Orbital Escalation: Modeling Satellite Ransomware Attacks using Game Theory

Efrén López-Morales
New Mexico State University

4th SpaceSec Workshop
February 23rd, 2026

NM STATE

Global Ransomware by the Numbers (2025)

- 49% of victims paid the ransom to get their data back.

Source: The State of Ransomware 2025, Sophos, Whitepaper (2025)

Global Ransomware by the Numbers (2025)

- 49% of victims paid the ransom to get their data back.
- The average ransom payment was $1 million.

Source: The State of Ransomware 2025, Sophos, Whitepaper (2025)

Global Ransomware by the Numbers (2025)

- 49% of victims paid the ransom to get their data back.
- The average ransom payment was $1 million.
- Nearly 50% of attacks targeted critical infrastructure.

Source: The State of Ransomware 2025, Sophos, Whitepaper (2025)

Ransomware Has Not Reached Orbit… Yet

- Satellite are high cost and take years to commission and launch.

Ransomware Has Not Reached Orbit… Yet

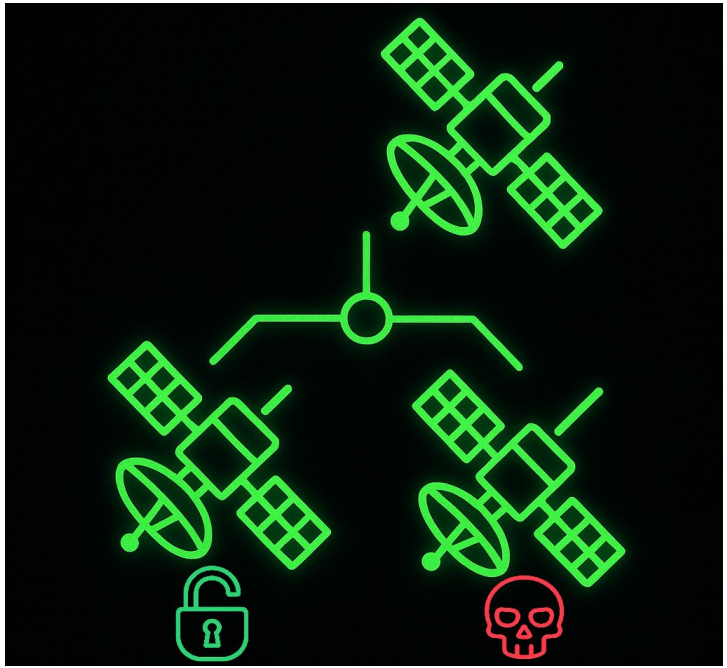
- Satellite are high cost and take years to commission and launch.
- Increasing interconnected and vulnerable, e.g., Ground Station as a Service.

Ransomware Has Not Reached Orbit… Yet

- Satellite are high cost and take years to commission and launch.
- Increasing interconnected and vulnerable, e.g., Ground Station as a Service.
- Limited physical recovery options.

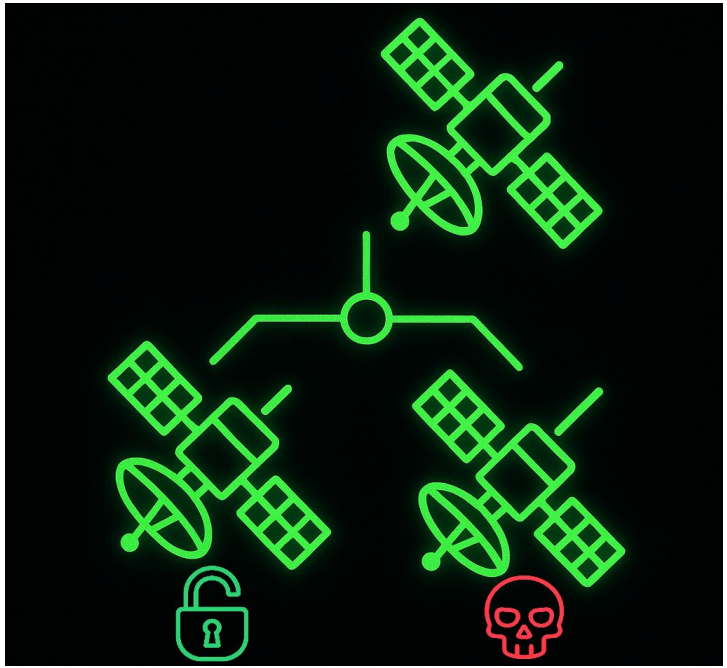
Is Satellite Ransomware Technically Plausible?

- WannaFly satellite ransomware proof of concept



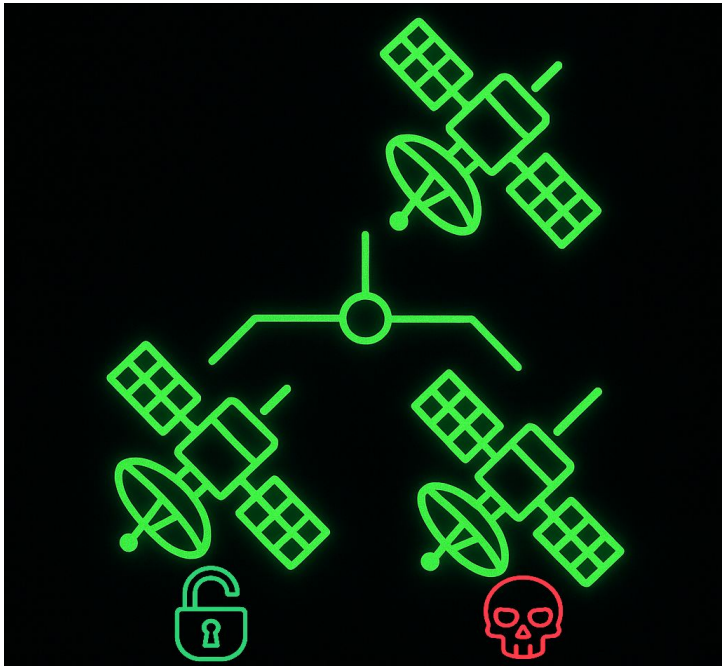
Is Satellite Ransomware Technically Plausible?

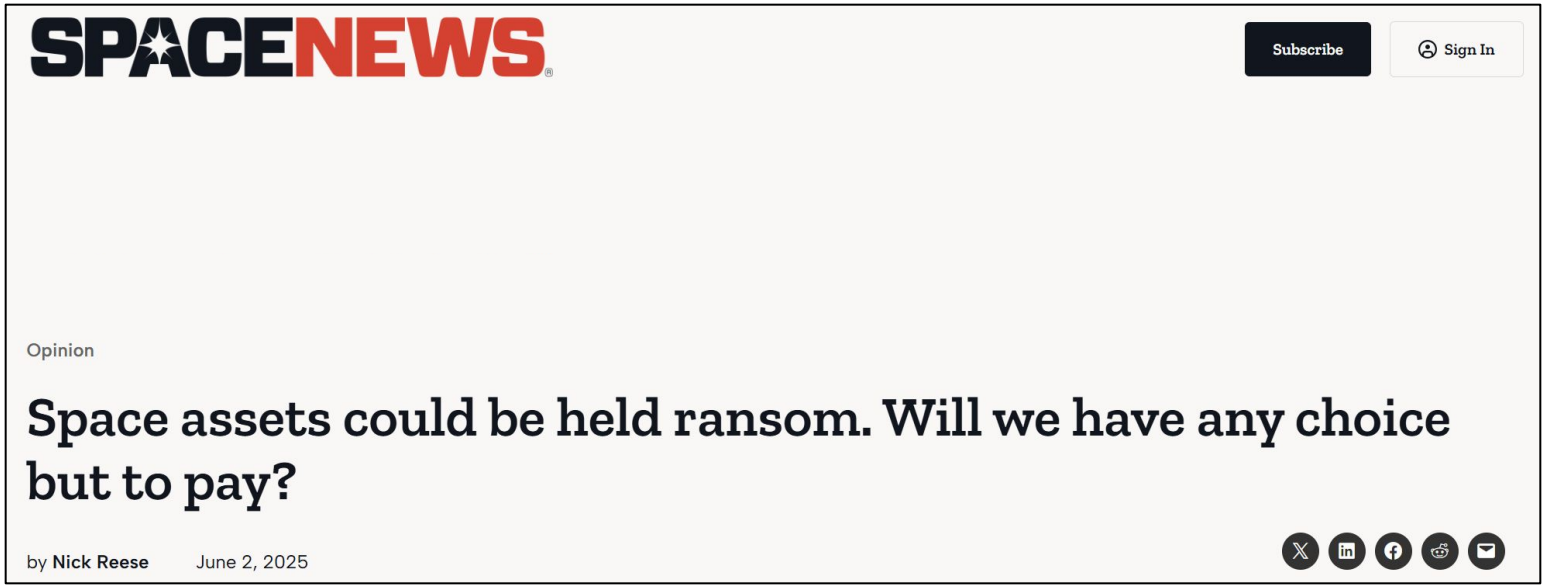
- WannaFly satellite ransomware proof of concept
- Satellite ransomware does not rely on encryption



Is Satellite Ransomware Technically Plausible?

- WannaFly satellite ransomware proof of concept
- Satellite ransomware does not rely on encryption
- This opens the door for alternative recovery options





Source: Space assets could be held ransom. Will we have any choice but to pay?, SpaceNews

Limited Policy Readiness for Satellite Ransomware

Policy options

To date, none of the major space policy documents since the reinvigoration of the National Space Council in 2017 address ransomware against space assets, even during an era when terrestrial systems have been harmed by ransomware.

How Should a Satellite Operator Respond?

- Pay the ransom immediately?

How Should a Satellite Operator Respond?

- Pay the ransom immediately?
- Attempt a recovery procedure?

How Should a Satellite Operator Respond?

- Pay the ransom immediately?
- Attempt a recovery procedure?
- Wait for next orbital pass?

The Orbital Escalation Game

A game-theoretic model for satellite ransomware attacks where:

The Orbital Escalation Game

A game-theoretic model for satellite ransomware attacks where:

1. Decisions are constrained by orbital windows

The Orbital Escalation Game

A game-theoretic model for satellite ransomware attacks where:

1. Decisions are constrained by orbital windows
2. The attacker escalates ransom across orbital passes

The Orbital Escalation Game

A game-theoretic model for satellite ransomware attacks where:

1. Decisions are constrained by orbital windows
2. The attacker escalates ransom across orbital passes
3. The defender chooses a response strategy

The Orbital Escalation Game

A game-theoretic model for satellite ransomware attacks where:

1. Decisions are constrained by orbital windows
2. The attacker escalates ransom across orbital passes
3. The defender chooses a response strategy
4. Is a Stackelberg game

Model Formulation

Players

Strategies

Defender Strategies
Pay
Refuse
Restore
Idle

Attacker Strategies
Set Initial Ransom
Set Escalation Policy

Payoffs

Expected Cost
Minimize

Payoff
Maximize

Information Set

Perfect Information
Knows strategies
Knows previous actions
Knows ground stations

Perfect Information
Knows strategies
Knows previous actions
Knows ground stations

Parameters

Defender
Restore cost
Restore duration
Restore probability
Downtime cost
Satellite loss

Attacker
Initial ransom
Ransom escalation
Exploit cost
Holding cost (upkeep)

Horizon

Defender
Pay
Refuse
Successful restore

Attacker
Ultimatum

Equilibrium Solution

Equilibrium Solution Steps

1. Calculate the defender’s expected cost
2. Calculate the attacker’s payoff
3. Use backward induction and Bellman equation

Defender’s Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender’s Expected Cost

$$V_k = \min\left\{ \underbrace{R_k}_{\text{PAY}},\ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}},\ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1-p_j) V_{k+d_j} \right]}_{\text{RESTORE}},\ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender's Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender's Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender’s Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender's Expected Cost

$$V_k = \min\left\{ \underbrace{R_k}_{\text{PAY}},\ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}},\ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1-p_j) V_{k+d_j} \right]}_{\text{RESTORE}},\ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender's Expected Cost

$$V_k = \min\left\{ \underbrace{R_k}_{\text{PAY}},\ \underbrace{c_{\downarrow} + V_{k+1}}_{\text{IDLE}},\ \underbrace{\min_j \left[C_j + d_j c_{\downarrow} + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}},\ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender’s Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender's Expected Cost

$$V_k = \min \left\{ \underbrace{R_k}_{\text{PAY}}, \ \underbrace{c_\downarrow + V_{k+1}}_{\text{IDLE}}, \ \underbrace{\min_j \left[C_j + d_j c_\downarrow + (1 - p_j) V_{k+d_j} \right]}_{\text{RESTORE}}, \ \underbrace{L_{\text{ref}}}_{\text{REFUSE}} \right\}$$

Defender’s Expected Cost

$$V_{K+1} = \min\{L_{\text{ref}}, R_{K+1}\}$$

Defender’s Expected Cost

$$V_{K+1} = \min\{L_{\text{ref}}, R_{K+1}\}$$

Defender’s Expected Cost

$$V_{K+1} = \min\{L_{\text{ref}}, R_{K+1}\}$$

Defender’s Expected Cost

$$V_{K+1} = \min\{L_{\text{ref}}, R_{K+1}\}$$

Attacker's Payoff

$$A_k = \begin{cases} R_k, & \text{if PAY,} \\ -c_{\text{hold}} + A_{k+1}, & \text{if IDLE,} \\ -c_{\text{hold}}\, d_j + (1 - p_j) A_{k+d_j}, & \text{if RESTORE j,} \\ 0, & \text{if REFUSE.} \end{cases}$$

Attacker's Payoff

$$A_k = \begin{cases} R_k, & \text{if PAY,} \\ -c_{\text{hold}} + A_{k+1}, & \text{if IDLE,} \\ -c_{\text{hold}}\, d_j + (1 - p_j) A_{k+d_j}, & \text{if RESTORE j,} \\ 0, & \text{if REFUSE.} \end{cases}$$

Attacker's Payoff

$$A_k = \begin{cases} R_k, & \text{if } \textsc{Pay}, \\ -c_{\text{hold}} + A_{k+1}, & \text{if } \textsc{Idle}, \\ -c_{\text{hold}}\, d_j + (1 - p_j) A_{k+d_j}, & \text{if } \textsc{Restore j}, \\ 0, & \text{if } \textsc{Refuse}. \end{cases}$$

Attacker's Payoff

$$A_k = \begin{cases} R_k, & \text{if PAY,} \\ -c_{\text{hold}} + A_{k+1}, & \text{if IDLE,} \\ -c_{\text{hold}}\, d_j + (1 - p_j) A_{k+d_j}, & \text{if RESTORE j,} \\ 0, & \text{if REFUSE.} \end{cases}$$

Backward Induction

- Solving the game starting from the last possible decision and working backwards to the present.
- Backward induction produces the subgame perfect equilibrium.

Case Study:
GPS III Satellite Ransomware Attack

Case Study Parameters

Parameter	Value
Downtime cost	$3M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Parameter	Value
Initial ransom	$112.5M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Parameter	Value
Initial ransom	$112.5M
Ransom escalation	$6M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Parameter	Value
Initial ransom	$112.5M
Ransom escalation	$6M
Exploit cost	$14M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Parameter	Value
Initial ransom	$112.5M
Ransom escalation	$6M
Exploit cost	$14M
Holding (upkeep)	$0.01M

Case Study Parameters

Parameter	Value
Downtime cost	$3M
Restore cost	Safe Mode: $0.01M Privileged TC: $0.01M
Restore duration	Safe Mode: 2 Privileged TC: 1
Restore probability	Safe Mode: 0.9 Privileged TC: 0.4
Satellite loss	$450M

Parameter	Value
Initial ransom	$112.5M
Ransom escalation	$6M
Exploit cost	$14M
Holding (upkeep)	$0.01M
Horizon	4 passes

Backward Induction Solution: End of Horizon

Ransom	Mission Loss
112.5M +	$450M
(4*6)= 24M =	
$136.5M	$450M
Best strategy: Pay	

Backward Induction Solution: End of Horizon

Ransom	Mission Loss
112.5M +	$450M
(4*6)= 24M =	
$136.5M	$450M
Best strategy: Pay	

Backward Induction Solution: Pass 4

Defender's Strategy	Cost
Pay	$130.5M
Idle	$139.5
Restore: Safe Mode	Not enough passes
Restore: Privileged TC	$85.91
Refuse	$450M

Backward Induction Solution: Pass 4

Defender's Strategy	Cost
Pay	$130.5M
Idle	$139.5
Restore: Safe Mode	Not enough passes
Restore: Privileged TC	$85.91
Refuse	$450M

Backward Induction Solution: Pass 4

Defender's Strategy	Cost
Pay	$130.5M
Idle	$139.5
Restore: Safe Mode	Not enough passes
Restore: Privileged TC	$85.91
Refuse	$450M
Best strategy: Restore: Privileged TC	

Backward Induction Solution: Pass 3

Defender's Strategy	Cost
Pay	$124.5M
Idle	$88.91
Restore: Safe Mode	$19.66
Restore: Privileged TC	$54.56
Refuse	$450M

Backward Induction Solution: Pass 3

Defender's Strategy	Cost
Pay	$124.5M
Idle	$88.91
Restore: Safe Mode	$19.66
Restore: Privileged TC	$54.56
Refuse	$450M

Backward Induction Solution: Pass 3

Defender's Strategy	Cost
Pay	$124.5M
Idle	$88.91
Restore: Safe Mode	$19.66
Restore: Privileged TC	$54.56
Refuse	$450M
Best strategy: Restore: Safe Mode	

Backward Induction Solution: Summary

Pass	Optimal Strategy	Cost
4+1	Pay	$136.5M
4	Privileged TC	$85.91M
3	Safe Mode	$19.66M
2	Safe Mode	$14.6M
1	Safe Mode	$13.9M

Ex ante and Ex post Equilibria

Pass	Optimal Strategy	Cost
4+1	Pay	$136.5M
4	Privileged TC	$85.91M
3	Safe Mode	$19.66M
2	Safe Mode	$14.6M
1	Safe Mode	$13.9M

Ex ante and Ex post Equilibria

Pass	Optimal Strategy	Cost
4+1	Pay	$136.5M
4	Privileged TC	$85.91M
3	Safe Mode	$19.66M
2	Safe Mode	$14.6M
1	Safe Mode	$13.9M

Pass	Optimal Strategy	Cost
4+1	?	?
4	?	?
3	?	?
2	?	?
1	?	?

Ex post Scenario

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Attacker Incremental	Attacker Cumulative
1	Safe Mode	$112.5M	$3M (downtime)	$3M	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M

Ex post Scenario

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Attacker Incremental	Attacker Cumulative
1	Safe Mode	$112.5M	$3M (downtime)	$3M	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M
2	Safe Mode	$118.5	$3 M (downtime) $0.01 M (SM cost)	$6.01M	−$0.01 M (hold)	−$14.02 M

Ex post Scenario

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Attacker Incremental	Attacker Cumulative
1	Safe Mode	$112.5M	$3M (downtime)	$3M	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M
2	Safe Mode (Failed)	$118.5	$3 M (downtime) $0.01 M (SM cost)	$6.01M	−$0.01 M (hold)	−$14.02 M
3	Privileged TC	$124.5	$3 M (downtime) $0.01 M (PT cost)	$9.02 M	−$0.01 M (hold)	−$14.03 M

Ex post Scenario

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Attacker Incremental	Attacker Cumulative
1	Safe Mode	$112.5M	$3M (downtime)	$3M	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M
2	Safe Mode (Failed)	$118.5	$3 M (downtime) $0.01 M (SM cost)	$6.01M	−$0.01 M (hold)	−$14.02 M
3	Privileged TC (Succeeded)	$124.5	$3 M (downtime) $0.01 M (PT cost)	$9.02 M	−$0.01 M (hold)	−$14.03 M
4	Game Ends	$130.5	$0.00 M	$9.02 M	$0.00 M	−$14.03 M

Ex post Scenario

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Attacker Incremental	Attacker Cumulative
1	Safe Mode	$112.5M	$3M (downtime)	$3M	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M
2	Safe Mode	$118.5	$3 M (downtime) $0.01 M (SM cost)	$6.01M	−$0.01 M (hold)	−$14.02 M
3	Privileged TC	$124.5	$3 M (downtime) $0.01 M (PT cost)	$9.02 M	−$0.01 M (hold)	−$14.03 M
4	Game Ends	$130.5	$0.00 M	$9.02 M	$0.00 M	−$14.03 M

Defender Expected Cost = $9.02 M

Attacker Payoff = –$14.03 M

Real-world Recommendations

- **Operational Readiness:** Satellite operators must know the available restore procedures and test them using digital twins, simulations, etc.

Real-world Recommendations

- **Operational Readiness:** Satellite operators must know the available restore procedures and test them using digital twins, simulations, etc.
- **Increase Contact Opportunities:** Having more ground stations helps defender implement more strategies

Real-world Recommendations

- **Operational Readiness:** Satellite operators must know the available restore procedures and test them using digital twins, simulations, etc.
- **Increase Contact Opportunities:** Having more ground stations helps defender implement more strategies
- **Response Planning and Training:** Operator can use our model to run wargames and train operators to act rationally under pressure.

Limitations of the model

- **Perfect Information Set:** Not realistic

Limitations of the model

- **Perfect Information Set:** Not realistic
- **Orbital Regimes:** LEO and MEO, not GEO

Limitations of the model

- **Perfect Information Set:** Not realistic
- **Orbital Regimes:** LEO and MEO, not GEO
- **Rationality Assumption:** Attacker might not be motivated by money

Limitations of the model

- **Perfect Information Set:** Not realistic
- **Orbital Regimes:** LEO and MEO, not GEO
- **Rationality Assumption:** Attacker might not be motivated by money
- **Discrete Passes:** Passes vary depending on orbit, ground stations

Future Work

- Parameterize passes using ground stations and minutes

Future Work

- Parameterize passes using ground stations and minutes
- Constellation-level modelling, e.g., Inter-satellite links (ISLs)

Future Work

- Parameterize passes using ground stations and minutes
- Constellation-level modelling, e.g., Inter-satellite links (ISLs)
- Bayesian extension to account for partial knowledge

Conclusion

- I introduced, the first game-theoretic model for satellite ransomware attacks
- The model encodes orbit constraints and 7 economic parameters
- I solved the equilibrium using backward induction
- I provided a GPS III satellite case study that illustrates how the model works

Thank you for listening!

Efrén López-Morales | elopezm@nmsu.edu | https://efrenlopez.org