Ethical Frameworks of Extramilitary Defense in Emerging Domains: Parallels in Cyber and Planetary Defense

International Academy of Astronautics 2025 Planetary Defense Conference
Poster Session 9 : The Decision to Act: Political, Legal, Social, and Economic Aspects / 260

Christopher Geiger [(1)], **Cwynn Geiger**[(2)]
[(1)] *Lockheed Martin, 6801 Rockledge Dr, Bethesda, MD, 20817, USA, 301-897-6000, christopher.a.geiger@lmco.com*
[(2)] *Lake Highland Preparatory School, 901 Highland Ave, Orlando, FL, 32803, 407-206-1900*

Keywords

Planetary Defense Governance, Cybersecurity, Ethics, Insurance, Extramilitary Defense

Abstract

Age-old concepts of sovereign military power have traditionally transferred into new physical and technological domains (e.g., air, undersea, electromagnetic spectrum) to create security. However, some recent emerging threat domains have been excluded from nations' military responsibility. Two current examples are cyber security and planetary defense. By addressing these topics outside of the military context and associated treaties, laws, and ethics; states, organizations, and individuals are developing new methods of defending their interests.

Across the globe, companies must defend themselves against cyber security attack from outside their country's borders with no assistance from their government's military defense. Cyber security is treated more like a natural disaster with attendant insurance, civil agencies, and remediation industry. Organizations have also developed industry-based Information Sharing and Analysis Centers (ISACs) to pool information and resources. The resulting cyber security ethical frameworks are based on professional codes, technology considerations, and applicable laws.

Planetary defense is another extramilitary domain with many parallels to cyber security. Information sharing and analysis is a critical aspect of the field and requires cross-organizational collaboration. The threat is more likely to be adequately addressed as a mutualized risk than by each individual alone. In addition, the threat manifests from an extraterritorial location (like a cyber advanced persistent threat) so it is not readily affected by legal sanction.

This paper explores the potential benefits of using cyber security ethical and cooperation frameworks to inform the field of planetary defense. It also highlights pitfalls in using climate change-related parallels with planetary defense based on systemic and political factors. The resources applied to cyber security are orders of magnitude greater than planetary defense. To the degree that cyber security investment's benefits are transferable they should be leveraged by other threat domains.

Ethical Frameworks

All risk management frameworks have an ethical component. While treating a risk it is important to consider effects on all stakeholders, including both intended and unintended consequences. In commercial activities, the imperative of ethical activities extends beyond the legally required to include consideration of financial materiality and double materiality.

Cyber defense governance incorporates a culture of compliance with ethical principles. Each cybersecurity framework aligns its activities to the mission and purpose of the protected organization's underlying activities and its associated ethical values. This is an important activity because it informs cost-benefit analysis, resource allocation, and risk appetite. The communication of these analyses and decisions to the entire affected community serves to spread awareness as well as collective assent for burden-sharing.

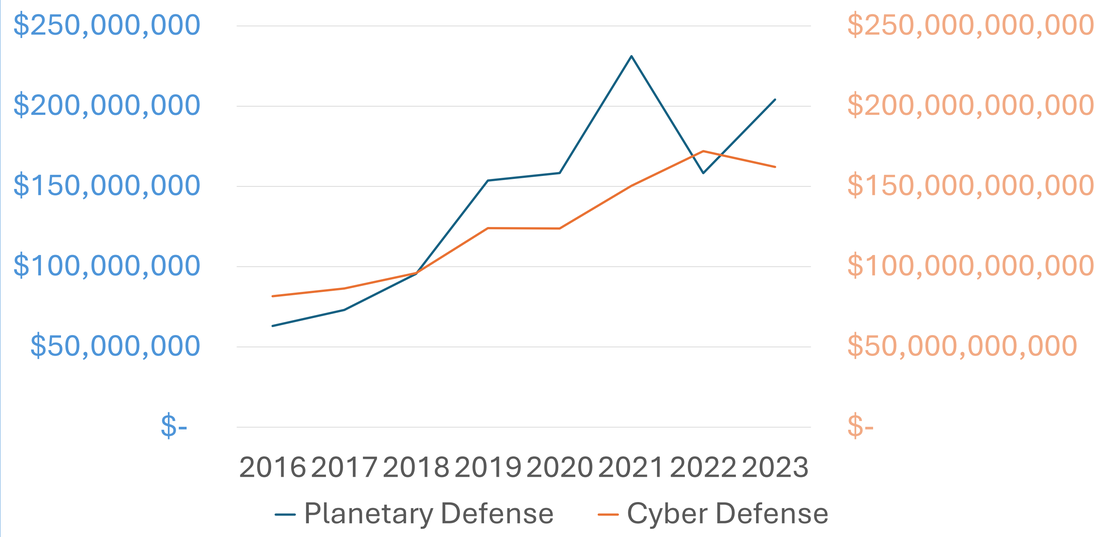
Planetary defense with an ethics-based governance framework could publish publicly accessible cost-benefit analyses to encourage wider engagement and support for more commercial or governmental resources.

An important aspect of cyber defense is cyber insurance. Insurance is the classic risk management tool to transfer part of a risk's realization costs to another party. To develop a robust planetary defense insurance market where costs can be mutualized, there must be a sound level of agreement between parties on the likelihood, velocity, and impact of a risk. Similar to established existing insurance markets, this will be easier to accomplish within a clear governance framework.

AI Statement

No Large Language Models (LLMs) or other generative Artificial Intelligence (AI) were used in this paper.

Global Planetary and Cyber Defense Spending[1,2]



Planetary and Cyber Defense Frameworks

Cybersecurity Framework (NIST CSF 2.0)[3]	Planetary Defense (NASA Planetary Defense Decision Cycle)[4]	Planetary Defense (ESA Planetary Defense Office)[5]
Identify	Assess	Observation
Protect	Search, Detect & Track	
Detect	Characterize	Data Provision
Respond	Plan, Coordinate, and Mitigate	Mitigation
Recover		
Governance		

Missing Governance?

A key overarching aspect of cyber defense is governance. Collective cyber defense is made practical through information sharing and commercial software platforms using the scale of many customers' network data. Similar to planetary defense, cyber defense governance is not universally regulated or mandated by national governments. In the absence of legal requirements or state protection, information security professionals have developed and self-imposed governance across organizations, industries, and states.

Like other risk management frameworks, cybersecurity activities are cyclical and continuous. Frameworks are best managed by a governance regime that coordinates resources and stakeholder activities and provides for accountability and transparency. A key missing attribute of planetary defense activities or frameworks is a governance structure. The successful international commercial cybersecurity field shows that effective governance can exist outside government and military requirements and oversight.

Specific cyber defense governance mechanisms that should be considered for planetary defense include information sharing agreements and standardization; integration with other risk-based activities; and a documented alignment with goals and a values-based ethical foundation.

References

1. Planetary Defense Roadmap Version 4.0, Space Mission Planning Advisory Group (SMPG), United Nations Office for Outer Space Affairs, March 2023.
2. Gartner Global Information Security Spending Forecasts, 2016-2023.
3. The NIST Cybersecurity Framework (CSF) 2.0, U.S. National Institute of Standards and Technology (NIST), U.S. Department of Commerce, February 2024.
4. NASA Planetary Defense Strategy and Action Plan, U.S. National Aeronautics and Space Administration (NASA), April 2023.
5. Asteroids and Planetary Defense, The European Space Agency, https://www.esa.int/Space_Safety/Planetary_Defence/Asteroids_and_Planetary_Defence, Accessed April 2025.