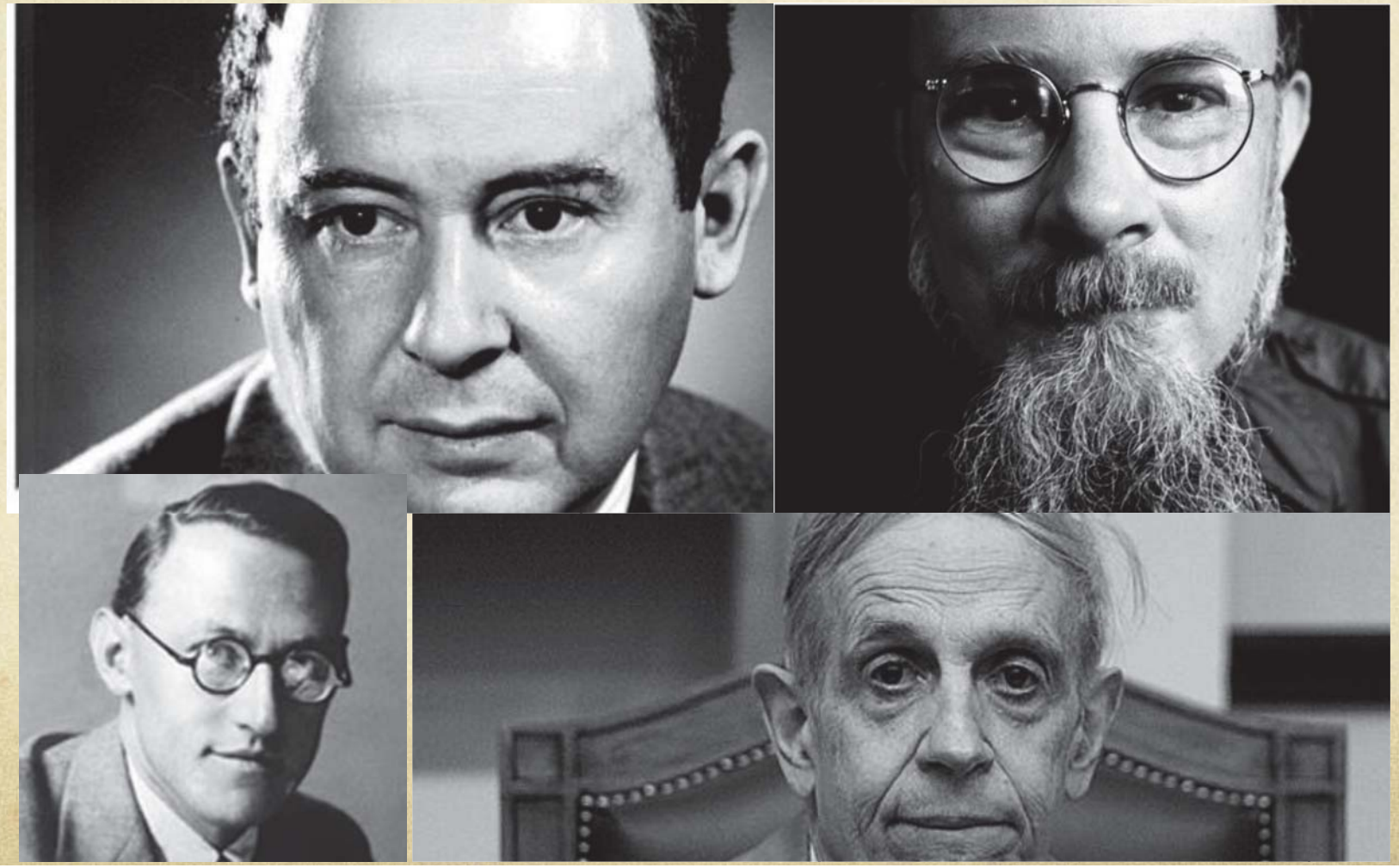
In March of 2013, what started as a minor dispute between Spamhaus and Cyberbunker culminated in a distributed denial of service (DDoS) attack that was so massive, it was claimed to have slowed internet speeds around the globe. The attack clogged servers with dummy internet traffic at a rate of about 300 gigabits per second.

The record breaking Spamhaus/Cyberbunker conflict arose 13 years after the publication of best practices on preventing DDoS attacks, and it was not an isolated event.

“Let your plans be dark and impenetrable as night, and when you move, fall like a thunderbolt.”

Sun Tzu, The Art of War, 544-469 BC

Game Theory



Classical Games

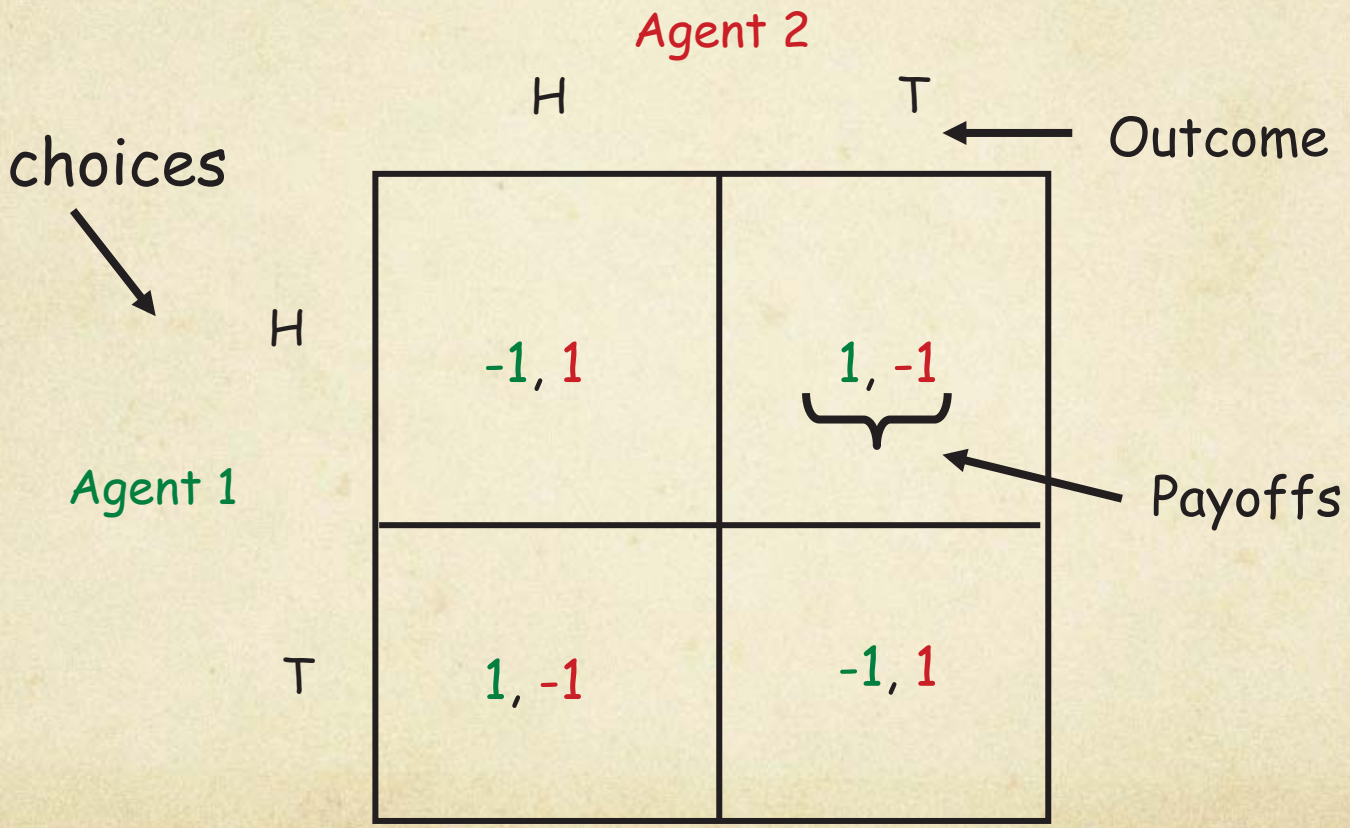
- Symmetric
  - Non-Cooperative Games
  - Zero-sum Games
- Asymmetric
  - Information-Asymmetric Games
  - Deception
- Repeated Games vs One-Shot Games
- Normal Form vs Extensive Form
- Nash-Equilibrium

Strategic Choices

- **A game:** *Formal representation of a situation of strategic interdependence*
  - Set of *players*, I; |I|=n
  - Each agent, j, has a set of *choices*, Aj
    - AKA strategy set
  - Choices define *outcomes*
    - AKA strategic combination
    - For each possible set of choices, there is an outcome.
  - Outcomes define *payoffs*
    - Agents derive utility from different outcomes

Normal form game*

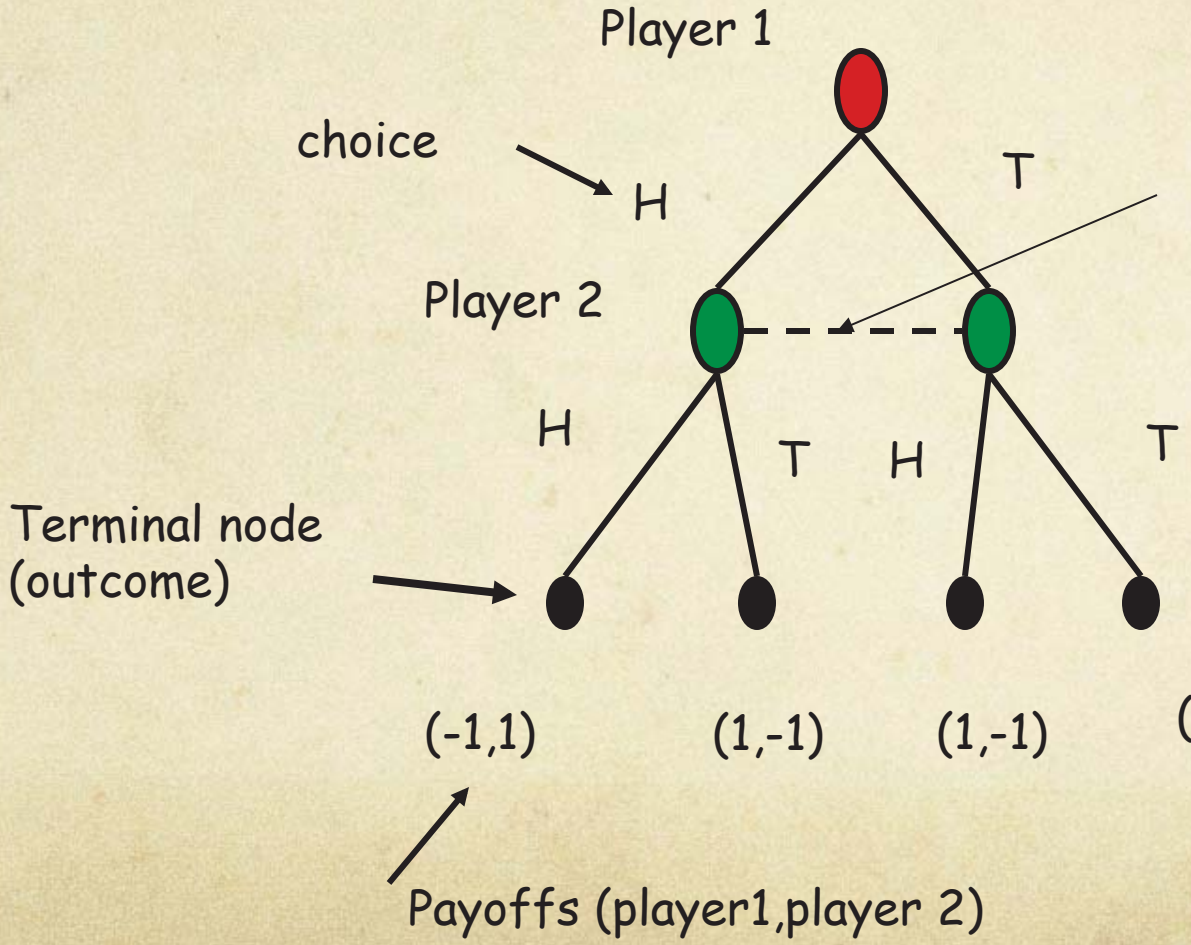
(matching pennies)



*aka strategic form, matrix form

Extensive form game

(matching pennies)

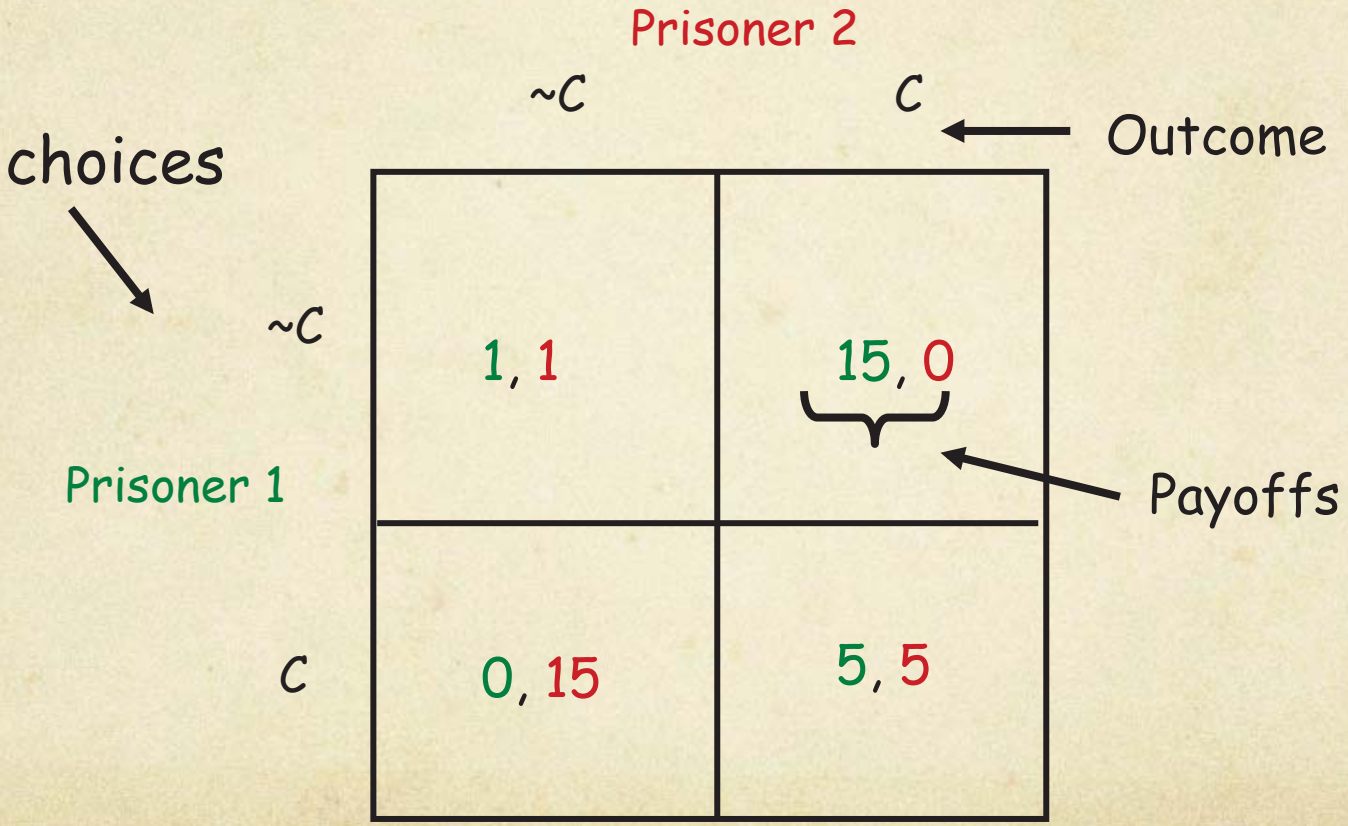


Player 2 doesn't know what has been played so he doesn't know which node he is at.

How fair would it be to say, "Let's play matching pennies. You go first." ?

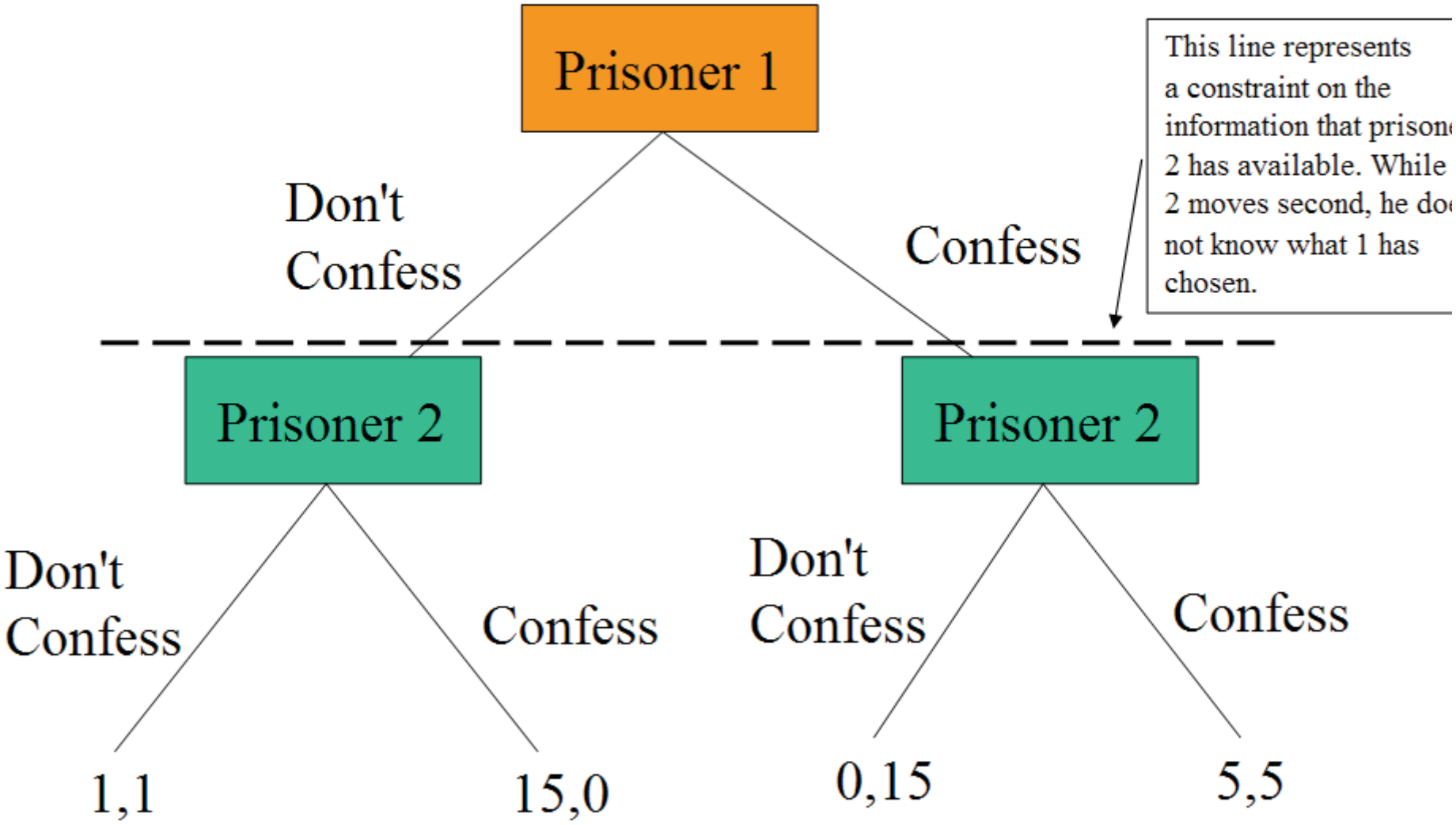
Normal form game*

(prisoner's dilemma)



*aka strategic form, matrix form

Prisoners' Dilemma in "Extensive" Form



Payoffs are: Prisoner 1 payoff, Prisoner 2 payoff.

“I thought to myself with what means, with what deceptions, with how many varied arts, with what industry a man sharpens his wits to deceive another and through these variations the world is made more beautiful.”

Francesco Vettori, 1474 - 1539

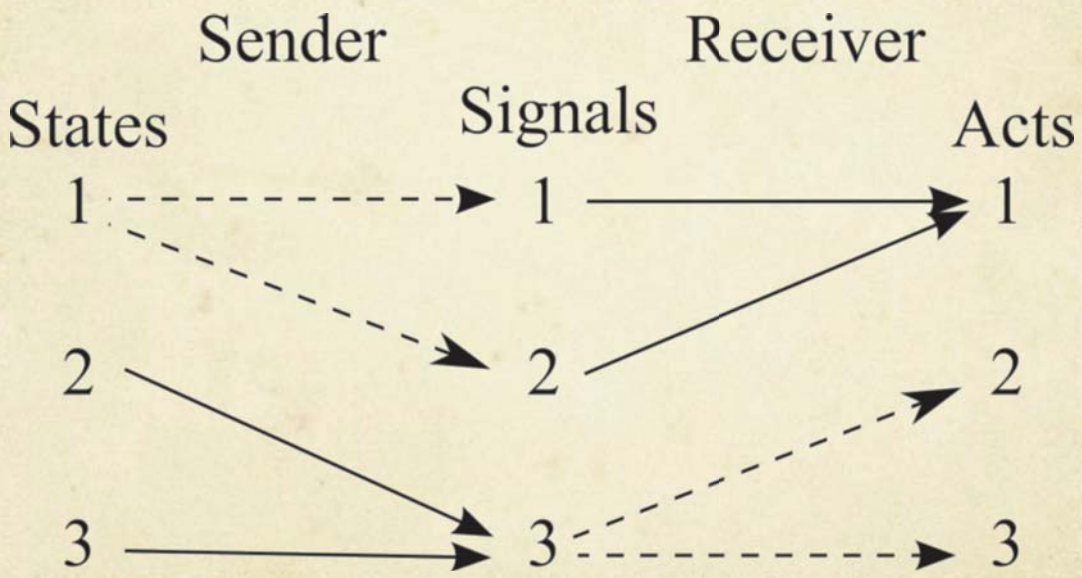
Asymmetric Games

- "Signaling" evolves between two agents: One Informed, the other Uninformed
- Deception by the Informed Agent

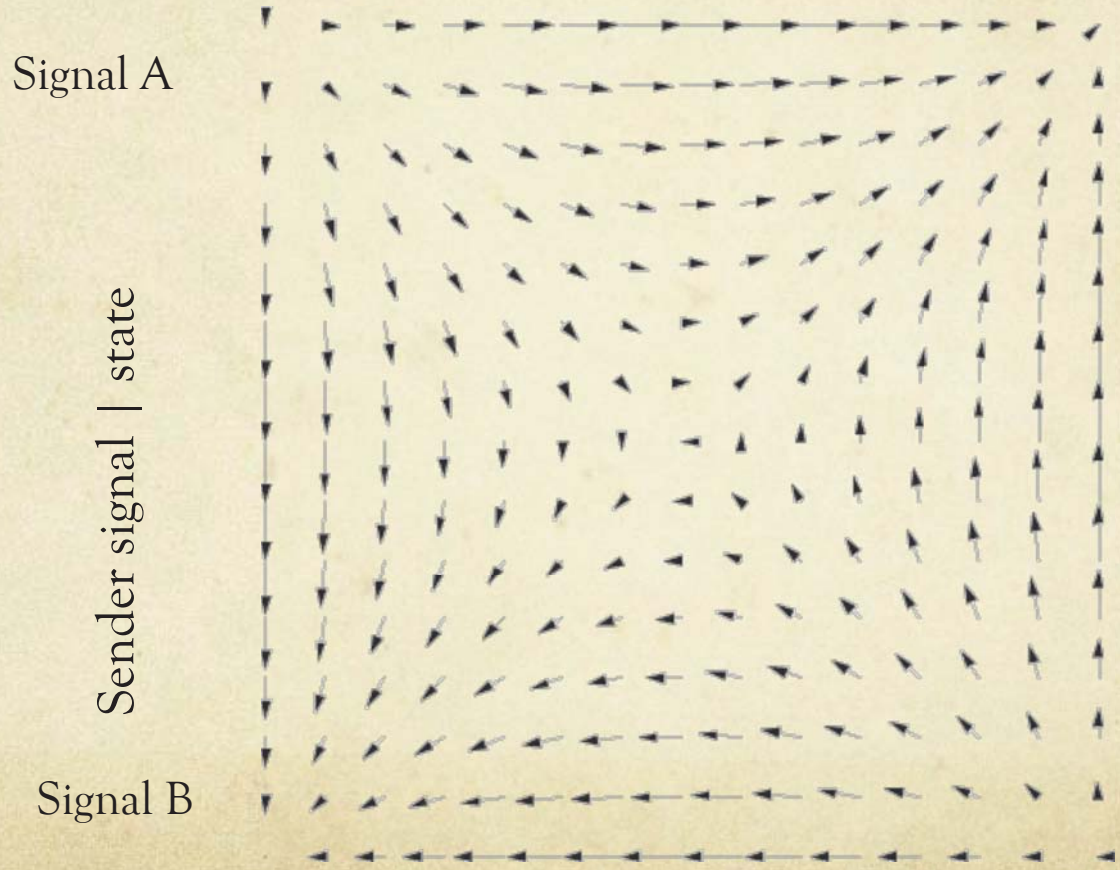
Image: etsy, Modernality

Lost in Translation

Signaling Games

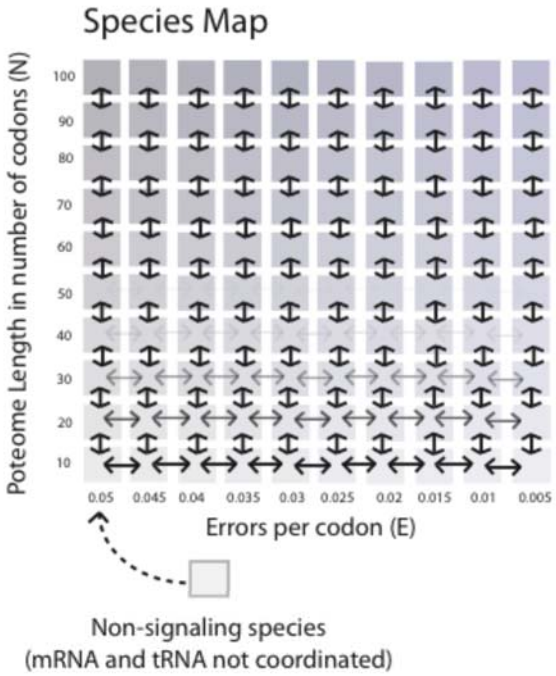


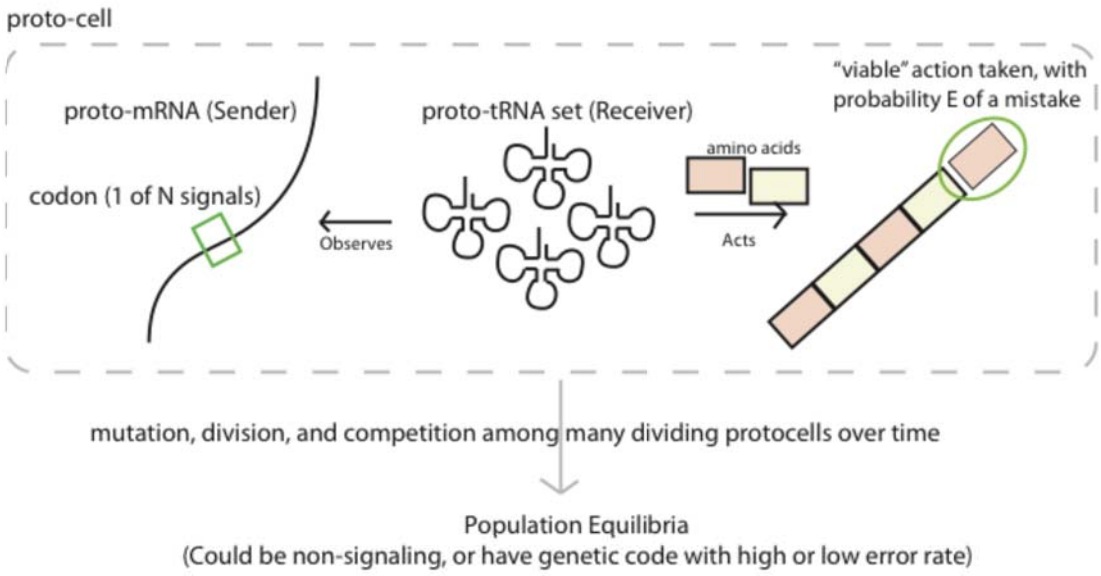
Information-Asymmetric Games



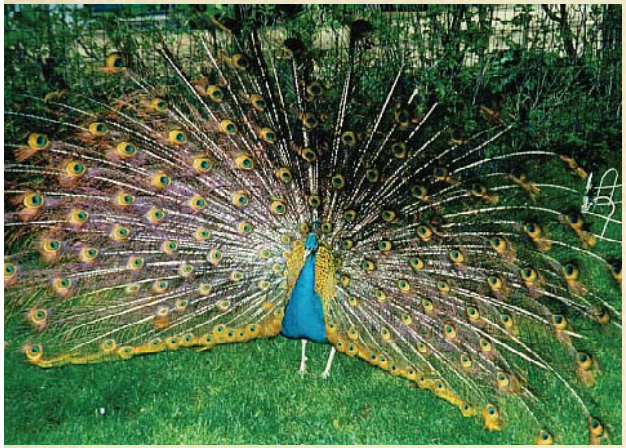
-*Signals: Evolution, learning, and information*
B. Skyrms 2010

The Genetic Code





Mate Selection



- You (a female) choose a mate (male) by displayed traits.
- You need to consider following: **Increased fecundity** (more offspring) & **Good genes** –Improved genetic quality.
- You use various sensory signals to select the male (based on displayed traits) – presumably, pleiotropic with fecundity, good genes, etc.
- Sensory exploitation – Male evolves display trait that exploits pre-existing sensory bias in female.
  - Runaway selection – Female preference increases because it is linked to 'sexy son' advantage.

Used-Car Markets

- You want to buy a used-car which may be either good or bad (a lemon). A good car is worth *more than* a bad one.
- The dealer knows quality but you don't.
- You cannot tell a good car from a bad one but believe a proportion q of cars are good.
- You need to decide whether to buy or not.
- Based on buyers' strategies, the dealer tries to dilute the proportion of good cars.

Bitcoins

- You receive certain number of bitcoins from a sender in the form of an electronic message.
- These bitcoins can be added to your bitcoin wallet.
- Only the sender knows whether the transaction is valid:
  - He may repudiate the transaction.
  - He may not have enough bitcoins in his own wallet.
  - He may have simultaneously made several transactions (*double spending*).

Malware

- You can receive a free app from an app-store.
- The app-developer knows whether the app is beneficent or malicious; but you don't.
- You must decide what action to take:
  - Ignore it
  - Download the App
  - Download and test; give the developer a reputation score, etc.

"The arrow shot by the archer may or may not kill a single person. But stratagems devised by wise men can kill even babes in the womb."

Kautilya, Indian Philospher, 3rd Century BC

Mechanism Design

- *How to avoid deception?*
  - **Credible (and Noncredible) Threats:** Use threats (and promises) to alter other players' expectations of his future actions, and thereby induce them to take actions favorable to him or deter them from making moves that harm him. To succeed, the threats and promises must be credible. (Somewhat Problematic).
  - **3-Players: (Sender + Receiver + Verifier) …**
  - **Handicap Principle:** Make signals costly to the signaler, costing the signaler something that could not be afforded by a player with less of a particular trait.

Bitcoins

- **Honest Signaling:** Based on a public-key crypto-system, using which the sender must digitally-sign the transaction. Receiver can verify each previous transaction to verify the chain of ownership. (Local Verification).
- **Verifiers: (Bit-coin Miners)** New transactions are broadcast to all nodes. Each miner node collects new transactions into a block. Nodes accept the block only if all transactions in it are valid and not already spent. Etc. (Global Verification).
- **Costly Signaling:** Each miner node works on finding a difficult proof-of-work for its block. New bitcoins are successfully collected or "mined" by the receiving node which found the proof-of-work.

M-Coins

- A concept similar to bitcoins – with few exceptions:
  - They expire and cannot be reused.
  - They are created by a group of trusted authorities; who have the ability to verify an agent's "attack surface."
  - They must be used *only* in a transaction when an agent is challenged.

It is double pleasure to deceive the deceiver.

Niccolo Machiavelli, 1469- 1527

Asymmetry-Breaking

- A sender may act in the “cooperate” behavior mode by sending a useful app honestly or the “defect” behavior mode by sending a malicious app deceptively…
- A receiver may act in the “cooperate” behavior mode by accepting trusted or the “defect” behavior mode by responding with a challenge.
- Failing the challenge (namely, in delivering an M-coin in response) results in eviction from the game.

Payoff Matrix

- **Parameters:**
  - a = the cost of app
  - b = the value of app
  - c = the cost of verification
  - d = the benefit of hack
  - e = the cost of getting caught
  - f = the benefit of catching malicious user, and
  - g = the cost of challenging a sender.

Sender,Receiver	receive trusted	receive challenge
send clean	$(a, -a+b)$	$(a-c, -a-g)$
send malware	$(a+d, -a-d)$	$(a-c-e, -a+f-g)$

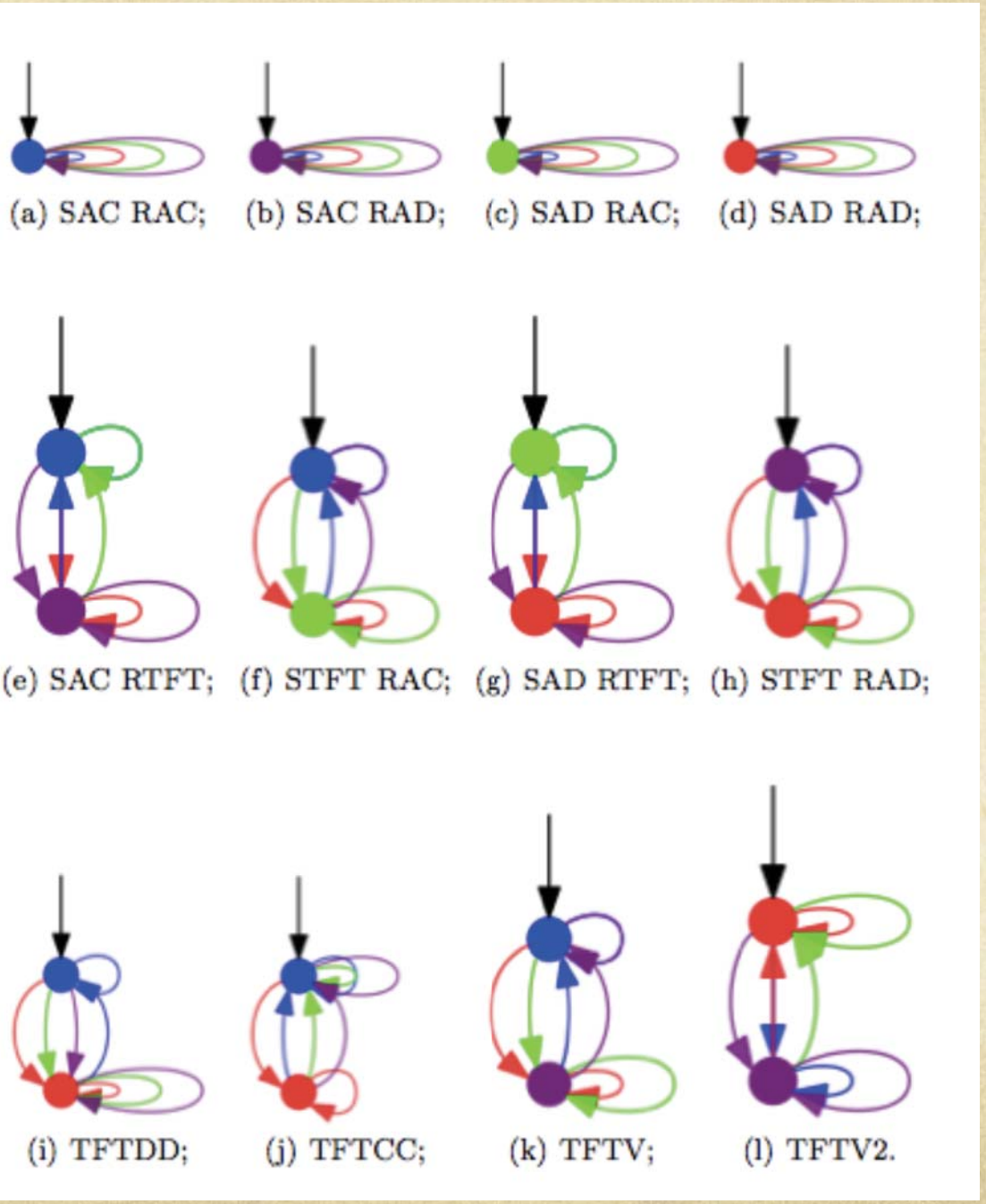
receiver → / sender ↓	CC	CD	DC	DD
CC	b	$b-c$	$-d$	$-c-d$
	b	$-g$	$b+d$	$d-g$
CD	$-g$	$-c-g$	$f-g$	$-c+f-g$
	$b-c$	$-c-g$	$b-c-e$	$-c-e-g$
DC	$b+d$	$b-c-e$	0	$-c-d-e$
	$-d$	$f-g$	0	$d+f-g$
DD	$d-g$	$-c-e-g$	$d+f-g$	$-c-e+f-g$
	$-c-d$	$-c+f-g$	$-c-d-e$	$-c-e+f-g$

A soldier will fight long and hard for a bit of colored ribbon.

Napoleon Bonaparte, 1769-1821

Utilities & Threats

- The utilities and deterrences are modified…
  - M-coins
  - Crowd Sourcing
  - Gamifications
- The population of players must evolve newer strategies independently in a repeated game…
- The agents can be thought of in terms of finite automata and the winning strategies are identified and shared.



(a) SAC RAC; (b) SAC RAD; (c) SAD RAC; (d) SAD RAD;

(e) SAC RTFT; (f) STFT RAC; (g) SAD RTFT; (h) STFT RAD;

(i) TFTDD; (j) TFTCC; (k) TFTV; (l) TFTV2.

It is not surprising that the lambs should bear a grudge against the great birds of prey, but that is no reason for blaming the great birds of prey for taking the little lambs. ... The birds of prey may say to themselves, "We bear no grudge against them, these good lambs, we even love them: nothing is tastier than a tender lamb."

Friedrich Nietzsche, On the Genealogy of Morality, 1844-1900

Games Evolving

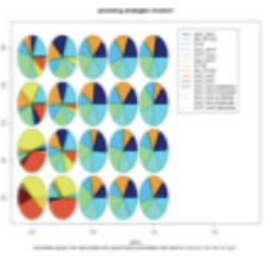
- **Initialization:** Time k = 0. Create a random population of N users who choose a repeated- game strategy randomly over a set of seed-strategies. The simulation model is constructed with the following update-cycle:
- **Pairing:** Using the population at time (k − 1) create N/2 random pairings.
  - **Population Structure parameter:** For each pair with probability α one strategy is selected with the other removed and replaced with a copy of the selected strategy.

Games Evolving

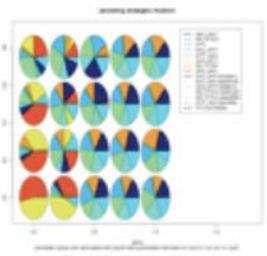
- **Strategize:** Each selected pair will play a repeated game with a number of plays dependent on a geometric distribution with continuation parameter δ.
- **Determine Payoff:** Strategy payoff is determined using automata and payoff matrix; a multiplicative discount factor for payoff may be introduced.

Games Evolving

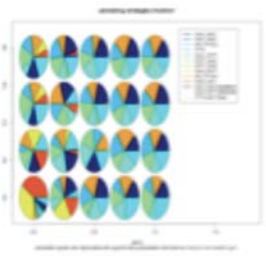
- **Next Round:** Time k. A population of size N is re-created by sampling the strategies at time $(k-1)$ using a distribution whose density is computed as proportional to population normalized performances.
- **Mutate:** Each user-agent is subject to the possibility of mutation with mutation rate μ ; a mutation creates a strategy one-mutation step from its previously selected strategy determined in the preceding step. Mutation steps may add or delete a state, re-label a state or re-assign an edge destination.



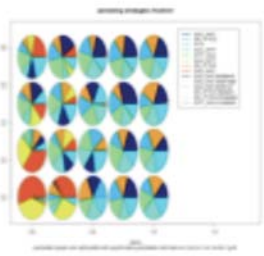
(a) 1111



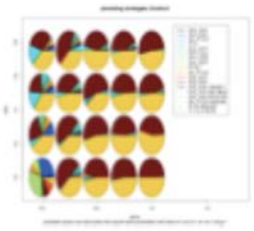
(b) 1118



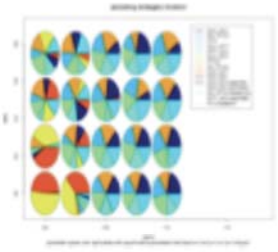
(c) 1811



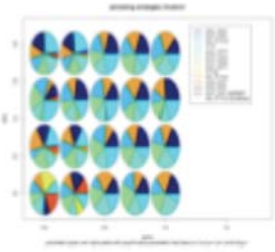
(d) 1818



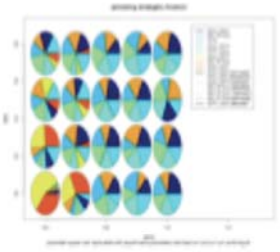
(e) 1181



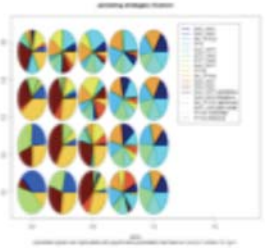
(f) 1188



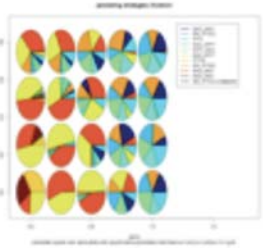
(g) 1881



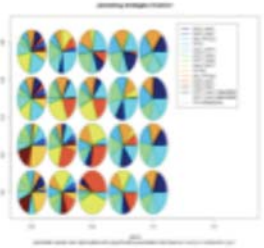
(h) 1888



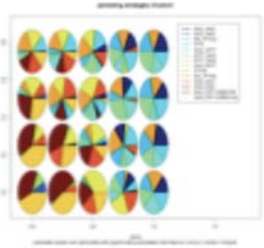
(i) 8111



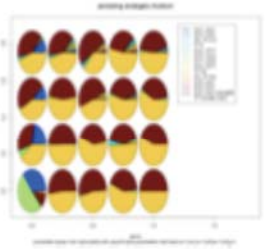
(j) 8118



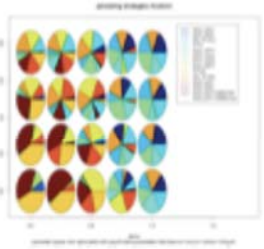
(k) 8811



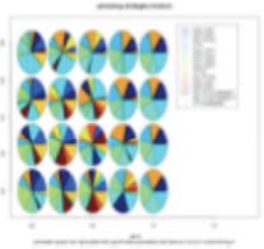
(l) 8818



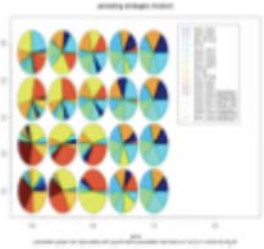
(m) 8181



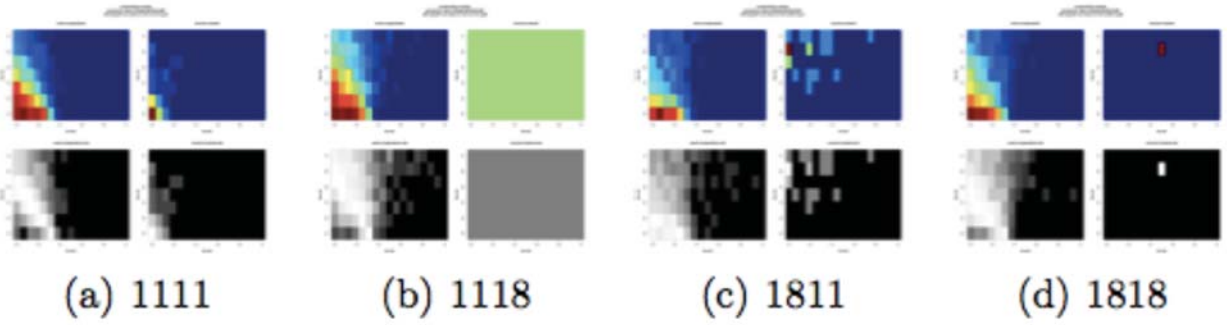
(n) 8188



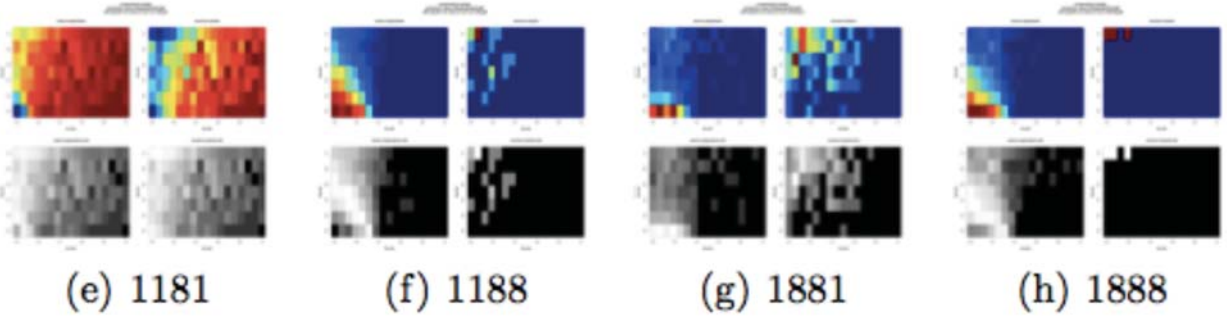
(o) 8881



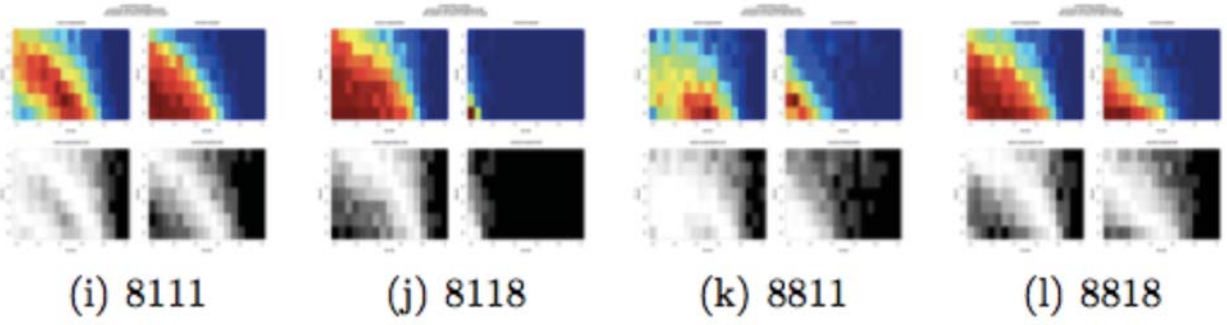
(p) 8888



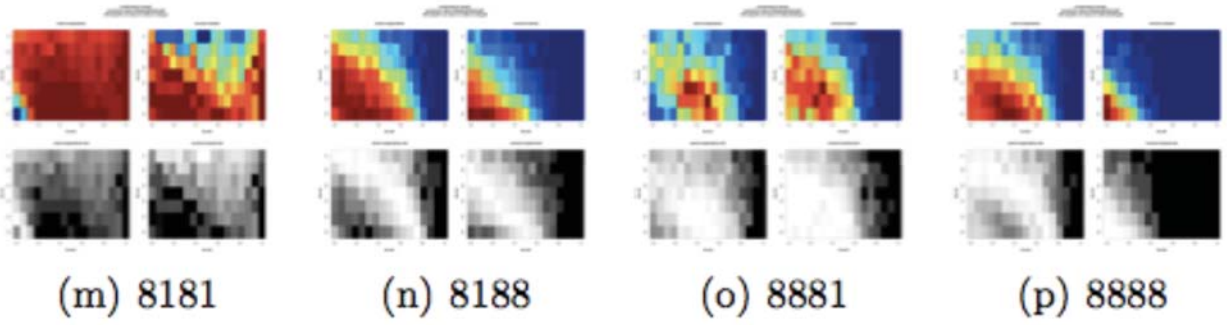
(a) 1111 (b) 1118 (c) 1811 (d) 1818



(e) 1181 (f) 1188 (g) 1881 (h) 1888

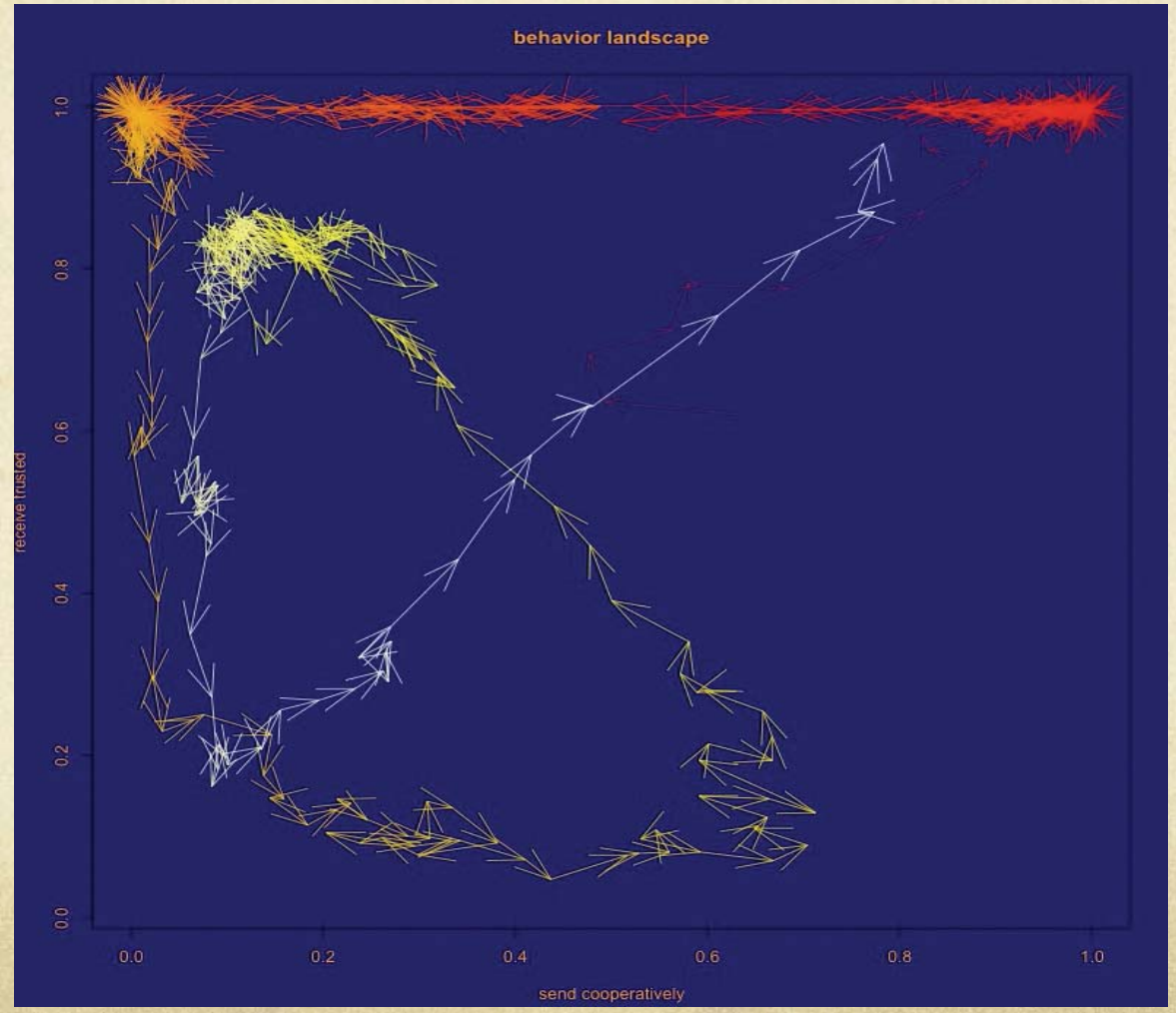


(i) 8111 (j) 8118 (k) 8811 (l) 8818



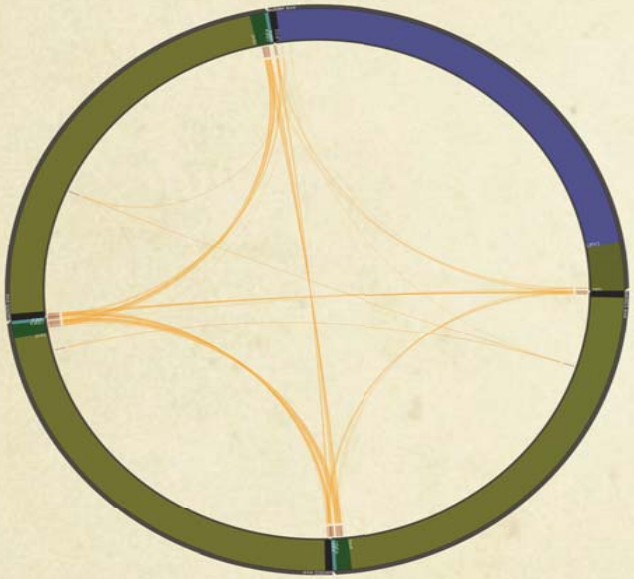
(m) 8181 (n) 8188 (o) 8881 (p) 8888

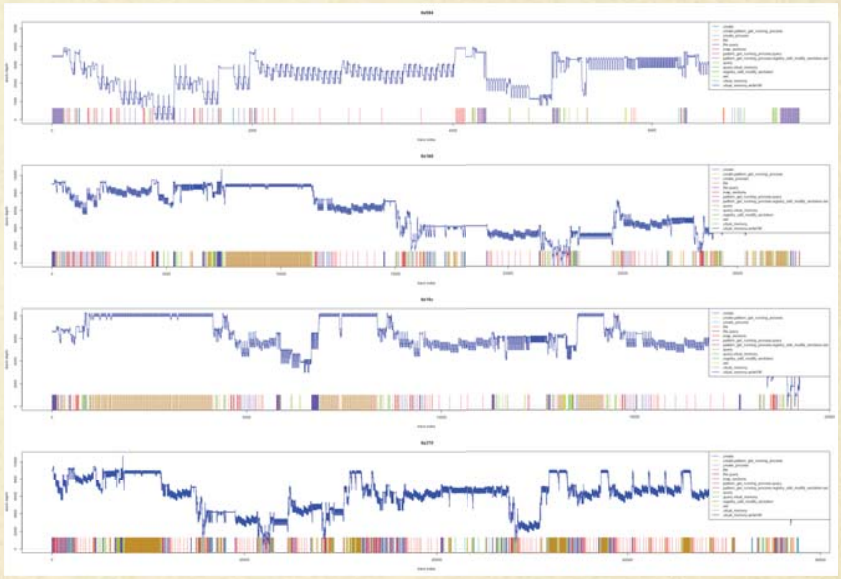
Population Behavior Simplex



Traces for Zbot

1.2.4.3 polymorphic code





Igitur qui desiderat pacem, praeparet bellum...

Vegetius (Publius Flavius Vegetius Renatus), Epitoma rei militaris, 450 AD.

In March of 2013, what started as a minor dispute between Spamhaus and Cyberbunker culminated in a distributed denial of service (DDoS) attack that was so massive, it was claimed to have slowed internet speeds around the globe. The attack clogged servers with dummy internet traffic at a rate of about 300 gigabits per second.

The record breaking Spamhaus/Cyberbunker conflict arose 13 years after the publication of best practices on preventing DDoS attacks, and it was not an isolated event.

How we differ...

- **Current approaches are static**: Based on vulnerability analysis and codified in a slowly evolving "best-practices." *Be as dynamic as the adversaries.*
- **Current approaches are mono-clonal**: Based on regulations that are enforced on "all enterprises." *Be as heterogeneous as the adversaries.*
- **Current approaches are expensive**: Require asymmetrically more expensive analysis by the malware defenders. *Be as fast, cheap and out-of-control as the adversaries.*
- **Current approaches are transparent**: The adversaries know how you would defend. *Keep the adversaries guessing your next step.*
- *Break the asymmetry!*

Conclusion

- "*There are no intrinsic* "laws of nature" *for cyber-security as there are, for example, in physics, chemistry or biology. Cyber-security is essentially an applied science that is informed by the mathematical constructs of computer science such as theory of automata, complexity, and mathematical logic.*" (JASON Report)
- Perhaps, NOT! We have proposed a two pronged attack:
  - Game Theory and Mechanism Design (Manichean)
  - Model Building and Checking (Augustine)

Road Ahead

- Multi-Cellularity: Evolution
  - Cancer
  - Neuroscience
  - Immune Systems
- Multi-Processing: Learning
  - Machine Learning
  - Cyber Security and M-coins
  - Markets and Bitcoins
  - GBGB (Glass Bead Game Blueprint)

Ralph Waldo Emerson, 1803-1882

"Nature has made up its mind that what cannot defend itself shall not be defended."

The End

Thanks

Software Engineering Institute(CMU)

- *W. Casey*
- *J.A. Morales*
- *J. Spring*
- *R. Weaver*
- *E. Wright*

Courant Institute (NYU)

- *T. Nguyen*

- *Brian Skyrms*
- *Bill Scherlis*
- *Dean Sutherland*