Policy Perspectives
Vol. 12/3, September 2024

CSS
ETH Zürich

Cyber Defense in Space: Quo Vadis?

Over the past decade, space and cyber commands have been established within armed forces. This analysis compares how France, Germany, the UK, and the US protect space infrastructure from cyberattacks.

By Clémence Poirier and Sarah Wiedemar

The global cyber threat landscape is expanding due to rising hacktivist activity, cybercriminal campaigns, and offensive state actors. All of these cyber threats have the potential to impact space systems throughout their entire lifecycles and across the user, ground, space, and control segment. In February 2022, Russia targeted ViaSat's KA-SAT network to cut off Ukraine's military communications, disabling around 40,000 modems. In 2023, Russian cybercriminal group LockBit targeted Boeing and SpaceX with ransomware.

In this context, militaries worldwide have increasingly recognized space and cyberspace as operational domains. Many have thus established cyber and space commands, often as new branches within their armed forces. These commands aim to develop new defensive and offensive capabilities to prepare for potential conflicts in space or cyberspace. Given the links between the cyber and space domains, determining responsibility for cyber defense in space is complex. In brief, while the US Space Force handles the cyber defense of space systems, cyber commands in France, Germany, and the UK have this mandate.

This Policy Perspective uses four case studies – France, Germany, the UK, the US – to explore space cyber defense governance and its potential shortcomings, including organizational structures, resourcing issues, and relationships with industry. Through desk research and interviews with relevant stakeholders, a clearer picture of size, capacity, and task distribution emerges. Each country has its own governance structure, constraints, and idiosyncrasies. Understanding how these different systems work as well as their comparative advantages and disadvantages is critical as new threats emerge. However, the formation of these commands is still relatively new, with space commands being especially recent, and not all of them are fully operational yet. Current organizational setups have not yet provided enough experience to analyze effective processes. Additionally, public information on this topic is scarce, offering only a partial view of organizational frameworks and their challenges.

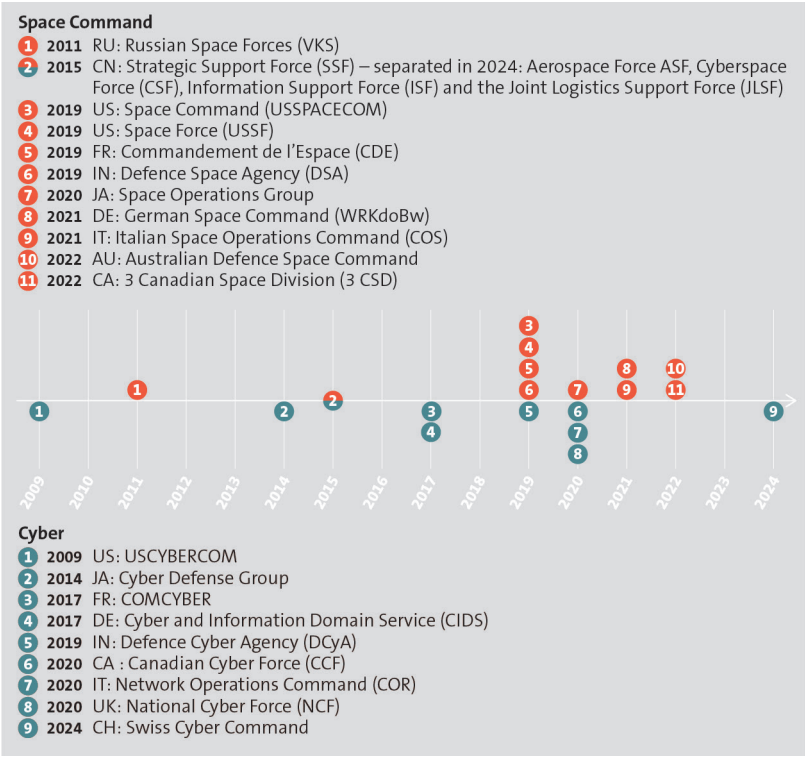
Key Points

- In France, Germany, and the UK, the authority responsible for the cyber defense of satellites depends on the nature of the targeted system.
- Cyber commands largely oversee the cyber defense of space systems in the three European nations, whereas in the US, the Space Force does.
- According to stakeholders in all analyzed countries, the distribution of cyber defense responsibilities is not always clear for space and cyber command staff.
- Countries establishing space commands should address satellite cyber defense responsibilities early to avoid gaps and duplication.

France

The French National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information* or ANSSI) is responsible for supporting operators of critical infrastructure, including those in space. For the cyber defense of military space systems, ANSSI has delegated its mission to the French cyber command (*Commandement de la cyberdéfense* or COMCYBER) due to its existing capabilities and overall responsibility for defending military systems in cyberspace.

In case of a cyberattack against a military space system, COMCYBER oversees the attack diagnosis, attribution, and repair of the system. During this process the French space command (*Commandement de l'Espace* or CDE) is kept in the loop. In case of a cyberattack against a commercial satellite, ANSSI is responsible for reporting the attack and coordinating with other authorities such as intelligence services and space agencies. COMCYBER may get involved if the satellite is linked to a military system. Usually, CDE is informed by the affected company due to existing trust relationships, but they do not have a legal obligation to do so.



The establishment of cyber and space commands worldwide. *Compiled and developed by the authors.*

COMCYBER was created in 2017 and employs 3,600 staff. By contrast, CDE, formed in 2019, employs 350 staff and aims to increase to 500 by 2025. Currently, CDE is too small to staff and maintain a dedicated cyber unit. Still, it is involved in some cyber-related missions. CDE oversees tracking cyber vulnerabilities in space systems. When one is identified, CDE is responsible for monitoring the system and overseeing its repair. Currently, this task is conducted by the Security Operations Center of the French Air Force. CDE aims to take over this function. Maintaining an up-to-date map of all vulnerabilities and deploying mitigation measures is a challenge due to the high volume of information, the complexity of space systems, and the number of stakeholders involved. The cybersecurity of CDE's IT systems is managed by the Joint Directorate of Infrastructure Networks and Information Systems (*Direction Interarmées des Réseaux d'Infrastructure et des Systèmes d'Information* or DIRISI). It is part of the French Armed Forces and in charge of the payload operations and cybersecurity of military communication satellites.

Among the European entities studied, France might be the most advanced in the integration of space cyber defense missions. Its approach appears to facilitate the most interactions between space and cyber commands, though it is not yet clear if this is the most efficient model.

United Kingdom

The cyber defense of military space systems more broadly falls to the National Cyber Force (NCF). Formed in 2020 as a partnership between the British Ministry of Defence and the Government Communications Headquarters (GCHQ), the NCF is essentially analogous to other cyber commands. Though it will eventually employ up to 3,000 staff, current staffing figures are not publicly available. The NCF, like the US Space Force, is divided into squadrons. As of today, however, there does not appear to be a full squadron dedicated to space cyber defense. It is likely that one or several squadrons deal with the topic in a broader portfolio.

In case of an attack against a military satellite, the UK Armed Forces' Cyber Force, which is part of the UK Strategic Command and works collaboratively with the NCF, is in charge. This information was provided during an interview, but there is no publicly available information about this cyber unit. In case of an attack against a commercial satellite, incident response is handled by the private sector. If the target satellite is used by the military, Strategic Command will engage with the private sector. The UK is also very reliant on the US for space capabilities, putting cyber defense in the hands of its ally. The UK would coordinate with the US in case of a cyber incident.

The UK Space Command was also founded in 2020, and it currently consists of 570 staff. Its mandate is

to monitor the space domain (Space Domain Awareness), support military operations on Earth with space capabilities, and develop new ones with industry and allies. Cyber defense is not part of its mandate. It may be involved in specific cybersecurity incidents, depending on the severity of the attack. It is involved in the development of cybersecurity standards and requirements. The cyber defense and cybersecurity of Space Command's IT infrastructure is provided by Strategic Command.

Germany

In Germany, the Cyber and Information Domain Service (*Cyber- und Informationsraum* or CIR) is responsible for protecting and defending the IT infrastructure of the Armed Forces, including military satellites, from cyberattacks. CIR was created in 2017 and employs about 13,500 staff. Unlike the UK and French cyber commands, CIR is responsible for operating some satellite payloads – a task usually handled by space commands or agencies.

In case of a cyberattack, the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* or BSI) within the Federal Ministry of Interior (*Bundesministerium des Innern und für Heimat* or BMI) together with the National Cyber Defence Centre (*Nationales Cyber-Abwehrzentrum* or Cyber-AZ) oversees incident mitigation. CIR is one of eight core authorities that make up the Cyber-AZ. BSI handles attacks on civilian or commercial satellites, including those used by the German Armed Forces, while CIR can provide forensic support. If the cyberattack is directed against a military satellite, CIR is responsible.

Germany's space command (*Weltraumkommando der Bundeswehr* or WRKdoBw) was founded four years after CIR (in 2021) and focuses on physical threats in space. It currently employs 200 people. Among other things, it oversees Space Domain Awareness, which includes monitoring the cybersecurity status of satellites. The WRKdoBw also operates satellite systems, and closely cooperates with CIR on satellite payload operations.

As in France, the distribution of responsibilities to the BSU or CIR depends on the nature of the targeted system, while the WRKdoBw, which has no role in incident mitigation, is kept informed. The German case distinguishes itself by the strong involvement of CIR in space activities, including cyber defense missions and the operation of satellite payloads. This even prompted some stakeholders in the Bundeswehr to consider the merger of the WRKdoBw with CIR. As of yet, CIR is only responsible for operating the payloads of satellites that fall under its mandate (i.e., space support to operations on Earth). Others fall under the responsibility of the WRKdoBw (e.g., operations in space). No country has unified its space and cyber commands so far. Overall, the UK and German space commands appear more removed from the task of cyber defense.

United States

Unlike the selected European countries, responsibility for the cyber defense of space assets mostly lies with the US Space Force (USSF). The USSF was established in 2019 as an agile organization with fewer personnel than other US military branches (about 14,000 in 2023), and with a budget of 29 billion USD in 2024.[1] The USSF comprises a Space Systems Command (SSC), a Space Operations Command (SpOC), a Space Training and Readiness Command (STARCOM), and an upcoming Space Futures Command (S4S).

At the time of writing, cyber defense operations are the responsibility of Space Delta 6 within SpOC. Missions are distributed across eight squadrons depending on the types of space systems involved. The 65th Cyberspace Squadron is in charge of the cyber defense of command and control, Space Domain Awareness, and launch operations. The 645th Cyberspace Squadron oversees the cyber defense of military launch pads. This Squadron also supports Space Launch Delta 45 (under the SSC) to defend launchers from advanced persistent threats (APT).[2] Until 2024, Delta 6 mostly conducted IT support missions but has gradually shifted to cyber defense.[3]

Within STARCOM, Space Delta 11 replicates combat capabilities and environments to help improve the organization's defense readiness. During the 2023 Moonlighter exercise, for example, Delta 11's 527 Space Aggressor Squadron was playing the red team to train Deltas' cyber defense capabilities.[4]

Moreover, the USSF has an element within the National Reconnaissance Office (NRO), which oversees space-based intelligence, surveillance, and reconnaissance (ISR). The Space Force Element has six Deltas, of which only Space Delta 26 has cyber defense responsibilities. It

Further Reading

Kari A. Bingen, et al., **U.S. Space Force Primer,** CSIS Aerospace Security Project, *Center for Strategic and International Studies,* 2022.
The report describes the governance and responsibilities of the U.S. Space Force.

Michel Friedling, **Commandant de l'espace, Enjeux, menaces et défis de la nouvelle ère spatiale,** *Bouquins,* 2023.
A testimony of the Former Head of the French Space Command recounting his experience establishing the French Space Command and its mandate.

comprises six cyber squadrons, whose mandate is not publicly described. In 2024, Space Delta 26 organized the Cyber Spartan Challenge to test cyber defense capabilities. SpOC's Delta 6 also took part in the exercise. It is unclear if and how the two Deltas work together in their day-to-day tasks.

Like other branches, the USSF is expected to contribute to the Cyber Command's Cyber National Mission Force. However, the lack of staff in the USSF prevents it from dispatching personnel to the Cyber Command without affecting its own abilities and missions.[5] The Cyber National Mission Force conducts both defensive and offensive cyber operations.

The USSF's organizational structure is still being revised. Many cyber squadrons are still under development and not yet fully operational. Moreover, the organization is still in the early stages of implementing combat squadrons and detachments, and it relies on industry for IT functions and some cybersecurity solutions.[6] It is unclear whether some cyber defense missions are contracted to the private sector.

Lessons Learned

This analysis describes several approaches to the cyber defense of space systems. In France, Germany, and the UK, space commands seem to focus on physical rather than cyber threats, with cyber defense not being part of their core tasks. European cyber commands are more often responsible for the cyber defense of satellites, which they consider to be simply another node to protect.

These case studies underscore the challenges and labor-intensive nature of establishing space commands and defining responsibilities in a domain that often intersects with others. During the interview process, representatives from the same country sometimes provided contradictory information. This could indicate siloed organizational thinking or transient setups that must be resolved as these commands become fully operational. It might also be a sign that the cyber defense of space assets are neglected. If this is the case, some of the analyzed countries might be ill-equipped and underprepared for a cyberattack on their military space infrastructure.

For countries considering the creation of a space command, lessons can be drawn from these four cases. First, it typically takes more than five years from the creation of a space command to its full operationalization. Within this period, the cyber threat landscape may evolve. Second, with the rise in cyberattacks on space systems, it is essential to clearly define responsibilities between space and cyber commands for cyber defense and cybersecurity to avoid gaps and unnecessary duplication. Third, most modern militaries heavily rely on commercial space systems. Defining responsibilities, cybersecurity requirements, and cooperation mechanisms between the state and the private sector is essential. It is also critical for commercial actors to understand which entities are in charge. Adversaries can exploit organizational confusion just as effectively as technical vulnerabilities. Fourth, defining responsibilities and allocating resources for the cyber defense of satellites is complex, even for countries with significant resources. As shown in the section analyzing the US, human resource allocation issues may arise between space and cyber commands. Fifth, since space commands are mostly staffed by personnel from other military branches, building expertise in niche areas like satellite cyber defense was identified as a major need by interviewed stakeholders.

Ultimately, responsibility for the cyber defense of satellites is gradually being integrated into armed forces. However, efforts are still required to achieve a comprehensive understanding, effective mitigation, and robust countermeasures against cyber threats.

Selected sources

1. "Space Force Organization," *United States Space Force,* 2024.
2. "645th Cyberspace Squadron," *Peterson and Schriever Space Force Base,* 2024.
3. "Guardians of the Digital Frontier: USSF Focusing on Defensive Cyber Operations," *Peterson and Schriever Space Force Base,* 2024.
4. "Space Force Guardians Hone Cyber Defense Skills Using On-Orbit Satellite," *United States Space Command,* 2023.
5. Mark Pomerleau, "Space Force Would Need More Resources to Contribute to Cyber Mission Force, Nominee Says," *DefenseScoop,* 13 September 2022.
6. Mark Pomerleau, "Space Force in Discussions to Establish a Cyber Component to US Cyber Command," *DefenseScoop,* 2023.

Clémence Poirier is a Senior Cyber Defense Researcher at the Center for Security Studies at ETH Zürich.
Sarah Wiedemar is a Cyber Defense Researcher at the Center for Security Studies at ETH Zürich.

Policy Perspectives is published by the Center for Security Studies (CSS) at ETH Zürich. The CSS is a center of competence for Swiss and international security policy.

Series Editor: Daniel Möckli
Issue Editor: Gorana Grgić
Layout: Miriam Dahinden-Ganzoni

Feedback welcome: PolicyPerspectives@sipo.gess.ethz.ch
More issues and free online subscription:
css.ethz.ch/en/publications/css-policy-perspectives

Most recent editions:
Prospects of a Transatlantic Arsenal of Democracy (12/2)
Time to Make 'Peace' with the Bandits (12/1)
Unequal Access to UN Human Rights Bodies (11/6)
Making Cyber Attribution More Transparent (11/5)
Satellite Imagery for Disaster Resilience (11/4)
Mind the E-Waste: A Case for Switzerland (11/3)

ISSN: 2296-6471; DOI: 10.3929/ethz-b-000694300