The Treks Companion

A Guidebook to the TREKS Cybersecurity Framework

Dr. Jacob Oakley

PREAMBLE

As an offensive security professional with seventeen years of experience who has spent the past five years intimately involved in the space industry, I thought it would be helpful to both communities to capture the perspective of how an adversarial hacker might decompose space system compromise campaigns and taxonomize that into a framework others could utilize. Hopefully, there is some benefit to putting out there how a hacker looks at a space system from a targeting, reconnaissance, and exploitation standpoint.

CONTENTS

ACKNOWLEDGMENTS

I would like to thank Dr. Gregory Falco and Dr. Andy Aldrin for being proponents and champions of cybersecurity for space. I look forward to adding more names to this page as this effort, framework, and guidebook evolve!

1 An Introduction to TREKS

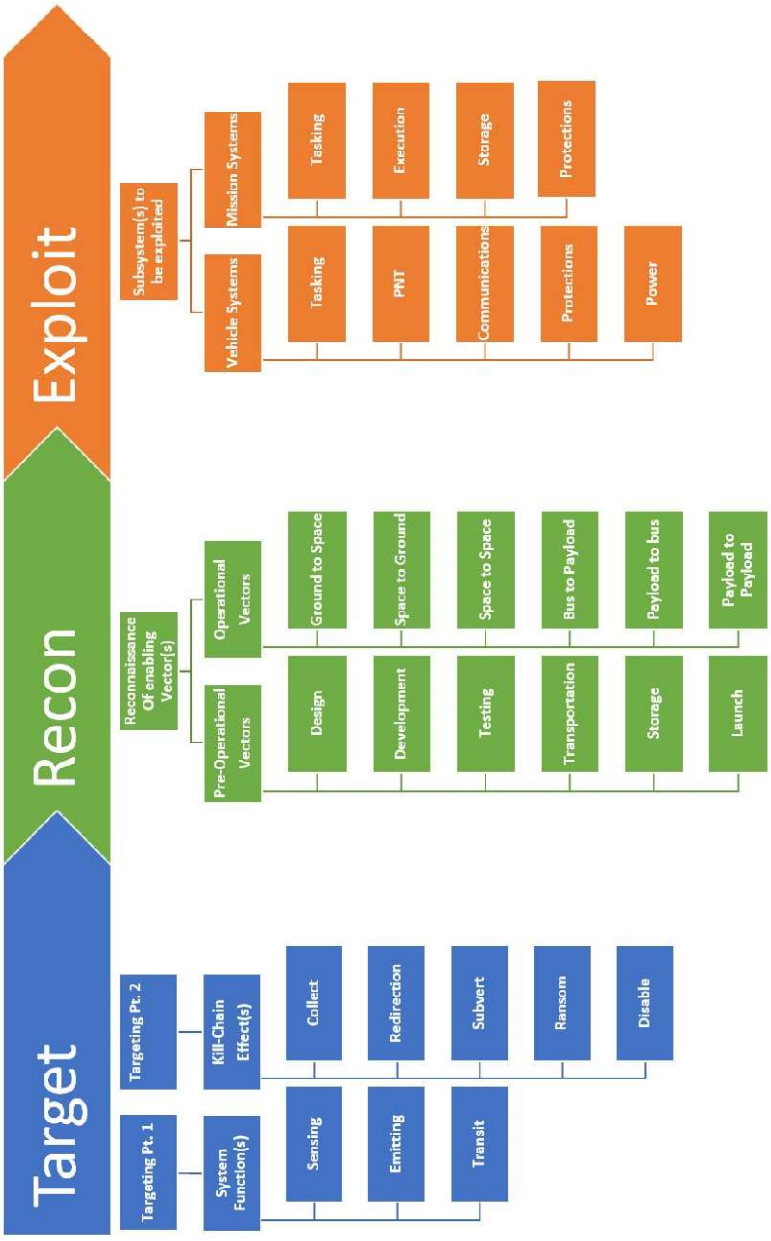
The Targeting, Reconnaissance, & Exploitation Kill-Chain for Space Vehicles (TREKS) Cybersecurity framework was developed to provide a taxonomy for understanding, protecting against, and decomposing cybersecurity compromises of space-resident systems, otherwise known as space vehicles (SVs).

Purpose

The purpose of this guidebook is to act as a reference to the included TREKS cybersecurity framework and aid in its use by the offensive and defensive cybersecurity communities as well as space system owners and operators. This guidebook will continue to be a living document that will be edited and updated based on feedback from both the space and cyber communities, with new versions released as appropriate.

TREKS is intended to provide a bridge between the existing frameworks available to address, categorize, taxonomize, and analyze cybersecurity compromises of traditional terrestrial-based network architectures and the future of cybersecurity for space where those frameworks become more applicable as compromises become more frequent, prolific, and acknowledged. This framework can provide a taxonomy that can be used to characterize foundational aspects of cyber threats to SVs in a way that allows for the identification of trends and enables analysis of this niche target set at the intersection of the space and cyber domains.

Figure 1: The TREKS Cybersecurity Framework



Utilizing the Framework

This framework should be utilized to typify an SV as a target, based on the type of that space vehicle and the actor's motivation, and to understand what vectors could be leveraged to execute effects that satisfy said motivation. The initial version of this framework could be seen as satellite centric, but the intent is to continuously build out the understandings surrounding this taxonomy to best incorporate all manner of SVs, from satellites to weapons to crewed vessels and labs and beyond.

Left to Right

As the owner of a space system or a professional tasked with assessing or protecting it from a cybersecurity perspective, the framework can be used in a traditional left-to-right method. By doing so, one can typify the SV as a potential target based on the task(s) it performs. This helps identify the attack vectors likely to enable activity that satisfies an actor's motivation for targeting the system. It then ties what SV subsystems could be exploited to achieve the enemy's desired, or system owner's most feared, kill-chain closing cyber effects.

Right to Left

Conversely, the framework could be followed right-to-left in a post-compromise scenario. Via this method, one could link the functionality of malware and exploits used in a compromise, or the damage assessment associated with them, and walk backward to identify which vectors the actor likely performed reconnaissance on to enable exploitation, as well as tie those aspects of the compromise to the target typification based on SV functionality and possible actor motivations.

Assumptions

When considering this framework for use in categorizing and associating potential and past compromise attributes for space vehicles, it is essential to understand the assumptions made when it was developed. TREKS focuses on the potential or existence of code execution on the

space vehicle itself, which requires the equivalent of insider access or a sufficiently sophisticated malicious actor capable of compromising a like context and privilege on the system. Also, this framework does not cover what would be considered electronic warfare threats, such as jamming or the ability to compromise encrypted communications to the SV.

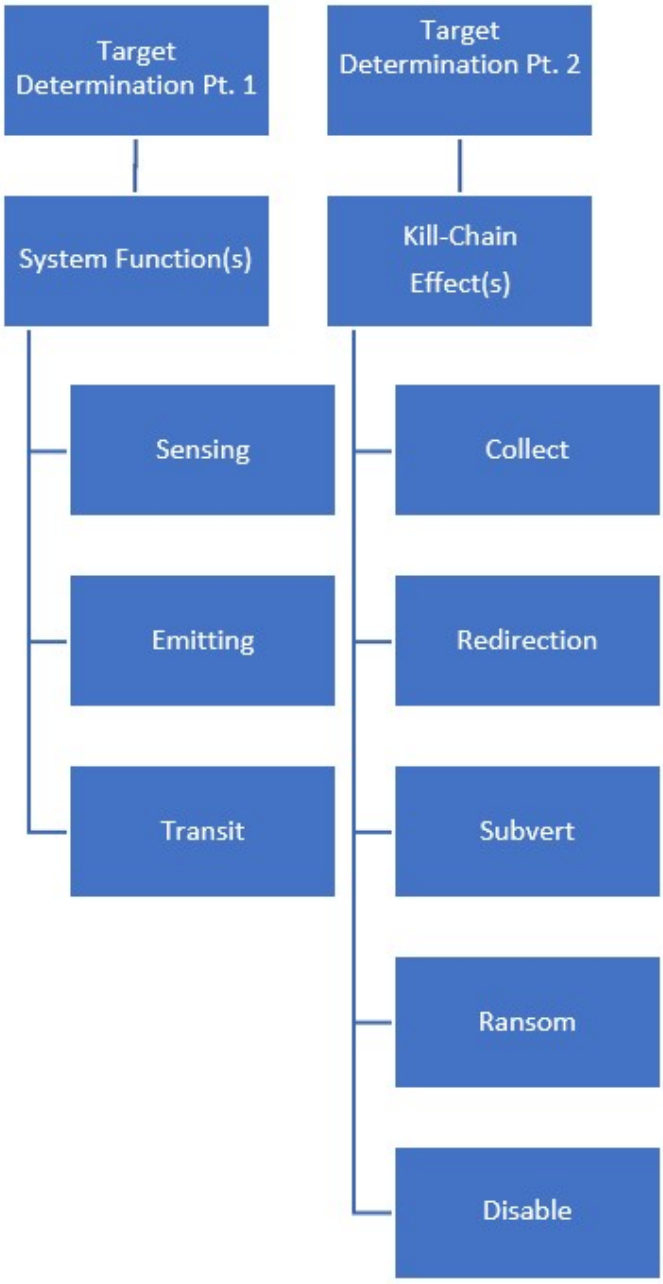
This is not to say those are not prolific threats to space systems. However, blurring the lines between electronic and cyber attack actions an SV may face is not necessarily a helpful thought experiment. Additionally, an attacker of adequate sophistication to break through the protection of encrypted communications to the satellite will then be capable of acting as a privileged insider when performing the execution of malicious code or otherwise altering SV device configurations.

It is also essential to understand that most SVs have components dedicated to the flight and operation of that system and others related to the mission or function it performs. For satellite SVs specifically, this refers to the satellite bus which hosts power generation, storage, navigation propulsion, etc. In contrast, satellite payload refers to the subsystems performing that SV function, such as taking images of the earth. The TREKS framework is heavily based on knowledge about satellite SVs as they are the quickest-growing space-resident attack surface. However, it is relevant to any SV, weapon, human flown, or otherwise.

2 Targeting

Targeting is a two-part phase that involves typifying the space system and marrying it to a malicious actor's motivation(s) intending to compromise it. The target type is based on the function(s) of the SV. The reason for the attack is framed as potential and likely intended cyber-enabled kill-chain effects that conclude a given campaign. From a defensive and system owner perspective, it is crucial to conceptualize that system as if it were being targeted for compromise. The adversarial stance informs follow-on phases of the TREKS cybersecurity framework and is invaluable in deciding where to focus security posture and resources within any organization or system.

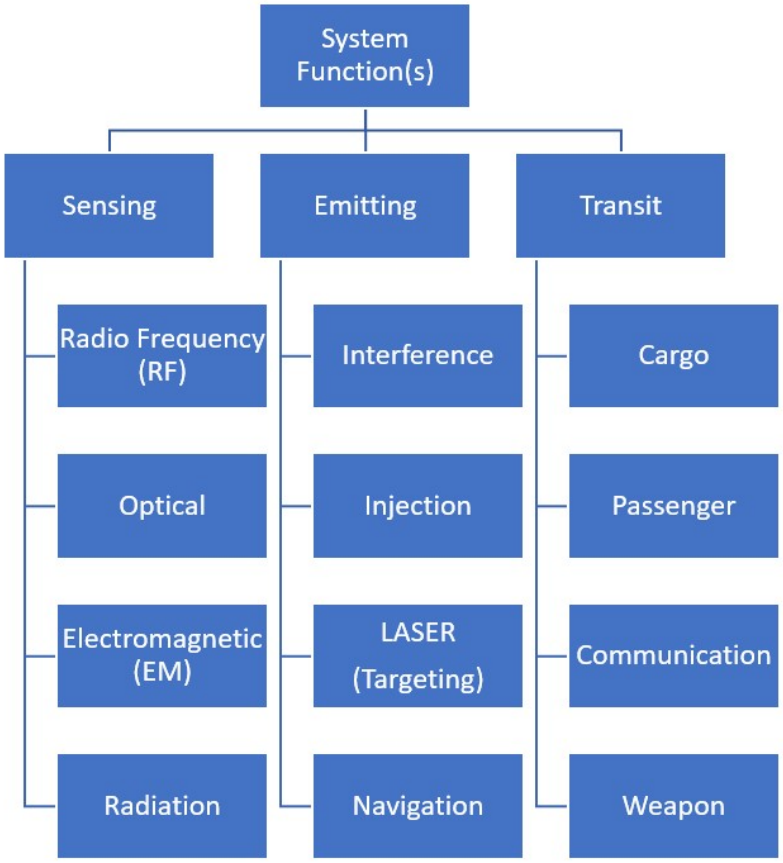
Figure 2: Target Determination Phase



System Functions

SV functions are broken into three unique, high-level types under which all sub-types and specific SVs fall. This is not to say a given SV cannot have more than one of these functions or subcategories within it, nor are the named sub-types exhaustive. The importance of these types lies in mapping compromises and planning to them so that as cybersecurity in space grows, it becomes easier to identify trends of those compromises based on system function types such that they may be more effectively mitigated.

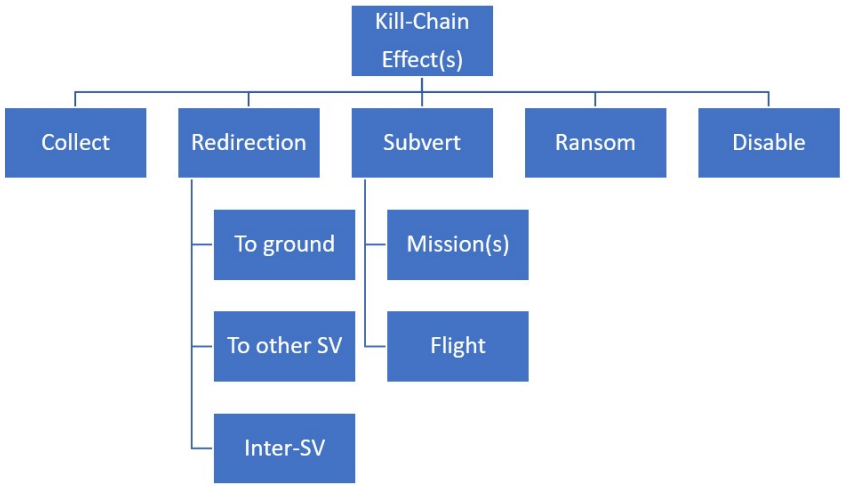
Figure 3: A Decomposition of System Functions



Kill-Chain Effects

The second part of phase one is where likely or realized kill-chain effects an SV could face are identified, further characterizing trends and approaches to cybersecurity and operations.

Figure 4: A Decomposition of Kill-Chain Effects



Collect

The effect of collection is that of intelligence gathering, intended to remain covert in nature and not otherwise affect the SV or system.

Redirection

This effect refers to an SV being compromised to enable access to a different portion of the compromised SV(bus to payload, payload to payload, payload to bus), another SV, or a ground segment system and would stay covert.

Subvert

Subversion of flight systems or SV mission-type functionalities could happen as either a covert or overt action depending on the motivation of the malicious actor.

Ransom & Disable

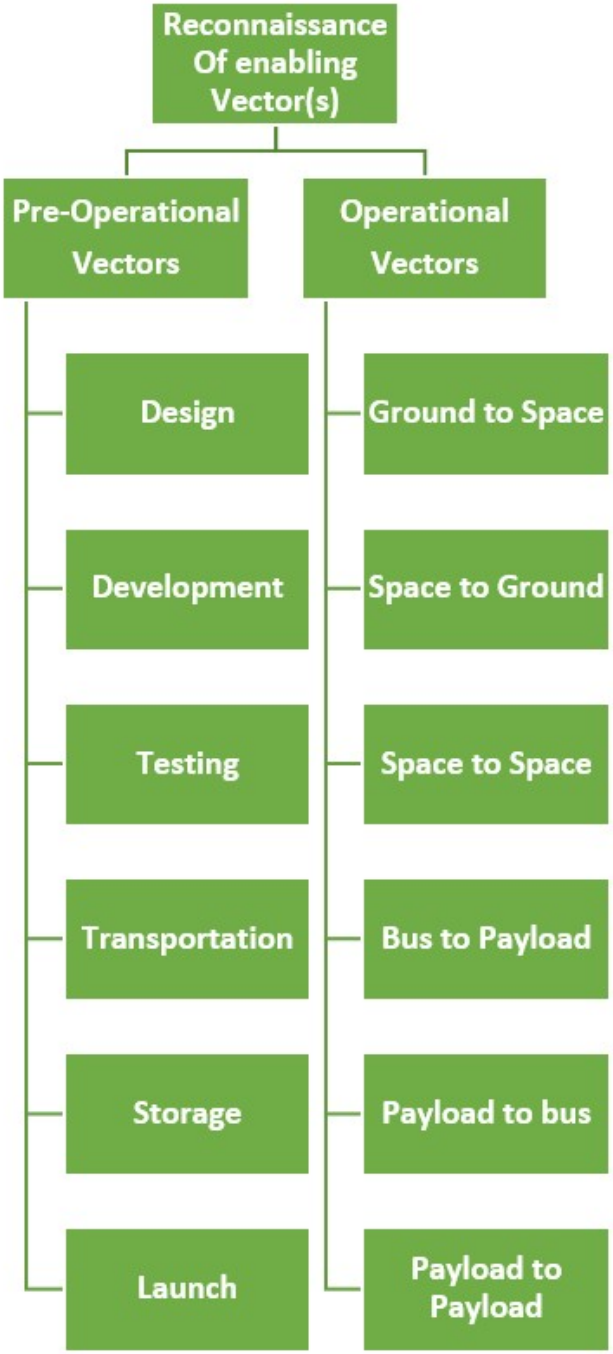
Ransoming or disabling a space system are two overt kill-chain effects. Thinking about disabling or ransoming space assets through cyber domain actions is interesting. For instance, if an SV was taken over and it had propulsion, which was then used to crash into another unrelated SV that could not move out of the way, it would be difficult to determine who would be at fault.

3 Reconnaissance

In this phase, pre-operational and operational vectors are identified that would enable or do enable access to exploitable sub-systems that facilitate kill-chain effects being executed. Vectors can either represent how malicious code could be introduced to the SV or how malicious code could otherwise impact the SV. As an example, consider transportation and storage. Some vectors are present in both pre-operational vectors and are still viable for exploitation even after the SV has been launched into orbit and begun carrying out its function(s).

Traditionally these are times in an SV's pre-operational lifecycle when interdiction is a risk. For example, someone could physically interact with SV components to introduce malicious code directly onto them to later deliver a kill-chain effect. However, malicious code could also alter environmental controls at a storage facility or crash the autonomous vehicle transporting it. Suppose the desired kill-chain effect was to disable the space vehicle. In that case, these are all viable vectors that would be subject to the reconnaissance of a malicious actor looking to achieve that goal. It is important to note that threat vectors that can lead to exploitation and effects that impact the SV don't necessarily need to be a part of the space system.

Figure 5: The Reconnaissance Phase



Pre-Operational Vectors

Important to note that many pre-operational vectors can also be present once operations begin, as things like new updates and software might be exposed to design, development, or cyber testing vectors before being introduced to the space vehicle.

Design

This pre-operational vector is where aspects of the SV are being decided and designed.

Development

This pre-operational vector is where aspects of the SV are created, implemented, and integrated.

Testing

This vector includes all testing that an SV and its components undergo, from validation of code and software to exercising environmental threats such as temperature and radiation.

Transportation

The pre-operational vector of transportation covers any point where components or the SV itself are in transit, whether from the factory to and from testing or on the way to the launch facility.

Storage

Like transportation, this vector covers any point where components, including hardware and software, are at rest post-design and through operations.

Launch

This vector covers any facilitation of compromise that could happen during the launch process, from ignition to deployment and stabilization of the SV before it begins executing its function(s).

Figure 6: Pre-Operational Vectors

Operational Vectors

Once the SV is in space and performing the tasks it was designed and intended to do, operational vectors are those ways that are still capable of enabling the exploitation of sub-systems and delivery of kill-chain effects.

Ground to Space

This describes the traditionally understood vector where compromise of terrestrial attack surface leads to an ability to maliciously task or exploit the SV.

Space to Ground

This operational vector is present in any space system where multiple ground stations talk to the SV or any other exploitation of a ground-based system from space.

Space to Space

When an SV is used to enable the exploitation of another SV, whether within a connected mesh constellation or an unrelated SV.

Bus to Payload

When bus and flight-related components of an SV are leveraged to enable and pivot to the hosted payload(s).

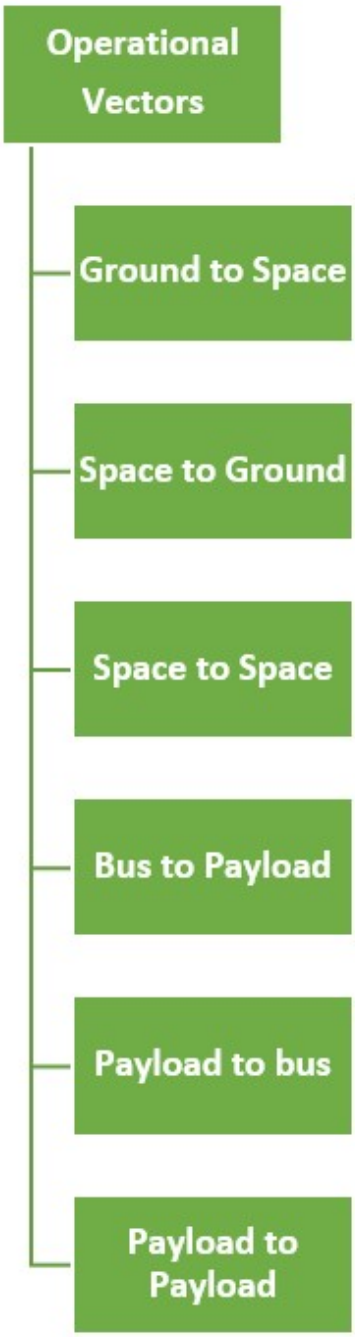
Payload to Bus

When a payload is compromised and leveraged to pivot to flight and bus-related components.

Payload to Payload

In a hosted payload system, this vector describes utilizing access to one payload to pivot to or compromise another on the same SV.

Figure 7: Operational Vectors

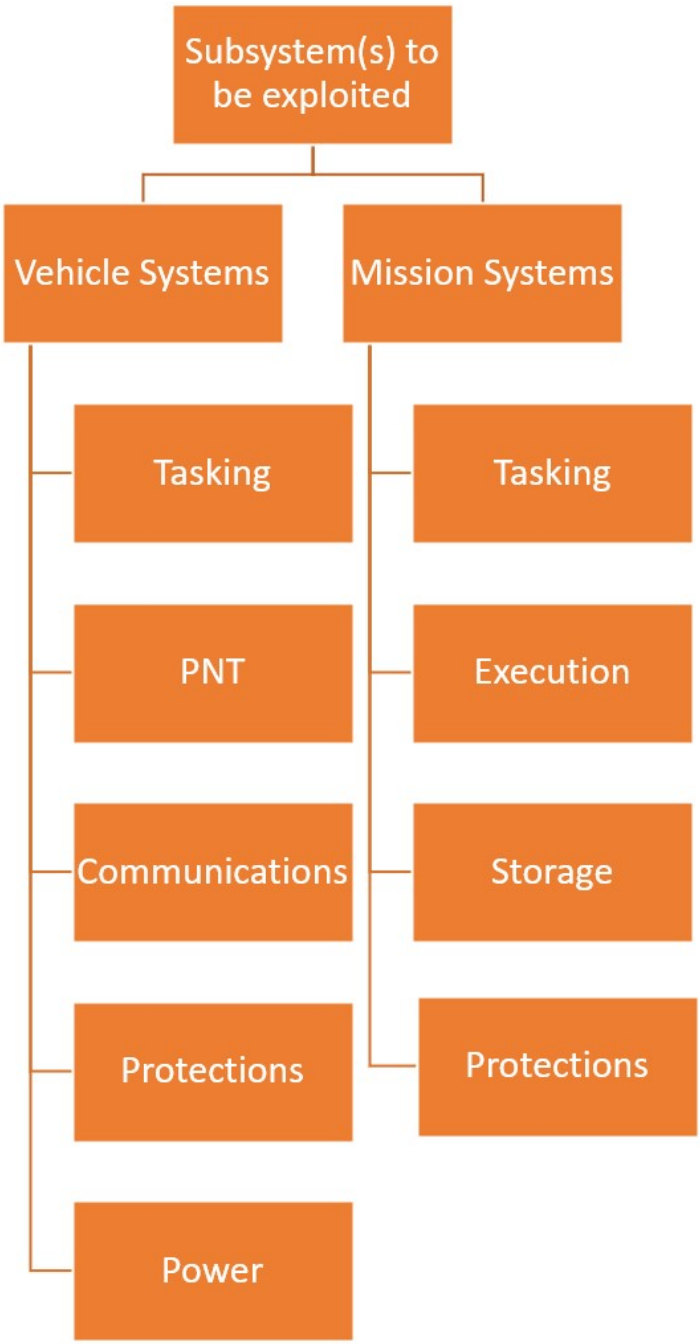


4 Exploitation

In this final phase of the TREKS cybersecurity framework, we look at the vector-enabled exploitation of SV subsystems to preposition and/or execute the desired chill-chain effect(s). From the defensive perspective, this means using an adversarial mindset to determine which SV-specific or mission-related subsystem(s) will likely be leveraged via probable vectors to deliver high-risk effects to the SV.

In a post-compromise scenario, this phase is the first step in walking backward from the discovered compromise to understand how and potentially why cyber effects were executed on an SV. When used as a forensic framework, this allows a kill-chain result to be linked to likely delivery mechanisms and, when combined with known information about the SV, such as its function(s), gives a full picture of the compromise and categorize aspects of it to be compared and leveraged as space resident cyber attack surface grows and is attacked.

Figure 8: Exploitation Phase



Vehicle Systems

SV systems are those related to the flight and operation of the SV but not directly tied to the function(s) being carried out.

Tasking

This refers to any sub-system or component tasking other parts of the SV.

PNT

PNT covers any portion of the SV responsible for position, navigation, time, and attitude, including knowledge of those details and an ability to correct them, such as through propulsion.

Communications

Communication refers to the mechanisms necessary to establish a link to the ground or other SVs, including encryption, software-defined radios (SDRs) tuning, and underlying communications protocols.

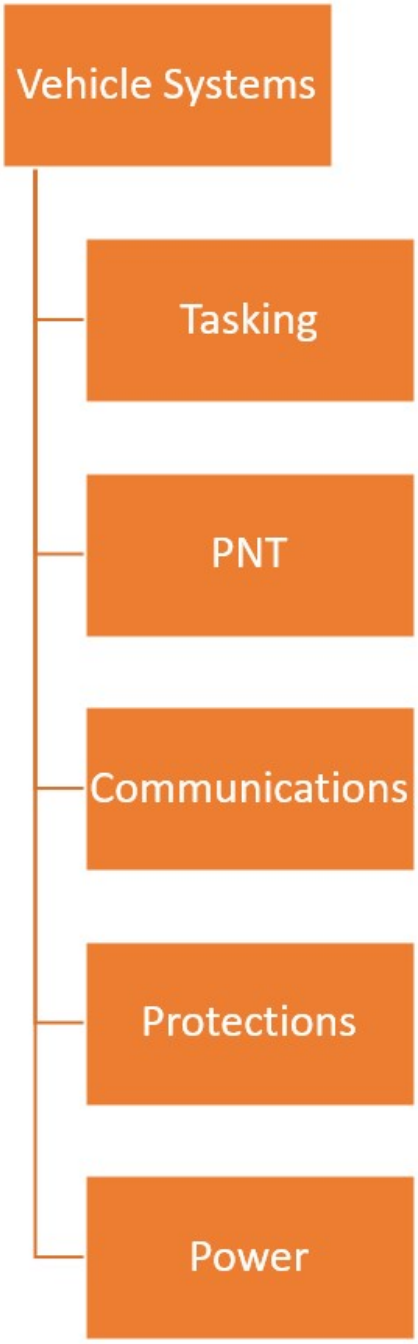
Protections

This refers to any SV resident mechanism responsible for protecting the SV, such as resource limiters that prevent abusive power utilization or processing, etc., as well as watchdogs that trigger protective measures based on any number of monitored SV characteristics.

Power

This covers any subsystem related to the SV's generation, distribution, storage, and power utilization.

Figure 9: Vehicle Systems



Mission Systems

These are the systems responsible for operating the function(s) of the SV, often referred to as the payload on a satellite.

Tasking

Any mechanism involved in tasking the function of an SV or getting data about or generated by that tasking to where it needs to go.

PNT

PNT here covers any portion of the SV mission function that utilizes and determines PNT data, such as tagging a photo taken by a satellite payload with where the satellite was and when the photo was taken.

Storage

This covers any mechanism related to storing mission function-related information.

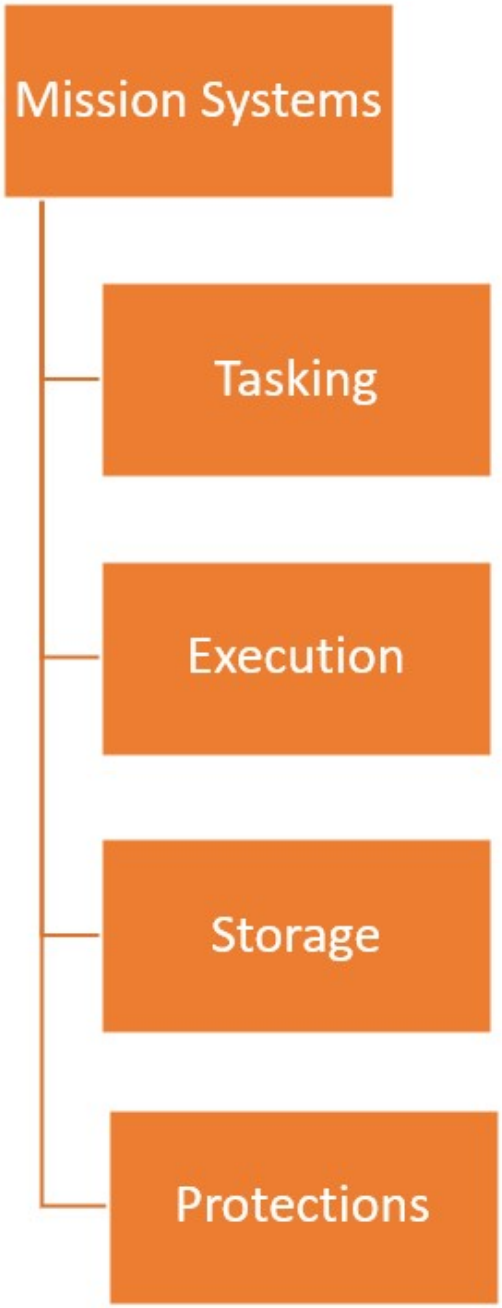
Protections

This refers to any SV resident mechanism responsible for protecting the payload, such as resource limiters that prevent abusive power utilization or processing, etc., as well as watchdogs that trigger protective measures based on any number of monitored SV characteristics.

Power

This covers any subsystem related to the generation, distribution, storage, and utilization of power within the mission function or payload, if such capabilities exist independent of the bus, for instance.

Figure 10: Mission Systems



5 Future Work

As was stated at the beginning of this guidebook, this is intended to be a continuously updated living document to make it easier to leverage and utilize the TREKS cybersecurity framework and act as a mechanism to keep the framework itself up to date.

ABOUT THE AUTHOR

Dr. Jacob Oakley is a cybersecurity professional and author with over 17 years of experience. A foremost expert on offensive cybersecurity, cyber warfare, and space system cybersecurity, he has advised Department of Defense (DoD) and Fortune 500 executives on strategically mitigating risks and threats to globally distributed, multi-domain network architectures.