Orbital Escalation: Modeling Satellite Ransomware Attacks Using Game Theory

Efrén López-Morales
New Mexico State University
elopezm@nmsu.edu

Abstract—**Ransomware has yet to reach orbit, but the conditions for such an attack already exist. This paper presents the first game-theoretic framework for modeling ransomware against satellites: the *orbital escalation game*. In this model, the attacker escalates ransom demands across orbital passes, while the defender chooses their best strategy, e.g., attempt a restore procedure. Using dynamic programming, we solve the defender's optimal strategy and the attacker's expected payoff under real orbital constraints. Additionally, we provide a GPS III satellite case study that demonstrates how our orbital escalation game can be applied in the context of a fictional but feasible ransomware attack to derive the best strategies at every step. In conclusion, this foundational model offers satellite owners, policy makers and researchers, a formal framework to better prepare their responses when a spacecraft is held for ransom.**

I. INTRODUCTION

Ransomware remains one of the most disruptive forms of cyberattacks, leveraging control over critical assets to extort payments (ransoms) from victims. The damage caused by ransomware includes loss of data, and business downtime. In 2024 the average ransom payment was $2.73 million [1].

While traditionally associated with terrestrial systems such as enterprise servers, hospitals, and critical infrastructure, recent incidents have drawn attention to the growing vulnerability of space-based systems. The 2022 cyberattack on Viasat's KA-SAT network, which disrupted satellite services across Europe, exemplifies the real-world risk of targeting satellite infrastructure via ground-side vectors [2]. Additionally, research has shown that ransomware techniques against Low Earth Orbit (LEO) satellites are feasible using vulnerabilities in components like NASA's Core Flight System (cFS) [3], [4].

A successful ransomware attack on an in-orbit satellite could potentially result in millions of dollars worth of damage. A single Medium Earth Orbit (MEO) satellite may cost hundreds of millions of dollars, serve irreplaceable national functions, and take years to design, launch, and commission. For example in 2022 it was reported that two new GPS III satellites had been ordered for $744 million [5]. These characteristics make satellite systems attractive to ransomware attackers seeking maximum leverage, and presenting a constrained decision space for satellite owners imposed by short communication windows (orbital passes).

Despite these stratospheric risks, there is no public space policy or guidance on how satellite owners should or even could respond when faced with a ransomware attack [6].

In comparison, such theories have successfully been developed for terrestrial systems, including, *game theory* models [7], [8] which provide strategies that help decision-makers respond when faced with a ransomware attack.

Game theory is a mathematical framework for modeling interactions between rational decision-makers [9]. It provides tools to analyze how agents with potentially conflicting objectives choose actions, anticipate responses, and optimize outcomes. In the context of computer security, game theory allows us to systematically study attacker-defender dynamics. However, to the best of our knowledge, game theory has not been applied to satellite ransomware attacks.

To solve this problem, this paper presents a game-theoretic model for satellite ransomware attacks that formalizes the interaction between the attacker, i.e., ransomware adversary, and defender, i.e., satellite owner. Our proposed model is designed as a Stackelberg game [10] (a sequential leader-follower game) where a particular satellite's communication window or orbital pass is used as the basis for attacker-defender strategies. At each orbital pass the attacker escalates their ransomware demands, i.e., increases the ransom and the defender chooses a strategy, such as a recovery procedure.

In addition to encoding LEO and MEO satellites' communication constraints, our model integrates 7 economic factors such as the downtime cost while the hostage satellite is not operational, and operational constraints such as limited restore procedures. By combining these temporal and strategic dependencies, our model captures how ransomware attacks can evolve across orbital passes, and how defenders can optimally time recovery actions to minimize total expected loss. We call this model, the *orbital escalation game*.

To evaluate our model, we develop a case study where a fictional Advanced Persistent Threat (APT) successfully takes a GPS III satellite hostage and use our model to explore multiple attack outcomes. Our case study shows how our model could be applied to potential ransomware incidents.

In summary, this paper makes the following contributions:

- We formulate, to the best of our knowledge, the first game-theoretic model for satellite ransomware attacks.

- We solve our model's equilibrium, i.e., the optimal strategies for attacker and defender, and discuss how these strategies can inform operational decisions.
- We provide a case study, that illustrates how our model can be applied to real-world satellite ransomware attacks.
- Finally, we provide an open-source analysis tool that implements our model[1].

II. BACKGROUND

A. Ransomware Threats to Satellites

While ransomware is well studied in terrestrial systems [8], [7], [11], [12], recent work has started to explore how these attacks unfold in the context of satellites.

Falco et al. [4] introduced *WannaFly*, a proof-of-concept ransomware attack tailored for LEO satellites. Their work demonstrated how a malicious payload uploaded to a satellite could mimic the logic of terrestrial ransomware by denying access to mission services until a ransom is paid. While the attack did not rely on strong encryption of the entire system, it effectively disrupted the availability of satellite resources.

Donchev et al. [3] extended this threat model by describing scenarios where ransomware targets satellite ground and space segments simultaneously. They emphasized how attackers might manipulate telecommands (TCs), to impose ransom demands, creating a multi-vector threat surface.

Together, these studies suggest that ransomware in satellites differs fundamentally from terrestrial settings. First, satellites often lack native full-disk or system-wide encryption, preventing attackers from using encryption-based ransomware. For example, the NanoMind A3200 on-board computer (OBC), widely used in CubeSats, includes an ARM9 processor [13] which does not support native encryption. Second, this limitation allows for alternative recovery strategies. For example, in 2024 a researcher managed to restore communications with a satellite that was considered lost [14]. Rather than requiring a decryption key, satellite operators could leverage safe-mode functions, and redundancy systems [15]. These restore functionalities are essential when modeling satellite ransomware attacks. The differences between terrestrial and satellite ransomware attacks are depicted in Table V.

B. Game Theory Model Building Blocks

Game theory uses fundamental components that define the interactions between players which we now describe.

Players. Players are the decision-makers in the game. They can be individuals, nation-states, or satellite operators [10]. In the context of ransomware attack models, players are labeled as "attacker" and "defender." The *attacker* launches the ransomware attack, and the *defender*, e.g., the satellite operator, reacts to the attacker's actions and makes strategic decisions to recover the satellite held for ransom.

Strategies. Strategies are the available actions each player can choose from at a particular stage in the game. Strategies are further categorized between *pure strategies* and *mixed*

[1] https://github.com/efrenlopezm/orbital-escalation-game

strategies [10]. Pure strategies are deterministic and their outcome is completely predictable. For example the "pay ransom" strategy always ends the game. Conversely, mixes strategies are nondeterministic and depend on probability. For example, the "recovery procedure" strategy may or may not succeed based on some previously known probability, e.g., 0.7.

Payoffs and Expected Costs. Payoffs quantify how desirable an outcome is to a player and players select strategies to maximize their payoffs, e.g., ransom payment [10]. Although payoffs apply to all players in the game, in cost-oriented settings, such as a ransomware attacks, it is more intuitive to model the defender as minimizing an *expected cost*, which plays a role equivalent to a payoff.

For example, if two players choose strategies that lead to a particular outcome, one player's payoff might be positive (a gain), while the other's is negative (a loss). In this paper, the attacker will be modeled as maximizing *payoff*, while the defender will be modeled as minimizing *expected cost*.

Information Set. The information set determines what each player knows at different stages of the game. Game theory models may have different assumptions about player information. For example, Stackelberg games, by definition assume that all players have *perfect* information, where each player knows all previous moves by all players at every decision point [10]. Because our model is a Stackelberg game, both attacker and defender have perfect information.

Equilibrium. The equilibrium is the optimal solution to the game assuming rational players. One game may have multiple equilibria, and each equilibrium differs depending on timing, information, and assumptions. Equilibria must be calculated which is also commonly known as *solving the game*. This involves finding a set of strategies where no player can improve their outcome by unilaterally deviating [10].

C. Stackelberg Games

Game theory has multiple types of games such as Nash games [16], where all players implement their strategies simultaneously and are often symmetric, e.g., all players use the same strategies. On the other hand, Stackelberg games, are sequential, e.g., players observe the opponent's strategy and then react, and they are asymmetric, e.g., players have different strategies. We model our orbital escalation game as a Stackelberg because ransomware interactions are inherently sequential and asymmetric, as such this type of games provide a natural framework to build our model.

Formally, in Stackelberg games, both players are fully rational and the follower has perfect information about the leader's move [17]. The leader, anticipating the follower's best response, chooses a strategy that maximizes their own utility given this knowledge. The solution to a Stackelberg game is the subgame perfect Nash equilibrium (SPNE) [18]. Lastly, in Stackelberg games, the concept of a *horizon* is used to define how far into the future the game extends. A finite horizon limits the number of sequences that can occur (e.g., the number of orbital passes).

III. THREAT MODEL

In our orbital escalation game, we consider an attacker capable of launching ransomware attacks against LEO or MEO satellites (e.g. state-sponsored actors) with the objective of coercing the satellite operator into meeting specific demands, e.g., ransom payment. The attacker may exploit vulnerabilities in the satellite's command and control infrastructure, ground segment interfaces, or on-board software. While terrestrial ransomware attacks almost always involve encrypting the system's data we consider any attack in which an adversary blocks the legitimate satellite owner from accessing and operating the spacecraft, which we discussed in Sec. II-A.

We also assume that the attacker has knowledge of the location(s) of the satellite's mission ground stations and the satellite's orbit which allows the attacker to predict future passes and their duration from both the attacker's location and the defender's ground stations.

For the defender or satellite operator, we consider that they maintain the capability to attempt to communicate with the spacecraft via an operational mission control system.

IV. ORBITAL ESCALATION GAME: MODEL FORMULATION

We model our orbital escalation game as a Stackelberg game between the ransomware attacker and the satellite operator defender. The key feature of our model is that both the attacker and defender strategies revolve around the hostage satellite's orbit. The attacker *escalates* their ransom every time a pass is completed and the defender can only implement a strategy during orbital passes, when ground station communication is possible. We now formally describe our model.

A. Players and Strategies

There are two players, the ransomware attacker and the satellite operator defender. The attacker initiates the game and commits up front to an extortion strategy defined as $\pi_A = (R_0, \Delta R)$, where R_0 is the initial ransom demand and ΔR is the increment added to the ransom after each orbital pass. Additionally, the attacker pays a one-time exploit cost C_{atk} to compromise the satellite and incurs a holding cost c_{hold} per orbital pass while the game continues. This holding cost may be due to the attacker's operational costs, e.g., electricity, however, it may also increase due the risks associated with their illegal activity, (the cost of getting caught).

At each orbital pass, the defender must select a strategy to respond. The available defender strategies are:

1) PAY: immediately transfer the ransom R_k to the attacker. This strategy ends the game.
2) IDLE: take no direct action, instead use the pass for indirection action, e.g., plan or communicate internally, incurring a downtime cost $c_{\downarrow}$ until the next orbital pass.
3) RESTORE j: attempt a recovery procedure j that has a direct cost C_j, requires d_j passes to complete, and succeeds with probability p_j.
4) REFUSE: declare refusal to pay. This terminates the game and incurs a mission loss L_{ref} for the defender.

B. Ransom Escalation Dynamic

The game's time dynamic or cadence is controlled by orbital passes, denoted $\{t_k\}_{k=1}^{K}$ where K defines the *horizon* of the game (maximum number of passes) as discussed in Sec II-C. At each pass k, the attacker's ransom has escalated to:

$$R_k = R_0 + (k-1)\Delta R$$

Fig. 1. Current ransom at orbital pass k.

Thus, waiting without paying is costly, both because downtime cost accumulates for the defender, and because ransom steadily increases. A shorter horizon compresses decision-making, forcing earlier payments or risk of mission loss, while a longer horizon creates opportunities to attempt recoveries.

C. Equilibrium Analysis

As with any game theory model, we need to solve our orbital escalation game's equilibrium, discussed in Sec. II-B. To achieve this, we need to analyze it from the perspectives of both attacker and defender.

First, we need to solve the *defender's decision problem* which yields the *expected cost* (Sec. II-B) and the corresponding optimal strategy. Second, given the optimal strategy, we need to solve for the the attacker's *expected payoff*.

1) Defender's Expected Cost: Solving the defender's decision problem provides the best-response strategy under any given attacker policy by minimizing the defender's expected cost, and it is necessary to solve the game equilibrium.

To solve the defender's decision problem we use dynamic programming. Specifically, we use the Bellman equation [19], which is a standard technique in dynamic programming that breaks a problem into a sequence of simpler subproblems.

We model the defender's decision problem as the Bellman recursive equation shown in Fig. 2. Let V_k represent the defender's *minimal expected cost* starting from pass k. At each decision point, the operator weighs four actions' costs: PAY, IDLE, RESTORE and REFUSE as described in Sec. IV-A.

If the game has not ended and the end of the horizon $(K+1)$ is reached, the defender is forced to simply compare between paying the escalated ransom or suffering mission loss as described in Fig. 3.

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

Fig. 3. Defender's end of horizon decision.

Together Eq. 2 and Eq. 3 capture the defender's best-response policy μ^*: a mapping from each orbital pass to the least costly available action.

2) Attacker's Expected Payoff: Given the defender's optimal response policy μ^*, the attacker's objective is to maximize their expected payoff by selecting ransom parameters

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

Fig. 2. Defender's decision problem equation modeled as a Bellman recursion at orbital pass k. Here V_k is the defender's minimal expected cost; $R_k = R_0 + (k-1)\Delta R$ is the ransom demand at pass k; $c_\downarrow$ is the per-pass downtime cost; V_{k+1} and V_{k+d_j} are continuation values after idling or a failed restore, respectively; C_j, d_j, and p_j are the direct cost, duration (in passes), and success probability of restore strategy j; and L_{ref} is the mission loss if the defender refuses to pay. At each pass the defender compares the four options and chooses the action that minimizes cost.

$\pi_A = (R_0, \Delta R)$. For example, in prior ransomware models [11], a rational attacker chooses an initial ransom below the defender's refusal loss to make payment the defender's preferred response, and setting a ransom escalation rate higher than the downtime costs renders delayed payment unattractive.

Let A_k denote the attacker's *expected continuation payoff* at orbital pass k, that is, the expected profit from this pass onward, excluding any past (sunk) costs. The attacker pays a one-time exploit cost C_{atk} when compromising the satellite and a holding cost c_{hold} per orbital pass while the satellite remains under their control. Conditioned on the defender's chosen action at pass k, the attacker's continuation value evolves as follows:

$$A_{K+1} = \begin{cases} R_{K+1}, & \text{if } R_{K+1} \le L_{\text{ref}}, \\ 0, & \text{otherwise.} \end{cases}$$

Fig. 4. Attacker's end of horizon payoff.

At the end of the horizon, the attacker's payoff depends on whether the defender ultimately decides to pay the ransom or to accept mission loss. This terminal condition is defined in Eq. (4). The attacker's total expected payoff from the start of the game is calculated using Eq.(6).

$$\Pi_{\text{att}} = -C_{\text{atk}} + A_{k_0}$$

Fig. 6. The attacker's total expected payoff Π_{att}, combining the initial exploit cost C_{atk} and continuation value A_{k_0} at the first pass.

D. Equilibrium Solution

The game reaches an *equilibrium* when both players' strategies are mutually optimal given the sequential order of play.

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

Fig. 5. Recursive formulation of the attacker's continuation value A_k at orbital pass k. Each term represents the attacker's expected payoff given the defender's chosen action (Pay, Idle, Restore, or Refuse).

The attacker first commits to a ransom policy $\pi_A = (R_0, \Delta R)$, where $R_0 \ge 0$ and $\Delta R \ge 0$. Given this policy, the defender observes π_A and plays a best-response policy μ^*. The attacker then anticipates this response and chooses the ransom policy that maximizes their total expected payoff: At equilibrium, the pair $(\pi_A^\star, \mu^*)$ satisfies:

- The defender's strategy μ^* is the optimal (lowest-cost) response to the attacker's ransom policy $\pi_A^\star$.
- The attacker's strategy $\pi_A^\star$ yields the highest expected payoff given that the defender responds optimally.

E. Model Assumptions

To make the orbital escalation game analytically tractable while preserving the key features of a realistic satellite ransomware scenario, we adopt the following four assumptions. First, the game is discrete and sequential in time, unfolding across orbital passes. Second, the model assumes complete information: both players know all relevant parameters of the game at all times, which is a necessary feature of Stackelberg games (Sec. II-C). Although in an operational setting the players will not actually have access to perfect information, our model serves as a conservative worst-case baseline. Third, costs and rewards are additive across passes. Fourth and final, the game terminates when the defender chooses PAY, REFUSE, when a restoration attempt succeeds or when the maximum horizon K is reached without resolution.

Our model's multiple parameters are summarized in Appendix C for better readability.

V. Case Study: GPS III satellite Ransomware Attack

In order to illustrate how our orbital escalation game works, we instantiate it via a case study where a real-world satellite, a GPS III satellite, becomes the target of a fictional ransomware attack. We selected the GPS III satellite because there is enough public documentation available regarding its cost and contribution to the US economy which allows us to create a more realistic case study. Due to space limitations we are unable to explain the reasoning for each of the parameters' values here, however, they are available in Appendix A.

A. Parameters

In this case study the defender is the operator of the GPS III constellation, namely, the U.S. Space Force, and the parameters are as follows:

$$\pi_A^\star = \underbrace{\arg\max_{R_0,\, \Delta R \geq 0}}_{\text{Optimization of ransom policy}} \left\{ \underbrace{-C_{\text{atk}}}_{\text{Exploit cost}} + \underbrace{A_{k_0}(\pi_A, \mu^*)}_{\text{Expected payoff given defender's best response}} \right\}.$$

Fig. 7. Attacker's optimization problem equation. Here $\pi_A = (R_0, \Delta R)$ is the attacker's ransom policy, where R_0 is the initial ransom demand and ΔR is the increment applied after each orbital pass. C_{atk} represents the one-time exploit cost paid to compromise the satellite, and $A_{k_0}(\pi_A, \mu^*)$ is the attacker's expected continuation payoff starting from the first orbital pass k_0, given the defender's optimal response policy μ^*. The symbol $\arg\max$ indicates that the attacker chooses the specific values of $(R_0, \Delta R)$ that maximize the total expected payoff.

- Mission loss $(L_{\text{ref}}) = \$450\text{M}$
- Downtime $c_\downarrow = \$3\text{M/pass}$
- Restore options (each usable once):
  1) Safe mode: $C_1 = \$10\text{k}$, $d_1 = 2$, $p_1 = 0.9$.
  2) Privileged TC: $C_2 = \$10\text{k}$, $d_2 = 1$, $p_2 = 0.4$.

On the other side, the attacker is D3FILERZ, a fictional state-sponsored Advanced Persistent Threat (APT) capable of successfully launching a ransomware attack against a GPS III satellite. The attacker has the following parameters:

- Attacker ransom policy: $R_0 = \$112.5\text{M}$, $\Delta R = \$6\text{M}$.
- Attacker costs: $C_{\text{atk}} = \$14\text{M}$, $c_{\text{hold}} = \$10\text{k/pass}$.

D3FILERZ also informs the U.S. Space Force they have only 4 passes to pay the ransom otherwise the GPS III satellite will be permanently lost. This sets the game horizon to $(K = 4)$, where each restore strategy can be used only *once*.

B. Solving the Defender's Optimal Response

Using the previously described parameters, we now solve the orbital escalation game.

1) Backward Induction Procedure: To obtain the defender's optimal strategy, we solve the Bellman Eq. (2) by *backward induction*, starting from the last orbital pass and moving toward the first. This means we first determine what the defender would optimally do if the game reached the end of the horizon, and then propagate those values backward so that every earlier decision accounts for the future consequences.

Terminal condition (K = 5). At the end of the four-pass horizon $(K = 4+1)$, if no decision has terminated the game, the defender faces one final comparison between paying the ransom or suffering total mission loss. The terminal condition value is calculated using Eq. (3). To calculate the ransom at the terminal orbital pass, we use Eq. (1) and substitute the values of D3FILERZ's ransom policy:

$$R_5 = R_0 + (5-1)\Delta R = \$112.5\,\text{M} + (5-1) \times \$6\,\text{M} = \$136.5\,\text{M}$$

Since $R_5 < L_{\text{ref}} = \$450\,\text{M}$, the minimal cost at the terminal step is $V_5 = \$136.5\,\text{M}$. This means that if the defender reaches the end without restoring the satellite, paying the ransom at that point is less costly than losing the mission outright.

Final Pass (K = 4). Working backward, we evaluate each preceding orbital pass, in this case, $k = 4$, by applying the defender's decision problem Eq. (2). At every pass, the defender compares four actions: PAY, IDLE, RESTORE and REFUSE as discussed in Sec. IV-A.

At pass $k = 4$ only one communication window remains before the game terminates. The defender compares:

Defender's Strategy	Formula from Eq.(2)	Cost ($M)
PAY	$R_4 = R_0 + (4-1)\Delta R$ $= 112.5 + (3 \times 6)$	$130.5\,\text{M}
IDLE	$c_\downarrow + V_5$ $= 3 + 136.5$	$139.5\,\text{M}
RESTORE 1 (SM)	$d_1 = 2 > 1$ (not enough passes)	N/A
RESTORE 2 (PT)	$C_2 + d_2 c_\downarrow$ $+(1-p_2)V_{4+d_2}$ $= 0.01 + 3 + (0.6 \times 136.5)$	$85.91\,\text{M}
REFUSE	$L_{\text{ref}} = 450$	$450\,\text{M}

The minimal expected cost is therefore $V_4 = \$85.91\,\text{M}$, achieved by RESTORE 2 (PT). Operationally, this represents a last-minute attempt to recover the satellite with the quick one-pass privileged TC before the final ransom deadline.

Pass (K = 3). At this stage, both restore options remain available since neither has been used yet. Safe Mode $(d_1 = 2)$ and Privileged TC $(d_2 = 1)$ are both feasible because they can complete before the terminal step $(k + d_j \leq K + 1 = 5)$. The continuation value from the next pass is $V_4 = \$85.91\,\text{M}$. At pass $k = 3$ defender compares:

Defender's Strategy	Formula from Eq.(2)	Cost ($M)
PAY	$R_3 = R_0 + (3-1)\Delta R$ $= 112.5 + (2 \times 6)$	$124.5\,\text{M}
IDLE	$c_\downarrow + V_4 = 3 + 85.91$	$88.91\,\text{M}
RESTORE 1 (SM)	$C_1 + d_1 c_\downarrow + (1-p_1)V_{3+d_1}$ $= 0.01 + 6 + (0.1 \times 136.5)$	$19.66\,\text{M}
RESTORE 2 (PT)	$C_2 + d_2 c_\downarrow + (1-p_2)V_{3+d_2}$ $= 0.01 + 3 + (0.6 \times 85.91)$	$54.56\,\text{M}
REFUSE	$L_{\text{ref}} = 450$	$450\,\text{M}

The minimal expected cost is therefore $V_3 = \$19.66\,\text{M}$, achieved by RESTORE 1 (SM). Operationally, this means that at the third orbital pass, the defender initiates the longer but highly reliable Safe Mode recovery, which completes just before the final ransom deadline. Its high success probability $(p_1 = 0.9)$ and low direct cost make it preferable to both paying and the riskier one-pass Privileged TC.

Remaining Passes (K = 2 and 1). Due to space limitations we are unable to develop the remaining two passes. Nevertheless, the remaining passes are calculated using the same method and the summarized results are shown in Table I.

TABLE I
BACKWARD INDUCTION SOLUTION FOR EACH ORBITAL PASS

| Pass	Avail. Restores	Feasible Actions	Optimal Strategy	V_k ($M)
5 (term.)	–	Pay, Refuse	PAY	$136.5 M
4	{SM,PT}	Pay, Idle, PT, Refuse	RESTORE 2 (PT)	$85.91 M
3	{SM,PT}	Pay, Idle, SM, PT, Refuse	RESTORE 1 (SM)	$19.66 M
2	{SM,PT}	Pay, Idle, SM, PT, Refuse	RESTORE 1 (SM)	$14.6 M
1	{SM,PT}	Pay, Idle, SM, PT, Refuse	RESTORE 1 (SM)	$13.9 M

Fig. 8. Prepared defender scenario decision tree. The edges that originate from restore attempt nodes include their success probabilities from Sec. V.

C. Calculating the Attacker's Payoff

Under the U.S. Space Force's optimal strategy derived above, the defender never chooses to pay the ransom and instead relies on restoration strategies. Consequently, D3FILERZ receives no positive ransom income, yet still incurs the exploit and holding costs. Using Eq. (6) and the recursive formulation in Eq. (5). we calculate the attacker's payoff by substituting the parameters $c_{\text{hold}} = \$10,000 = \$0.01 M$ (holding cost), $C_{\text{atk}} = \$14 M$ (exploit cost) and $K = 4$ (number of passes):

$$\Pi_{\text{att}} = -C_{\text{atk}} + A_{k_0} = -14 - 0.04 = -\$14.04 M$$

Therefore, D3FILERZ ends the game with a *negative expected payoff* of $-\$14.04 M$ due to the fact that the U.S. Space Force's optimal strategy does not include PAY or REFUSE.

D. GPS III Satellite Case Study Summary

Overall, the case study equilibrium reveals that the U.S. Space Force should prioritize restoration attempts rather than payment with Safe Mode being the optimal strategy during the first three orbital passes, while Privileged Telecommand being optimal during the final pass.

However, these results represent the ideal equilibrium strategies assuming that the restore attempts are successful. In a real operational setting, the outcome of the game could change due to factors such as failed restore attempts, or communication delays. We explore these in the next section.

This case study is an illustrative application of our model rather than a general claim about ransomware response strategies across all space missions. The equilibrium outcome observed for GPS III is shaped by mission-specific assumptions, e.g., mission loss cost. Different mission profiles, such as lower cost satellites, may yield substantially different equilibria.

VI. REALIZED GPS III SATELLITE SCENARIOS

In the previous section (Sec. V) we obtained the *equilibrium under ideal circumstances*, in this section we present two scenarios with *realized outcomes* of the GPS III satellite case study. The purpose is to translate the mathematical equilibrium
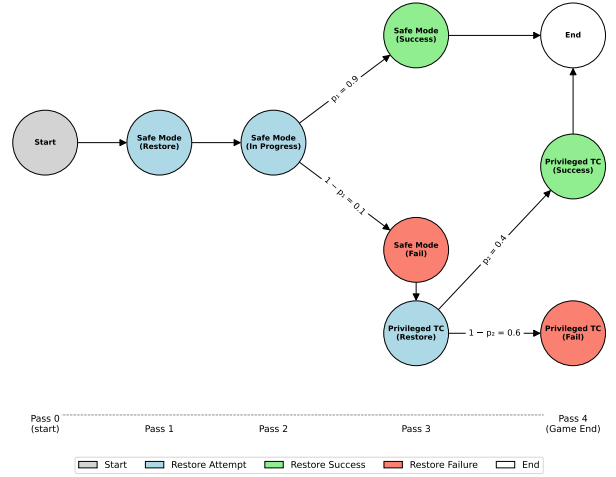
into an operational narrative that shows how the defender's and attacker's strategies unfold once random outcomes, such as restore success or failure, occur. Specifically, we present an *unprepared defender* and a *prepared defender* scenario. In the unprepared defender scenario, the U.S. Space Force is not ready to implement their restore strategies, i.e., there is no standard operating procedure, while in the prepared defender scenario, clear procedures are in place to initiate the restore procedures.

A. Unprepared Defender

We now describe the strategies that the *unprepared defender* (U.S. Space Force) implements during the available four passes. At each pass we compare the *realized selected strategy* vs the strategy recommended by the equilibrium under ideal circumstances as shown in Table I.

At **Pass 1**, the equilibrium recommends RESTORE (SM), i.e., safe mode. However, the U.S. Space Force is forced to instead implement IDLE because they need time to find out how to initiate safe mode. This incurs downtime $c_{\downarrow} = \$3 M$, for the defender and a holding cost $c_{\text{hold}} = \$0.01 M$ for the attacker, and the ransom R_1 escalates to $112.5 M$.

At **Passes 2–3**, after some internal coordination, the defender initiates the two-pass RESTORE (SM) procedure. Across these two passes they incur $c_{\downarrow} = \$6 M$, plus the safe mode cost of $C_j = \$0.01 M$. Therefore the defender's expected costs reaches $9.01 M$, while the ransom R_3 has escalated to $124.5 M$. For the attacker, three passes of holding cost have accrued, leaving the attacker with a negative $14.03 M$ payoff.

At **Pass 4**, Unfortunately, safe mode did not stop the ransomware attack. The equilibrium policy at pass 4 recommends the RESTORE (PT) strategy, but again, the defender lacks a procedure for issuing the privileged command. Thus, they are forced to remain in IDLE. This pass adds another $c_{\downarrow} = \$3 M$, raising the defender's expected cost to $12.01 M$, while the ransom reaches $R_4 = \$130.5 M$. For the attacker, another holding cost of $0.01 M$ is incurred, for a $-14.04 M$ payoff.

At **Pass 5**, the game has reached its terminal condition discussed in Sec. V-B1 which recommends paying the ransom as the least costly option. Therefore the U.S. Space Force is forced to pay the ransom amount $R_5 = \$136.5\,\text{M}$ to D3FILERZ and the game ends. In total, the unprepared defender's expected cost is $\$148.51\,\text{M}$, combining four passes of downtime, the failed safe-mode attempt, and the final ransom payment. The attacker, after subtracting their exploit and holding costs, obtains a $\$122.46\,\text{M}$ payoff.

B. Prepared Defender

We now describe the strategies that the *prepared defender* implements. At each pass we compare the *realized selected strategy* against the strategy recommended by the equilibrium under ideal circumstances as shown in Table I.

At **Passes 1–2**, the equilibrium recommends the RESTORE (SM) strategy, i.e., safe mode. The U.S. Space Force follows its previously tested and documented standard operating procedures (SOPs) and immediately initiates it. Over these two passes, the defender incurs $c_{\downarrow} = \$6\,\text{M}$ in downtime and the safe mode execution cost of $C_j = \$0.01\,\text{M}$, and the ransom escalates to $R_2 = \$118.5\,\text{M}$. For the attacker, two passes of holding cost accrue, for a cumulative payoff of $\$-14.02\,\text{M}$.

At **Pass 3**, the U.S. Space Force determines that safe mode did not stop the attack. The equilibrium recommends RESTORE (SM) again, but this strategy cannot be reexecuted. Therefore, the defender implements RESTORE (PT). This pass incurs the restore cost $C_k = \$0.01\,\text{M}$ and one pass of downtime $c_{\downarrow} = \$3\,\text{M}$, and the ransom escalates to $R_3 = \$124.5\,\text{M}$. The attacker's cumulative payoff is $\$-14.03\,\text{M}$.

At **Pass 4**, the privileged telecommand succeeds, restoring nominal operations and liberating the hostage GPS III satellite.

In total, the prepared defender's expected cost is $\$9.02\,\text{M}$, composed of three passes of downtime, the safe-mode cost, and the privileged-telecommand cost, while avoiding any ransom payment. The attacker, after subtracting the exploit and holding costs, ends with a negative payoff of $-14.03\,\text{M}$.

The realized prepared defender game decision tree is illustrated in Fig. 8, with its per-pass economic parameters accounting summarized in Table II.

C. Realized Scenarios Summary

Under our model's finite-pass structure, escalating ransom, and costly downtime, the unprepared defender loses critical early passes to IDLE, triggering compounding delays resulting in a $\$148.51\,\text{M}$ expected cost and an attacker payoff of $\$122.46\,\text{M}$. The prepared defender, by contrast, executes both restore actions within the model's tight pass constraints, avoids any ransom payment, and liberates the GPS III satellite for only $\$9.02\,\text{M}$ while leaving the attacker with a $\$-14.03\,\text{M}$ payoff. These outcomes, show that mission operational preparation, is a key factor in satellite ransomware attacks.

VII. DISCUSSION

A. Real-World Implications for Satellite Mission Operations

Operational Readiness. Mission operators should document their available recovery strategies and test them in simulations, digital twins or testbeds so that their success rates, costs, and duration (number of required passes) are known.

Increase Contact Opportunities. Our model reveals that contact opportunities are crucial during an attack. As such, operators should increase the number of contact opportunities for each pass, e.g., increasing the number of ground stations. This could be accomplished by deploying mobile ground stations or creating partnerships with other missions.

Response Planning and Training. Operators should conduct wargames using the orbital escalation game to gain experience and prepare standard operating procedures in the event of a ransomware attack. This would allow operators to make rational decisions under pressure and avoid mistakes.

These implications may resemble conventional mission practices, but their security motivation, pass-dependent urgency, and quantified economic justification are new.

B. Limitations

Modeled Orbital Regimes. Our model relies on orbital passes to dictate the phase of the game, making our model applicable to LEO and MEO satellites only as GEO satellites are always in communication with their ground stations.

Perfect Information Assumption. Under our model's perfect information assumption, the attacker is assumed to know the defender's set of recovery procedures and may therefore plan actions to mitigate them. In practice, however, successful "counter-recovery" strategies require additional attacker capabilities (e.g., uplink jamming) and are out of the scope of our model. Additionally, in practice, an attacker may not always know which specific recovery procedure the defender has attempted. In general, our Stackelberg model's perfect information assumption provides a conservative worst-case baseline that ensures that the defender's equilibrium strategies remain robust even under maximal attacker awareness.

Rationality Assumption. Our model assumes that all players are fully rational and assumes that each player seeks to maximize expected utility given the available information and constraints. In practice, real-world attackers may exhibit bounded rationality, pursue non-economic objectives, or deviate from equilibrium behavior due to political reasons.

Discrete Passes. The current model uses discrete orbital passes as contact opportunities in satellite operations. In practice, however, real-world missions may involve multiple geographically distributed ground stations, inter-satellite links (ISLs), and heterogeneous uplink capabilities, allowing both defenders and attackers to interact with a spacecraft outside of a single line-of-sight pass. These factors can increase the number, duration, and overlap of effective interaction opportunities, and thus are not fully captured by a single-pass abstraction.

C. Generalizability

The orbital escalation game provides a general analytical framework for studying attacker-defender interactions in space systems that unfold over repeated, constrained control opportunities. While this work instantiates the model in the context

TABLE II
PER-PASS ACCOUNTING FOR THE PREPARED DEFENDER REALIZED SCENARIO. ALL COSTS IN MILLIONS OF DOLLARS.

Pass	Realized Strategy	Ransom	Defender Incremental	Defender Cumulative	Remaining Restores	Attacker Incremental	Attacker Cumulative
1	RESTORE (SM)	$112.5 M	$3 M (downtime)	$3 M	{SM, PT}	−$14 M (exploit) −$0.01 M (hold)	−$14.01 M
2	RESTORE (SM)	$118.5 M	$3.00 M (downtime) $0.01 M (SM cost)	$6.01 M	{PT}	−$0.01 M (hold)	−$14.02 M
3	RESTORE (PT)	$124.5 M	$3.00 M (downtime) $0.01 M (PT cost)	$9.02 M	{}	−$0.01 M (hold)	−$14.03 M
4	Game Ends	$130.5 M	$0.00 M	$9.02 M	{}	$0.00 M	−$14.03 M
	Defender Expected Cost = $9.02 M				**Attacker Payoff = −$14.03 M**		

TABLE III
COMPARISON BETWEEN OUR WORK AND PREVIOUS WORK

Work	Defender Strategies	Economic Params	Game Stages	Domain
Laszka et al. (2017) [11]	2	7	2	Terrestrial
Caporusso et al. (2019) [8]	3	5	3	Terrestrial
Li et al. (2021) [7]	2	6	4	Terrestrial
Orbital Escalation Game	**4**	**7**	**Multiple Passes**	**Space**

of ransomware, the same game structure can be applied to other classes of space security scenarios.

For example, coordinated jamming [20] campaigns involving multiple rogue ground stations targeting subsets of a LEO constellation can be modeled as interaction cycles, where both attacker interference allocation and defender mitigation decisions are shaped by geography-dependent access and cost.

VIII. RELATED WORK

Prior game-theoretic models of ransomware primarily focus on enterprise or generic network environments. *Laszka et al.* [11] developed the first formal ransomware model as a two-stage game between organizations and an attacker, emphasizing backup investments and ransom decisions. Their model captures key economic incentives but remains static, with limited strategic depth and no temporal evolution. *Caporusso et al.* [8] later proposed a descriptive finite-state machine model capturing sequential escalation and negotiation but without economic parameters. *Li and Liao* [7] proposed a model that includes enterprise settings, integrating risk perception and insurance but retaining a single-stage structure.

In contrast, our model introduces a multi-stage ransomware game tailored to satellite operations. Our model expands the defender's action space to four strategies, incorporates seven economic parameters derived from mission costs and recovery outcomes, and unfolds over multiple orbital passes. As depicted in Table III, our model offers the most comprehensive formulation of ransomware dynamics to date, integrating richer economic factors and defender strategies.

IX. FUTURE WORK

The orbital escalation game model opens several directions for extension. First, we plan to relax the perfect information assumption by formulating a Bayesian game [21] extension that captures uncertainty and partial knowledge between attacker and defender.

Additionally, future work may refine the abstraction of communication windows by parameterizing them using deployment-specific characteristics, including the number and geographic distribution of ground stations, contact durations measured in seconds or minutes, and uplink redundancy for both defenders and attackers.

Beyond orbital passes, the framework can be extended to capture alternative ransomware scenarios. For example, launch segment attacks, reentry or crewed spacecraft scenarios which may be better modeled as one-shot rather than sequential games. Related game theory models have been explored in other space settings, such as docking operations [22].

Another direction is a sensitivity analysis [21] of the model to characterize how equilibrium strategies change as key parameters vary. By exploring mission loss, or ransom, such analyses can identify how and why equilibria shifts and derive new satellite mission operation recommendations.

Finally, an important extension is to move from single asset analysis to constellation-level interactions. In such settings, attackers may selectively disrupt subsets of satellites, while defenders must consider partial service degradation, recovery prioritization, and alterative recovery vectors such as ISLs.

X. CONCLUSION

Although no satellite ransomware incident has yet been documented, research shows that they are feasible. Satellite operators and policymakers should therefore be prepared. In this paper, we introduced the *orbital escalation game*, the first game-theoretic model for satellite ransomware attacks. We hope that satellite owners, and researchers employ our model, and its open-source analysis tool, to plan their responses before, during, and after a spacecraft is held for ransom.

REFERENCES

[1] Sophos, "Ransomware payments increase 500% last year, finds sophos state of ransomware 2024," 2024, accessed: 2025-07-16. [Online]. Available: https://www.sophos.com/en-us/press/press-releases/2024/04/ransomware-payments-increase-500-last-year-finds-sophos-state

[2] "Case study: Viasat attack," https://cyberconflicts.cyberpeaceinstitute.org/law-and-policy/cases/viasat, accessed: 2025-05-24.

[3] M. Donchev and D. Smyth, "Evaluating an effective ransomware infection vector in low earth orbit satellites," *arXiv preprint arXiv:2412.04601*, 2024.

[4] G. Falco, R. Thummala, and A. Kubadia, "Wannafly: An approach to satellite ransomware," in *2023 IEEE 9th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*, 2023, pp. 84–93.

[5] S. Erwin. (2023) Space force orders three gps satellites for $744 million. Accessed: 2025-09-15. [Online]. Available: https://spacenews.com/space-force-orders-three-gps-satellites-for-744-million/

[6] N. Reese, "Space assets could be held ransom. will we have any choice but to pay?" *SpaceNews*, June 2025, accessed: 2025-06-03. [Online]. Available: https://spacenews.com/space-assets-could-be-held-ransom-will-we-have-any-choice-but-to-pay/

[7] Z. Li and Q. Liao, "Game theory of data-selling ransomware," *Journal of Cyber Security and Mobility*, pp. 65–96, 2021.

[8] N. Caporusso, S. Chea, and R. Abukhaled, "A game-theoretical model of ransomware," in *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9.* Springer, 2019, pp. 69–78.

[9] J. Von Neumann and O. Morgenstern, *Theory of Games and Economic Behavior*. Princeton University Press, 1944.

[10] M. J. Osborne *et al.*, *An introduction to game theory*. Springer, 2004, vol. 3, no. 3.

[11] A. Laszka, S. Farhang, and J. Grossklags, "On the economics of ransomware," in *International conference on decision and game theory for security*. Springer, 2017, pp. 397–417.

[12] S. Liu, R. Bazzi, F. Fang, and T. Bao, "Teamwork makes the defense work: Comprehensive vulnerability defense resource allocation," in *Proceedings of the 24th International Conference on Autonomous Agents and Multiagent Systems*, ser. AAMAS '25. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2025, p. 1362–1370.

[13] GomSpace, "Nanomind a3200 on-board computer," https://gomspace.com/shop/subsystems/on-board-computers/nanomind-a3200.aspx, 2023, accessed: 2025-09-19.

[14] PistonMiner, "How a german researcher resurrected beesat-1 after more than a decade," https://en.clickpetroleoegas.com.br/como-um-hacker-alemao-ressuscitou-um-satelite-abandonado-ha-12-anos-e-transformou-o-impossivel-em-realidade/, 2024, accessed: 2025-09-19.

[15] ESA / eoPortal Directory, "Giove-a (galileo in-orbit validation element-a) satellite mission," https://www.eoportal.org/satellite-missions/giove-a, 2024, accessed: 2025-09-19.

[16] J. F. Nash, "Equilibrium points in n-person games," *Proceedings of the National Academy of Sciences*, vol. 36, no. 1, pp. 48–49, 1950.

[17] H. von Stackelberg, *Marktform und Gleichgewicht.* Springer, 1934, english translation: Market Structure and Equilibrium, 1952.

[18] D. Fudenberg and J. Tirole, *Game Theory.* MIT Press, 1991.

[19] R. E. Bellman and S. E. Dreyfus, *Applied dynamic programming.* Princeton university press, 2015.

[20] U. Planta, J. Rederlechner, G. Marra, and A. Abbasi, "Let me do it for you: On the feasibility of inter-satellite friendly jamming," in *2024 Security for Space Systems (3S)*, 2024, pp. 1–6.

[21] R. Gibbons, "An introduction to applicable game theory," *Journal of Economic Perspectives*, vol. 11, no. 1, pp. 127–149, 1997.

[22] T. Hiramatsu and N. G. Fitz-Coy, "Game theoretic approach to post-docked satellite control," in *Proceedings of the 20th International Symposium on Space Flight Dynamics*, 2007.

[23] J. Foust. (2016) Spacex wins $82 million contract for 2018 falcon 9 launch of gps 3 satellite. Accessed: 2025-09-15. [Online]. Available: https://spacenews.com/spacex-wins-82-million-contract-for-2018-falcon-9-launch-of-gps-3-satellite/

[24] A. C. O'Connor, M. P. Gallaher, K. Clark-Sutton, D. Lapidus, Z. T. Oliver, T. J. Scott, D. W. Wood, M. A. Gonzalez, E. G. Brown, and J. Fletcher, "Economic benefits of the global positioning system (gps)," 2019.

[25] U. S. S. Force, "Smc and its partners poised to launch fourth GPS III satellite," https://www.losangeles.spaceforce.mil/News/Article-Display/Article/2365822/smc-and-its-partners-poised-to-launch-fourth-gps-iii-satellite/, Sep. 2020, accessed: 2025-12-02.

[26] O. Samir, "Attitude determination and control of gps satellites: Stabilization, orbital insertion, and operational control mechanisms," *arXiv preprint arXiv:2508.01660*, 2025.

[27] National Aeronautics and Space Administration (NASA), "New horizons exits brief safe mode, recovery operations continue," https://www.nasa.gov/general/new-horizons-exits-brief-safe-mode-recovery-operations-continue/, 2017, accessed: YYYY-MM-DD.

[28] J. Willbold, M. Schloegel, M. Vögele, M. Gerhardt, T. Holz, and A. Abbasi, "Space odyssey: An experimental software security analysis of satellites," in *2023 IEEE Symposium on Security and Privacy (SP).* IEEE, 2023, pp. 1–19.

[29] Federal News Network, "Stuxnet holds appeal as alternative weapon of war," https://federalnewsnetwork.com/the-federal-drive-with-terry-gerton/2011/09/stuxnet-holds-appeal-as-alternative-weapon-of-war/#:~:text=He%20deconstructed%20the%20Stuxnet%20source,And%20nobody%20died, Sep. 2011, accessed: 2025-10-02.

[30] D. R. Staff. (2022) Apt groups make quadruple what they spend on attack tools. Dark Reading. Accessed: 2025-10-17. [Online]. Available: https://www.darkreading.com/cyberattacks-data-breaches/apt-groups-make-quadruple-what-they-spend-on-attack-tools

[31] NASA Jet Propulsion Laboratory, "Nasa's voyager team focuses on software patch for thrusters," https://www.nasa.gov/missions/voyager-program/nasas-voyager-team-focuses-on-software-patch-thrusters/, NASA, 2022, accessed: 2025-10-15.

[32] F. K. Dana, S. K. Monfared, and S. Tajik, "Logical maneuvers: Detecting and mitigating adversarial hardware faults in space," in *Network and Distributed System Security Symposium (NDSS)*, 2023. [Online]. Available: https://www.ndss-symposium.org/ndss-paper/auto-draft-622/

[33] J. Rederlechner, U. Planta, and A. Abbasi, "One small patch for a file, one giant leap for ota updates," in *Proceedings of the Workshop on Security of Space and Satellite Systems (SpaceSec)*, San Diego, CA, USA, Feb. 2026.

APPENDIX A
GPS III SATELLITE CASE STUDY PARAMETER DETAILS

Mission Loss. For mission loss we added the estimated cost for procuring the satellite and the cost for launching it. In 2022 it was reported that two new GPS III satellites had been ordered for $744M [5]. Using this figure we can infer that a single satellite costs around $372M. Additionally, in 2016 it was reported that the cost of launching a GPS III satellite was $82M [23]. Adding these makes up for a total of $454M which we round to $450M.

Downtime cost. According to a 2019 report [24], the U.S. economy derived approximately $68.7 billion in benefits from GPS in 2017 alone. Assuming an active constellation of 31 satellites [25], this implies an average contribution of $2.2 billion per satellite per year. Dividing this evenly over time, we estimate a per-satellite downtime cost of approximately $6M per day, or $3M per orbital pass (assuming two passes per day). We adopt a $3M per pass downtime cost.

Restore Strategies. Satellites, including the GPS III satellites have a safe mode [26] that allows them to shutdown non-essential systems. Additionally, engaging safe mode may take several hours or days [27] which is why we decided to assign the safe mode strategy a restore duration of 2 passes. Because safe mode is a standard, contingency procedure routinely

tested during spacecraft operations, we assign it a relatively high probability of success (0.9).

Regarding the Privileged TC strategy we could not find any evidence for its use in GPS III satellites, however, these types of telecommands have been documented in other satellites [28] and we assigned a restore duration of 1 pass as it involves sending one telecommand. Due to its less standardized use we assign a lower success probability (0.4).

Initial Ransom. Following the strategic attacker framework by Laszka et al. [11], we set the ransom below the defender's refusal loss to maximize the likelihood of payment while ensuring attacker profit. We conservatively set the ransom at 25% or \$112.5M of the estimated mission loss (\$450M).

Ransom Escalation. To ensure that delaying payment is economically unattractive, the per-pass ransom escalation ΔR should be set larger than the defender's per-pass downtime cost c_{down}. As a conservative baseline, we set the escalation to twice the downtime cost: \$6M.

One-time Exploit. To estimate the cost of the one-time exploit we looked at previous instances of the cost of developing malware for Cyber-Physical Systems, specifically, Stuxnet. It is estimated that Stuxnet's development costed \$10M in 2010 [29], which equals \$14M in 2025 dollars.

Holding Cost. We estimate the attacker's per-pass holding cost based on the recurring expenses of sustaining APT infrastructure. Reports indicate that APT groups invest up to \$10,000 in tools for their activities [30]. As such we assign a conservative holding cost of \$10,000 per pass.

These parameter descriptions strengthen the realism of the fictional attack described in Sec. V.

APPENDIX B
MODEL PARAMETER SUMMARY

Table IV summarizes all of our model's parameters (Sec. IV) and provides information on how each parameter affects the game's equilibrium and its real-world satellite operational relevance.

APPENDIX C
RANSOMWARE COMPARISON

Table V showcases the differences between terrestrial and satellite ransomware attacks which are further discussed in Sec. II-A.

TABLE IV
SUMMARY OF MODEL PARAMETERS AND SYMBOLS

Parameter	Symbol	Effect on Equilibrium
Initial ransom demand	R_0	Higher initial ransom accelerates Pay/Refuse threshold; extreme demands trigger immediate Refuse.
Ransom escalation per pass	ΔR	Faster escalation pushes the defender toward early Pay/Refuse; very steep escalation makes Refuse dominant.
Downtime cost per pass	$c_{\downarrow}$	High $c_{\downarrow}$ pushes defender toward Pay; low $c_{\downarrow}$ enables Idle/Restore strategies.
Restore cost (strategy j)	C_j	High C_j makes restore strategies unattractive or infeasible.
Restore duration (in passes)	d_j	Long d_j makes restore unattractive when $c_{\downarrow}$ is high or when few passes remain.
Restore success probability	p_j	High p_j makes Restore optimal; low p_j favors Pay or Idle.
Mission replacement cost / terminal loss	L_{ref}	If $L_{\text{ref}} < R_k$, defender Refuses; if $L_{\text{ref}} > R_k$, Pay may dominate.
Attacker exploit cost	C_{atk}	High attacker cost discourages launching or escalating attacks.
Attacker holding cost per pass	c_{hold}	High c_{hold} penalizes long games; benefits the defender when choosing Idle.
Game horizon (number of passes)	K	Short horizon forces early Pay/Refuse; long horizon supports Idle/Restore.

TABLE V
COMPARISON OF RANSOMWARE IN TERRESTRIAL VS. SPACE SYSTEMS

Aspect	Terrestrial	Satellites
Execution Environment	• Windows/Linux • High CPU/RAM • Crypto libraries	• RTOS / bare-metal • Limited CPU/RAM • Often no crypto libraries
Attack Vector	• Phishing • Leaked credentials	• Uplink entry • GS compromise
Denial Mechanism	• Encrypt filesystem • Key-tied ransom	• Modify Flight Software • Disable FS exploit [4]
Impact	• Financial downtime • Local/regional	• Valuable asset loss [5] • Nationwide/Global [24]
Detection	• Network monitoring	• Telemetry anomalies
Recovery	• Restore backups • Reimage systems • Cloud failover	• Firmware patch [31] • Safe mode [27] • Privileged TC [28] • Hardware reconfig [32] • OTA update [33]