Chapter 13
Understanding US Cyber Security Policies During the Donald J. Trump and Biden–Harris Administrations

Tamar Karazanishvili
International Black Sea University, Georgia

ABSTRACT

Cybersecurity threats are one of the main national security, public safety, and economic challenges every nation faces in the 21st century. The Russia-Ukraine War becomes a defining feature of the US national cyber security strategy too. The purpose of this chapter is to analyze the increasing role of cybersecurity in US politics. It is evident that US cybersecurity strategies at a national level seems to be increasing across multiple sectors too. The chapter analyses Trump's and Biden's national cyber security strategies and challenges. It deals with different initiatives of both presidential administrations and the implications on national security of the country. The chapter focuses on the measures taken by US politicians in strengthening cybersecurity at a national level and combating both state or non-state-sponsored cyber threats.

INTRODUCTION

Cyber security became one of the top national security issues of the 21st century. The Russia-Ukraine war became another threat globally for states to think about cyber security strategies and it is the defining feature of the US national cyber security strategy too.

Due to enduring uncertainties and differences of authority and accountability on different levels, managing cyber insecurities continues to be the most challenging governance issue in contemporary politics. Cavelty M. and Wenger A. define in their book (2022) that the cyber security is "transboundary in nature, occur[s] at multiple levels across sectors, between institutions, and will impact all actors, both public and private, in complex, interconnected, and often highly politicized ways". As it evolves at

DOI: 10.4018/978-1-6684-8846-1.ch013

the intersection between fast-paced technological development, the political and strategic use of these tools by state and non-state actors, and the various attempts by the state and its bureaucracies, society, and the private sector to define appropriate responsibilities, legal boundaries, and acceptable rules of behavior for this space (Cavelty M., Wegner A. 2022).

Cavelty M. (2022) states that cyberspace is a complex system that is influenced by both human and technical factors. “The security of cyberspace is not just a technical problem. It is also a social and political problem. There is still much research to be done on how to secure cyberspace”. Besides, cyberspace is not independent from other systems. This makes it vulnerable to cyberattacks that can have a cascading effect on other systems. Cyber security is a key national security issue because it is also a social and political problem. As Cavelty mentions in his book, the cyber-incidents during the US elections in 2016 highlighted the importance of cyber security for democratic processes; during the US elections in 2016 - attributed to the Russian government as well as semi-state actors - started a new chapter in the cyber security debate. “The hack and leak operations highlighted the issue of strategic manipulation – also called influence operations – as a threat to democratic processes”. Current technological environment affords different actors with new opportunities (Cavelty M., Wegner A. 2022).

In addition, the cyber security discourse has changed considerably over the last 20 years: “Cyber security is moving upward in the political agenda and expanding sideways as a problem area to a multitude of additional policy domains with advancing digitization” (Cavelty D. 2019).

Beyond the technical realm, cyber security has become a type of security that refers to offensive and defensive activities of state and non-state actors in cyberspace, serving the pursuit of wider security political goals through the exploitation of various related opportunities. The role of the state in cyber security matters remains politically contested because cyber security is not only about national security; as the question is whether who should have the role, and what kind of role, they should have in different governance arrangements that aim to enhance national and international security. Obviously, states alone cannot ensure an increase of cyber security, not least because many crucial networks are in private hands. Hence, cyber security politics are defined by national and international negotiation processes about the boundaries of responsibilities of state, economic, and societal actors and the agreement or disagreement over the means these actors use (Cavelty M., Wegner A. 2022).

Consequently, analyzing current cybersecurity challenges as well as the US role, as a global actor in world politics, on cyber security priorities, strategies and policies is crucial as it is mentioned above it includes the social, technical as well as political fragmentations. The given chapter aims to analyze Donald J. Trump’s and Biden-Harris’ Administrations’ cybersecurity policies.

Cyber Security in World Politics

Despite different approaches taken by various countries in terms of cybersecurity, politics and the approaching cyberwar, it’s obvious that cybersecurity has solidified as one of the top national security challenges of the 21st century.

Certainly, different communities interpret “security” in cybersecurity differently. On a fundamental level, digital technology security is based on risk management techniques created by computer professionals to help make computers and computer networks more reliable. Yet, recent major cybersecurity incidents, including the attacks on healthcare institutions, show that cybersecurity is also very much about protecting people and their interests, not just information security. Cybersecurity keeps evolving as a politically relevant issue and it does that at the junction of rapid advances in