Space & Cyber Brief Series

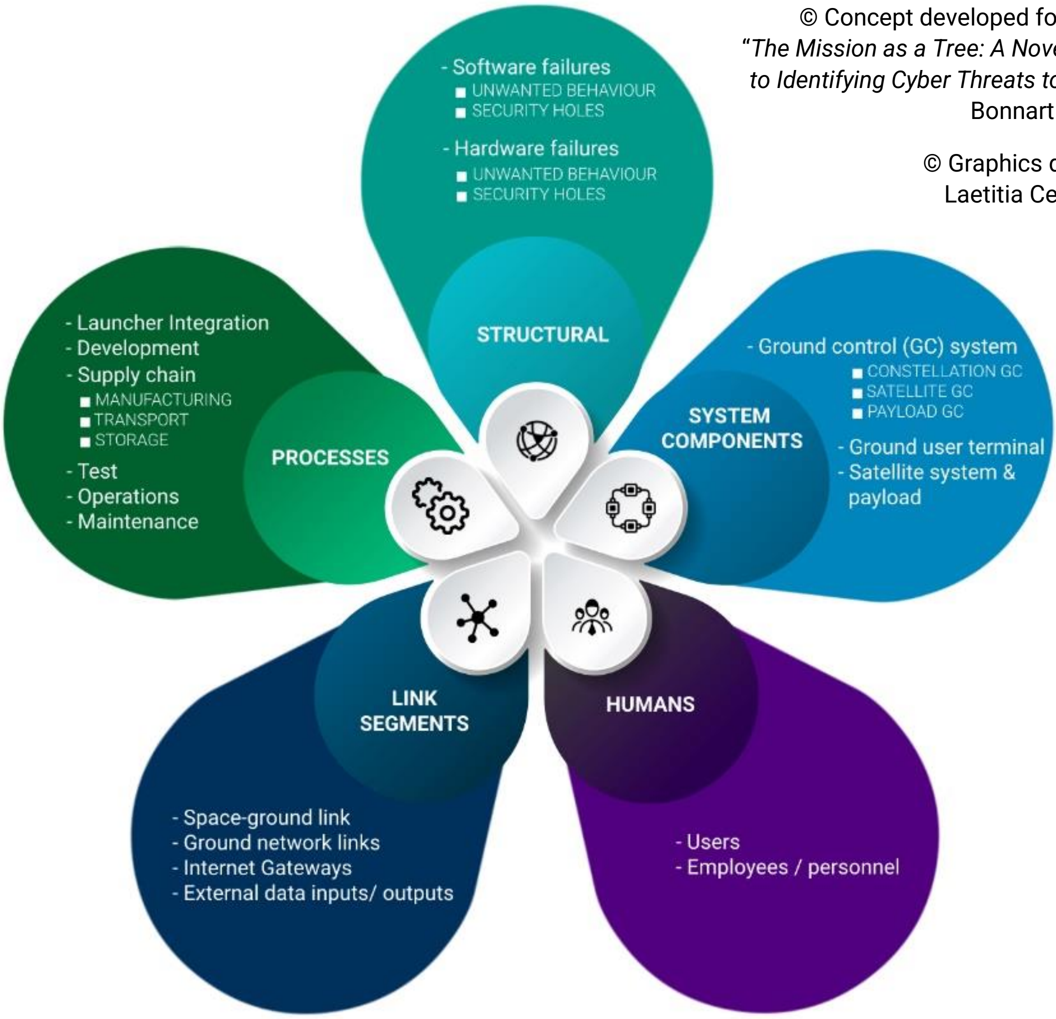
The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #1

Author: Laetitia Cesari Zarkan | Reviewed by Antonio Carlo, Paola Breda, Antonia Russo

INTRODUCTION

Along with the development of the internet, cyber security flaws and risks multiply as computers information, communications, and technology systems opened up to the world.
In the cyberspace there is no "zero risk". Despite the tests, robust procedures and the adoption of preventive measures, it is impossible to guarantee a 100% level of safety and security for software, hardware or applications.
Cyber security flaws are deep rooted issues, which is both good news and bad news. Good news, because it allows for more creativity in building better systems, more flexibility, and better capacity to face threats, and more efficiency in adapting a protective measures against a hostile environment. In the cyberspace, overcoming adversity makes us stronger, more alert, and resilient. Bad news, because these flaws are exploited to bypass the online protection barriers of individuals, companies, state entities or organizations, which may have a disastrous outcome.



© Concept developed for the article *"The Mission as a Tree: A Novel Approach to Identifying Cyber Threats to Satellites"*, Bonnart et al., 2020

© Graphics designed by Laetitia Cesari Zarkan

Space & Cyber Brief Series

The SGAC Space and Cyber Security Project Group provides an international forum, where members can share their thoughts, views and opinion on international space and cyber policy issues to raise awareness among the next generation of space professionals about the global scale of space activities.

2022 - #1

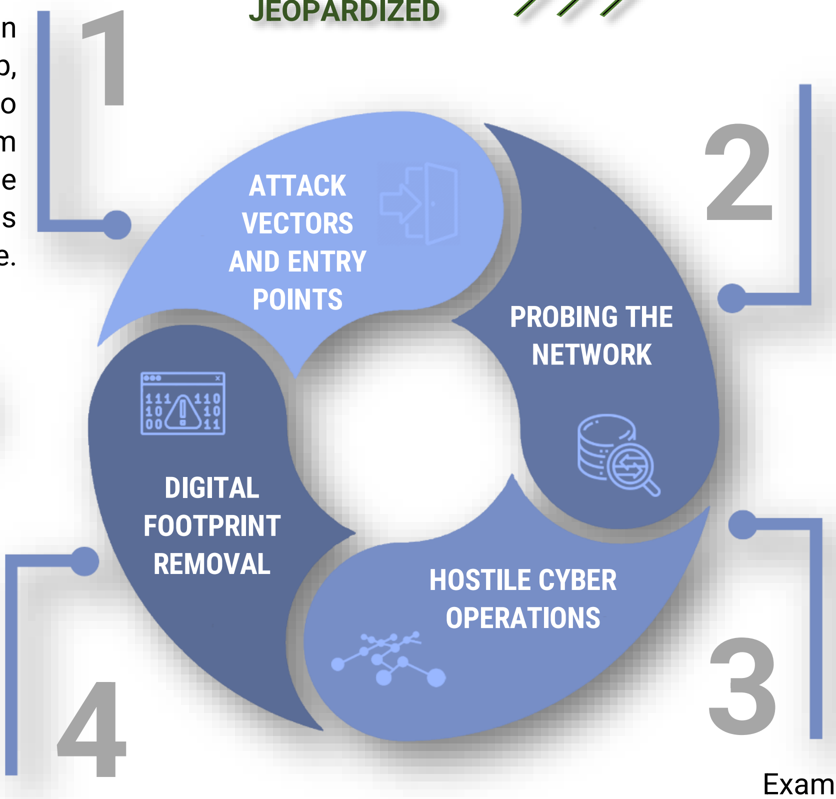
Author: Laetitia Cesari Zarkan | Reviewed by Antonio Carlo, Paola Breda, Antonia Russo

ANATOMY OF A CYBER ATTACK AGAINST A SPACE SYSTEM

The space infrastructure is spread and complex, with a ground and a space segment and bridged by communication links. Such an infrastructure offers a vast surface area of attack for hostile cyber operations.

THE SYSTEM IS JEOPARDIZED

The hostile actor uses a breach vulnerability in an app or in the network setup, a flaw, an email or a file to infiltrate the system architecture and gives the order to install a malicious software.



The malware will look for other potential flaws or vulnerable access points or communicate with command and control websites to receive further instructions and/or malicious codes.

THE MALICIOUS CODE "OPENS THE BACK DOOR" AND/OR WAITS FOR ORDERS

Examples:

- Creating new entry points
- Modifying data or giving orders to the space system
- Blocking systems or data
- Deleting data
- Collecting data that will be stored on a relay server before transfer

Thereafter, the hostile actor can delete the trail of clues to prevent investigators from connecting the dots and identifying the source of the hostile cyber operation.

WHEN SPREAD INSIDE THE SYSTEM ARCHITECTURE