Research Summary Melike Melis Dilisen
PhD Year 1, Graduate School of Media and Governance, Keio University

CONFLICTS BETWEEN INDIVIDUAL AND NATIONAL CYBERSECURITY:

The Chinese “Secure and Controllable” Cyberspace Policy

Anonymity is an important cloak for individuals to protect themselves in cyberspace. Yet, the governments have been trying to uncover this cloak in order to gather intelligence more effectively to protect their states against any possible threats and striving to store information about their citizens more than ever. For the sake of a high level of intelligence, do governments actually make their citizens target of the malicious actors by their own hands?

This paper is about the examination of the protective role of state vis-à-vis its individuals in cyberspace and this relationship’s position in the literature of International Relations (IR) Theory, more specifically, *Realism*. Being the predominant theory of IR, Realism’s one of the main assumptions has been the centrality of the individual’s security to the state’s *raison d’état*. Thus, as long as the state’s security is preserved, the individual security would follow suit. Nevertheless, realism might fall short in taking the domain of cyberspace into account.

In order to understand the shortcomings of the theory, the author uses the People’s Republic of China (PRC) as a case study and employs Harry Eckstein’s *crucial case-study approach* to test the Realism’s assumptions with the empirical findings. Despite owning the world’s most ambitious cyber surveillance agenda, the PRC is also host to one of the highest cyber-theft cases as well as the most malware-infected computers. The PRC’s ambitious goal of *cybersovereignty* and its surveillance mechanism under the title of “secure and controllable” Internet have been creating pitfalls to individual cybersecurity. By creating more vulnerabilities that malicious actors can abuse, the Chinese surveillance system might counter-intuitively turn its citizens into open targets for outside cyberattacks.

To show the link between cyber control mechanisms for greater intelligence and individual cybersecurity, the empirical findings are retrieved from four main subjects; *encryption system*, *Green Dam Youth Escort Firewall Software Program*, *pre-installed malware cases*, and *Real-Name Registration System*. Throughout the analysis of these subjects, the central inquiry will be whether the national security framework provides effective protection for individuals in the Chinese cyberspace. Additionally, it will also involve an ontological sub-question whether national security is inherently opposed to individual security in cyberspace, followed by a theoretical discussion of Realism.

Since the mass surveillance at the expense of individual security is not only practiced by authoritarian states anymore, this research will also help us in understanding the implications of the cybersecurity strategies of liberal countries on their citizens. Especially after 9/11, we are often presented with privacy vs security dilemma, but do we really acquire more security in exchange of our privacy? If the national security-centric practices inflict harm on individual security, should we reconsider the *object* of security? The realist precursor Thomas Hobbes positions the modern conceptualization of sovereignty at the heart of the security discussion coming along with the social contract between state and citizen. Hobbes’ contractual construction of state sovereignty posited the role of security guarantor of its people as the raison d’état of state. Citizens surrender their liberty in exchange for protection. However, if the state practices in the cybersecurity are carried out at the expense of the individual security, should the contract be renewed?

How does it relate to CCRC research themes?
Research Relevance to the Theme 2

In his seminal work *Leviathan*, Thomas Hobbes depicts the state of nature in his investigations into the earlier times of the human being. He suggests the state of nature was a lawless, violent place in which people had to struggle with the risks they are surrounded with, and live in constant fear. In order to avoid the threats and risks to their security, individuals conceded to give up some of their rights and freedoms and handed them to a superior political authority, which will guarantee the agreement amongst people and hence their security. Such a scenario became an increasingly popular theme that we are accustomed to seeing in science fiction literature taking place in cyberpunk and post-apocalyptic stories. The primitive condition of state of nature haunted by chaos became a prospect of future for the world we live in.

Today, with the deeper integration of ICTs (information and communication technologies) in our daily life, we are facing more risks and vulnerabilities in the technology surrounding us. Yet, to address these risks, would a mere social contract be enough? In fact, would the very governmental bodies we hope that could save us from the chaos start aggravating these vulnerabilities? This research examines such security risks and vulnerabilities in cyberspace awaiting the netizens of the global network, and it is connected to the second research theme of CCRC; “Virtual and Physical Infrastructural Security in a Connected Age”. In the cyber domain, where equivocal nature of cybersecurity is wavering between a public good and private good, protection of individual security becomes more problematic. However, with the increasing number of international cybersecurity attacks and cyber-espionage activities, national security became the hot topic in the cybersecurity agenda and individuals are mostly left in the shadow of the states.

Inheriting the wisdom from the old paradigms of warfare, policymakers are applying the national security framework to the cyber domain. Yet, this research aims to show that the lessons taken from the conduct of war on a territorial setting might not yield the same results for the globally connected cyberspace. In order to demonstrate the shortcomings of an orthodox national security strategy, the research will be using the People’s Republic of China’s cybersecurity strategy as a case study. In the 2nd theme of the CCRC, it is stated that “cyber civilization is becoming ever more vulnerable to cyber threats”. In order to address these vulnerabilities in the individual level more effectively and protect the netizens of the cyber civilization, this research will present the vulnerabilities created by the national cybersecurity strategy of China and finally call for a paradigm shift in the way states perceive security in cyberspace.