**PROPOSED CYBER STANDARDS**

In the field of political science, proposed cyber standards generally refer to frameworks, guidelines, or regulations designed to enhance cybersecurity and protect critical information infrastructure. These standards can be proposed by governments, international organizations, or industry bodies and typically aim to address various aspects of cybersecurity, including prevention, detection, response, and recovery from cyber incidents. Here are some key areas where cyber standards are often proposed:

**1. National Cybersecurity Strategies:** Governments develop comprehensive strategies to protect national interests in cyberspace. These strategies outline policies, objectives, and measures to enhance cybersecurity across different sectors.

**2. International Cooperation and Agreement**: Standards often involve international cooperation to address cross-border cyber threats. Organizations like the United Nations, NATO, and the European Union work on developing common cybersecurity policies and frameworks.

**3. Industry Standards and Best Practices:** Various industry bodies, such as the International Organization for Standardization (ISO) and the National Institute of Standards and Technology (NIST), propose standards and best practices for cybersecurity. Notable examples include ISO/IEC 27001 for information security management systems and the NIST Cybersecurity Framework.

**4. Data Protection and Privacy Regulations:** Cyber standards often include regulations on data protection and privacy. The General Data Protection Regulation (GDPR) in the European Union is a prominent example, setting standards for data handling and protection.

**5. Critical Infrastructure Protection:** Standards are developed to protect critical infrastructure sectors like energy, finance, healthcare, and transportation from cyber threats. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and similar organizations in other countries work on these standards.

**6. Cyber Incident Response and Reporting:** Guidelines and standards for responding to and reporting cyber incidents are crucial. These include incident response plans, coordination mechanisms, and mandatory reporting requirements.

**7. Cybersecurity Workforce and Education**: Standards for cybersecurity education and workforce development aim to build a skilled workforce capable of addressing cyber threats. This includes certification programs, training standards, and educational curricula.

**8. Cyber Norms and Ethics**: In political science, there is also a focus on developing norms and ethical standards for state behaviour in cyberspace. This includes discussions on responsible state behaviour, cyber warfare, and the application of international law to cyberspace.

These proposed cyber standards are essential for creating a secure and resilient digital environment, protecting national security, economic stability, and the privacy and rights of individuals.