Implications of the National Cybersecurity Strategy

Cybersecurity has risen to the top of the priority list for governments and companies worldwide in the quickly changing digital environment of today. A comprehensive strategy to cybersecurity is required given the rising frequency and severity of cyberattacks on sensitive data, critical infrastructure, and national security. In response to this need, the United States developed the National Cybersecurity Strategy, which serves as a road map for the nation's strategy for safeguarding its digital assets and fending off cyberthreats. The 2018-released strategy covers the main goals, guidelines, and steps the US will take to guarantee its cybersecurity.

The National Cybersecurity Strategy's greater involvement for the government in guaranteeing cybersecurity is one of its political ramifications. According to the policy, the government should take the lead in the nation's cybersecurity initiatives, collaborating closely with the corporate sector, foreign partners, and individual citizens to safeguard sensitive data and key infrastructure. Questions about privacy and civil liberties, as well as the harmony between security and freedom, are raised by this expansion of government control.

The National Cybersecurity Strategy's effect on international relations is another political issue. The policy acknowledges the value of cooperating with foreign partners to guarantee a safe and open digital environment. The United States has been working closely with its allies to develop international cybersecurity norms and to cooperate on efforts to address cyber threats. The National Cybersecurity Strategy has also impacted the relationship between the United States and other countries, particularly those that have been accused of engaging in malicious cyber activities.

Additionally, the National Cybersecurity Strategy has significant economic ramifications. The economy may be significantly impacted by the rising frequency and intensity of cyber-attacks, which can also interrupt business operations, harm brand reputation, and result in financial losses. The strategy emphasizes the necessity of safeguarding the nation's economic interests and calls for investments in R&D as well as the development of a workforce capable of addressing the problems of the digital age in cybersecurity.

Concerns about privacy have grown as a result of the government's expanded responsibility in guaranteeing cybersecurity. The National Cybersecurity Strategy acknowledges the value of preserving individual privacy and civil liberties, but the growing amount of sensitive data being collected and controlled by the government raises concerns about how these rights will be upheld. The Electronic Frontier Foundation has advocated for greater transparency and accountability in government cybersecurity efforts and criticized the approach for not doing enough to address privacy issues.

The National Cybersecurity Strategy must strike a balance between the necessity for security and the defense of individual liberties. In order to achieve security, it is necessary to strike a careful balance between maintaining civil liberties and privacy while also implementing increasingly stringent security measures. The strategy acknowledges this difficulty and demands for the development of a framework that upholds civil liberties and privacy while maintaining national security.

In conclusion, The National Cybersecurity Strategy of the United States has significant political ramifications, including increased governmental control, global ties, economic factors, privacy issues, and the need to strike a balance between security and freedom. It is crucial to deal with these issues and make sure that the nation has a thorough and effective strategy to cybersecurity as the digital world continues to develop. The National Cybersecurity Strategy serves as a guide for the nation's strategy for safeguarding its digital assets and fending off cyberthreats, and it is crucial to keep reviewing and updating the plan as the cybersecurity landscape changes.

Works Cited

Valeriano, B., & Jensen, B. (2021, May). Building a national cyber strategy: The process and implications of the cyberspace solarium commission report. In *2021 13th International Conference on Cyber Conflict (CyCon)* (pp. 189-214). IEEE.

Smeets, M. (2020). US cyber strategy of persistent engagement & defend forward: implications for the alliance and intelligence collection. *Intelligence and national security*, *35*(3), 444-453.

Kshetri, N. (2021). Recent US cybersecurity policy initiatives: challenges and implications. *Computer*, *48*(7), 64-69.

Ghelani, D. (2022). Cyber security, cyber threats, implications and future perspectives: A Review. *Authorea Preprints*.