# Timing of Cyber Conflict

presented by Padraic Cashin

Robert Axelrod and Rumen Iliev

# When do you attack?



- When expending resources yields value greater than possible future value
- Each entity has a **Threshold**, T, for **Stakes**, s; minimum level of stakes before an attack will be considered.
- Resources consist of exploits, back doors, bot nets, etc.

# Model Assumptions



- Entities know the current stakes, but only know the distribution of future stakes
- Future stakes are out of your control
- Future effectiveness of a resource can only be estimated

# Shelf Life of Resources



- Vulnerabilities can be discovered and patched.
- A vulnerability is **stealthy**, S, if it remains viable after use
- A vulnerability is **persistent**, P, if it remains viable when not used

# Persistence vs Stealth



- Persistent resources are not currently deployed. Stealthy resources have already been used.
- $P = \Pr(\text{resource survives} \mid \text{not use it})$
- $S = \Pr(\text{resource survives} \mid \text{use it})$

# Value vs Gain

- The **gain**, G, of a resource is the immediate value from deploying a resource
- The **value**, V, of a resource is the sum of immediate gains and all future gains
- The value of a resource over time is discounted by a fixed percent, w

# Defining Value



Robert Axelrod and Rumen Iliev

Value of a stealthy resource:

$$V_S = G(T) + wSV \tag{1}$$

Value of a persistent resource:

$$V_P = wPV \tag{2}$$

Expected value over–time:

$$V = \Pr(s \geq T)[G(T) + wSV] + (1 - \Pr(s \geq T))wPV \tag{3}$$

# Determining Optimal Timing of Attacks



- Distribution of stakes is linear. Based on the role of a die.
- The discount rate is fixed at $w = 0.9$
- Analyse the effects of stealth and persistence on threshold

# Effect of Persistence

| T \ P | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 | 0.9 | 1.0 |
|---|---|---|---|---|---|---|---|---|---|---|
| 6 | 1.09 | 1.20 | 1.33 | 1.49 | 1.70 | 1.98 | 2.37 | 2.94 | 3.88 | 5.71 |
| 5 | 1.98 | 2.16 | 2.37 | 2.62 | 2.93 | 3.33 | 3.86 | 4.58 | 5.64 | 7.33 |
| 4 | 2.68 | 2.98 | 3.13 | 3.42 | 3.77 | 4.20 | 4.74 | 5.43 | 6.37 | **7.69** |
| 3 | 3.19 | 3.41 | 3.66 | 3.95 | 4.29 | 4.69 | 5.17 | **5.77** | **6.52** | 7.50 |
| 2 | 3.52 | 3.72 | 3.96 | 4.22 | **4.52** | **4.87** | **5.27** | 5.75 | 6.32 | 7.02 |
| 1 | **3.66** | **3.85** | **4.05** | **4.27** | 4.52 | 4.79 | 5.11 | 5.47 | 5.88 | 6.36 |

Stealth is set to half of Persistence. Using a resource doubles the likely hood it will be discovered.

# Effect of Stealth

| T \ S | 0.1 | 0.2 | 0.3 | 0.4 | 0.5 | 0.6 | 0.7 | 0.8 |
|---|---|---|---|---|---|---|---|---|
| 6 | 2.60 | 2.70 | 2.82 | 2.94 | 3.08 | 3.23 | 3.39 | 3.57 |
| 5 | 3.74 | 3.99 | 4.26 | 4.58 | 4.95 | 5.39 | 5.91 | 6.55 |
| 4 | 4.20 | 4.55 | 4.95 | 5.43 | 6.02 | 6.76 | 7.69 | 8.93 |
| 3 | **4.29** | **4.69** | **5.17** | **5.77** | 6.52 | 7.50 | 8.82 | 10.71 |
| 2 | 4.14 | 4.57 | 5.09 | 5.75 | **6.60** | **7.75** | 9.39 | 11.90 |
| 1 | 3.85 | 4.27 | 4.79 | 5.47 | 6.36 | 7.61 | **9.46** | **12.50** |

Persistence is fixed at 0.8

# Results



- As Persistence increases Threshold increases
- As Stealth increases Threshold goes down
- Patience increases when stealth is low, persistence is high, and large stakes are rare

# Case Study 1: Stuxnet



- Low Persistence, High Stealth, and High Stakes
- Multiple resources used at once, high cost of use
- Gain was not estimated properly due to source code leaks

# Case Study 2: Attack on Saudi Aramco

- Broad attack on Saudi and US oil pipelines (30,000 workstations infected)
- Very High Stakes, Low Stealth
- Attackers immediately deployed a resource en masse

# Case Study 3: Chinese Cyber Espionage



- Wide spread deployment of cyber resources
- Moderate Stealth against vigilant targets, Minimal Stakes
- Either persistence is very low or expect High Stealth against outliers

# Case Study 4: Refusal to Export Minerals



- Chinese refused to export rare–earth minerals due to Japanese detainment of Chinese fishing crew.
- Very High Persistence, Low Stealth, Low Value
- China might have a artificially low threshold or low patience

# Effect of Zero–Day Markets

- Increased pressure to find exploits leads to simultaneous discover; Decreases Persistence.
- Lower Persistence lowers Threshold; Increase resource deployment
- Prices predicted to drop as exploits become available and less persistent

# Conclusions



- Model explains cyber conflict frequency using economic models
- Entities attempt to maximize resource effectiveness
- Resources are both perishable and detectable
- Assumes each entity will act perfectly

# What Happens if an Attack is False?

- Evidence of an Attack can be Spoofed
- Attacks are not necessarily resource intensive; non–state attacks are possible
- Attacks can be attributed to different entities incorrectly, or can be left unattributed
- Each entity has unknown capabilities

# The Blame Game

- Two player Bayesian Game, players have imperfect knowledge of each other but can estimate a probability of state
- Players are either the Attacker ($\mathcal{A}$) or the Blamer ($\mathcal{B}$)
- $\mathcal{A}$ chooses to attack $\mathcal{B}$ or not
- $\mathcal{B}$ chooses to blame $\mathcal{A}$ or not

# Behavior and Equilibria



- $\mathcal{A}$ attempts to determine if $\mathcal{B}$ is **knowledgeable**
- $\mathcal{B}$ attempts to determine if $\mathcal{A}$ is **vulnerable**
- Equilibria exist if no attack – no blame or attack – blame occurs
- Third parties can disrupt cooperative equilibrium