State-led Back-scratching Alliance in Cyber Warfare

China's Strategies in Sino-American Cyber Warfare
in the Post-Cold War Era

SeulAh Choi and **Gon Namkung**
(Ewha Womans University)

〈CONTENTS〉

· **Key words :** cyber warfare, non-state actors, state capacity, relations between state and society, Sino-American cyber warfare, role of the state

【ABSTRACT】

The confluence of the end of the Cold War, globalization, and the information revolution created a new space not only for the emergence of cyber warfare but for non-state actors as major participants. This growing phenomenon raises questions the relationship between the state and society in cyber warfare. Whether traditional capacity of the state has declined is debatable; however, private actors have gradually been empowered. This paper argues that cyber warfare shows a new or at least novel type of the state-society relationship, or state-led back-scratching alliance. The state, continuing to be resilient, has redefined and redeployed its roles of mobilizing private actors on the one hand while regulating them on the other. Depending on the state's strategic

The Korean Journal of International Studies, Vol. 11, No. 2 (December 2013), 295-325.

interests, the state can choose and combine one of these strategies in cyber warfare, in the form of selective censorship, unofficial condoning, coercive collaboration and reciprocal partnership. This paper analyzes thirteen cases of China's cyber warfare against the United States to examine in detail how the state has redefined its role in cyber warfare and to evaluate whether redeployment involves more or less state capacity.

Ⅰ. Introduction

In April 2001, an American surveillance plane conducted a routine mission over China to gain valuable electronic intelligence that could not be obtained by satellites orbiting in space. The Chinese government decided to send jet fighters to follow and intercept the surveillance plane. A Chinese F-8 fighter plane and an American EP-3 surveillance plane collided in mid-air. The American plane made an emergency landing on Hainan Island in China, while the Chinese plane, along with its pilot Wang Wei, lost control and was lost at sea. The two countries blamed each other publicly for causing the collision.[1)]

Following the collision, the tech-savvy American citizens were outraged at the detention of the American crew and plane and expressed their fury over the Internet by defacing approximately sixty-five Chinese websites.[2)] In response, Chinese civilian hacking groups, such as the Honker Union of China and the Chinese Red Guest, declared war against the United States and pronounced the week of May 1-May 7, 2001, to be "Hack the USA" week.[3)]

---

1) Shirley A. Kan *et al.*, *China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications*, Congressional Research Service, Library of Congress, RL30946 (10 October 2010), pp. 1-7.

2) Malcolm Beith, "The U.S.-China Hacker Conflict," *Newsweek* (6 May 2001), available at <http://www.newsweek.com/us-china-hacker-conflict-152877> (accessed on 30 March 2012).

3) Rose Tang, "China warns of massive hack attacks," *CNN* (3 May 2001), available at <http://edition.cnn.com/2001/WORLD/asiapcf/east/05/03/china.hack/index.html?_s=PM:asiapcf> (accessed on 16 August 2012).

They attacked more than 1,000 US websites, including those belonging to the White House, the US Air Force and the Department of Energy. The sites were either shut down or had their contents replaced with images of China's red flag, tributes to the dead Chinese pilot, or messages such as "Beat Down the Imperialism of America" and other anti-American or pro-Chinese slogans.[4] This incident is generally referred to as the first Sino-American cyber warfare in the post-Cold War era.[5]

The civilian individuals or hacker groups such as the Honker Union of China or PoisonBox in the United States declared war themselves and voluntarily played a key role as major actors in this cyber warfare. Given that traditional warfare is waged between states, by public militaries, it is noteworthy that societal actors have become the major players in cyber warfare, not only as challengers but also as providers of security. Non-state actors such as individuals, organizations, and private companies can create and acquire the electronic means to attack and consequently the ability to disrupt critical infrastructures, causing tremendous impacts on a society as a whole. Although the major impacts in the incident mentioned above were limited to the symbolic effects of humiliation, cyberattacks such as denial-of-service attacks, or infecting with viruses or worms against an adversary's critical infrastructures can certainly have substantial consequences including huge financial losses or even the paralysis of the military system.

As non-state actors have empowered themselves with substantial disruptive power, scholars and national security policy makers argue that public-private partnerships are inevitable in cyber warfare.[6] One of the primary reasons of such partnerships is that states lack expertise and skills to wage cyber

---

4) *Ibid.*; Elizabeth Becker, "F.B.I. Warns That Chinese May Disrupt U.S. Web Sites," *New York Times* (28 April 2001), available at <http://www.nytimes.com/2001/04/28/world/fbi-warns-that-chinese-may-disrupt-us-web-sites.html> (accessed on 20 April 2013).

5) Craig S. Smith, "May 6-12, The First World Hacker War," *New York Times* (13 May 2001), available at <http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html> (accessed on 16 August 2012).

6) Alexander Kilmburg, "Mobilising Cyber Power," *Survival* 53-1 (February-March 2011), pp. 43-44; John Arquilla, "Thinking About New Security Paradigms," *Contemporary Security Policy* 24-1 (October 2003), pp. 216-219; Emily O. Goldman, "Introduction: Security in the Information Technology Age," *Contemporary Security Policy* 24-1 (October 2003), pp. 9-10; Paul Cornish *et al.*, *On Cyber Warfare* (London: Chatham House, Royal Institute of International Affairs, November 2010), pp. 21-23.

warfare, thus need private actors equipped with high-technology and knowledge. Emphasizing public and private partnerships, most of the previous research studies have focused on the influence of empowered non-state actors by comparison with that of the state[7]; some of these studies even assert that cyber warfare challenges the conventional view of the state as the supreme player in the international system and its conclusive influence on warfare.[8] While some maintain the primacy of states in cyber warfare,[9] their rationale—such as the specific role or strategies of states—is unconvincing.

Assuming the importance of non-state actors as well as public-private partnerships in cyber warfare, This article asks how state-society relations appear in cyber warfare. Simply put, how does the state encourage private actors to be involved in waging cyber warfare? How could public-private partnerships in cyber warfare be possible? Four strategies of the state—that is, *selective censorship*, *coercive collaboration*, *unofficial condoning*, and *reciprocal partnership*—offer illumination. Even though non-state actors have become more and more important, they are likely to exercise and demonstrate their capacity only under certain circumstances, which depend on the state's strategies of cyber warfare. States do not merely back up societal actors by simply retreating; rather, they adapt and redeploy to mobilize private actors on the one hand while regulating them on the other by adopting these options. Everything depends on the constellation of state interests.

Understanding state-society relations in cyber warfare is paramount not only on the level of national security policy but also security studies.[10] On a

---

7) Johan Eriksson and Giampiero Giacomello, "The Information Revolutions, Security, and International Relations: (IR) Relevant Theory?" *International Political Science Review* 27-3 (July 2006), p. 222. Several other studies point to this same conclusion. See, Jeffrey Carr, *Inside Cyber Warfare* (O'Reilly Media Inc., 2009), pp. 15-29; Nazli Choucri, *Cyberpolitics in International Relations* (MIT Press, 2012), pp. 5-12; Walter S. Baer,"Rewarding IT Security in the Marketplace," *Contemporary Security Policy* 24-1 (October 2003), pp. 190-192; Natasha Solce, "The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force," *Albany Law Journal of Science and Technology* 18-1 (September 2008), pp. 303-304; Blaise Cronin and Holly Crawford, "Information Warfare: Its Application in Military and Civilian Contexts," *The Information Society* 15-4 (July 1999), pp. 257-262.

8) Victor D. Cha, "Globalization and the Study of International Security," *Journal of Peace Research* 37-3 (May 2000), pp. 391-403.

9) Johan Eriksson and Giampiero Giacomello, *op. cit.*, p. 226.

basic level, the new relationships can be a barometer of a state's cyber capabilities because one dimension of a state's cyber capabilities is the integral extent of the private sector.[11] In addition, understanding these relationships can offer a basis to examine further research agendas such as the linkages between the patterns of civil-military relations and the inclination to wage cyber warfare:[12] Is the state more likely to carry out cyber attacks if its civilians participated in military operations? If so, then to what extent? Or does civilian involvement in cyber warfare restrict commanders to conduct more prudent commands by conforming to public opinion?

States' strategies in cyber warfare also can provide valuable implications for two groups of security studies specialists: while state-centric theorists find cyberspace-related issues difficult to address due to the plurality of empowered non-state actors in cyberspace, specialists who seek to widen the discipline are less encumbered since they accept a broader national security concept encompassing a host of non-state actors as major actors. However, if the states' roles are found to be paramount in cyber warfare, the latter group will need to reassess the relationship between states and societal actors.[13]

I review previous research studies about the influence of cyber warfare on the relationship between state and society and distinguish the state's different strategies of mobilizing the private sector on the one hand while regulating

---

10) According to Klimburg, a state's cyber power consists of three parts: "coordination of operational and policy aspects across governmental structures, coherency of policy through international alliances and legal frameworks, and cooperation of non-state cyber actors." These are respectively referred to as "integrated governmental capability," "integrated government capability," and "integrated national capability" Alexander Klimburg, *op. cit.*, p. 43.

11) When we think of state-society relations in general, it is complicated to distinguish between the two in clear-cut way because state and society are different. However, at the same time, they are not totally separate. In the context of cyber warfare, in this paper, state, as supreme provider and challenger of cyber security, refers to officials and physical institutions that make, implement strategies that are applied across the whole society. Private sector is the summary term for civilians or groups in a state sharing political and economic circumstances and environment. In this paper, the private sector could be categorized as three distinctive non-state actors in cyber warfare context: individual hackers or hacker groups, commercial firms and academia.

12) Timothy J. Junio, "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate," *Journal of Strategic Studies* 36-1 (February 2013), pp. 125-126.

13) Daniel W. Drezner, "The Global Governance of the Internet: Bringing the State Back In," *Political Science Quarterly* 119-3 (Spring 2004), p. 479.

the private sector on the other in cyber warfare, depending on the state's strategic interests. I then empirically analyze 13 cases of China's cyber warfare against the United States to examine in detail how the state has redefined its role in cyber warfare and to evaluate whether the redeployment involves more or less state capacity.[14]

Ⅱ. The Influence of Cyber Warfare on the Relationship between State and Society

How does cyber warfare affect the relationship between state and non-state actors? Despite the plethora of literature on cyber warfare, relatively few works focus on this relationship. When scholars analyze actors in cyber warfare in terms of theoretically oriented security studies, two contentious positions arise: those of traditionalists and those of wideners of security.[15] The former usually come from the realist camp, whose primary approach is state-centric. Even in this new kind of conflict, they maintain the traditional security concept, which is centered on the nation-state and interstate war. By insisting on a narrow military definition of security, traditionalists would deny that societal actors might wield any degree of power, maintaining that there is no need to extend the concept of security even in light of previous forms of unconventional challenges, such as globalization, supernationalism,

14) We are aware that the term 'cyber war' is ambiguous and controversial due to the lack of conceptual basis on cyber warfare. There is a debate whether cyberattacks can constitute an act of war per se. We are in agreement with John Stone's stance that cyberattacks can constitute an act of war, meeting particular characteristics of war such as those motivated in political aspects, instrumental in character, but not necessarily lethal. Assuming cyber war is feasible, this article accepts Timothy Junio's definition of cyber war as "a coercive act involving computer network attacks." According to him, 'network attack' means "information is disrupted, degraded, or destroyed" and 'coercive' refers to "using force to change or preserve a political status quo." However, we have chosen to use 'warfare' rather than 'war' since warfare is a more open-ended term and practical in researching and examining activities in such an underexplored field. For discussion on the debate, see Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35-1 (February 2012), pp. 5-32; John Stone, "Cyber War Will Take Place," *Journal of Strategic Studies* 36-1 (November 2012), pp. 101-108. For the definitions, see Timothy J. Junio, *op. cit.*, p. 126; Paul Cornish *et al., op. cit.*, pp. 1-4.

15) *Ibid.*, pp. 227-235.

and complex independence. Given that these previous challenges have the emergence of empowered societal actors in common, traditionalists view these trends as epiphenomena that cannot undermine the anarchic system in international relations. In this vein, they have the potential to show insistence on the primacy of state even in cyber warfare.[16)]

On the other hand, the wideners of security largely come from a mix of liberalist and critical theorist camps.[17)] They assume that the conventional state-centric approach is insufficient to deal with the challenges posed by cyber warfare. Their main claim is that the traditional security concept should be extended to include not only other new security threats but also a range of new players such as nongovernmental organizations, commercial firms, and individuals. Although some of them admit that states are the central actors, they differ from traditionalists in that they argue that states are not by any means the only players with significant roles in waging cyber warfare.[18)]

Emphasizing the importance of non-state actors with substantial disruptive power, wideners of security provide valuable insights into cyber warfare. Their primary rationales to justify the claim that societal actors are major players in cyber warfare are the necessity of public and private partnerships in cyber warfare and a blurring of the distinction between civil and military spheres in its targets.[19)] These issues are largely overlapping and interrelated. First, public and private partnerships are inevitable when governments realized that they cannot provide enough skills or technologies when waging cyber warfare, thus needing civilian hackers or experts who possess high technology and knowledge.[20)] Cyber warfare can be understood in terms of competition for information dominance, the key factor to defeat opponents. Therefore, military forces and conventional data fights are no longer effective strategies in cyber warfare; rather, high-technology specialists and their relevant companies are indispensable factors.

Second, the major potential targets of cyber warfare are the nation's critical infrastructures as the groundwork of a state, and many of these are usually

---

16) *Ibid.*, pp. 228-229.
17) *Ibid.*, p. 227.
18) *Ibid.*, pp. 229-235.
19) *Ibid.*, p. 231.
20) Jeffrey Carr, *op. cit.*, pp. 15-29; Natasha Solce, *op. cit.*, pp. 303-304; Paul Cornish *et al., op. cit.*, pp. 21-23.

owned and operated by the private sector.[21] For example, in the United States, the private sector own and operate about 85% of the state's critical infrastructures.[22] One of the reasons a nation's critical infrastructures become potential targets is due to the catastrophic impacts on society when they are attacked, spreading from the military to business and, from the national level to the societal or individual level. In particular, civilian telecom networks, as one of the nation's critical infrastructures, are the major potential targets because they are the backbone of the intelligence capabilities running the command and control of the state. In this vein, the distinction between civil and military spheres becomes blurred in terms of targets in cyber warfare; thus, it is necessary and even desirable for the state to depend on civilian participation and resources.

In May 1998, the White House issued Presidential Decision Directive (PDD) 63 to build a framework for critical infrastructure protection based on the report of the President's Commission on Critical Infrastructure Protection (PCCIP).[23] One of the main goals of this framework is to "seek the voluntary participation of private industry to meet common goals for protecting our critical systems through public-private partnerships."[24] Also, the National Strategy to Secure Cyberspace developed by the President's Critical Infrastructure Protection Board in September 2002 in the United States conceded that the "government alone cannot secure cyberspace."[25] As a result, Microsoft has voluntarily created a special Security Response Center and collaborated with the Department of Defense (DOD), so that together

---

21) Critical infrastructures largely involve "agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping." Gregory J. Rattray, *Strategic Warfare in Cyberspace* (MIT Press, 2001), pp. 17-22; Matt Bishop and Emily O. Goldman, "The Strategy and Tactics of Information Warfare," *Contemporary Security Policy* 24-1 (June 2010), pp. 119-120; Jeffrey Carr, *op. cit.*, p. 8; Natasha Solce, *op. cit.*, p. 303; Paul Cornish *et al., op. cit.*, p. 22.

22) The Department of Homeland Security, "Critical Infrastructure Sector Partnerships," available at <https://www.dhs.gov/critical-infrastructure-sector-partnerships> (accessed on 20 September 2013).

23) The White House, *Fact Sheet: Protecting America's Critical Infrastructure: PDD 63* (22 May 1998), available at <http://www.fas.org/irp/offdocs/pdd-63.htm> (accessed on 20 September 2013).

24) *Ibid.*

25) The White House, *The National Strategy to Secure Cyberspace* (February 2003), pp. 2-11.

they could catch and resolve any software vulnerabilities as well as improve the DOD's new products.[26] The company also has focused on training its developers in "secure coding practices" for cyber security.[27]

Due to the issues of public-private partnerships and the integration and interdependence between the civilian and military spheres in terms of targets, previous researchers have begun to doubt the conventional capacity of the state[28]; some of them even assert that the state is no longer the primary actor of first and last resort in cyber warfare.[29] Further, those researchers who assert states' resilience as central actors rarely provide the concrete roles or strategies of states in cyber warfare.

However, empowered private actors in cyberspace do not necessarily mean the decline of state capacity in cyber warfare. Previous researches generally assume that states and the private sector have a zero-sum relationship, as if an actor's gain of utility is exactly balanced by the losses of the utility of the other players. Due to the unwarranted assumption, they cannot see that there is no logical contradiction that explains the concurrent relationship between the rise of the private sector and the state's greater role. Thus they fail to consider a *condoning strategy* or *coercive collaboration* as a conscious state choice and thereby misinterpret the state's role in cyber warfare. Furthermore, when wideners pursue ambiguous concepts represented by human security, they fail to provide empirical support or offer reasonable grounds for doing so. This approach produces results with only middling analytical and explanatory power and limited policy implications. In addition, realists need to widen their perspective of security in that cyber threats can potently affect the security of states and include national security threats themselves, beyond merely economic and psychological dimensions.[30] Traditionalists also need to establish why their views of the supremacy of states are more applicable than their counterargument.

---

26) Natasha Solce, *op. cit.*, p. 304.
27) Walter S. Baer, *op. cit.*, p. 205.
28) Johan Eriksson and Giampiero Giacomello, *op. cit.*, p. 222.
29) Victor Cha, *op. cit.*, pp. 392-393.
30) Amit Sharma, "Cyber Wars: A Paradigm Shift from Means to Ends," *Strategic Analysis* 34-1 (February 2010), pp. 72-73.

Ⅲ. State's Back-scratching Strategies in Cyber Warfare

States continue to be the primary players in cyber warfare, maintaining their role as the principal providers and challengers of security. This is attributed to the fact that the state does not merely withdraw when supporting and serving societal actors such as individual hackers, nongovernmental organizations, and commercial firms. Rather, the state has transformed and redeployed its dual roles to adapt to this new national security threat, remaining resilient—mobilizing or forging partnership with private actors on the one hand while regulating them on the other depending on the state's strategic interests.

The main reason that this dual role of the state is necessary in cyber warfare to protect national security is that tensions inevitably exist between the state and societal actors. In some cases, it is beneficial for non-state actors to collaborate voluntarily with the government to augment national security. For example, private companies' partnership with the government makes it easier for them to report cyberattacks because they have less need to fear financial losses than if they were working independently.[31] It is also possible that working with the government will make commercial firms less prone to being attacked and being capable in much more efficient problem solving. The customer's expectation toward the commercial organizations can also increase when they are classified as part of critical national infrastructure.[32]

However, commercial organizations or individual hackers more often have fewer incentives to partner with the government because motivations and goals between the private and public sector cannot always be aligned. The loyalty of societal actors is primarily to themselves, their shareholders, and their boards of directors rather than to the state, and their primary goal is to fulfill personal interests or make profits rather than to protect national security.[33] Given that a series of practices for cyber security impose financial and operational costs on both individuals and commercial firms, actors in the private sector are unlikely to feel the need to spend their funds to deal with a national security problem that has not proven to be a disruptive risk.

As a leading example of such partnerships, the National Coordinating

31) Natasha Solce, *op. cit.*, p. 304.
32) Paul Cornish *et al.*, *op. cit.*, pp. 22-23.
33) *Ibid.*, pp. 22-23.

Center for Telecommunications (NCC) in the United States has tried to cooperate with both the federal and the private sector to perform an essential role for US cyber security. Since the White House designated NCC as the Information Sharing and Analysis Center (ISAC) for Telecommunications in January 2000, twenty-four Federal Government agencies and more than fifty communications and IT commercial firms have worked together in the ISAC. They routinely share information pertaining to cyber security threats, vulnerabilities, events, and solutions to back up the NCC's national security missions.[34)]

However, today many companies in the United States are concerned about the potential drawbacks and are thus hesitant to join ISACs.[35)] One of the reasons for this is that commercial firms are likely to fear disclosure of cyberattacks to the public, and the public can access these agencies' records and information under the Freedom of Information Act (FOIA) when they share such information with the government.[36)] If customers become aware of previous cyberattacks against a company that possesses their sensitive information, it can lead to liability lawsuits against the firms that volunteer such information. In addition, legal responsibilities stemming from disclosing breaches or vulnerabilities related to their products or service, in addition to growing antitrust scrutiny related to sharing information and data with other companies, could be further disincentives for societal actors to coordinate and cooperate with the government.[37)] This suggests that the incentives for coordinating and cooperating with the government in the private sector may not readily exceed the negative effects of doing so. Thus it is necessary for the private sector to guarantee that the incentives for collaborating with the government must exceed its downsides of doing so if public-private partnerships in cyber warfare can be established and run effectively.

For these reasons, states need specific mechanisms such as incentives or

---

34) The Department of Homeland Security, "National Coordination Center for Telecommunications," available at <http://www.dhs.gov/national-coordinating-center-telecommunications> (accessed on 21 September 2013).

35) Walter S. Baer, *op. cit.*, pp. 190-191.

36) *Ibid.*, p. 191; Gina Marie Stevens, *Homeland Security Act of 2002: Critical Infrastructure Information Act*, Congressional Research Service, Library of Congress, RL 31762 (February 2003), pp. 1-3.

37) Walter S. Baer, *op. cit.*, p. 191.

regulations to mobilize the private sector for waging cyber warfare on behalf of the state. At the same time, in cases where that individuals or nongovernmental organizations carry out cyberattacks voluntarily, or once societal actors are mobilized regardless of their motivations, the state also needs appropriate means to control them in a manner that meets the state's strategic interests. In this context, the first role of the state in cyber warfare is forging partnerships or collaborating with and mobilizing private actors. This involves the state's "infrastructural power," once regarded as one of the state capacities "to forge partnerships with powerful groups in society, to harness the capital and resources of the people on behalf of a jointly defined project."[38] The state has used various methods to rally private actors around the flag and make them perform expected actions whether these come from the state's coercion or incentives, if without, they would not have considered.

The other role of the state is regulating or controlling private actors in order to meet the state's strategic interests. This involves the state's "authoritative power," which is also considered as one of the state capacities to "formulate an agenda and act independently with little constraint, even in the face of substantial societal opposition."[39] This capacity is especially necessary when interests of individuals or commercial organizations, such as the self-satisfaction or economic gains associated with cyber warfare, run counter to those of the government. For example, patriot hackers carry out cyberattacks voluntarily based on nationalism, destroying large volumes of data on the targeted adversary's website. In all likelihood, their voluntary actions may negate the state's crafted operations in cyber warfare, defame the state's reputation in international society or exacerbate diplomatic relations with the attacked country. The actions of societal players are not always aligned with the state's interests; thus specific means are needed to control them in the state's intended ways.

This discussion leads to the following question: what forms do the state's

---

38) Since the characteristic of state capacity has been studied in areas outside of security studies, we draw on the available literature in political economy. According to Jonah Levy, state capacity can be understood in one of two ways: "authoritative power" and "infrastructural power." We accept these distinctions of state capacity to achieve better understanding of its role in cyber warfare. Jonah D. Levy, *The State after Statism* (Cambridge, MA: Harvard University Press, 2006), pp. 382-391.

39) *Ibid.*

strategies take in order to serve its role of mobilizing non-state actors on the one hand while regulating them on the other? In order to capture the state's redefined role, this paper has developed a typology of the different kinds of state strategies used in cyber warfare, which are based on the state's capacities. This article also assumes the state needs specific mechanisms such as incentives and regulations to implement its strategies with private actors. The following figure is a simplification of the government's range of strategies; although it may be difficult to clarify state capacity in a clear-cut way, it can be a good basis for understanding different states' strategies.

Table 1. *State Strategies in Cyber Warfare*

State Strategies in Cyber Warfare	Form of State Capacity	
	Authoritative Power	**Infrastructural Power**
Regulation	Ⅰ Selective Censorship	Ⅱ Coercive Collaboration
Incentive	Ⅲ Unofficial Condoning	Ⅳ Reciprocal Partnership

Selective censorship generally occurs when the private player's voluntary cyber actions prevent or conflict with the state's strategic interests. If cyberattacks of civilian hackers or organizations are likely to be identified, thus resulting in harm to the state's reputation for not controlling them and spilling over into diplomatic conflicts, the state imposes strict censorship, through means such as fines or imprisonment, on the non-state actors to make them stop or adjust their actions. In this sense, the state uses its authoritative capacity to determine how the power of civilian hackers or groups can actually be used. For example, in February 2003 when relations between the United States and Iraq were under high-tension and there existed increasing cyberattacks on both sides, the US government announced that the state did not condone even patriotic cyberattacks against Iraqi computer systems regardless of the motivations and that felony punishment could be imposed for committing such acts.[40] Given that this announcement came less than a

40) William Jackson, "NIPC to hackers: Don't try this at home," *GCN* (14 February 2003), available at <http://gcn.com/articles/2003/02/14/nipc-to-hackers-dont-try-this-at-home.aspx> (accessed on10 April 2013).

week after the George W. Bush administration had signed a secret order to allow the government to develop guidelines for launching cyberattacks and the government had overtly mentioned that "In this and other ways, patriotic hackers risk becoming tools of their enemy,"[41] it seems clear that the government recognized that actions of individual hackers or groups at that time could play a negative role in satisfying the state's strategic interests.

Coercive collaboration typically occurs when the state mobilizes and coerces the private sector to collaborate with the government. For example, the Chinese government shut down the Patriot Hackers-Black Base website and arrested its members in February 2006. The group members, however, were released on the condition that they focus their effort on training people for the government and work with the government to improve the state's network security.[42] As another example, in Israel in 2010, the government forced thousands of civilian hackers to choose either to go to jail or do military service in Unit 8200, the largest unit in the Israel Defense Forces, being suspected of developing the Stuxnet worm and comparable in its function to the United States' National Security Agency. Most of the hackers chose the latter option.[43] In such situations, hacker organizations or technological experts would be unlikely to collaborate with the state voluntarily if not for the state's coercion.

Unofficial condoning takes place when voluntary actions of private actors covertly meet or at least do not hinder the government's strategic interests. Unlike selective censorship, the state consciously leaves the situation as it is. In some forms of cyberattacks (e.g., distributed denial-of-service, which mainly involves forging senders' IP addresses), the attackers or the location of the attacking computers cannot readily be identified unlike other forms of

---

41) David Pace, "Government Warns 'Patriot Hackers' Against Cyber Attacks on Iraqi Interests," *CRN* (12 February 2003), available at <http://www.crn.com/news/security/18821779/government-warns-patriot-hackers-against-cyber-attacks-on-iraqi-interests.htm> (accessed on 10 April 2013).

42) Byran Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepared for the U.S.-China Economic and Security Review Commission* (McLean, VA: Northrop Grumman Corp., 2009), p. 42.

43) Anissa Haddadi, "Unit 8200: Cyber Whizzkids behind Israel's High-Tech 'Secret Weapon'?" *International Business Times* (1 December 2011), available at <http://www.ibtimes.co.uk/articles/259505/20111201/unit-8200-israel-s-high-tech-secret.htm> (accessed on 24 September 2013).

cyberattacks such as network-exploitation.[44] If it is almost impossible to identify the government's involvement, or if the benefits of a cyberattack override its negative effects even if identified, the state can tolerate non-state actors as by adopting a strategy of unofficial condoning. For example, Iranian and Indian officials actually made public records for condoning hackers who operate in the state's interest.[45] In Sino-Japanese cyber warfare in 2000, when the Japanese officials asked the Chinese police to have the websites of known hackers in the Guanxi shut down for attacking Japanese websites, the Chinese authorities responded that they had no intentions of doing so because they were patriotic hackers.[46] Similarly, the Russian government described patriot hackers' cyberattacks against the pro-Chechen websites from 2002 to 2004 as an "expression of their political position, which is worthy of respect" rather than as illegal.[47] All of these actions of condoning are conscious actions of the state.

Reciprocal partnership is formed when the state forges partnerships with societal actors by providing a variety of incentives, which range from simple job offerings, long-term investments, and preferential funding for R&D to information, technology, and communication sectors to removing disadvantages in working with governments.[48] All of these methods are intended to strengthen the incentives for the private sector to cooperate with the government. For example, the defense industrial base in the United States works so closely that even it can take over operation tasks in collection of intelligence. The costs of forging partnerships with these private sectors are borne by the government.[49] In addition, the US government implemented the Critical Infrastructure Information Act of 2002 (CIIA) to exempt "the critical infrastructure information" from disclosure of requirements under the Freedom of Information Act. The purpose of CIIA was to prevent unwillingness of the private sector to share information with the government,

---

44) Alexander Kilmburg, *op. cit.*, pp. 42-43.
45) Myriam Dunn Cavelty *et al.*, *Strategic Trends: Key Developments in Global Affairs* (Zurich: Center for Security Studies, 2012), p. 114.
46) Scott Henderson, "Beijing's Rising Hacker Stars... How Does Mother China React?" *IO Sphere Journal* (Joint Information Operations Warfare Command) (Fall 2008), p. 28.
47) Alxander Kilmburg, *op. cit.*, p. 50.
48) Natasha Solce, *op. cit.*, p. 303.
49) Alxander Kilmburg, *op. cit.*, p. 52.

thus could be the basis for enhancing public-private partnerships.[50]

From these strategies in the typology, we can learn that individual hackers, nongovernmental organizations, and commercial firms can play essential roles in waging cyber warfare, but only under certain constellations of state interests. The role and influence of non-state actors vary widely from quadrant to quadrant depending on the state's strategy. This implies that these four types of state strategies for mobilizing private actors on one hand and regulating them on the other are inherently political and state-constructed action. Furthermore, the state's capabilities in cyber warfare are determined by how well the state penetrates its authoritative and infrastructural power into the private sector. To be specific, the capabilities of the state in cyber warfare can be basically defined as how to organize different combinations of these strategies: *selective censorship*, *unofficial condoning*, *coercive collaboration*, and *reciprocal partnership*. In this vein, the variation of a state's cyber power may have more to do with policy issues rather than with matters of its inherent material or military capabilities. These various options or strategies can give an edge to states in cyber warfare when used in the appropriate combination.

Ⅳ. An Empirical Analysis of China's Cyber Warfare against the United States

The Chinese government has tried to modernize its military program and has transformed its ability to fight cyber warfare since it witnessed the evolution of war from the Gulf War to the Kosovo conflict.[51] Especially for the Chinese authorities, waging cyber warfare is one of the most effective ways to overcome its inferiority in military capabilities compared to the United States.[52] Regarding the actors in cyber warfare, there are two key

50) Gina Marie Stevens, *op. cit.*, pp. 1-3.
51) Vinod Anand, "Chinese Concepts and Capabilities of Information Warfare," *Strategic Analysis* 30-4 (October/December 2006), pp. 781-782; Paul J. Bolt and Carl N. Brenner, "Information Warfare across the Taiwan Strait," *Journal of Contemporary China* 13-38 (February 2004), pp. 132-133.
52) Magnus Hjortdal, "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence," *Journal of Strategic Security* 6-2 (May 2011), p. 6.

entities in the Chinese government: the 3rd and the 4th Departments of the General Staff. The latter is referred to as the Electronic Countermeasures and Radar, which is known for having primary authority over offensive cyber warfare in the People's Liberation Army (the PLA).[53] Unit 61398 at the Shanghai headquarters is generally known as part of the 3rd Department and the base camp for cyber warfare against North American security targets. Unit 61398 is also famous for having hundreds of staff and special fiber-optic communications infrastructure.[54]

The Chinese private sector in cyber warfare can be categorized mainly into three actors: individual hackers or hacker communities, commercial firms, and academia.[55] Chinese hacker communities, such as the Honker Union of China and the Red Hacker Alliance, have from a few thousand to 300,000 members, many of whom are in their young twenties. They publicly regard themselves as patriotic youth dedicated to actively defending their country.[56] Commercial enterprises, especially state-owned telecom enterprises, participate in cyber warfare, providing their technology, specialists, infrastructures, and services.[57] Telecom industries such as Huawei Technologies, China Mobile, and Alcatel Shanghai Bell are notable examples. The government has showered them with a variety of tax incentives, long-term subsidies, and favorable procurement contracts. Through their close ties with the Chinese

---

53) *Ibid.*, p. 11; Bryan Krekel *et al.*, *op. cit.*, p. 25.

54) "A giant cage: Masters of the Cyber-universe," *Economist* (April 2013), pp. 12-13; Mandiant Intelligence Center, *APT1 Exposing One of China's Cyber Espionage Units* (2013), p. 16.

55) In case of China, in particular, it might make little sense to discuss state-society relations as Chinese government has consistently monopolized power and authority against the Chinese society. China has never had a genuine "civil society," which usually refers to individuals or organizations on their own without the state's engagement. However, differentiating civil society and society, referred to as private sector in this article, it assumes that Chinese private sector could be categorized into three actors though they are likely to be influenced by the Chinese government. This article does not focus mainly on whether China would govern and influence Chinese society in the context of cyber warfare, but rather what strategies the Chinese government would take toward Chinese society in order to encourage and allow them to be involved in waging cyber warfare. Lucian W. Pye, "The State and the Individual: An Overview Interpretation," *China Quarterly* 127 (September 1991), pp. 436-466.

56) Scott Henderson, *op. cit.*, pp. 25-26.

57) William T. Hagestad II, *21st Century Chinese Cyber Warfare* (United Kingdom: IT Governance Publishing, 2012), pp. 145-161.

government, they are able to become successful transnational commercial organizations exporting their services and goods all over the world.[58] Universities and research institutes such as Shanghai Jiaotong University, and the National University of Defense Technology have maintained an intimate network with the government by supporting cyber warfare related education or technology.[59]

The Chinese government has traditionally championed the notion of the People's War, which refers to the mobilization of the entire population to struggle on behalf of the nation. It regards cyber warfare as a form of the People's War as well and non-state actors as an integral part of the national capability and an essential component of national security. In this context, the Chinese authorities particularly emphasize the integration of military and civilian roles in cyber warfare.[60] Based on the notion of the People's War and capable private personnel resources, the Chinese government has used its infrastructural power to mobilize societal actors and exercised its

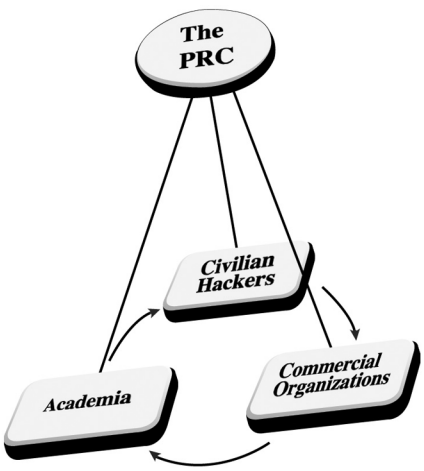

Figure 1. *State-led Back-scratching Alliance: The Chinese Government as the Umbrella*

58) "The state advances," *Economist* (October 2012), pp. 39-40.
59) Melanie Lee, "Cyber Spying Collaboration Discovered Between Shanghai Jiaotong University, People's Liberation Army," *Huffpost Tech* (23 March 2013), available at <http://www.huffingtonpost.com/2013/03/23/cyber-spying-chinese-university_n_2941700.html> (accessed on 1 May 2013).
60) Paul J. Bolt and Carl N. Brenner, *op. cit.*, pp. 134-135; Scott Henderson, *op. cit.*, pp. 25-30.

authoritative power to control them to meet its strategic interests. The capacity of the Chinese government has been empirically proved by previous incidents of China's cyber warfare against the United States in the post-Cold War era.

Table 2 lists cases of China's cyber warfare against the United States. Researching and even identifying cyber attackers is difficult since much of the evidence is shrouded in secrecy, difficult to reference, and often not available at all. Admitting the difficulty of attribution problem, we select thirteen cases of Chinese cyberattacks against the United States on the basis of the report on the 'Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation' released by the US-China Economic and Security Review Commission in 2009. This paper assumes that the thirteen cases were originated from China despite potential arguments to the contrary.

The first finding from analyzing these cases is that China's cyber warfare against the United States has evolved from large-scale distributed denial of service and web defacements to network exploitation and data theft. It refers to the shift of cyberattacks from less sophisticated but more visible cyberattacks to more sophisticated but less visible cyberattacks. While cyberattacks at the early phase of Sino-American cyber warfare were carried out only after physical diplomatic conflicts, currently they do not necessarily take place during war, but happen at any time. These changes of cyberattacks are closely reflected in the change of strategies of the Chinese government in Sino-American cyber warfare.

At the early stages of Sino-American warfare, the Chinese government remained in the background limiting the penetration of its authoritative capacity into the private sector either to condone or impose restrictions on the voluntary actions of the various non-state actors. Depending on the constellation of the state's interests, the Chinese government just tolerated cyberattacks of individual hackers or organizations in some cases while actively censoring them in other cases. For example, following the accidental bombing of the Chinese embassy in Serbia in May 1999, a great number of Chinese civilian hackers rallied around the flag and formed systematic hacker groups, such as Javaphile, to carry out large-scale cyberattacks against the US government.[61] Similarly, following the collision of the US surveillance aircraft and the Chinese fighter plane in April 2001, Chinese hacker groups,

Table 2. *The Cases of China's Cyber Warfare against the United States*

May, 1999	Defacements of US government websites after US bombing of the Chinese embassy in Serbia	**April, 2001**	The First Sino-American cyber warfare after the collision of US surveillance plane and Chinese fighter plane
May, 2002	To remark the one year anniversary of the first Sino-US cyber war (Failure)	**November, 2004**	Intrusion at multiple unclassified US military systems
August, 2005	Intrusion into US Department of Defense codenamed "Titan Rain"	**July, 2006**	Penetration into the US Department of State networks
August, 2006	Penetration into the NIPRET	**August, 2006**	Penetration into the computers of conservative congressmen's who are vocal critics of China's human rights records
November, 2006	Attacking US Naval War College computer infrastructure	**June, 2007**	Penetration into the email system of the Secretary of Defense
October, 2007	Sending E-mail with malicious attachment in the Oak Ridge National Lab	**November, 2008**	Penetration into the White House information system
November, 2008	Intrusion at NASA's most critical sites including the Kennedy Space Center		

Source: Byran Krekel, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepared for the US-China Economic and Security Review Commission* (McLean, VA: Northrop Grumman Corp., October 2009), pp. 68-74.

such as the Honker Union of China, became the center for attacking hundreds of American websites and destroyed large volumes of data on American web servers.[62)]

These incidents of cyber warfare were perpetrated by numerous Chinese individual hackers and groups carrying out cyberattacks against the US

61) Byran Krekel, *op. cit.*, p. 68; Ellen Messmer, "Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says," *CNN* (12 May 1999), available at <http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/> (accessed on 20 May 2012).

62) Byran Krekel, *op. cit.*, p. 68.

government. These attacks did not seem to be at the Chinese government's direction but were voluntary actions of societal actors inspired by patriotism or nationalism. The Chinese government deliberately condoned their actions and left them unfettered.[63] Since the Chinese government has consistently put censorship on cyberspace, known as the 'Great Firewall,' to block or restrict access to Internet websites or contents that the government regards as sensitive or inappropriate,[64] condoning attacks of civilian hackers against the United States was apparently a conscious act of the state. The Chinese government purposely did nothing.

However, after a large-scale denial of service attack against the White House during the 2001 incident, the Chinese government suddenly changed its strategy from unofficial condoning to selective censorship. The government not only directly ordered leaders of hacker organizations to stop their actions but also published editorials in the People's Daily, the official newspaper of the Communist Party: "The attacks by the Honker Union of China, or Red Guests, on US websites are unforgivable acts violating the law. It is web terrorism."[65] Interestingly, right after the statement of the Chinese government, the leaders of civilian hacker groups announced a temporary termination of attacks and effectually stood down.[66] In practice, Wan Tao, the leader of the Red Hacker Alliance which was one of the leading hacker groups carrying out cyberattacks at that time, mentioned that the decision to cease cyber warfare against the United States was based on directions from the Chinese government.[67]

Similarly, when there was a plan to wage cyber warfare against the United States celebrating "the first anniversary of Sino-American cyber warfare" in 2002, it did not materialize because the Chinese government asked them not to do so.[68] The five major Chinese hacker organizations, including the Honker Union of China and the Red Hacker Alliance, issued a statement that

---

63) *Ibid.*, pp. 37-39.
64) *Ibid.*, p. 38.
65) *Ibid.*, pp. 37-39; Alexander Klimburg, *op. cit.*, pp. 44-45; Mandiant Intelligence Center, *op. cit.*, p. 51; Scott Henderson, *op. cit.*, pp. 28-29.
66) Byran Krekel, *op. cit.*, p. 32.
67) Scott Henderson, *op. cit.*, pp. 29-30.
68) Desmond Ball, "China's Cyber Warfare Capabilities," *Security Challenges Journal* 7-2 (Winter 2011), p. 96.

announced the end of anniversary attacks after negotiating among themselves in May 2002.[69] The incident in 2002 was another example of the government's selective censorship, demonstrating that the government has effective authoritative capacity to make individual hackers or organizations harmonize their plans with the government's desire.

The change in the state's strategy from condoning to censorship in mid-2002 occurred because overlooking their actions was no longer advantageous for the government. Since selected targets of the Chinese hacker groups until then were based on political or nationalistic symbols, such as websites of the White House or the Department of Energy, their attacks possibly may not have been aligned with the real Chinese campaign objectives. Their web defacements and large-scale distributed denial-of-service could annul backchannels of the Chinese military operations because data destruction of American servers could also eliminate important intelligence of the Chinese government itself.[70] Furthermore, as the US officials warned and condemned not only illicit attacks by Chinese civilians but also the Chinese government's irresponsible reaction toward them, the diplomatic efforts of the Chinese government to resolve the physical crisis could also be invalidated.

Taking selective censorship as the strategy, the Chinese government's opposition to civilian cyberattacks has extended self-censorship into the private sector. Thus in practice civilian hackers or groups have remarkably deterred large-scale cyberattacks against the United States.[71] By controlling patriotic cyberattacks by the private sector, the Chinese government, covertly and overtly, has started to exercise infrastructural capacity to mobilize individual hackers, commercial organizations, and academia under the name of the People's Republic of China. In practice, eleven incidents from 2004 identified in this article were carried out by the state's substitutes or by the state itself. Granted, cyberattacks have inherent problems of clear attribution and there is no direct evidence indicating the Chinese government's direct involvement. However, the method, focus, and scope of resources of these incidents suggest they are beyond the capability of independent civilians or organizations, thus indicating the strong possibility of state-led operations.[72]

---

69) Scott Henderson, *op. cit.*, pp. 29-30.
70) Byran Krekel, *op. cit.*, pp. 39-40.
71) *Ibid.*, pp. 37-38.
72) *Ibid.*, pp. 51-58.

Above all, most of the incidents listed in the table that occurred after 2004 were computer network exploitation, which were operations conducted through the use of computer network to gather sensitive data from targets or adversary networks. Since computer network exploitation generally requires considerable resources and much more sophisticated skills, numerous researchers believe that such attack could have been undertaken only by state actors.[73] Even if some of them were carried out by civilian hacker groups, such as the incidents in August 2005 and August 2006, these private players acted as the agents of the state, which was their customer. This is most likely, because none of the data that they had stolen had any monetary value or personal interests, which are the main motivations of cybercriminal organizations or civilian hackers.

For example, in the incident of August 2006, it was a Chinese civilian group that carried out cyberattacks against the Non-classified Internet Protocol Router Network (NIPRNET) and had downloaded up to 20 terabytes of data.[74] The NIPRENT is one of the key logistics networks and databases at the Department of Defense in the United States, which support command and control operations. Since a vast amount of information is accessed and transmitted between myriad civilian and military nodes in the United Sates, these nodes have been pointed out as potential high priority targets for the Chinese government.[75] Although the attack against the NIPRET could have been presumably planned and carried out by a group with civilian hackers or engineers, their focus and scope of resources suggest that the incident in 2006 reached beyond the independent actions of civilian hackers or groups, suggesting state-level operation. This is because the collection of intelligence on the US military information system needs something more to ensure its success such as researchers of defense related engineering, military and strategic planners and even policy experts specialized in Sino-American relations.

This kind of analysis can also apply to other incidents of China's cyber

---

73) Alexander Klimburg, *op. cit.*, pp. 42-43.

74) Dawn S. Onley, "Red Storm Rising: DoD's Efforts to Stave off Nation-state Cyber Attacks Begin with China," *Government Computer News* (17 August 2006), available at <http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx> (accessed on 20 March 2012).

75) Byran Krekel, *op. cit.*, pp. 23-28.

warfare against the United States listed in the table. One thing that these eleven incidents had in common was that they were network-exploitation cyberattacks intended to steal information or data from the United States. All types of data that the attackers focused on and intercepted in these cases were related to political and military information: contents of emails of congressmen, who condemned Chinese human rights abuses, which disclosed the identities and locations of many Chinese political dissidents and refugees; user login credentials of the US Department of State; and technology blueprints and databases at the nuclear weapons laboratory.[76)]

Stolen data are potentially related to the security threat, which is the primary concern of the Chinese government.[77)] In addition, they cannot be monetized by civilian cybercriminals if they do not have the state as their customer, suggesting that they are the state's proxy or substitute regardless of their actual affiliation. However, besides politico-military data theft proved in the aforementioned cases, economic-valued data theft, such as information on system design and manufacturing procedures in various sectors of industry, has increased, which could negatively affect the national security of the United States in the long run.

The cyberattacks of Titan Rain and APT1 also show similar characteristics and patterns. Located in Guangdong Province, Titan Rain is one of the most notorious teams for their persistency in carrying out cyberattacks against the US government information networks from 2003 to 2006.[78)] Activated in 2006, "APT1" was exposed as one of China's cyber espionage units to have breached hundreds of organizations around the world, including the US governmental and industrial networks. Interestingly, the Mandiant Intelligence Center, one of the most prominent cyber security firms, argues that APT1 is part of Unit 61398, the 3rd Department of the PLA.[79)] If true, it demonstrates that state-led cyberattacks have prevailed in China, presumably mobilizing non-state actors under the Chinese government to utilize their expertise and resources.

---

76) *Ibid.*, pp. 68-74.
77) Peter Van Ness, "Unconventional Threats to China's National Security: A Teaching Note," *Journal of Contemporary China* 9-23 (August 2000), pp. 134-135.
78) William T. Hagestad II, *op. cit.*, pp. 12-13.
79) Mandiant Intelligence Center, *op. cit.*, pp. 9-10.

If these cases occurred under the umbrella of the Chinese government, how did the Chinese government mobilize the private sector as state proxies? To make civilian hackers or groups carry out cyberattacks only within national security frameworks, the Chinese government has developed coercive collaboration and reciprocal partnership as its central strategies. An example of coercive collaboration occurred in 2006 when the Chinese government shutdown the website of The Patriot Hackers-Black Eagle Base and arrested its members. However, the group members were released and transformed into the Black Eagle Honker Base when they took a vow that they would focus their efforts on training people for the government and would work with the government to improve the state's network security.[80] After the Chinese government expanded the anti-hacking laws and actually used the law to convict and arrest individual hackers, especially those operating underground, this kind of coercive collaboration has been more prevalent.

Concerning reciprocal partnership, the Chinese government has formed mutually beneficial alliances with civilian hackers or commercial organizations by providing a host of incentives to mobilize them, such as financial rewards, prestige, and respect. For example, the Chinese government has disbanded hacker groups that operated underground and allowed them to evolve into formal information security research companies or offered government jobs to the hackers. For example, NSFocus and XFocus—now prominent commercial information security firms—evolved from civilian hacker groups, such as the Green Army Alliance, which was an active hacker group that conducted various cyberattacks against American websites.[81] The Chinese government also holds a PLA-sponsored hacking contest and recruits talented hackers by offering a prize or providing a government job in return for utilizing their skills. Tan Dalin, one of the winners of this contest, confessed that he organized members and carried out a barrage of cyberattacks against multiple US government agencies all through 2006. After an initial round of successful attacks against the United States, the amount of his funding from an unidentified funding source tripled.[82]

---

80) Byran Krekel, *op. cit.*, p. 42.
81) *Ibid.*, p. 41; *Economist* (April 2013), pp. 12-13.
82) Alexander Klimburg, *op. cit.*, pp. 46-47.

In addition, the Chinese government has established close partnerships with commercial organizations, especially telecom enterprises, such as Huawei, China Telecom, and ZTE, by providing a range of tax incentives, long-term subsidies and low-interest rate loans. Such incentives help these private firms to develop advanced IT systems in China and thereby to win overseas contract, helping them to become global companies. Researchers point out that the Huawei enterprise may be the compelling potential player in cyber warfare since its relationship with the Chinese government is too close and interconnected. In addition, Huawei has expanded its telecom-equipment into approximately 140 countries, suggesting a strong feasibility that networks of the company can be integrated into critical infrastructures of a great many countries and thus can be used by the Chinese government or even to shut down unexpectedly during wartime.[83)]

Most likely in recognition of this potentially perilous situation, the Australian government blocked Huawei from participating in a project of its national broadband network on security grounds.[84)] The US House Permanent Select Committee on Intelligence initiated an investigation about Huawei and ZTE for alleged connections to the Chinese government in the same context in 2012.[85)] The committee concluded that these companies' provision of equipment to the nation's critical infrastructure could undermine US national security.[86)]

Ⅴ. Conclusion

The necessity of public and private partnerships and interweaving civilian and military spheres are remarkable in cyber warfare. This article assumes that these phenomena do not weaken the state capacity in cyber warfare. Some of the previous research studies unnecessarily confined their analysis to the dichotomous question of empowered societal actors versus declining state

83) "Who's afraid of Huawei?" *Economist* (August 2012), p. 9; Byran Krekel, *op. cit.*, pp. 49-50.
84) *Economist* (August 2012), p. 9.
85) "The state advances," *Economist* (October 2012), pp. 39-40.
86) Make Rogers and Ranking Member C.A., *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*, US House of Representatives, 112th US Congress (8 October 2012), pp. 11-43.

capacity. Thus they failed to see that there is no logical contradiction between mounting the private sector and the state's greater role in cyber warfare.

This article argues that states have adapted and redeployed their roles to cope with this new threat to national security, maintaining the most supreme players. The dual roles of the state are mobilizing the private sector on the one hand while controlling it on the other, depending on the state's strategic interests. It is important that such societal actors as individuals, organizations, commercial firms, and academia play significant roles in waging cyber warfare by providing technological skills, planning defensive or offensive strategies in cyberspace and even making their own decisions to declare cyber warfare. However, they can exercise and demonstrate their power only under certain circumstances, which depend on the state's strategies of cyber warfare. By projecting state capacity, through either infrastructural power or authoritative power, states can choose and organize combinations of strategies, selecting from selective censorship, coercive collaboration, unofficial condoning, and reciprocal partnership. These strategies are an inherent construction of the state's capacity, and they can change according to the situation or the mission depending on the constellation of the state's interests.

The analysis of thirteen cases of China's cyber warfare against the United States in the post-Cold War era clearly shows that non-state actors can attack critical infrastructures in the United States with electronic means and relevant systems. However, only by considering the state's strategies is it possible to set the conditions under which non-state actors will wield their influence. Determining how the capacity of non-state actors can actually be used largely depends on the constellation of the Chinese government's interests. This implies that the Chinese government unchangeably continues to be the supreme player.

In addition, we can observe that the evolvement of Chinese cyberattacks from large-scale distributed denial of service or web defacements to network exploitation has clearly reflected the shift of the Chinese government's strategies. While controlling the private sector through unofficial condoning and selective censorship, the Chinese government began to mobilize the private sector within the national security framework through reciprocal partnership and coercive collaboration.

While this article examines the Chinese government's strategies in cyber

warfare, the dual roles of the government and strategies for achieving them should be generally applicable to the other states in international society. How a state organizes and combines these strategies to mobilize the private sector on one hand while controlling it on the other basically defines the state's cyber power.

In this way, cyber warfare shows a new or at least novel type of the private sector-state relationship, or *state-led back-scratching alliance*.

REFERENCES

"A giant cage: Masters of the Cyber-universe." *Economist*. April 2013, pp. 12-13.

Anand, Vinod. "Chinese Concepts and Capabilities of Information Warfare." *Strategic Analysis* 30-4. October/December 2006, pp. 781-782.

Arquilla, John. "Thinking About New Security Paradigms." *Contemporary Security Policy* 24-1. October 2003, pp. 216-219.

Baer, Walter S. "Rewarding IT Security in the Marketplace." *Contemporary Security Policy* 24-1. October 2003, pp. 190-192.

Ball, Desmond. "China's Cyber Warfare Capabilities." *Security Challenges Journal* 7-2. Winter 2011, pp. 29-30.

Becker, Elizabeth. "F.B.I. Warns That Chinese May Disrupt U.S. Web Sites." *New York Times*. 28 April 2001. Available at <http://www.nytimes.com/2001/04/28/world/fbi-warns-that-chinese-may-disrupt-us-web-sites.html> (Accessed on 20 April 2013).

Beith, Malcolm. "The U.S.-China Hacker Conflict." *Newsweek*. 6 May 2001. Available at <http://www.newsweek.com/us-china-hacker-conflict-152877> (Accessed on 30 March 2012).

Bishop, Matt and Emily O. Goldman. "The Strategy and Tactics of Information Warfare." *Contemporary Security Policy* 24-1. June 2010, pp. 119-120.

Bolt, Paul J. and Carl N. Brenner. "Information Warfare across the Taiwan Strait." *Journal of Contemporary China* 13-38. February 2004, pp. 132-133.

Carr, Jeffrey. *Inside Cyber Warfare*. O'Reilly Media Inc., 2009. Available at < http://oreilly.com/ >.

Cavelty, Mariam Dunn. *Strategic Trends: Key Developments in Global Affairs*. Zurich: Center for Security Studies, 2012.

Cha, Victor D. "Globalization and the Study of International Security." *Journal of Peace Research* 37-3. May 2000, pp. 391-403.

Choucri, Nazli. *Cyberpolitics in International Relations.* Cambridge, Massachusetts: MIT Press, 2012.

Cornish, Paul, David Livingstone, Dave Clemente, and Claire Yorke. *On Cyber Warfare*. London: Chatham House, Royal Institute of International Affairs, November 2010.

Cronin, Blaise and Holly Crawford. "Information Warfare: Its Application in Military and Civilian Contexts." *The Information Society* 15-4. July 1999, pp. 257-262.

Department of Homeland Security. "Critical Infrastructure Sector Partnerships." Available at <https://www.dhs.gov/critical-infrastructure-sector-partnerships> (Accessed on 20 September 2013).

_____. "National Coordination Center for Telecommunications." Available at <http://www.dhs.gov/national-coordinating-center-telecommunications> (Accessed on 21 September 2013).

Drezer, Daniel W. "The Global Governance of the Internet: Bringing the State Back In." *Political Science Quarterly* 119-3. Spring 2004, p. 479.

Eriksson, Johan Eriksson and Giampiero Giacomello. "The Information Revolutions, Security, and International Relations: (IR) Relevant Theory?" *International Political Science Review* 27-3. July 2006, p. 222.

Goldman, Emily O. "Introduction: Security in the Information Technology Age." *Contemporary Security Policy* 24-1. October 2003, pp. 119-120.

Haddadi, Anissa. "Unit 8200: Cyber Whizzkids behind Israel's High-Tech 'Secret Weapon'?" *International Business Times*. 1 December 2011. Available at <http://www.ibtimes.co.uk/articles/259505/20111201/unit-8200-israel-s-high-tech-secret.htm> (Accessed on 24 September 2013).

Hagedstad II, William T. *21st Century Chinese Cyber Warfare*. United Kingdom: IT Governance Publishing, 2012.

Henderson, Scott. "Beijing's Rising Hacker Stars... How Does Mother China React?" *IO Sphere Journal* (Joint Information Operations Warfare Command). Fall 2008, p. 28.

Hjortdal, Magnus. "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence." *Journal of Strategic Security* 6-2. May 2011, p. 6.

Jackson, William. "NIPC to hackers: Don't try this at home." *GCN*. 14 February 2003. Available at <http://gcn.com/articles/2003/02/14/nipc-to-hackers-dont-try-this-at-home.aspx> (Accessed on 10 April 2013).

Junio, Timothy J. "How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate." *Journal of Strategic Studies* 36-1. February 2013, pp. 125-126.

Kan, Shirley A., Richard Best, Christopher Bolkcom, Robert Chapman, Richard Cronin, Kerry Dumbaugh, Stuart Goldman, Mark Manyin, Wayne Morrison, Ronald O'Rourke, and David M. Ackerman. *China-U.S. Aircraft Collision Incident of April 2001: Assessments and Policy Implications*. Congressional Research Service, RL30946. 10 October 2010.

Klimburg, Alexander. "Mobilising Cyber Power." *Survival* 53-1. February-March 2011, pp. 42-43.

Krekel, Byran. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation: Prepared for the U.S.-China Economic and Security Review Commission*. McLean, Virginia: Northrop Grumman Corp., October 2009. Available at <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-030.pdf>.

Lee, Melanie. "Cyber Spying Collaboration Discovered Between Shanghai Jiaotong University, People's Liberation Army." *Huffpost Tech*. 23 March 2013. Available at <http://www.huffingtonpost.com/2013/03/23/cyber-spying-chinese-university_n_2941700.html> (Accessed on 1 May 2013).

Levy, Jonah D. *The State after Statism*. Cambridge, Massachusetts: Harvard University Press, 2006.

Mandiant Intelligence Center. *APT1 Exposing One of China's Cyber Espionage Units*, 2013. Available at <http://www.mandiant.com>.

Messmer, Ellen. "Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says." *CNN*. 12 May 1999. Available at <http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/> (Accessed on 20 May 2012).

Onley, Dawn S. "Red Storm Rising: DoD's Efforts to Stave off Nation-state Cyber Attacks begin with China." *Government Computer News*. 17 August 2006. Available at <http://gcn.com/Articles/2006/08/17/Red-storm-rising.aspx> (Accessed on 20 March 2012).

Pace, David. "Government Warns 'Patriot Hackers' Against Cyber Attacks On Iraqi Interests." *CRN*. 12 February 2003. Available at <http://www.crn.com/news/security/18821779/government-warns-patriot-hackers-against-cyber-attacks-on-iraqi-interests.htm> (Accessed on 10 April 2013).

Pye, Lucian W. "The State and Individual: An Overview Interpretation." *China Quarterly* 127. September 1991, pp. 436-466.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Cambridge, Massachusetts: MIT Press, 2001.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35-1. February 2012, pp. 5-32.

Rogers, Make and Ranking Member C.A. *Investigative Report on the US National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE*. US House of Representatives, 112th US Congress. 8 October 2012.

Sharma, Amit. "Cyber Wars: A Paradigm Shift from Means to Ends." *Strategic Analysis* 34-1. February 2010, pp. 72-73.

Smith, Craig S. "May 6-12, The First World Hacker War." *New York Times*. 13 May 2001. Available at <http://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html> (Accessed on 16 August 2012).

Solce, Natasha. "The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force." *Albany Law Journal of Science and Technology* 18-1. September 2008, pp. 303-304.

Stevens, Gina Marie. *Homeland Security Act of 2002: Critical Infrastructure Information Act*. Congressional Research Service. RL 31762. February 2003.

Stone, John. "Cyber War Will Take Place." *Journal of Strategic Studies* 36-1. November 2012, pp. 101-108.

Tang, Rose. "China warns of massive hack attacks." *CNN*. 3 May 2001. Available at <http://edition.cnn.com/2001/WORLD/asiapcf/east/05/03/china.hack/index.html?_s=PM:asiapcf> (Accessed on 16 August 2012).

"The state advances." *Economist*. October 2012, pp. 39-40.

Van Ness, Peter. "Unconventional Threats to China's National Security: A Teaching Note." *Journal of Contemporary China* 9-23 (August 2000).

White House. *Fact Sheet: Protecting America's Critical Infrastructure: PDD 63*. 22 May 1998. Available at <http://www.fas.org/irp/offdocs/pdd-63.htm> (Accessed on 20 September 2013).

_____. *The National Strategy to Secure Cyberspace*. February 2003.

"Who's afraid of Huawei?" *Economist*. August 2012, p. 9.

[Received September 30, 2013; Revised November 28, 2013; Accepted November 29, 2013]