Practices and Political Implications of American Cybersecurity Policy since the CNCI (2008)*

Sunghyun Kim • Gon Namkung
(Ewha Womans University)

I. Introduction

Conventionally, one would expect the United States to lack headway in its development of cybersecurity and related policymaking, particularly because the US is an advanced, constitutional democracy. There has always been a significant debate between those who push for national security and those who highlight the importance of individual freedom and privacy. As President Barack Obama emphasized at the 2009 release of the White House Cyberspace Policy Review, the American pursuit of cybersecurity is not to include

* This work was supported by the National Research Foundation of Korea Grant funded by the Korean government (NRF-2010-330-H00003).
monitoring of private sector networks or Internet traffic and the US will indeed work on preserving and protecting the personal privacy and civil liberties that Americans value and cherish. There are thus difficulties involved with cybersecurity efforts because they must carefully take into account the surrounding issues of “privacy, liberty, innovation, and the open nature of the Internet.” There is also the debate on the US government’s extent to regulating industry. To realize and execute a comprehensive cybersecurity policy, public-private partnerships must take place but the regulation debate, along with US laws that limit information sharing, impede such policymaking. Just as much as these difficulties exist, there has also been widespread criticism upon the US government for not being able to put forth a comprehensive and consistent national cyber agenda.

However, from what I have seen through the study of America’s cybersecurity policy through a framework that I have created, there have been significant advancements and breakthroughs, especially since the launch of the 12 initiatives of the Comprehensive National Cybersecurity Initiative (CNCI) in 2008. Important developments and achievements in regarding practices have taken place, which also carry noteworthy political implications that need to be further considered for future policymaking. Although cyberspace is understood to have evolved without much priority or emphasis given to security as much as it should have, I was able to find that key cyber defensive measures and related political implications have shown progress within the US since this time. Thus, depending on perspective, one can understand that notable transformations have taken place in light of US cybersecurity policy.