Emergency Response Team Framework for Space Systems (ERTFSS)

Alexandre Khalfallah*, Shivank Vyas*, Shubhankar Kulkarni*, Anusha Joshi*
*Johns Hopkins Univeristy

***Abstract*—Just like the police force is needed to catch criminals on the ground, a special team is needed to catch cybercriminals. This team is called a Computer Emergency Response Team (CERT) or a CSIRT (Computer security Incident Response Team). As satellite operations are very different from a classical network, the actions and missions of a CERT must be adapted. In this paper, a tool is proposed to help these teams handling satellite-related incident . This framework can guide the CERT during the process on space systems.**

In this paper, a framework is proposed to deal with satellite-related cyberattacks. The goal of this framework is to provide technical steps to solve the issues and go beyond just providing guidelines.

I. Introduction

A. Background

With the increase in the number of companies using satellites, there has been an increase in the number of satellites in orbit. All of these satellites are vulnerable to attacks due to the lack of inbuilt security in their software, as well as CubeSats, which makes satellites accessible to a wider range of attackers.

Companies that have a satellite that can be accessed by anyone with an antenna or a CubeSat are significantly increasing their attack surface. The satellite is another component that can be accessed by anyone and could be attacked by anyone. As many satellites may be connected to the same ground station or to a company's network, a compromised satellite can lead to serious damages, including disabled satellites that cannot be controlled [9] or extensive damage to the entire network.

There are several mitigation techniques that can be implemented in satellites, including a Threat-Based Approach provided in [12] that includes all of the attacks and mitigation actions for analysis tools. However, not all mitigation plans work for spacecraft, and can still lead to attacks. In such cases, a Computer Emergency Response Team (CERT) will have to handle the incident.

For all of the aforementioned reasons, it is important to research and learn about CERTs. Many frameworks for CERTs applied to computer science have previously been developed [10][17][13]. The spacecraft field has many fundamental differences with computer science, so many actions have to be adapted, such as the mitigation steps in [12]. There is a lack of literature detailing CERTs for spacecraft, in contrast to papers focusing on general networks.

B. Scope, contribution and audience

The scope of the paper will be to build a framework focused on all of the steps to be taken in the case of an attack. The framework ERTFSS will detail four steps in Figure 1 (Before the attack, Analysis of the attack, Response to the attack, and After the attack). Each of the steps is at a low technical level and provides more elements than other frameworks like the NIST framework [10], notably by providing a list of countermeasures and tools specific to the space industry. The paper is structured so that each of the steps has its own dedicated section with subsections about the different types of guidelines.

The audience for this paper is companies or governments that have already sent or plan to send a satellite into orbit, and want to learn more about any security issues and how to handle such incidents using a CERT. The main contribution of this paper will be to adapt computer science-focused guidelines for CERTS to satellite-focused guidelines.

II. Related work

A. Existing help for CSIRT

there are many documentation to help CSIRT on different steps of their work. There are works on the creation of CSIRT [1] and on their organisation in the team[2]. Some works propose a way to prepare the CSIRT to be ready to respond to the attack[3] or to identify and classify them using framework[26]. Few papers talk about the kernel of the CSIRT work, the technical answer. These studies give a high point of view of the answer[4] For fellow who are studying CSIRT or companies who want to create one with few initial skills, it is hard to know the technical requirements and tools.

B. Existing incident response framework

There are many incident response framework [10][21] which are already made, with as reference

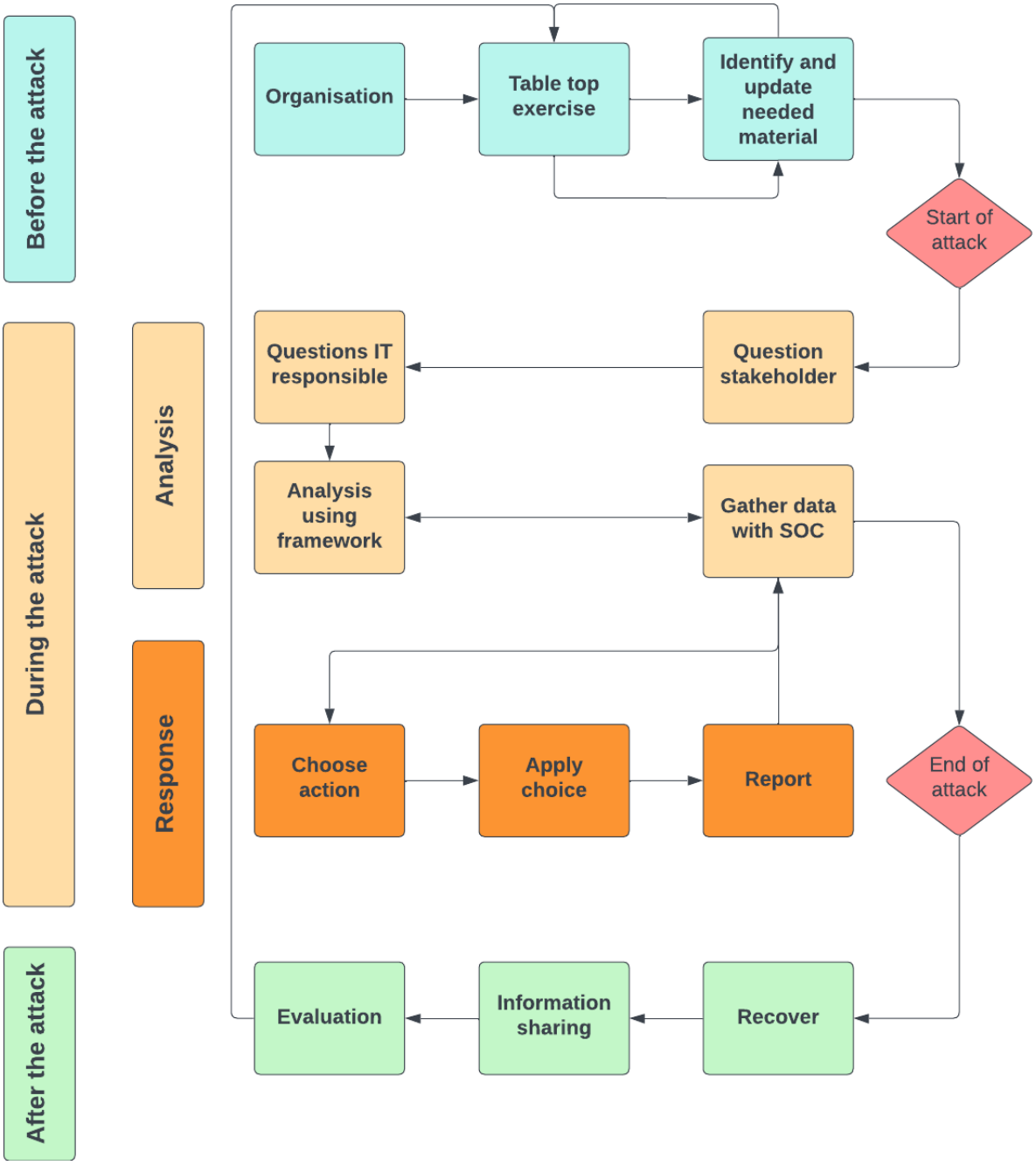

Figure 1. ERTFSS Framework description

the NIST framework [10] they can apply to companies networks and do not take into consideration the possible particularities of each sector. they can be applied for satellite but there will be many issues and they will not be optimized.

To be applicable to the most companies, they use a very high level point of view and have very few concrete technical steps to apply for your network [21]. that is why having only global incident response frameworks are not a good solution.some sectors already have their ones like petroleum industry [5]. CSIRT are still associated to a state or sold as a service, while CSIRT should develop themselves as sector based [6]

C. Satellite security framework

The field of space cybersecurity suffered from a big lack of projects. Now the field is developing thanks to many initiatives [7]. The most famous are projects like SPARTA [12] or ISAC [8].

ISAC (Information Sharing and Analysis Center) is a concept that originated in the United States in the 1990s to provide a platform for sharing cyber threat

intelligence and best practices between organizations within a particular industry sector. Today, there are multiple ISACs covering various industries, including the space industry.

The SPARTA project brings together a consortium of 44 partners from 14 countries, including space agencies, academic institutions, and private companies. The project aims to develop and implement a comprehensive cybersecurity framework for the space industry, covering both ground-based and space-based assets and operations.The SPARTA project will focus on developing innovative cybersecurity solutions to enhance the resilience of the space industry against cybersecurity threats and to ensure the secure and reliable operation of space-based systems and services. These projects are space cybersecurity frameworks before and after the attack. there is no framework known to help to deal with an attack during the attack. That part is crucial to limit the impact of the attack and prevent from spreading through the whole network.

D. Specificity of satellite network

The CERT protocol in satellites is similar to the CERT protocol in other contexts for the main steps and guidelines (Identify, Contain, Eradicate, Recover)[10]. However, there are a few key differences that are specific to the use of CERTs in the context of satellites which leads to very different details for each of these steps and to a requirement of a specific framework. The following list is a non-exhaustive list of all the items which can lead to critical change in the method of incident response in the context of satellites compared to initial NIST method by analyzing for each of the steps of its methodology [10]:

Identify:

The purpose of this step is to have information about what is happening in the satellite and having reliable information about the attack to take adapted decision. This purpose have to be adapted to satellite for the following reasons.

- Limited access to affected systems: Satellites are physically inaccessible once launched, making it difficult to directly inspect or isolate the affected systems.
- Unreliable communication: Limited bandwidth and latency issues can hinder real-time monitoring and analysis of satellite systems.
- Dynamic environment: Satellites in orbit experience frequent changes in communication links, making it challenging to consistently track affected systems.

The mission can also be to collect data and artefacts about the attack to analyze later to understand what happened and where does the attack come from.This purpose have to be adapted to satellite for the following reasons.

- Remote data collection: Collecting evidence from satellites is challenging due to limited access and communication constraints.
- Data volatility: Satellite systems often have limited storage capacity, leading to the rapid overwriting of data and loss of potential evidence.
- Legal and regulatory constraints: Collecting and preserving evidence from satellite systems may be subject to international laws and treaties, complicating the process.

Contain:

The purpose of this step is to isolate the infected component to avoid it to spread through the network and infect other satellites. The CSIRT completes this task by unplugging the compromised system from the network.This purpose have to be adapted to satellite for the following reasons.

- Irreversible consequences: Quarantining a satellite system may render it inoperable, causing significant financial and operational losses.
- Interdependencies: Satellite systems are often interconnected, making it difficult to isolate a specific system without disrupting overall functionality.
- Limited redundancy: Satellites have limited redundancy due to constraints in weight, size, and power, reducing the options for isolating or replacing affected systems.

Eradicate:

The purpose of this step is to exploit the information we have about the attack. The CSIRT get this information from very different and resources consuming systems they are used to. This purpose have to be adapted to satellite for the following reasons.

- Complex systems: The specialized and intricate nature of satellite systems can make it challenging to pinpoint the root cause of an incident.
- Limited diagnostic tools: Due to the constraints of satellite systems, there may be limited built-in diagnostic capabilities for incident analysis.
- Multiple attack vectors: Identifying the root cause can be difficult when dealing with multiple potential attack vectors, such as ground stations, satellite links, and onboard systems.
- Proprietary technology: Satellites often use pro-

prietary technology, limiting the availability of information about potential vulnerabilities.
- Evolving threat landscape: The rapid evolution of cyber threats makes it difficult to identify all potential vulnerabilities in satellite systems.
- Resource constraints: Limited resources, including bandwidth and computing power, may hinder the identification of vulnerabilities and weaknesses.

  Once the information is obtained and analyzed, the CSIRT have to develop and implement the containment measures by taking into consideration the impact on the system based on their knowledge on the system and experience. This purpose have to be adapted to satellite for the following reasons.

- Limited update capabilities: Satellites may have limited options for deploying updates or patches to address vulnerabilities.
- Operational risks: Implementing containment measures may introduce new risks or disrupt critical operations.
- Time-sensitive nature: The urgency of some satellite missions may not allow for sufficient time to develop and implement containment measures.

  Recover:

  Once the attack is stopped, the CSIRT or the local IT team has to recover the system to restart the production. to achieve it, many analyzes and tests have to be done to very the attacker will not come back and has no more access to the system. This purpose have to be adapted to satellite for the following reasons.

- Limited testing capabilities: The remote nature of satellites makes it difficult to perform comprehensive testing to validate eradication and containment measures.
- Dynamic environment: Satellites operate in a dynamic environment, making it challenging to ensure that eradication and containment measures remain effective over time.
- Unpredictable threat landscape: New and evolving threats may render eradication and containment measures ineffective or introduce new vulnerabilities.

CERTs for satellites have to operate in a unique environment, with constraints and challenges that are different from other types of computer systems. due to technologies used, the context and the location the CERT team has to get adapted processes for satellites to avoid the risks induced by their processes.

III. Adaptation to satellite

A. Threat model

In the actual case, our threat model will be satellite segment oriented to be a use case of satellite hacking. Attacks on ground stations or user segments are similar to actual papers in computer science. The threat model will be based on the following elements:

- The attacker has an antenna
- The attacker has technical knowledge
- The attacker took control of the satellite
- The attacker's goal is to spread through the network and infest ground stations and other satellites
- The attacker has resources and software like malware
- The goal of the attacker is not to destroy the satellite
- The satellite is likely to be attacked. There are many possible Types of attacks specified for satellites and many countermeasures against these attacks are detailed in the SPARTA project[12].

The attack will be defined by three attack trees in Table I: one to compromise the satellite (Infection attack tree), one to compromise the network (Spread attack tree), and one to put pressure on the company in case of discovery of the attack (Pressure attack tree). For all of these attacks, the tree is made in the form of a table with the Cyber Kill Chain [16] as a row and one column for each attack tree.

B. Before the attack

1) CERT organisation:

The CERT is in charge of preparing for and responding to IT incidents such as cyber-attacks, system outages, and data breaches. The team may also be in charge of creating incident response strategies, identifying, and fixing system vulnerabilities, restoring operations and minimizing damages. They also prioritize collaboration with the government, law enforcement, academia, and industry. These teams place a premium on producing threat intelligence and best practices for security responses. To be effective, a CERT will need some skills [2] for the following reasons:

Cyber Kill Chain	Infection attack tree	Spread attack tree	Pressure attack tree
Reconnaissance (Get information about the network)	Look for satellite frequency	Discreet reconnaissance tools (nmap)	Network architecture
Weaponization (Prepare tools for the attack)	Same frequency between antenna and satellite	Flaw analysis tool (CVE)	Adapting malware to give pressure to the company
Deliver (Identify a way to use the attack and send it)	Identify flaws	Listen to protocol and service to find weaknesses	Install malware during the connection
Execute (Execute the planned attack)	Execute exploit	Use weakness found	Execute virus automatically in case of connection lost
Installation (Place where tools are located)	In satellite	In other computer	In network
Command and control (How is the attack controlled by the attacker)	Via antenna link	via initial flaw found previously	Communication channel via server
Objective (Goal of the attack)	Infect satellite	Spread through network	Pressure on company

Table I
THREE ATTACK TREES DURING APPLIED DURING THE HACK BASED ON THE CYBER KILL CHAIN

- Malware analysis-Analyze files the hacker will include in the network
- Threat intelligence - To understand the attacker, his capabilities, and his actions
- Communication - To write reports and communicate with stakeholders
- Forensics - Gather artifacts and analyze them
- Networking - Identify malicious packets and information leaks
- Log analysis - Identify malicious actions and indices of compromise
- Operating System knowledge - Find malicious processes, viruses and attack technical functioning
- Leadership - Dealing with the team and take decisions
- Pentesting background - Know tools, possible attacks and flaws
- Satellite knowledge - To adapt the actions to satellite components and network

2) What is needed:

To be effective, a CERT needs to be prepared and have tools, depending on the access from the CERT to the network he will have to respond on, not all of the actions could be done. The CERT will need software, hardware, and training.

Hardware:

- Out of domain computers-to act on not compromised devices
- 4g module - to have access from a not compromised network
- Fireproof closet closed with a locker - to have access to computers only in case of emergency and be safe in case of fire (take care about the key/password only the team leader got it), the closet has to be in a room accessible without information system
- Antenna - to communicate with the satellite
  software defined radio - To encode messages in the antenna

Software and data:

- Out-of-network way of communication - To conversations does not have eavesdropped.
- Password for all of the tools - tools may not often be used passwords may be forgotten, and the possibility of using a password manager.
- Communication tree for each company - To know how to spread information through the whole company without using the company network (may have privacy issues)
- Software associated with required skills - To not lose time installing during the attack.
- Communication template with the press - Some attacks may be mediatized, a thoughtful and calm reaction may be needed.
- Relevant documents from the company - Asking for documents to know the company's topology.
- Any prepared data from framework - Asking all of the data in the following parts to not lose time during the attack.
- Detection rules (YARA rules... [28]) - May be found on repositories
- All of the security software installed before the attack. - many software can be useful even if

the system is compromised like vulnerability management software

- Disaster recovery plan - Faster recovery part
- Incident response plan - faster response part
- report templates(possibility of using IODEF [32]) - Faster reporting and information sharing

Training:
Some emergency response teams are only associated with a few networks and are not regularly activated. They have to maintain their efficiency by doing tabletop exercises. They can be done with a fake satellite for a more realistic process or with a copy of the network. These attack simulations are organized by the team on a regular basis (once a year), it has many advantages:

- Train the team
- Make the team not forgets processes and good practices
- Update software on a regular basis
- Update documents
- Verify the process is still coherent
- makes the team discover new processes and update its knowledge

C. Analysis of the attack

1) Questions:

The stakeholders in this situation can include database managers, server engineers, cloud engineers, production machine operators, product owners, and satellites from the same constellation or connected to the same ground station.

Bringing all of these stakeholders to a common point will allow them to conduct a risk assessment of the attack from their own perspective, ensuring that all potential scenarios for tackling the attack are considered.

One of the key challenges in dealing with stakeholders during an attack is understanding their preferences and priorities. The emergency response team should always seek to understand the importance of each system to the company and the stakeholders' preferences for how to deal with it. To do this, the team can ask simple, straightforward questions that can be easily answered. For example, the team could ask stakeholders: "When can the emergency response team switch off the service of your system?" Based on the answer to this question, the team can determine the appropriate course of action. The possible answers to the question are limited to certain graduated instances, like:

1-The component can be turned off as the attack starts
2-The component can be turned off as soon as the attacker can have access to the server
3-The component can be turned off as soon as the attacker has an administrator (highest rights) account
4-The component can be turned off as soon as the attacker is in the same server
5-The component always has to stay open, whatever is happening and whatever the consequences

These data will help the CERT to take a decision when the analysis of the attack is done, this process will help to save time by directing the stakeholder to do the needful, hence mitigating the situation in a very efficient way.

It is very important to ask questions to the stakeholders whenever there is an attack. It will help us to understand a few major parameters, like the attack's impact, the threat actor's motivation, and where the attacker is located. The questions asked will help to establish the scenario and evaluate it by utilizing some of the analysis frameworks stated in the paper. Hence taking appropriate actions becomes reasonable and logical by asking different questions [13]. The part below will encompass documents like Network topology and functional description of systems from the IT teams or the ground team. Then, a set of key questions satellite-related are proposed to ask to some stakeholders. Each question has to get a precise goal to bring new information which could be useful for the analysis and helps to identify the threat. In each of the following questions, a goal example is proposed.

For the IT team of the Ground station:

- Logical network topology: Even when a group of devices is not physically connected to one another, they can be regarded as a single management unit using logical abstractions like a Virtual Local Area Network (VLAN). This includes things like domains on networks running Microsoft Windows.

- The function (purpose, role) of main devices: To identify which computer programs and devices are essential to the organization, and which other network components rely on a particular device

- Organization's directory: It is likely that you need to involve other people from the organization, either to gather more information or to inform about the incident.

With these documents, there are some really

important questions that we need to ask to specific stakeholders

The following questions are the ones from which the CERT team can start assessing.

Satellite Operator:

- What do you see? How does this differ from the usual behavior? What is the usual behavior? - This will help to understand the type of attack
- This symptom that is happening to your system (or reporter's device) is doing to others? - To understand whether the attack is local or is spreading across the network
- When are the symptoms first noticed in a satellite? - To know when the attack took place.
- Has anything changed before the symptoms occurred? - To understand if there was any update/work done on the system and find out possible vulnerabilities.
- Are the symptoms still occurring or have they stopped? If Yes, When did they stop? Did anything change before they stopped? - It will help to assess the type of country from where the attack originated based on the work hours.
- What measures have you taken to mitigate the attack and restore operations? - To assess the effectiveness of the response and identify any additional steps that may be necessary
- How is connected your satellite to the ground station and to other satellites? - It will help to identify the next possible targets by the attacker using Lateral movements
- What are the mission objectives affected by the satellite? - It will help the CERT team to evaluate the goal of the attackers

For Servers Engineer:

- Any changes in the database over the past few weeks? - It will help to know if the hacker has reached the database
- Where is the server located? - To identify the compromised location of the attacker in the network
- Where is the malicious traffic from the attacker coming from? - It will help to understand the attacker's server or attacker's method
- What is the IP address of your satellite? - The goal is to identify the malicious packets.
- What version of the Operating system and SCADA software is running on the satellite? - To find the possible flow of the satellite.

For Product Owners/ Systems Engineer:

- Are the subsystems working correctly? - To get an idea about the privilege of the hacker in the satellite.
- Is there any change in the logs coming from the sub-systems of the satellite? - To get an idea about the privilege of the hacker in the satellite.

2) Using framework:

ICAR Whenever an attack occurs there are various questions that the CERT team should ask to understand the severity of the attack. According to the [26], it is very important to Identify, classify and find the right information for an adaptive response. The best approach is to first identify the stakeholders involved in the attack With these documents there are some really important questions that we need to ask specified stakeholders. For this paper, we are considering all the stakeholders related to CERT.

D4I: It is a digital forensic framework proposed in [16] that allows the analysis of an attack by linking the Cyber Kill Chain, Indices of Compromise, and Chain of Artefact based on the Artefact Categorisation by SANS [17]. This analysis lets the CERT understand how the attack was made and provides indices on the attacker. All of the proofs found in the system must follow forensic good practice to be usable in front of a court to prosecute the intruder.

Automation language: As the quantity of data is raising, many analyses are not feasible fully by the hands of forensics experts, and many tasks have to be automatized in forensics thanks to many languages created by researchers. these languages will help forensic experts of the CERT team to find suspicious files through all of the data following rules defined by the CERT team. these files will be analyzed by the forensic expert to have clear conclusions. All of these languages are based on different rules which can be specific to satellites and bring different elements so they can be complementary in the analysis like:

- VQL, a SQL-like language to request files based on rules [27].
- YARA, a set of rules user-defined and domain-specific to identify and classify malware samples[28]
- XOVAL, an XML-based language to detect wrong configurations in a network [29]
- XLIVE, a scenario-based framework that lets doing a list of files with a high probability to find information depending on the scenario.[30]
- XIRAF, an indexing and querying tool by bite range for forensics investigation[31]
- IODEF, a text-based language to communicate security events for CERT teams.[32]

3) Using the SOC:

Information security (IS) incidents have recently increased in number, variety, and severity as well as disruption. The majority of IS occurrences are reduced by preventive controls based on the conclusions of the IS risk assessment, but not all of them. The SOC (Security Operations Center) team is internal to the company and manages internal tools to gather information about the network and the endpoints. Its main mission is to quickly identify IS incidents and then work with the CERT team to minimize loss and destruction, mitigate exploited vulnerabilities, and restore the satellite infrastructure, including its network and services.

To identify useful elements, many techniques can be used, as shown in TableII[33]. Some of the most important correlation techniques that help organizations are statistical and rule-based, as both techniques help to identify risks and threats in a very effective manner. For example, statistical methods utilize algorithms to identify threats in satellite systems based on the presence and potential severity of aberrant event patterns. On the other hand, rule-based techniques are very effective in identifying specific satellite threats. To apply all of these techniques, the SOC needs a lot of effective data, such as traffic sniffing, device configuration, and centralization of data. A set of identification rules is proposed in [33].

All of the information needed to apply the actions in TableIV comes from the SOC analysis or framework analysis in III-C2. Under attack conditions, having enough information to master risks and consequences is crucial."

4) Identify compromised systems:

During an attack, it is important to identify compromised parts of the network, it will help the Emergency response team on many points:
- Focus on a part of the system
- Know which servers are compromised
- Be aware of the attacker's actions
- Identify lateral movements (a focus is made in III-C5)
- Identify potentially compromised components(in same network)

All of these elements are very useful to handle the incident. There are many ways to find the compromised parts, to achieve it the SOC team (section III-C3) has to be involved, each technique has its merits and limits:

-Analyze processes, Malware will create processes the user never saw before, however malware can use a common name for their processes, a step-by-step methodology is proposed in [14]
-Analyze network communication, In [15] the main way to identify compromised endpoints is to focus on the number of connections, compromised computers are doing more connections with servers than other computers
-List of changes, when a malicious user has access to a network, it will add malware using a compromised account for many purposes. This malware can be identified by looking for actions made by compromised accounts. This malware can be used to harm the network (delete data, stop crucial components, overheat machines...)in case of loss of connection from the attacker, it is important to detect and analyze (it may give information about the attacker using reverse engineering during or after the attack depending on skills of the emergency response team) and delete (or keep a copy out of network for deeper analyze).
-Actions made by compromised accounts may help to find the same virus or identify actions to repair and systems to analyze to recover the network.

5) Lateral movement:

The two main Authentication protocols used in Active directories are NTLM and Kerberos, there are many attacks to log in without having the user password, respectively Pass-the-Hash and Pass-the-Ticket. these attacks need to get login information which can be gathered in many ways like (i) Windows memory analysis when credentials are not deleted by windows (ii) being connected to the same workstation as the victim. Depending on conditions different technologies will have different behavior [18].
Before executing the steal of credentials, the attacker has to be a local administrator but may not has to be a local administrator to use the credentials depending on the technology used. In the paper [18], logs rules detection are proposed to detect lateral movements.
All of the elements can be applied as it is to satellite

Type of Technique	Description	How it works	Effectiveness
Statistical	Assess the seriousness of a satellite-related incident	Identify satellite threats based on aberrant network event patterns. Assigns a satellite threat score depending on asset value.	Depends on the quantity of data, the effectiveness of collection, and the algorithm used
Rule Based	By observing a particular sequence of events within a predetermined time window, SOC uses established rules that use conditional logic to detect possible attack scenarios	Provide rules to implement them on a custom basis after carefully examining network traffic.	Depends on rules chosen, risk false positive, need maintain
Service Level	Method which helps to evaluate losses from compromised network elements or components rendered out of service	SOC creates models of mission processes and analyzes the effects of various satellite accidents on these operations	It is essential to the objective because it makes it simpler to estimate losses caused by compromised network components or dysfunctional components.
Vulnerabilities	Using vulnerability management scanners, returning a score for each asset.	It helps eliminate false positives by reducing noise and helps determine which assets are actually vulnerable to the attack	Without more information, fixing random vulnerabilities will have a low impact
Mixed	The detection of actual threats can significantly be increased when different correlations are used together.	By utilizing the different techniques together	Helps for decision and correlation, depending on the algorithm used and available information.

Table II
REFERENCE TABLE FOR THE QUANTITATIVE VALUE OF EFFORT

systems by focusing mainly on machines communicating with the spacecraft.

D. Response to the attack

1) Organisation during the attack:

When an attack is identified, the Emergency Response Team will have to only use elements out of the compromised network to be sure the attacker does not have access to their information and anticipate their action. To achieve it, the Emergency response Team will use all of the material they prepared before the attack in III-E3.

All of the actions made in the network have to be coherent with policy and wishes made by stakeholders in III-C1. At the end of the incident handling the goal will be to recover the network and reverse all of the actions made by the attacker and Emergency Response Team, to achieve it, a report with all of the actions and decisions made by the team has to be submitted. The responsible for the network has to know all of the actions.

To apply the actions chosen, the CERT will need information, all of this information will come from the SOC team III-C3 and the analysis they can do during the attack thank to frameworks in section III-C2.

During the whole process, it is essential the hacker does not discover eradication efforts. As the attacker stays quiet there is limited damage. If the attacker discovers eradication efforts, law enforcement support [21] has to be contacted. The damage will depend on the profile and behavior of the attacker.

2) Possible actions:

In table IV there is a list of possible actions [21][26][22]the CERT could apply. Each action has an impact on the company services and on the attacker. The CERT will have to know at which moment to apply all of these rules depending on stakeholder requirements. For each action, an effort is associated using the table III based on the quantity of information and preparation needed. These actions can be used in an automation decision tree or in an incident response plan[23][24]. Thanks to these actions, the CERT will be able to use all of the analysis he made previously to lead strong response actions while mastering the impact on the company. These decisions have to respect as possible wishes of the stakeholders in III-C1.

The CERT will need to prioritize action, they can use the RICE score model which is a prioritization tool rating these actions according to four criteria (Reach, Impact, Confidence, and Effort). The score is calculated thanks to the following formula

$$SCORE = \frac{Reach * Impact * Confidence}{Effort}$$

An emergency response team can gain three advantages by using a scoring methodology like RICE. It can help individuals make more informed decisions, reduce personal biases in decision-making, and support them in arguing for their priorities before other stakeholders like the executive staff.

Getting a sense of how many stakeholders you anticipate your effort will reach in a specific time frame is the first step in calculating your RICE score.

Reach may refer to a numerical objective, such as how many new satellites, networks, or systems

Score	Description
Low	No preparation needed
Med	Need preparation and investment before attack
High	Need some information about attacker
Very High	Need a lot of information about the attacker, time, and skills

Table III
REFERENCE TABLE FOR THE QUANTITATIVE VALUE OF EFFORT

will be created due to a cyberattack. To reduce subjectivity, a descriptive score is proposed.
3 = Enormous impact-make the attacker out of the network
2 = Medium impact-Limit attacker spreading
1 = moderate impact- break what hacker made
0.5=Low impact-Gather information about hacker

Impact is how much will this feature impact the objective when a customer encounters it. The following reference table can be used.
3 = Stop work from the whole company.
2 = Stop customers.
1 = Stop a department of the company.
0.5 = Latency for some services.

Confidence component aids you to identify the probability your action has an impact on the attacker in the fixed reach time

When determining your confidence score for a given attack, the purpose of your options are:
3 = reach goals whatever attacker actions
2 = reach goals if attacker still has not done an action
1 = reach goals if the attacker does an action

Effort score is calculated thanks to the Effort column in table IV and scores are determined thanks to table III. These scores can be adapted depending on attack conditions. Each Score can be defined as a number (Low=0.5, Med=1, High=2, Very High=3)

To put it another way, if you consider RICE to be a cost-benefit analysis, the other three components are all potential advantages, whereas effort is the only number that represents costs.

In this model, scoring reach is equivalent to quantifying effort. Your score is just an estimation of the total number of resources (product, engineering, etc.) required to accomplish the project in a certain amount of time.

E. After the attack

1) Recovery:

The CERT must prepare a comprehensive recovery plan, ideally before an attack happens. This should focus on resuming normal satellite operations as quickly as possible. There are big challenges in that part because a wrong recovery could lead to a comeback from the attacker using the same flaw or malware he uploaded. For that part, it is crucial to use the report made during the attack to remember all of the actions and revert all of them. The recovery phase should follow the following three-step framework [34] with an Initiation part to identify the conditions of recovery, an Execution part to apply the steps chosen before then a Termination part to evaluate the process(Figure2).
Initiation:

- Validate the security of network-based communications. If deemed to be untrustworthy, the team should incorporate alternative methods to communicate with stakeholders; such as in-person meetings and telephone conversations.
- Understand the adversary's motivation and develop a profile that includes command and control channels, tools, and technical capabilities.
- Identify the impacted resources and earmark the high-value assets for further analysis. This should be followed by identifying necessary infrastructure systems that need to be remediated in addition to the directly affected systems.
- Meet with internal and external stakeholders to discuss the criticality and impact of the attack.
- Determine the last good state of the data based on the time metrics gathered during the investigation.
- Determine the order of restoration based on the prioritization of the high-value assets and system dependencies. Critical satellite functions should be prioritized over unimportant dependencies.

Execution:

- The time of recovery is chosen by the responsible of the network (CERT does not take that responsibility)
- Use previous not compromised backup or a similar one, verify their integrity before any use
- Apply patches on all of the exploits the attacker used to he does not come back. Focus on the

Action	Impact on attacker	Cost for company	Effort
Safe mode	Attacker can't break functionalities main components are not used	Users can't use functionalities and redundant components are used [20]	Med
Manually shut down the communication system with satellite time to take decision	Attacker can't access the ground station	Ground station does not have news from satellite	Low
Other satellites in the constellation do not talk with that satellite	Attacker can't spread to other satellites	Reducing service to users	Med
Disconnect entities in the compromised zone	Attacker can't use these servers or access sensible information	Service can't use this server	High
Lock compromised accounts	Attacker can't use these accounts, has to find new one	User has no access to his account	High
Raise strict rules on Firewall	Reduce the probability of an attacker spreading out of this firewall	Issues with communications if rules are not effective	Med
Change password compromised account	Attacker will have to find the new password but the password change does not make Kerberos tickets invalid	New password has to be sent via a secure way to the employee	High
Kill and remove the malicious programs which may have several uses(access to the server, destroy servers, come back if the attacker kicks out...)	Attacker could not use them	Spend time, using tools in III-C2 may help	Very High
Deployment of an automated intrusion response system (AIRS), for appropriate response options to be automatically selected	Attacker has less time to react as all of the actions, are automatized	Not effective if the hacker uses unexpected behavior	Med
Skipping of deep root cause analysis of a confirmed type incident	attacker has less time to react once discovered	CERT has less information to adapt their response	Low
Immediate data backup on unused media	Attacker can't delete this information	Data is still accessible by users and attacker	Low
Forensic analysis to get information about attacker's actions	CERT has more information to fight him (files used, techniques used, compromised hosts)	Need of time, may be limited by using automation tools like XOVAL framework [19]	Low
Kill components with redundancy	If the attack is detected early attacker is only in one component, the attacker is out.	Sacrifice of one component to do not lose all of them, to do at the end of mission	Very High
Use honey pots	Attacker lose time	Gather information about the attacker	Med
Patch vulnerabilities	Hacker can't use it	May take time and few effectiveness	Very High

Table IV
TABLE OF ACTIONS FOR SPACECRAFT, THEIR IMPACT, COST, AND EFFORT RELATIVE TO TABLE 1

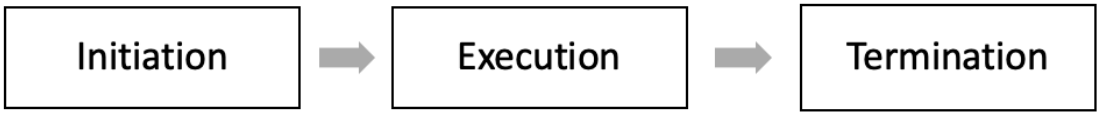

Figure 2. Recovery description

link between the ground station and the satellite.

- Change all of the passwords
- Identify and restore or remove all of the files modified or created by compromised accounts
- Restore the compromised tools thanks to saint repositories
- Each restoration activity should be tracked and recorded.
- Restore resources and functions according to the aforementioned order. Ensure that no system is brought back online before any systems that they are dependent on.
- Implement security controls across all layers looking for indices of compromise.
- Restore the last known good state of data based

on the determined timeline.

- Collaborate with internal stakeholders to confirm that the newly built systems have overcome the original weaknesses and are no longer susceptible to the same vulnerability.

Termination:

- Once the satellite is restored to a known good state, vulnerabilities are remediated and the adversary is out of the system, the CERT can declare the end of the recovery event.

- Discuss the implications of any compromised systems with the relevant stakeholders and plan for an appropriate workaround.

- Work with the business stakeholders and satellite command administrators to enable additional security controls for future missions.

Once the safe mode has been activated, some steps are necessary to recover the satellite. There is no auto-recovery to the attacker does not recover it by himself. To recover the satellite, the following steps are required[20]:
- Configuration of the spacecraft SCV (Satellite Configuration Vector) for nominal operations after completion of failure diagnosis
- In case OBSW (On-Board SoftWare) patches were applied, selection of the OBSW boot image
- Reboot the desired OBC redundancy with the selected OBSW image and load the SCV
- Wait until OBSW has applied SCV and has switched all redundancies to desired settings

2) Reporting and Information Sharing:
Owing to its relatively recent emergence, cybersecurity efforts tend to be isolated actors functioning independently of each other. However, no single organization can have visibility over the entire problem space.
The scale of the cybersecurity challenges facing global institutions further highlights the need, and incentive, for establishing a cohesive ecosystem to address some of the major shared challenges.
Trusted, secure, and scalable cyber information sharing enables enterprises to defend themselves, enhance resilience, and conduct collaborative investigations to detect threat actors. CERTs must establish and follow a security incident reporting process that includes timely notifications to the relevant Cybercrime offices.

However, there are several barriers [25]that need to be addressed for successfully integrating collective efforts. Systemic improvements in cooperation and governance through the engagement of multiple public, private, and civic stakeholders will be crucial in overcoming these barriers. The ability to share the correct and timely insights with the relevant actors in a methodical manner will make it possible to effectively protect assets, intellectual property, and business operations.

Information Sharing and Analysis Centers (ISACs)[8] can serve as an industry resource to collect data about industry-wide incidents, threats, and vulnerabilities. Typically nonprofit, ISACs have the potential to dive deep into available data, communicate critical data far and wide and maintain global situational awareness.

Over time, a repository of incident reports will be developed and can be used to support future system security investment decisions. The effectiveness of such networks will be directly dependent on the number of participants. ISACs create awareness about the frequency, type, and extent of cyber incidents which leads to support for improved preparedness and responsiveness should a cyber attack occur.

3) Evaluation and improvement:

As mentioned in , regular feedback is crucial for building cyber-resilient satellite networks. The increasing volume of stakeholders, in terms of scale, domain, and interest, points toward a constantly changing threat landscape. To generate situational awareness, CERTs must frequently assess what has been and what can be done about malicious activities, especially novel cyber-attacks. The data from the aforementioned repositories should be used as a foundation for making future strategic, operational, and technical decisions. The Team should focus on enhancing proactive as well as preventative security in the organization. In the longer term, successful resolution of vulnerabilities should be followed by initiatives to establish the necessary infrastructure to support deployment into the wider ecosystem.

Evaluation exercises must be conducted after every attack, and include relevant team members across various departments. Brainstorming activities and tabletop exercises should be primarily organized to ensure cross-functional collaboration and diversity of opinion. Through this, the team should answer questions across key areas of potential improvement, and discuss what future steps must be taken. Questions examples can be found in chapter 4

of [13]. While the specific parameters should be decided by the team, some topics and potential questions to ask are:

1. Incident Response Time: This should include the time taken to detect, acknowledge, recover and contain. How can the team optimize its current workflow to improve its efficiency in any way and deliver quicker results? Can the efficiency of existing strategies be improved in any way?

2. Stakeholder Management: There are often multiple stakeholders involved, such as vendors, suppliers, and any other third parties. Were all stakeholders accessible and available when needed? What challenges did the team face when managing stakeholders? Is the existing Service Level Agreement (SLA) meeting the team's requirements?

3. Communication: This should include all internal and external modes of communication. Were any bottlenecks observed in the incident response? What challenges did the team experience with the existing modes of communication during the attack?

4. Technical Capabilities: This should include all technical resources such as tools, software, and equipment being used by the team. Are the existing technology satisfying the team's needs as well as industry standards? Did the attacker use any techniques that are new to the team? How can the existing systems be protected against similar threats in future missions? What changes should be incorporated in the design of future satellites?

While collecting feedback, it is important to minimize subjectivity and focus on actionable steps. This can be implemented through various methods such as feedback forms, online surveys, or as per the team's requirements and capabilities. The use of quantifiable metrics, such as scores or rankings, is highly recommended.

IV. Conclusion

In this paper, many computer science related papers have been adapted to get a space-related framework for space systems. In that framework, a precise set of elements needed, questions to ask, analysis of the attack, and possible response are provided. The goal of all of these elements is to be space-related and help CERT to effectively respond to attacks on space systems.

References

[1] Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability, John Haller

[2] WHAT SKILLS ARE NEEDED WHEN STAFFING YOUR CSIRT?, Carnegie Mellon University

[3] National Incident Management System, FEMA

[4] Defining IncidentManagement Processesfor CSIRTs: A Work in Progress Chris Alberts

[5] A framework for incident response management in the petroleum industry Author links open overlay panel, Martin Gilje Jaatun et al

[6] The Sector CSIRT Framework: Developing Sector-Based Incident Response Capabilities, Justin Novak et al

[7] Defending spacecraft in the cyber domain, Brandon Bailey et al

[8] Space ISAC Releases Statement on SPD-5,space ISAC

[9] The Role of Software in Spacecraft AccidentsNancy G. Leveson

[10] Computer Security Incident Handling Guide, NIST, Paul Cichonski

[11] ESCALATION AND DETERRENCE IN THE SECOND SPACE AGE,Todd Harrison,Zack Cooper

[12] Cybersecurity Protections for Spacecraft: A Threat Based Approach April 29, 2021 Brandon Bailey

[13] Computer Incident Response and Product Security ,Damir Rajnovic

[14] Forensic Analysis of Compromised Systems A. Baláž, R. Hlinka

[15] An Unsupervised Multi-Detector Approach for Identifying Malicious Lateral Movement Atul Bohara, Mohammad A. Noureddine, Ahmed Fawaz, William H. Sanders

[16] D4I - Digital forensics framework for reviewing and investigating cyber attacks Athanasios Dimitriadis a, Nenad Ivezic b, Boonserm Kulvatunyou b, Ioannis Mavridis

[17] Windows forensics analysis SANS Institute https://www.sans.org/security-resources/posters/windows-forensic-analysis/170/download (2019)

[18] Detecting Lateral Movements in Windows Infrastructure M.SORIA-MACHADO, D.ABOLINS, C.BOLDEA,K.SOCHA

[19] Towards machine-assisted formal procedures for the collection of digital evidence Martın Barrere, Gustavo Betarte and Marcelo Rodrıguez

[20] A survey on Fault Detection, Isolation and Revocery (DFIR) Module in Satellite Onboard Software, Fatemeh Salar Kaleji

[21] INCIDENT HANDLING STEP BY STEP COMPUTER SECURITY, THE SANS INSTITUTE

[22] A cybercrime incident architecture with adaptive response policy George Tsakalidis, Kostas Vergidis

[23] Automatic Intelligent Real-time Intrusion Detection System: A Data Mining Model, Oriola Oluwafemi

[24] Automated Intrusion Response Decision Based on the Analytic Hierarchy Process ,Zheng Wu, Debao Xiao

[25] Cyber Information Sharing: Building Collective Security INSIGHT REPORT OCTOBER 2020

[26] Cybercrime Offences: Identification, Classification and Adaptive Response ,George Tsakalidis

[27] Live Response Training Range mit Velociraptor, Severin Marti, Sinthujan Lohanathan

[28] Evaluating Automatically Generated YARA Rules and Enhancing Their Effectiveness,Nitin Naik, Paul Jenkins

[29] Towards machine-assisted formal procedures for the collection of digital evidenceMartın Barr'ere, Gustavo Betarte and Marcelo Rodrıguez

[30] A proposal for automating investigations in live forensics Seokhee Lee, Antonio Savoldi

[31] XIRAF – XML-based indexing and querying for digital forensics W. Alinka, R.A.F. Bhoedjanga

[32] An incident object description exchange format (iodef) extension for structured cybersecurity information, T Takahashi, K Landfield

[33] Security Operations Centers for Information Security Incident Management,Natalia Miloslavskaya

[34] NIST Special Publication 800-184 Guide for Cybersecurity Event Recovery, Michael Bartock, Jeffrey Cichonski