PROPOSED CYBER STANDARDS IN POLITICAL SCIENCE.
Proposed cyber standards in political science refer to suggested guidelines and regulations for the use of technology and the internet within the realm of governance and politics. These proposed standards typically aim to address cybersecurity concerns, data privacy, and ethical considerations in the digital age. They may include recommendations for securing government networks, protecting sensitive information, and ensuring the integrity of digital communication channels. The development and implementation of such standards are crucial for maintaining trust in political institutions and safeguarding democratic processes in an increasingly interconnected world.
The proposed cyber standards in political science are as follows:

1. **DEVELOPMENT OF INTERNAL LEGISLATION TO PROTECT PERSONAL INFORMATION.**
The development of internal legislation to protect personal information is a proposed cyber standard in political science because it addresses the need to safeguard individuals' privacy and data security within the context of governance and political activities. This type of legislation sets boundaries and rules for the collection, storage, and use of personal information by government entities, political organizations, and related stakeholders.
By establishing clear legal frameworks and guidelines for handling personal data, such legislation contributes to the protection of citizens' privacy rights and helps mitigate the risk of unauthorized access, misuse, or exploitation of sensitive information. In doing so, it aligns with the broader goal of proposed cyber standards to enhance cybersecurity, uphold ethical practices, and promote trust in the digital domain within the realm of political science.

2 **INCREASED OVERSIGHT OF GOVERNMENT-OPERATED CYBER NETWORKS.**
Increased oversight of government-operated cyber networks is a proposed cyber standard that addresses the need for enhanced monitoring, regulation, and governance of digital infrastructure within the public sector. This type of oversight aims to ensure the security, reliability, and ethical use of government-operated cyber networks, including those used for communication, data storage, and information exchange.
By implementing stricter oversight measures, such as regular audits, compliance checks, and transparent reporting mechanisms, policymakers and cybersecurity professionals can better identify and address potential vulnerabilities, unauthorized access attempts, and other security threats. This helps to strengthen the resilience of government-operated cyber networks and reinforces public trust in the systems that underpin essential services and democratic processes.
Moreover, increased oversight contributes to the alignment of government-operated cyber networks with established cybersecurity standards and best practices, ultimately promoting the responsible and effective use of digital technology within the public sector.

3. **DEVELOPMENT OF A LEGAL FRAMEWORK TO OVERSEE THE USE OF CYBER WEAPONS.**
The development of a legal framework to oversee the use of cyber weapons is indeed emerging as a critical issue in both political science and international law. In the context of the increasing prevalence of cyber warfare and cyber espionage, the lack of comprehensive international legal standards creates a scenario where state and non-state actors can engage in hostile cyber operations with ambiguous legal repercussions.
Political scientists and legal experts have proposed establishing a set of cyber standards for several reasons:

1. Accountability:A legal framework would clearly define what constitutes a cyber weapon and a cyber attack and would set out the repercussions for states or individuals who violate these standards.

2. Deterrence:By establishing clear consequences for the use of cyber weapons, a legal framework could potentially deter malicious cyber activities.

3. International Security: Common standards would contribute to international security by reducing the likelihood of escalatory behavior in cyberspace that could lead to severe conflicts.

4. Norm-Building: A legal framework helps establish international norms and expectations regarding state behavior in cyberspace.

5. Legitimacy: Legal frameworks can also lend legitimacy to state actions that are taken in self-defense or as part of an approved international operation.

6. Cooperation: A unified legal stance on cyber operations facilitates international cooperation in cyber defense, law enforcement, and intelligence sharing among countries that might otherwise have conflicting views on acceptable behavior.

7. Clarity and Stability:A framework provides clarity and stability by setting out the rights and obligations of states and non-state actors in cyberspace, which is important for preventing misunderstandings that could lead to conflict.

Developing such standards, however, is a complex task due to the unique nature of cyberspace, the rapid evolution of technology, and the difficulty of attribution of cyber attacks. Political scientists analyze these challenges and explore the implications of these developments for international relations theory, especially concerning sovereignty, power, and conflict.

Additionally, there's a need for collaboration between nations to agree upon such standards, requiring diplomatic negotiation and agreement. This process involves the integration of existing international law principles, such as the Law of Armed Conflict (LOAC), with new understandings pertinent to the domain of cyberspace.

In essence, political science scholars highlight the need for and challenge of developing this legal framework and provide insight

into how it can shape global interactions in the cyber domain.

In conclusion, the proposed cyber standards in political science are meant to ensure the well-being of the citizens of a country technologically.