Chapter 2
The Role of State Actors in Cybersecurity:
Can State Actors Find Their Role in Cyberspace?

Seunghwan Yeo
Virtual Research Associates, Inc., USA

Amanda Sue Birch
The Fletcher School, Tufts University, USA

Hans Ingvar Jörgen Bengtsson
The Fletcher School, Tufts University, USA

ABSTRACT

The growing impact of cyber activities across political, social, economic, and military domains makes cyberspace an essential dimension of human security. The role of states in cybersecurity requires a different approach from conventional security models because the classic concept of statehood comprising territory, population, and nationality is absent in cyberspace. Additionally, security issues in cyberspace are not always between or among states and they frequently lack clear attribution and motivation. This new paradigm of individual and knowledge-centered cyberpower means state actors no longer fully monopolize violence, per Max Weber's definition of a state. Furthermore, unlike the interstate dynamic between nuclear powers, cyber warfare is offense-dominant due to the absence of efficient deterrence. The immediate security concern should be addressing the protection of cybercitizens across borders. Therefore, state actors must cooperate to establish a multilateral uninterrupted network in order to safeguard the cyber commons via mutually assured collective cybersecurity.

INTRODUCTION

Cybersecurity consists of measures to protect the operations of a computer system or the integrity of its data from hostile action. (Kello, 2013, p. 18)

Can state actors fulfill traditional security roles in cyberspace? This paper explores national and international cybersecurity by examining the feasibility of securing the power of a state actor in cyberspace.

DOI: 10.4018/978-1-5225-7912-0.ch002

The analysis includes examining differences between classical security and cybersecurity and explores why nation states' attempts to command and control the digital commons so far have not been successful.

The role of government in the cyber realm is important but still elusive. Conventional military strategies and tactics do not adapt well to the constantly evolving cyber domain. Furthermore, cyber anxiety and cyber threats entice governments to spend more to improve cybersecurity. Worldwide spending on cybersecurity for both the public and private sectors is projected to reach nearly $80 billion dollars in 2015 (Ranger, 2015; Gatner Inc., 2015). But the quest for security is at odds with the underlying purposes of cyber technology. The purpose of most cyber innovations is to improve convenience and productivity, but preserving this convenience via overreaching cybersecurity measures may impose inconveniences and decrease productivity. Finding the right balance point is both elusive and essential.

The objective of this paper is to further explore the role of state actors in cyberspace in three main sections. The first section defines actors in cyberspace. The second section describes the rise of a new security paradigm, explores the resulting cybersecurity framework, and identifies the nature of cyber-power. The third section addresses why state actors find it difficult to take the role of peacekeepers in cyberspace. Finally, case studies illustrate historical state intervention in cybersecurity to explain why the classic state role is not effective in cyberspace.

BACKGROUND

Two terms that will be used throughout this paper merit mention up front. The term 'actor' in this paper only refers to cyber actors in a technical security sense. This definition excludes individuals with broad social media impacts on platforms such as Twitter and YouTube who do not have technical computer programming skills. The second term to mention up front is 'cyberspace.' This paper uses Singer's definition: "the realm of computer networks and users behind them." (Singer & Friedman, 2014, p.13). This includes all networked systems that support improved human activities ranging from closed military networks to internal networks and to the World Wide Web (Kello, 2013, p.17).

Networks are made up of people connected beyond spatiotemporal restrictions. The number of Internet users was nearly three billion worldwide by the end of 2014 according to The International Telecommunications Union (ITU) (ITU, 2014). In the 1970s, only large corporations, governments, and organizations could have networked computers and only a few authorized operators could even touch those computers. This lasted until the personal computer (PC) evolution in the 1980s. Nowadays, palm-sized smartphones have more computing power than the mainframes in the late 1980s. No one at the time could have predicted that computers would be as prevalent as they are today.

Most people can access the Internet easily but few users understand what the threats are, what to defend, and how to defend. Only security providers exclusively control both collective and personal cyber defense. As the evolution of smart devices continues, the architecture becomes more complex and users therefore tend to rely on cyber specialists. In fact, Microsoft Windows users in the late 1990s and early 2000s had higher administration privileges on their machines than smart device users have today. Operating system manufacturers like Apple and Google no longer allow device owners to be super-users with powerful rights or permissions known as root, administrator, admin, or supervisor. To meet users' desires for convenience, users decide voluntarily to become consumers of the predefined user interface by giving up rights to access the system core. Users legitimately gain device ownership by purchase, but the owners no longer have administrative access to their devices and are therefore consumers or