Chapter 16
Analyzing Cybersecurity Strategies in Democratic and Authoritarian Regimes:
A Comparative Study of the United States and China

Mari Malvenishvili
Cyber Security Studies and Education Center, Georgia

ABSTRACT

This chapter aims to analyze the cybersecurity policies and strategies of the United States and China, representing democratic and authoritarian regimes, respectively. The study explores the key roles played by cyber security policies, legal frameworks, and international relations in these countries. By examining these aspects, the authors discern the disparities between cyber security policies in democratic and authoritarian regimes. The chapter highlights the diverse approaches employed to ensure cyber security and the challenges faced by both countries in countering cyber threats and safeguarding their national interests.

INTRODUCTION

The United States and China are economic rivals that recognize the vital role of information resources in securing the long-term survival of their respective nation-states. Both countries prioritize the secrecy, security, accessibility, and reliability of their information infrastructure to safeguard sensitive data and knowledge, thereby safeguarding their national interests (Donilon, 2014). China, boasting one of the world's fastest-growing internet economies, possesses dedicated cyber security capabilities that pose a threat not only to the United States but also to other Western nations.

The United States, through its national security adviser, has explicitly identified Chinese cyber intrusions as a significant concern for its military, highlighting the sophisticated and targeted theft of confidential business information and proprietary technologies (Donilon, 2014). Despite these cyber security

DOI: 10.4018/978-1-6684-8846-1.ch016

challenges, the relationship between the United States and China has maintained a degree of stability, largely driven by their trade relations. According to the Office of the United States Trade Representative (2022), China is the United States' largest goods trading partner, with a total goods trade of $559.2 billion in 2020. This economic interdependence and the principles of international trade, as postulated by Angell (2007), contribute to peace and stability.

However, beneath the economic ties lie stark differences in political regimes. The United States adheres to democratic governance, while China is widely perceived as maintaining an authoritarian rule. Democracy entails the broad distribution of authority among the people, granting citizens the right to sovereign power and participation in decision-making processes. In contrast, autocracy and oligarchy concentrate decision-making authority in the hands of a single individual or a select few (Duignan, 2012). Morlino (2009) identifies several characteristics that distinguish good democracies, including the rule of law, accountability (both electoral and inter-institutional), competition, participation, protection of rights and freedoms, political, social, and economic equality, responsiveness to public opinion, and engagement with civil society.

The influence of political regimes extends beyond cyber security and permeates a country's overall strategy, whether in economics, healthcare, or other domains. Scholars have engaged in extensive discussions on the concept of national strategy. Foster (1990) defines strategy as a conventional formula encompassing ends, ways, and means to project national power. However, Meiser (2017) criticizes simplifying strategy-making, arguing that it reduces it to a formulaic allocation of resources, impeding creative and adaptive thinking. While some find Meiser's perspective extreme, they acknowledge the importance of adopting a broader perspective that incorporates the interests and decisions of other actors, including allies and adversaries, to capture the essence of strategy. In terms of grand strategy, Posen (2014) and Gray (2010) emphasize the use of military force by states to pursue their interests.

In the context of cyber security, both China and the United States, as major global powers, rely on cyberspace for their economic, social, and overall well-being (Remington, 2019). They share common concerns about national security and the reliability of their information systems. Despite their divergent political regimes, they both recognize the significance of cyber security in protecting classified data, preventing theft and loss, and countering cyber-attacks and breaches that could be exploited by adversaries such as terrorists.

LITERATURE REVIEW

Cyber security has emerged as a critical concern in the modern world, posing significant challenges to countries, businesses, and individuals. This literature review aims to provide an overview of past research on cyber security, with a specific focus on democratic and authoritarian regimes in the United States and China (Edel & Brands, 2019). In a democratic regime, power is held by the people and exercised through accountable leaders elected by them, whereas an authoritarian regime concentrates power in the hands of a small group of individuals (Kendall-Taylor et al., 2020). These two types of regimes differ in their objectives and the means used to achieve them. Authoritarian regimes decide what is best for the people, imposing their values regardless of public opinion, while democratic regimes uphold free and fair elections, freedom of expression, the rule of law, and the separation of powers among the executive, legislative, and judiciary branches (Kendall-Taylor et al., 2020).