# FIELD: POLITICAL SCICENCE

## TOPIC: PROPOSED CYBER STARNDARDS

What are proposed cyber standards?

Proposed cyber standards in the field of political science refer to suggested guidelines and principles aimed at addressing cybersecurity challenges and risks within political systems and processes. These standards are designed to enhance the security, resilience, and integrity of information and communication technologies (ICTs) employed in political institutions and activities.

While specific proposals can vary, some common elements of proposed cyber standards in political science may include:

1. Data protection and privacy: Establishing mechanisms to safeguard the privacy and confidentiality of sensitive political data, including personally identifiable information (PII) of citizens, campaign information, and government records.
2. Personally Identifiable Information (PII): PII refers to any information that can be used to identify an individual. In the political context, PII may include voter registration data, party affiliation, political preferences, and contact information. Proposed cyber standards advocate for the implementation of measures to protect PII from unauthorized access or disclosure. This involves employing encryption techniques to secure stored and transmitted data, implementing strict access controls to limit who can access PII, and conducting regular audits to monitor and detect any potential breaches.
3. Campaign Information: Political campaigns collect and manage vast amounts of data, including donor information, campaign strategies, voter demographics, and communication records. Protecting this information is crucial to maintain the integrity of the campaign and ensure the privacy of individuals involved. Proposed cyber standards suggest practices such as secure storage of campaign data, regular backups, and strong authentication methods to prevent unauthorized access. Additionally, campaigns may implement protocols to govern the collection, use, and retention of campaign data, ensuring compliance with relevant privacy laws and regulations.
4. Government Records: Political institutions and government agencies handle a wide range of sensitive information, such as legislative documents, policy discussions, and confidential communications. Proposed cyber standards emphasize the need to protect the confidentiality and integrity of these government records. This involves implementing secure information management systems, ensuring proper access controls based on user roles and responsibilities, and maintaining audit trails to monitor access and changes to government records. Encryption and digital signature mechanisms can also be employed to enhance the security and authenticity of government records.
5. Compliance with Data Protection Regulations: Proposed cyber standards in political science also advocate for compliance with relevant data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union or similar data protection laws in different countries. Compliance with these regulations ensures that political entities handle personal data responsibly, obtain proper consent for data collection and processing, and provide individuals with rights over their data, such as access and deletion.
6. Risk assessment and management: Identifying potential cyber threats and vulnerabilities within political systems and adopting measures to mitigate and manage these risks effectively.
7. Identification of Cyber Threats: Risk assessment begins with identifying potential cyber threats that political systems may face. These threats can include various forms of malicious activities, such as hacking attempts, data breaches, phishing attacks, malware infections, or distributed denial-of-service (DDoS) attacks. Proposed cyber standards suggest conducting regular vulnerability assessments, analyzing threat intelligence, and staying informed about emerging cyber threats relevant to the political domain.
8. Risk Analysis: Once threats and vulnerabilities are identified, a comprehensive risk analysis is performed. This involves evaluating the potential impact and likelihood of each identified risk. Impact assessment considers the potential harm or damage that a cyber threat can cause to political processes, public trust, or the integrity of data. Likelihood assessment evaluates the probability of a threat exploiting vulnerabilities and materializing into an actual incident. Risk analysis helps prioritize and allocate resources effectively to address the most critical risks.
9. Ongoing Risk Management: Risk assessment and management are not one-time activities but an ongoing process. Proposed cyber standards highlight the importance of continuously monitoring and reviewing risks within political systems. This includes regularly reassessing threats, vulnerabilities, and potential impact, and adapting risk management strategies accordingly. Additionally, conducting post-incident analysis and learning from past incidents helps refine risk management practices and enhance overall cyber resilience.
10. Secure infrastructure: Ensuring the security of critical ICT infrastructure used in political processes, such as election systems, government networks, and communication channels, through robust authentication, encryption, and access controls.
11. Election Systems: Election systems play a crucial role in democratic processes, and their security is of utmost importance. Proposed cyber standards advocate for securing election infrastructure through various measures. This includes implementing robust authentication mechanisms to ensure that only authorized individuals can access and administer election systems. Encryption is utilized to protect the integrity and confidentiality of data transmitted or stored within election systems. Access controls are established to limit access to sensitive election-related data, ensuring that only authorized personnel can make changes or access critical information.
12. Communication Channels: Communication channels used by political actors and government officials need to be protected to prevent unauthorized interception or tampering of sensitive information. Proposed cyber standards suggest using encryption protocols to secure communication channels, such as email encryption or secure messaging platforms. Additionally, secure virtual private network (VPN) connections are established to provide encrypted communication between remote locations. Two-factor authentication is recommended to enhance the security of communication accounts and prevent unauthorized access.
13. Access Controls: Robust access controls are crucial in securing political infrastructure. Proposed cyber standards highlight the importance of implementing strong user authentication mechanisms, such as multifactor authentication or biometric authentication, to ensure that only authorized individuals can access sensitive systems and data. Role-based access controls are established to assign appropriate privileges and restrict access to information based on user roles and responsibilities. Regular access reviews and audits are conducted to ensure that access privileges are up to date and aligned with organizational needs.
14. Legal and regulatory frameworks: Developing comprehensive legal and regulatory frameworks that define responsibilities, obligations, and sanctions related to cybersecurity in political contexts, including laws governing cybercrime, data protection, and election security.
15. International Cooperation: Legal and regulatory frameworks in the political science field may also encompass provisions for international cooperation in addressing cyber threats. Cybersecurity challenges often transcend national boundaries, and collaboration between countries is essential to effectively combat cybercrime and enhance overall cybersecurity. Legal frameworks can establish mechanisms for sharing threat intelligence, coordinating investigations, and extraditing cybercriminals. They can also promote cooperation in the development of cybersecurity norms, standards, and information-sharing platforms among nations.
16. Data Protection Laws: Legal frameworks related to data protection are essential for safeguarding sensitive political information and ensuring the privacy rights of individuals. These laws govern the collection, storage, processing, and sharing of personal data within political systems. They establish obligations for political entities to handle personal data responsibly, obtain informed consent, provide data breach notification, and offer individuals rights over their data, such as access and deletion. Data protection laws help protect citizens' privacy, maintain public trust, and ensure the secure handling of sensitive information within political processes.
17. Cybercrime Laws: Legal and regulatory frameworks encompass laws and regulations that define and criminalize cyber activities that pose a threat to political systems. These laws typically cover offenses such as unauthorized access to political systems, data breaches, hacking attempts, and dissemination of false information or propaganda. Cybercrime laws provide a legal basis for prosecuting individuals or groups engaged in malicious activities targeting political institutions. They may also establish penalties and sanctions for such activities, serving as a deterrent against cyber threats in the political context.
18. Awareness and training: Promoting cybersecurity awareness and providing training programs to political actors, staff, and stakeholders to enhance their understanding of cyber threats, best practices, and appropriate behavior online.

1. Incident response and recovery: Developing protocols and frameworks for responding to cyber incidents promptly and effectively, including incident reporting, investigation, and recovery procedures.

International cooperation: Encouraging collaboration and information sharing among political entities at national and international levels to collectively address cyber threats and exchange knowledge on effective cybersecurity measures.

In conclusion, proposed cyber standards in the field of political science encompass a range of guidelines and principles aimed at addressing cybersecurity challenges within political systems. These standards emphasize the importance of data protection and privacy, risk assessment and management, secure infrastructure, legal and regulatory frameworks, awareness and training, incident response and recovery, and international cooperation. By adopting these proposed cyber standards, political institutions can enhance the security, resilience, and integrity of their information and communication technologies, protect sensitive political data, mitigate cyber risks, and promote a culture of cybersecurity awareness among political actors, staff, and stakeholders. Ultimately, these standards contribute to the overall security and stability of political systems in the face of evolving cyber threats.