Chapter 15
China's Cyber Security Policy and the Democratic World

Irakli Kervalishvili
Georgian Technical University, Georgia

ABSTRACT

In the modern world, transferring data into digital format, electronic commerce, social media, and receiving public services through online platforms are very relevant. The more states become dependent on cyberspace, the more reasons and means hostile actors have for cyberattacks, stealing and distorting information, and paralyzing systems. We must keep in mind that cyber security is not only about computer programming and information technology. Cyber security is a vital part of national security, as cyber-attacks target people, public opinion, and public and business sectors. China is indeed quite an aggressive cyber actor, but there is another, non-democratic state that has much greater economic-technological resources, ambition, and aspiration for cyber expansionism.

INTRODUCTION. THE NATIONAL CYBER SECURITY STRATEGY AND THE EMERGENCE OF HARD DIGITAL FRONTIERS

The development of the Internet, and the innovation that is associated with it, have been facilitated by an environment that has been relatively free from control. Unfortunately, however, as a result of deep integration into the social framework, the Internet has become a potential tool for influencing geopolitical conflicts, including interference in the internal affairs of other states, undermining national security, destabilizing financial infrastructure, and attacking critical infrastructure. While states derive social and economic benefits from the Internet, they fear the threat it poses to national security. In response to these threats, countries are beginning to tighten their Internet borders and develop their cyber weapons not only as a tool for deterrence but also to apply pressure during conflicts. The potential downside of such state-by-state regulation is slowing down the innovation process that the Internet has traditionally spurred and limiting the freedom of speech that has contributed to social inclusion in society. On the other hand, innovation and freedom cannot flourish in a chaotic environment with rampant crime and a

DOI: 10.4018/978-1-6684-8846-1.ch015

lack of rules, norms, and ethics. With this in mind, national policymakers face the challenge of finding a balance between regulation and the potential chaos of the Internet, while at the same time promoting the development of freedoms. In trying to strike such a balance in the national interest, cyberspace boundaries play an important role alongside international efforts to build confidence in cyberspace and slow down Internet fragmentation.

The sophistication and effectiveness of cyberattacks have steadily increased since the first Morris worm cyberattack in 1988 and have recently become a key part of the national defense strategies of several countries. Cyberspace is now considered a separate domain of conflict along with land, sea, air, and space, clearly defined in the military doctrines of the world's most powerful states, including China. Each country is strengthening its defenses while at the same time working furiously to develop cyber weapons and testing the cyber defenses of other countries. Cyber attacks have already been used to supplement military interventions in response to the policies and actions of other countries and to interfere in the elections of other countries. The ferocious cyber arms race shows no signs of abating. States now face a dilemma: whether to work together to de-escalate the cyber arms race and allow the Internet to thrive unhindered or to build boundaries on the Internet and threaten its growth and evolution.

Several attempts have been made to work out a treaty to curb the growth of cyber weapons; however, the lack of attribution, the increase in vulnerabilities, and the escalation of economic rivalry between states make reaching a consensus on these treaties very difficult. Although the attribution of cyber incidents is constantly improving due to improved analytic technologies, the activities of states in the development of cyber weapons are still undercover. From a game theory perspective, the situation suggests that each state is trying to maximize its cyber arsenal in the belief that other countries are also maximizing their efforts to develop cyber arsenals. The earliest use of cyber weapons took place in conflicts between Russia and the former Soviet republics of Georgia and Estonia. In these cases, the attacks were used for media propaganda, website corruption, and so on. Over time, however, cyberattacks have become more sophisticated, targeted, and dangerous. Likewise, more nation-states are turning to cyberattacks and starting to use cyberattacks to achieve their geopolitical goals.

Expanding the Vulnerability Landscape

The top three innovations of this decade are the smart grid, connected vehicles, and human implantable devices. All three of these innovations will radically change society in many ways, some of which are currently hard to even imagine. The discussions related to cyber-physical systems are very timely, as their impact on the future of society will be enormous.

We create networks of three classes: monolithic networks of devices and sensors in the power system; millions of ad hawk networks in the transport network; and a huge personal network of wearable devices. Each of these networks has many calls. Much of the discussion here is related to the static networks of cyber-physical systems such as industrial control, electricity, and gas distribution. The ever-changing systems of connected vehicles and wearable devices have not yet been considered. Let's take a closer look at the evolution of the Internet of Things (IoT).

Gartner estimates that 21 billion IoT devices will be in use in the next few years. Cisco estimates that there will be more than 50 billion such devices, and Intel goes even further, predicting the use of 200 billion IoT devices (Eddy, 2015). Indeed, we are just beginning to understand the potential and possibilities of the Internet of Things. The list of possible benefits expands as they come in - efficiency gains, process optimization, and cost reductions are the most important ones that will take place for any