IAC-20,E9,2.D5.4,7,x59767

The Mission as a Tree: A Novel Approach to Identifying Cyber Threats to Satellites

Mr. Sébastien Bonnart, Space Generation Advisory Council (SGAC), France, sgac@sbonnart.fr;
Mr. Aaron Pickard, Space Generation Advisory Council (SGAC), United States, pickardaaron@gmail.com;
Dr. Nebile Pelin Mantı, Space Generation Advisory Council (SGAC), Turkey, npmanti@gmail.com;
Mr. Devanshu Jha, Space Generation Advisory Council (SGAC), India, devanshu.jha7@gmail.com;

The authors present a novel approach to identifying cyber threats to satellite missions. The methodology is innovative in both its applicability across domains of space actors in terms of satellite function and ground station location, and its further generalizability to address other kinds of threats to uncrewed spacecraft.
A threat analysis is conducted, following the four categories defined by the *Open Threat Taxonomy: threat agents, threat targets, threats actions, and threat consequences.* This up-to-date assessment is conducted by cybersecurity and subsystem technical experts, and varies by mission type, geopolitical context, and other factors.
Similar to mind-mapping diagrams, the results of the analysis are visualised in a "tree" (structure) which has 4 main branches. A *threat target*-branch is populated using the result of a detailed functional analysis of the space mission under consideration. A *threat agents*-branch is populated with general cybersecurity concepts that are not specific to space missions. The *threat actions*-branch is populated by inventorying all imaginable actions that could be taken against each item of the *threat target*-branch. Evaluation of the potential impacts of each action may add new items in the *threat consequences*-branch.
The most important contribution from this paper is to provide detailed lists of *threat actions* and *threat consequences* that have been synthesised during this generic threat analysis. These lists draw from recognized cybersecurity frameworks, yet diverge from the usual cybersecurity traits as they specifically focus on actions and consequences that are related to the space environment.
The presented analysis lays ground for enhanced cybersecurity threat and risk evaluations for space missions as it provides a significant number of combinations of *threat agents*, *targets*, *actions*, and *consequences* so that better informed decisions can be taken. Better decisions ultimately lead to augmented security for a critical infrastructure the world has come to rely on.

Introduction

The space and cybersecurity domains are both of a similar age, have similar complexity levels, and require a significant amount of knowledge to contribute to in a technical way. This makes it difficult for outsiders to productively engage with technical conversations in both fields. There is also significant overlap in the disciplines. Space missions, in this age of computer-based command and control, simply cannot avoid cybersecurity threats to their lifecycle. Similarly, space systems represent an important vector for both offensive and defensive cyber operations in the national security domain. Efficient conversations about both of these areas of overlap are complicated by the different vocabularies in the fields. This paper addresses the first area of overlap, cybersecurity threats to space missions, by presenting a novel approach to identifying cybersecurity threats to them. The concept is based around the construction of a taxonomy, to be used first of all as a vocabulary reference.
First, our threat model is introduced by a definition of cyber threat. A literature review presents the current references in studying cybersecurity threats to the space domain. Then, a general approach to deconstructing threats by building a taxonomy is provided. The current state of satellite missions is analyzed to identify general and mission-specific elements of threats. Finally, the paper presents another direct application of the threat taxonomy tree, for the benefit of risk assessments.

I. Nomenclature

A frequent issue in literature relating to cybersecurity and space technologies is that both fields rely on well-developed technical terminology that is unfamiliar to people who do not intimately know the field. The intersection of these fields suffers from this even more intensely. Therefore, the paper shall define its key technical terms. We propose to use the Open Threat Taxonomy definition in order to introduce our threat model.

A **space mission** is the complete architecture required to execute a space mission. This comprehensive understanding of the system includes but is not limited to space and ground segment hardware/software; communications; designers, operations and support personnel; supply chains; and any other mission-specific capability or process.

A **threat** to a space mission is composed of four main elements, also referred to as **components**.

A **threat agent** is the person group or entity performing/triggering the action with intent to cause damage.

A **threat target** is the part of the space mission that is being attacked.

A **threat action** is the operation performed by the agent on the threat target.

A **threat consequence** is a potential negative result of the threat action.

II. Literature Review

The Consultative Committee for Space Data Systems, an organization of national space agencies, published Informational Report CCSDS-350.1-G-2, "Security Threats Against Space Missions", in December 2015[1]. This document provides a high-level overview of threats against space missions. It makes a key distinction between "threat" and "risk" that influenced the development of the paper. A threat, according to CCSDS, requires capability and intent to harm the mission; risk is seen as a function of probability of the threat occurring, and the harm its occurring would cause. This understanding enabled the paper to focus on threat identification and the role that it plays in risk mitigation. CCSDS also uses a four-threat model that corresponds strongly to the one this paper proposes, and influenced its development. Its key terms are "threat source agent", "threat event", "vulnerability", and "mission impact", and it also organizes them in a linear path from the source agent to mission impact. It provides a robust description of threat agents and threat actions to space mission architectures, as well as potential consequences. Figure 4-2 provides a process for assessing threats; the methodology this paper proposes covers aspects of both "Identify Threats to Space Missions" and "Assess Impact of Threats on Scenarios". This document represents the state of the art in thinking about cyber threats to space mission architectures.

The United States Department of Commerce's National Institute of Standards and Technology developed a four-component approach towards risk assessment. Its Information Technology Laboratory's Computer Security Division published this approach in NIST Special Publication 800-30, "Guide for Conducting Risk Assessments", which first appeared in September 2012[2]. It uses the terminology of "threat source", which correlates to "threat actor"; "threat event", which correlates to "threat action"; "vulnerability", correlating to "threat target", and "adverse impact", which relates to this paper's vision of a "threat consequence". This paper has been heavily influenced by Special Publication 800-30, and innovates upon it in two ways. First, it proposes a tree-like organization of threat components, where increased depth indicates a more granular threat. It is thought that this will make the threats' characteristics, and relationships between them, simpler to visualize. Second, it advocates for a threat target, or vulnerability-driven, approach. It is possible that this approach may miss potential threats to the space mission architecture, because unrecognized threats cannot be effectively mitigated. However, this remains a possibility for any cybersecurity risk assessment protocol - if the threat cannot be identified, it cannot be systematically mitigated. By approaching the problem from the starting point of threat targets, it is thought that a more comprehensive set of potential threat actions, and quite confident that a more comprehensive set of threat consequences, can be identified, than would be possible if the assessment began with the threat actors.

MITRE Corporation's Homeland Security Systems Engineering & Defense Institute published a paper entitled "Cyber Threat Modelling: Survey, Assessment, and Representative Framework" in April 2018[3]. While not a space-centric document, it identified the feasibility of a system-centric

modelling approach to defensive cyber operations, and demonstrated the viability of a tree to model threats to a system in such a way that increased depth, distanced from the root or central node, indicated an increased level of granularity. Additionally, it surveys approaches to cyber threat modelling that informed the structure of the model presented in this paper.

The Centre for East-West Cultural and Economic Studies's bulletin *Culture Mandala* published an essay by Jason Fritz entitled "Satellite Hacking: A Guide for the Perplexed" in 2013[4]. It describes cybersecurity threats to satellites, and ways that satellite operators have countered them. This publication provides a very helpful high-level primer on the cybersecurity threats to computing architectures with significant components in space.

III. Methodology

The novel approach proposed by this paper is the use of a tree-like data structure as a model to describe the components of cyber threats to space missions. The actual threat inventory, performed by associating agents, targets, actions and consequences of the taxonomy will be covered in chapter 5.

The root of the structure is the mission itself. It has four child nodes, which are themselves the root of subtree-like structures. The four top-level child nodes are "threat agents", "threat targets", "threat actions", and "threat consequences".

Each subtree-like data structure, or substructure, is itself a multilevel taxonomy. This makes it easier to group elements of the analysis into "buckets" to understand potential threats at different levels of the architecture.

The data structure should be as granular as necessary, and for hardware substructures can reach down to the level of components on printed circuit boards. With each level of depth from the root, the area under consideration becomes more granular. For example, the "threat target" substructure refers to all potential threats to the space mission architecture. It has, in all cases, a child node that refers to the threat target of the integrated space segment. This node, in turn, has child nodes that refer to the threat targets of space segment hardware and space segment software.

The procedure for developing this tree-like substructure is as follows:

- The threat target substructure is constructed first, and is based primarily on a functional analysis of the space mission architecture. This requires interdisciplinary coordination between cybersecurity subject matter experts, systems engineers, responsible engineers for various subsystems, and subject matter experts in the mission's personnel and supply chain.
- The cybersecurity subject matter experts continue to engage with the mission's technical personnel to understand the threats to each potential target, which populate the threat action substructure.
- The cybersecurity subject matter experts continue to engage with the mission's technical personnel to understand the effects of each potential threat action, which populates the threat consequence substructure.
- Business or policy analysts, as appropriate, engage with cybersecurity experts to determine which individuals or institutions might have the means or motive to accomplish any of the identified threat actions. This information populates the threat actor substructure. Standard bodies provide resources that can complement and facilitate this step such as ground station information records.

The taxonomy tree, as a structuring analysis tool, is a visual, structuring resource that helps decompose and compare threat aspects in a way compatible with rational, systematic frameworks[5].

Building these multi-level trees has many advantages such as helping identify new elements from a common parent, and the possibility to work incrementally by adding more levels/details as the analysis develops.

The process of building a specific taxonomy tree allows working very precisely on a threat aspect as it provides scalability thanks to the ability to choose the level in the tree. Additional levels of focus can be achieved by adding an unlimited number of levels but also by the possibility to add sister nodes to the node we are interested in, in order to make its meaning more accurate. This capability makes the taxonomy tree an ideal vocabulary reference when discussing threat aspects.

The taxonomy tree can be related to a decision/event tree as each branch of a tree should be mutually exclusive, and because the aim is to have all branches be collectively exhaustive[5]. However, the different levels do not represent sequentiality but only a different focus on a unique threat component. This is what makes the taxonomy trees radically different from the attack trees[6] which relate the successive steps in an attack sequence.
As a threat classification structure, the taxonomy tree provides an alternative to the cybersecurity MITRE ATT&CK[7] knowledge base. MITRE classifies real-world observed attack *techniques* in a range of predefined categories labeled *tactics*. This classification cannot be directly transposed to the 4 threat components of many threat assessment models such as the one we selected for this paper. Moreover, the taxonomy tree offers more structure, while more easily opening the threat analysis to non-cyber threats. MITRE ATT&CK remains a great resource in order to populate the mission's threat taxonomy, however.

After establishing the full taxonomy tree, threats can be identified by associating agents, targets, actions, and consequences, and then evaluated.

IV. Providing a space mission cybersecurity threat taxonomy

Based on the knowledge of space missions from the authors, and information drawn from recognized cybersecurity publications[4,8,9] a space mission threat taxonomy is proposed : https://framindmap.org/c/maps/869322/public. Elements related to the space aspects of the mission are the most detailed, as they are the focus of this paper. This taxonomy is provided as an example and shall be adapted to every project as described in the previous chapter.

Threat agents branch
The threat agents branch of the proposed taxonomy (Figure 1) was largely inspired by the CCSDS report on security threats against space missions[1]. A specific project would be able to detail several other levels of leaves for better accuracy.

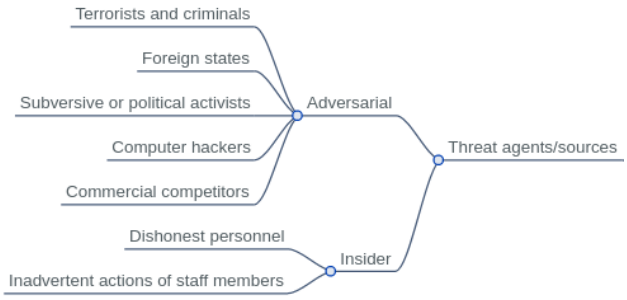

Figure 1: threat agents

Threat targets branch
The threat target branch (Figure 2) has been deliberately kept high level for readability. Like the threat agent branch, it should be expanded when full and precise knowledge of the project is available.
Humans, as users and employees supporting every step and aspect of the project/mission,should not be ignored when populating this branch as they are the entry-point of most relevant cyber attacks[10].

Threat action branch (partial)
The threat action (Figure 3) is the part of the taxonomy that was the most developed, imagining a LEO satellite mission. This paper only includes a small snapshot but the full tree is available at https://framindmap.org/c/maps/869322/public
Once again, a real mission would provide technical data in order to further develop the tree.

Threat consequence branch
The threat consequence branch (Figure 4) has also been populated by imagining all potential effects of each threat action.

Space cybersecurity threat components
Furthermore, additional cybersecurity threat elements may be found by analyzing the new angles that may be opened by the specificities of the space environment and the evolution of its industry.
The development time and lifespan of the mission shall be accounted for when providing for cybersecurity. Because cybersecurity requirements evolve rapidly, the components of the mission that

are not maintainable are future potential cybersecurity threat targets. For instance, any space-side software and firmware that cannot be quickly updated over the air, cybersecurity functions that are hardware provided, and limited security support timespan of any COTS software are all potential future threat targets. Examples of such current situations would be the lack of encryption in communication with the Globalstar constellation or any currently flying satellite that continues to rely onCOTS-provided OpenSSL library v. 1.0.1f/1.0.2-beta1 or earlier, (i.e.,vulnerable to the famous Heartbleed[11] exposure), or a hardware vulnerability potentially affecting some satellites that use the common Xilinx 7-Series FPGA[12].

Long lifespan missions are more sensitive to the evolution of cybersecurity standards and practices, as it is impossible to predict the nature of requirements 10 years from now. It is therefore impossible to guarantee that any system will be sufficiently upgradable to satisfy them. For instance integration of AI in space missions and attacks on AI are currently both blooming cybersecurity fields. Moreover, some instances of agile satellites navigating within close proximity to other satellites represent threats from physical interference but also from a cybersecurity point of view: space awareness (identification of technologies and material), possibility of communication replay, electro-magnetic information gathering[13], or other techniques.

The use in space of any COTS subsystem developed for ground applications is another element to be scrutinized for cybersecurity threat targets and actions. These include third-party supplier level backdoors[14]; increased updatability requirement as exploits are more likely to be publically available; increased attack surface by providing functionalities that are not used, but still enabled even if not documented by the manufacturer. An extreme practical example would be the use of Android hardware for NASA PhoneSats[15], which are unlikely to have the communication bandwidth allowing them to download the hundreds of megabytes required for an OS update. As of 03/02/2020 there were 247 known CVEs of level 10 (e.g., critical severity) affecting various versions of Android[16].

In addition to being analyzed as any other COTS subsystem, Open-source software can be a great cybersecurity asset when maintained. Open-source software is typically secured by the expectation that any exploit discovered will be quickly patched and the update quickly applied to affected instances[17]. However, the risk of adversary code modification during the development or the maintenance phases has to be addressed.

Regarding the assessment of threat consequences, the space environment shall be remembered as very hostile, such that any disturbance in the environmental control of the spacecraft: temperature management, attitude control, orbit control, vacuum, etc. would usually result in failure of the mission with no physical access possible to fix the issue.

The fact that the satellite is orbiting at a long distance has a consequence of allowing communication from a large part of the earth. This should be considered in order to evaluate threat actors, and acknowledged as increasing the likeliness of DDOS attacks, jamming attacks, and decreasing the protections against space awareness and eavesdropping. This should also have an impact on system design as to ensure proper isolation of external communications and internal busses. These are reinforced by the arrival of massive satellite constellations[18] (wider attack surface) but also of their end-user ground terminals that may be coordinated to perform distributed attack such as jamming, brute-forcing, DOS, on any satellite working in the same frequency band event if not part of the constellation.

Finally, the consequence of cost limitation decisions shall be closely monitored from a cybersecurity perspective through the whole project design and execution. The continuous integration infrastructure required in order to fully validate software updates before pushing them represents considerable investment and maintenance. A practical example to evaluate would be the risks associated with the ride-share of the launch with other satellites, which increases the chances of a threat agent to perform an action on a satellite when installing another satellite on the launcher.

This in-depth analysis will result in a very developed taxonomy tree that can be used to characterize any potential threat to the mission, and should be updated periodically in order to take in account the cybersecurity, project, and context evolutions.

V. Practical application for risk assessment

The classical risk assessment frameworks come down to the identification of a probability and a quantitative evaluation of the damage in order to compute the risk as their product. This part proposes a solution to efficiently list and evaluate the risk associated with all possible threats leveraging the taxonomy.

In the model used by this paper, a threat is defined by a combination of the 4 components described in part 1: actor, action, target, consequence). In order to perform a comprehensive threat analysis, all combinations of 4 components of each main branch of the taxonomy should theoretically be listed and evaluated. Assessing each possible threat as per the short taxonomy proposed brings out a magnitude of 10e6 combinations to be analyzed. The solution to keep the analysis manageable is to use the taxonomy for scalability: associating probability and damage evaluation at a higher level nodes of the taxonomy and multi-scaling the analysis where it is high.

In order to allow scalability of the study, the mission's threat model shall define breakdown and aggregation rules for the set of variables used by the model (such as the one proposed by the Guide for Conducting Risk Assessments from NIST[2]).

On the sample model used in this paper (figure 5), one can distinguish two types of variables:

- The "item variables", relative to a threat component in itself: for instance the quantitative evaluation of a threat consequence, which may be inspired from the CVE rating for classical cybersecurity threats
- The "link variables" relative to a threat item association: for instance, representing the likelihood of a designated threat source to perform a designated threat action.

A breakdown operation is the definition of the values of the child nodes based on the knowledge of the parent on the taxonomy tree.

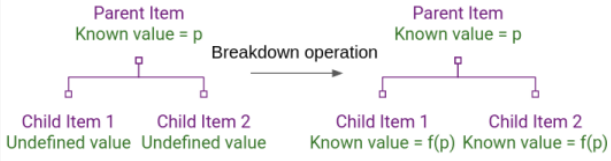

Figure 6: breakdown operation

A basic example of such a rule is f(p)=p.

Similarly, an aggregation operation is the definition of the values of a parent node based on the knowledge of all its child nodes on the taxonomy.

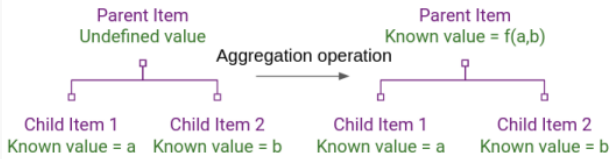

Figure 7: aggregation operation

A basic example of such a rule is f(a,b)=max(a,b).

Scalability operations can be applied to both item variables and link variables, considering the values associated with the link with the parent and to the link with the children. The mission threat model may provide different scalability rules for item and link variables. Moreover, more complex rules for aggregation and breakdown may combine several variables of each node in order to produce scalability.

The final benefit for our proposed taxonomy tree is found when accounting for threat escalation by building an attack tree[19]. The attack tree is a concept very different from the taxonomy presented in this paper as it is a way to describe chronological paths from multi-step attacks. However when building an attack tree, the multi-scalability of the threat definition offered by the threat taxonomy hugely increases the efficiency and accuracy of the attack tree assessment.

This way, all space mission cybersecurity threats can be efficiently identified and evaluated according to the mission's threat model in an accurate, multi-scalable focus by using the taxonomy tree.

Conclusion

We have presented the taxonomy both as a way to better describe threat components, and also as a tool in order to efficiently perform space mission cybersecurity risk assessment. By undertaking a functional decomposition of the mission architecture, and engaging space and cybersecurity experts throughout the process, cybersecurity risks to missions may be assessed. It is hoped that this approach is easier to implement than those

approaches currently in use. Even if it is more difficult, due to the need for coordination between subject matter experts in different fields, or for other reasons, it is the belief of the authors that the interdisciplinary approach proposed serves as an effective validation of other threat identification practices because of its dissimilar methodology.

A future work to be performed in the direct continuity of this paper would be to implement the taxonomy tree and perform a threat assessment on an existing or imaginary space mission.

Further theoretical research in approaches to defensive cybersecurity operations in the space domain should consider a modification of the data structure proposed here. In particular, the authors would consider how modifying the directed root tree they present into a more generic directed graph would affect the functional analysis, and the high level understanding of the satellite as a system with cybersecurity vulnerabilities. This interest is driven by the potential for a component to fulfill different functions in different spacecraft subsystems, which is an improvement opportunity for this model.

Practical research rooted in space cybersecurity might focus on developing countermeasures, policies, and best practices to counter threats identified through this approach. Furthermore, the authors wonder whether graph-based approaches to threat assessment affect how wargames are used in understanding threats to complex architectures, and whether the use of these taxonomies would affect resource allocation in addressing identified vulnerabilities.

References

1. "Security Threats against Space Missions." 2 Dec. 2015, CCSDS. *CCSDS 350.1-G-2*
2. "Guide for ConductingRisk Assessments." Sep. 2012, NIST, *Special Publication 800-30 Revision 1*
3. "Cyber Threat Modeling - The MITRE Corporation." 7 Apr. 2018, https://www.mitre.org/sites/default/files/publications/pr_18-1174-ngci-cyber-threat-modeling.pdf. Accessed 30 Sep. 2020.
4. “Satellite Hacking: A Guide for the Perplexed” 2013, Fritz J. et al. *Culture Mandala: Bulletin of the Centre for East-West Cultural and Economic Studies*
5. “The Thinker's Toolkit: fourteen powerful techniques for problem solving.” 1995, Jones D. M. *New York : Times Business*
6. "Mission-Centric Cyber Security Assessment of Critical Systems." 12 Sep. 2016, Pecharich J. et al. https://trs.jpl.nasa.gov/bitstream/handle/2014/47027/CL%2316-4097.pdf. Accessed 30 Sep. 2020.
7. "MITRE ATT&CK®”, The MITRE Corporation. https://attack.mitre.org/. Accessed 30 Sep. 2020.
8. “Cybersecurity for Space: Protecting the Final Frontier” 2020, Oakley J. G. *Apress*
9. “Challenges to Security in Space” 18 Mar. 2019, US Defense Intelligence Agency
10. "The Human Factor 2019 Report“ 2019, Proofpoint. https://www.proofpoint.com/us/resources/threat-reports/human-factor. Accessed 30 Sep. 2020
11. "Heartbleed Bug." 2014, https://heartbleed.com/. Accessed 30 Sep. 2020.
12. “The Unpatchable Silicon: A Full Break of the Bitstream Encryption of Xilinx 7-Series FPGAs”, Maik Ender et al. https://www.usenix.org/system/files/sec20fall_ender_prepub.pdf. Accessed 30 Sep. 2020
13. "How the NSA Monitors Target Computers with Radar Wave Devices." 10 Jan. 2014, Pierluigi Paganini. https://resources.infosecinstitute.com/nsa-monitors-target-computers-radar-wave-devices/. Accessed 30 Sep. 2020.
14. “Managing Cyber Risks In Global Supply Chains: Part II” 22 Sep 2020, Pellathy D. et al. Supply Chain Management Review
15. “NASA's Latest Space Technology Small Satellite Phones Home” 4 Dec. 2013, Hoover R et al, *NASA Ames news release AR13-83*
16. "Google Android : List of security vulnerabilities - CVE Details." The MITRE Corporation. https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html. Accessed 30 Sep. 2020.

17. “Cybersecurity Principles for Space Systems” 11 Dec. 2018, Falco G. *Journal of aerospace information systems*
18. “What space missions can learn from cyber-security breaches and counter-measures in the telecommunications industry” 25 Oct. 2019, Millwood S. *IAC*
19. “Attack Trees” Dec. 1999, Schneier B. *Dr. Dobb's Journal*

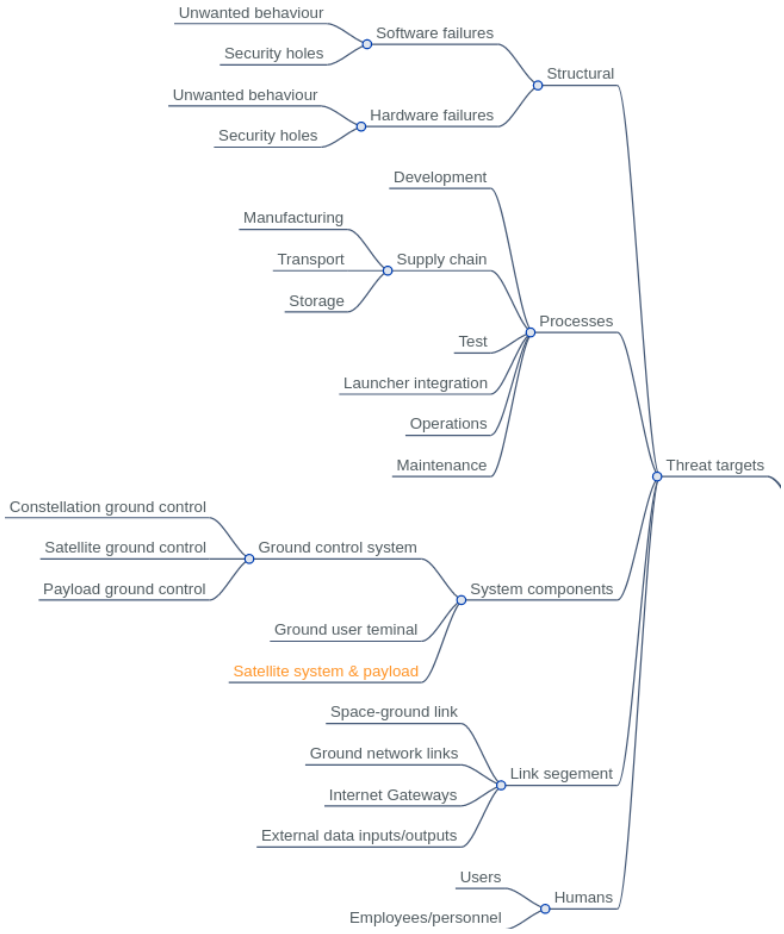

Figure 2: threat targets

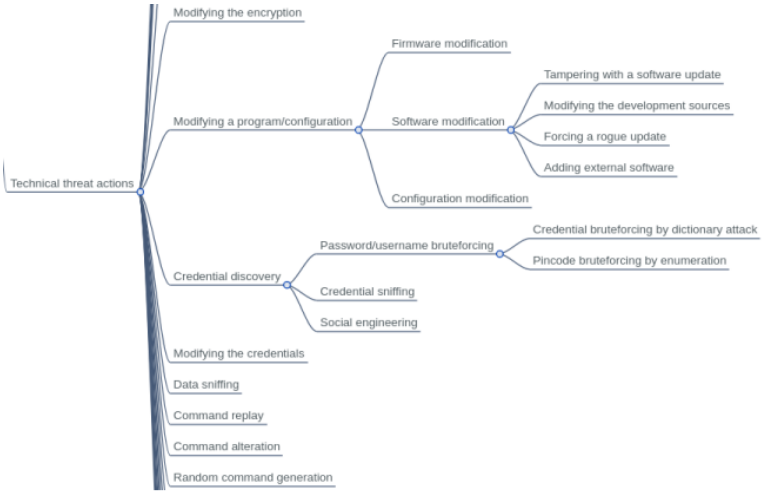

Figure 3: threat actions (partial)

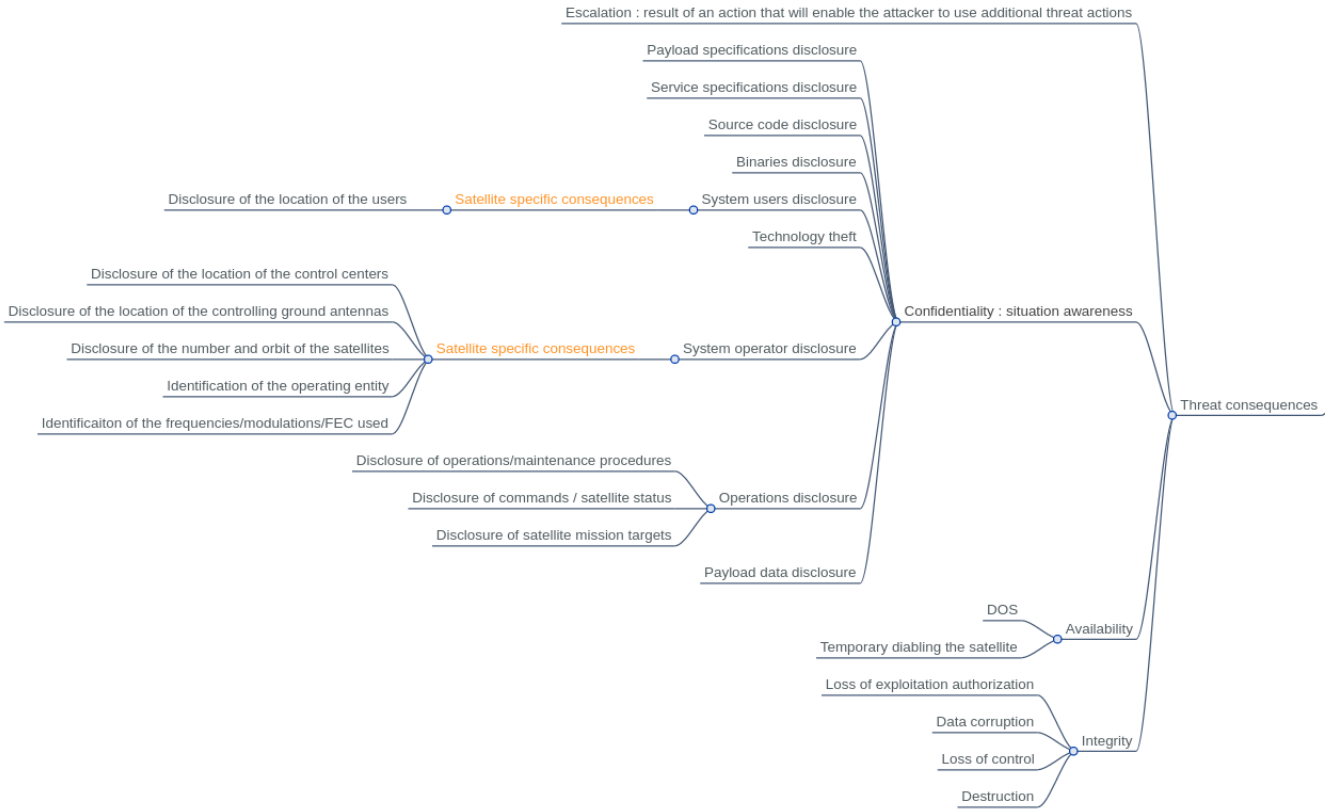

Figure 4: threat consequences

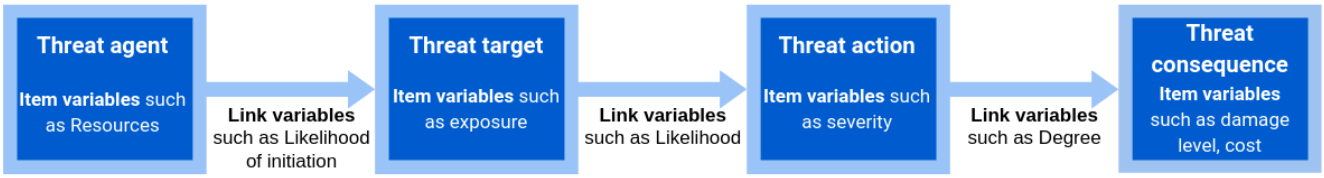

Figure 5: threat model variables