DECEMBER
2014

Warring State
China's Cybersecurity Strategy

By Amy Chang
Foreword by Joseph S. Nye, Jr.

Center for a
New American
Security

Acknowledgements

I would like to thank my colleagues at CNAS for their critical feedback, especially Ben FitzGerald, Dafna Rand, Shawn Brimley, and Ely Ratner for their substantive guidance and expertise. Thanks to CNAS interns Alexandra Sander and Cecilia Zhou for their research assistance.

I would also like to express my gratitude to Joseph S. Nye Jr. for his support and guidance from the time this report was only an idea over a year ago to its fruition. Thanks, also, to Ian Easton, Andrew Erickson, Dan Hartnett, Joe McReynolds, and Leigh Ann Ragland for their feedback.

Data are collected through English- and Chinese-language primary sources such as newspapers, government official speeches and government statements. This report also relied on interviews with U.S. government officials, policy makers, analysts, practitioners and scholars. They are individuals with expertise in U.S. cybersecurity policy, Chinese cyber activity, U.S.-China relations, Chinese defense, defense policy, and are individuals with experience and understanding of high-level dialogue between the United States and China.

The views expressed in this report are those of the author alone, and retains sole responsibility for any errors in fact, analysis or omission.

Cover Image
LUKAS HLAVAC/Shutterstock.com

TABLE OF CONTENTS

DECEMBER 2014

Warring State

China's Cybersecurity Strategy

By Amy Chang

Foreword by Joseph S. Nye, Jr.

About the Author

Amy Chang is a Research Associate at the Center for a New American Security.

WARRING STATE: CHINA'S CYBERSECURITY STRATEGY

By Amy Chang

ABBREVIATIONS IN REPORT

APT	Advanced persistent threat
BUPT	Beijing University of Posts and Telecommunications
C4ISR	Command, control, communications, computer, intelligence, surveillance and reconnaissance
CCP	Chinese Communist Party
COSTIND	Commission for Science, Technology and Industry for National Defense
CWG	U-S.-China Cyber Working Group
CYBERCOM	U.S. Cyber Command
DOD	U.S. Department of Defense
DOJ	U.S. Department of Justice
FBI	Federal Bureau of Investigation
GGE	Group of Governmental Experts
GSD	General Staff Department
ICT	Information and communications technology
LSG	Leading Small Group
MIIT	Ministry of Industry and Information Technology
mRAT	Mobile remote access trojan
MSS	Ministry of State Security
NCIX	Office of the National Counterintelligence Executive
NSA	National Security Agency
PLA	People's Liberation Army
PRC	People's Republic of China
S&T	Science and technology
SILG	State Informatization Leading Group
SNISCSG	State Network and Information Security Coordination Small Group
STRATCOM	U.S. Strategic Command
U.N.	United Nations
UNCLOS	United Nations Convention on the Law of the Sea

FOREWORD

By Joseph S. Nye, Jr.
Harvard University

Cyberspace and information technology have enabled the economic, political, and cultural integration of the United States and China. However, interdependence creates costs as well as benefits. Increased interconnection has also contributed to major obstacles in the bilateral relationship, generating mutual distrust of incentives, actions, and norms in cyberspace. Information technology raises new challenges for states by allowing actors to exploit networks, conduct cyber espionage, or compromise national security with greater ease. It is difficult for American policymakers to both ameliorate tension in the bilateral cyber relationship and impose costs on negative behavior in cyberspace, while also limiting undesirable repercussions on broader U.S. engagement strategies and policies towards China.

As China continues to develop and grow in influence, the United States must also be prepared to confront challenges to Western dominant norms in policy areas such as cybersecurity. China has been actively promoting a counter-narrative: justifying stringent Internet controls through propaganda, denying involvement or accountability in cyber espionage, and accusing the United States of committing similar actions against China.[1] In light of these challenges, how should the United States view China's strategic intentions? What is China trying to achieve?

The analysis of cybersecurity and China is often treated as specialized and distinct fields. While each community provides valuable insight into strategic thinking on cybersecurity, one is often left with a desire for integrative approaches, and it is here that Amy Chang makes a meaningful contribution.

As a China analyst fluent in Chinese, Amy combines policy analysis, China studies, and cross-cultural understanding to shed light on China's strategy, motivations, and objectives in the cyber domain. She uses her language skills to integrate

understanding of China's military modernization, Chinese Communist Party dynamics, and cyber policy to provide compelling arguments for why China's primary domestic political incentive to retain Communist Party rule drives many aspects of its cybersecurity strategy.

In this report, Amy illustrates the development over three decades of China's cybersecurity strategy, and highlights individuals and entities that have significant influence over the direction of China's cyber strategy. She also explains China's operationalization of this strategy in economic, political, and military contexts. Though the Chinese government currently faces bureaucratic burdens and other domestic obstacles in implementing an optimal cyber strategy, it has since 2012 dedicated significant effort to remedy its shortcomings. Amy also describes Chinese interpretations of U.S. activity in cyberspace, which informs us how even disparities in language used by officials or in terminology to describe "cyber" could lead to misinterpretation of strategic intention.

Amy's conclusions provide a rare insight into the domestic political, economic, and military motivations that drive China's behavior in cyberspace. The perspectives provided in this report merit close consideration by experts and policy makers who wish to improve U.S. effectiveness in cyber negotiations, norm building, and policymaking.

I. EXECUTIVE SUMMARY

By Amy Chang

The United States-China cyber relationship has rarely been more fraught than it is today. Despite high levels of attention to cybersecurity issues in both countries over the past several years, the two nations continue to face substantial obstacles in developing cooperative efforts and improving mutual understanding on the issue. In the cyber context, relations have devolved to near-complete distrust of each other's motives, actions, and agendas, affecting other facets of the bilateral relationship.

What can be done to improve this situation?

Devising an optimal strategy to address the challenges in the U.S.-China cyber relationship first requires an understanding of motives, agendas, and stakeholders embedded in the process. In this light, this report uses interdisciplinary methods and analysis and Chinese language research to provide unique insight on China's cybersecurity strategy, including its development since the 1990s, its infrastructure and influencers, and its objectives and incentives in the cyber realm – especially as it pertains to China's foreign policy and its interactions with the United States.

China's foreign policy behavior, including its cyber activity, is driven primarily by the domestic political imperative to protect the longevity of the Chinese Communist Party (CCP). Ensuring domestic stability, territorial integrity, modernization, and economic growth, while simultaneously preparing for the possibility of militarized cyber conflict in the future, are all objectives that directly or indirectly support the continuation of CCP rule. China espouses laws, norms, standards, and agreements in bi- and multilateral fora that allow for sufficient flexibility of interpretation to serve domestic needs and interests.

Senior CCP officials have also issued high-level directives and created several high-level Leading Groups and Leading Small Groups to provide

coordination and strategic guidance on cybersecurity. Concurrently, there has been a noticeable increase in civilian and military research and development on cybersecurity strategy and defensive and offensive cyber tools over the past several years.

Beijing's thinking about cybersecurity, and its cybersecurity strategy consists of three main component drivers: economic, political, and military. Important manifestations of those drivers are:

- Maintaining economic growth and stability, which involves industrial economic cyber espionage of U.S. and other foreign targets
- Protecting the governing power of the Chinese Communist Party through information control, propaganda, and targeting of domestic sources of potential unrest
- Using computer network operations to signal dissatisfaction with foreign powers over developments outside of China (e.g., maritime territorial disputes, foreign allegations of Chinese hacking activity) that negatively affect China's reputation
- Preparing for military scenarios and ensuring military superiority in the event of cybered conflict with an adversary through military modernization, computer network operations research, and human capital cultivation
- Studying and understanding potential adversaries' military infrastructures, motivations, objectives, capabilities, and limitations in the cyber domain
- Advancing alternative narratives of government control over/handling of cybersecurity internationally (e.g., promoting sovereignty of states to control the Internet within a country's borders) and domestically (e.g., justifying domestic surveillance, information control)

Domestic policy and military developments over the past several years indicate that cybersecurity is a high priority for the Chinese government. Despite high-level guidance and strategic direction from President Xi Jinping and senior civilian and military officials, implementation of China's cybersecurity strategy remains fragmented and its bureaucratic structure remains disorganized, characterized by competition for stakeholder resources and influence on policy direction.

Chinese behavior will not change in the foreseeable future, unless major shifts in politics (e.g., changes in U.S. approaches to engagement/conflict with China) or incentives change China's domestic and foreign policy risk calculus and objectives. To achieve this, the United States must understand China's perspectives and goals and distinguish areas of common interest and contention, and craft an appropriate strategy that provides incentives and shapes China's behavior. Such a strategy cannot be contained purely in the cyber context, and must be iterative and collaborative across U.S. public and private sectors.

This report contributes a solid foundation of understanding of China's cybersecurity strategy and aims to inform U.S. efforts in negotiating with China on cyber issues. As such, this report hopes to illuminate, though it is not a solution in itself. Any solution must leverage U.S. advantages in this realm and increase China's risk calculus sufficiently to alter China's behavior. A follow-on policy brief providing recommendations for addressing the U.S.-China cyber relationship will be released in early 2015.

II. INTRODUCTION

The United States and China are inextricably linked in cyberspace, where their economic, military, and diplomatic relationships manifest as an extension of the two governments' policies toward each other. While the bilateral cyber relationship has always been tumultuous, it is currently in its most contentious state. Tensions in this sphere have generated negative externalities on the broader U.S.-China relationship.[2]

Cybersecurity policy is a multi-faceted issue with no conclusive or coordinated strategic paradigm to cope with, manage, or combat cyber threats. While there are plenty of areas for cooperation in the cyber realm between the United States and China, if issues are not well thought out or managed properly, frictions could be exacerbated. This is of paramount importance in the case of a fragile U.S.-China relationship. Despite joint interest in formulating bilateral cybersecurity measures, however, the United States and China still face substantial obstacles on the path towards cooperation – differences in objectives, values, and practices across the diplomatic, intelligence, military, and economic elements of national power.

As governments increasingly rely on information technology and cyber capabilities to carry out their responsibilities, such technologies are playing an ever more integral role in international relations, increasing the need for understanding and stability in cyberspace. U.S.-China conflict and/or cooperation in this realm will inform the trajectory of Internet governance, future models for bi- and multilateral cybersecurity cooperation, and potential norms of behavior.

Evidence of China's intrusive cyber activity against U.S. national security infrastructure and industry is abundant. Reports such as the Department of Defense's *Annual Report to Congress* on China, Mandiant's *APT1* and books such as *Chinese Industrial Espionage* discuss in detail the numerous occasions where China[3] has exfiltrated critical information from foreign businesses, governments and militaries. While invaluable contributions to the study of China's security structure, public discourse has been largely focused on offering a recounting of various actions China has taken against the United States, resulting in a relative dearth of discussion that situates China's behavior in the broader context of its strategic imperatives and modes of thought. This shortage of publicly available analysis of China's network security strategy, drivers, and motivations has led to a paucity of clear and effective U.S. responses.[4]

Because China is secretive about issues of national security, and because China's network security policies encompass overlapping economic, political, and military considerations, unpacking these strategic questions is not a simple endeavor. This report attempts to fill gaps in existing Western analyses of China's cyber domain strategy by addressing, at a strategic level, China's relevant ambitions and incentives, and their effects on the U.S.-China cyber relationship. Guiding questions for this report included:

- What are China's motivations and incentives in cyberspace?
- How do China's priorities in cyberspace manifest in its foreign policy?

Questions of network security inherently have economic and military implications, but in the Chinese context, they arguably carry political implications as well. Following the momentum created by previous Chinese leaders on promoting information technology development and modernizing China's military, President Xi Jinping and the central government have exerted significant effort since his 2012 leadership accession to weave together and operationalize a comprehensive approach to and organizational structure for network security. The recent establishment of

Although Chinese national security developments have a degree of opacity, it is clear that China's network security priorities are motivated, just as all of China's myriad military modernization priorities are, by the Chinese Communist Party's primary goal of maintaining its own governing power.

the National Security Commission and Central Network Security and Informatization Leading Small Group, with Xi as their head, are two examples of a dedicated effort at the top to prioritize national and network security. Despite China's ongoing efforts to coordinate and organize the network security infrastructure, it remains fragmented, partly as a result of the disjointed state of the Chinese government's frequently overlapping and conflicting administrative bodies and managing organizations.[5]

Although Chinese national security developments have a degree of opacity, it is clear that China's network security priorities are motivated, just as all of China's myriad military modernization priorities are, by the Chinese Communist Party's (CCP) primary goal of maintaining its own governing power. Ensuring domestic stability, territorial integrity, modernization, and economic growth, while simultaneously preparing for the possibility of militarized cyber conflict in the future, are all objectives that directly or indirectly support the continuation of CCP rule.

The CCP's self-preservation priorities drive its foreign policies and foreign cyber activity, which complicates U.S. ability to shape China's behavior in cyberspace. Many within the United States – from the government to the military to civil society – consider China's activity as specifically targeted against U.S. interests and assets. In reality, Chinese aims are more diffuse, comprehensive and based on domestic concerns. This means that China would be more likely adhere to international norms and standards of behavior when they allow for sufficient flexibility of interpretation to serve these domestic interests (such as supporting the legitimacy of the Communist Party and maintaining internal political and economic stability). As a result, properly understanding the drivers of Chinese behavior and foreign policy is essential for U.S. effectiveness in negotiations, norm building, and policymaking toward China, regardless of whether the policies are aimed at improving the U.S.-China cyber relationship or at imposing costs on negative behavior.

This report refers to Chinese cyber strategy as "network strategy," because in China the term "cyber" is rarely used and not fully congruent with how the term is understood in the U.S. policy community. Semantic issues such as these reveal the deep gaps between the two countries' security infrastructures: While the United States uses the term "cybersecurity"[6] to refer to the protection and defense of a wide array of electronic and communications information, China uses the term "network security" (网络安全, *wangluo anquan*) to refer more specifically to the protection of digital information networks. The term "information security" (信息安全, *xinxi anquan*) refers to a broader swath of information and communications systems. A more in-depth explanation of terminology will follow.

This report intends to inform U.S. policymakers and analysts interested in cybersecurity of China's network security strategy, as well as how China

views the United States in the cyber domain. It aims to assist in navigating the bilateral cyber relationship, with hopes that improvements in this realm would ameliorate other tensions of the broader U.S.-China relationship. This report focuses on understanding the sources, motives, ideologies, and bureaucratic structure of the Chinese network security strategy.

With China as a key player in international and U.S. cybersecurity considerations, understanding China's intentions and objectives would aid both the public and private sectors in finding areas of common interest and contention, as well as opportunities for behavior shaping (e.g., deterring or punishing bad behavior in cyberspace). Armed with a deeper understanding of China's network security strategy, the United States could improve defenses against malicious cyber activity targeting U.S. assets and gain leverage in disincentivizing China from continuing these activities. It would also allow the United States to make tailored improvements in its defense against antagonistic Chinese cyber activity. Finally, it could alleviate concerns about the prospect of cyber conflict instigated by either side, which has in recent years placed stress on the bilateral relationship. A follow-on policy brief to be released in early-2015 based on this research will offer recommendations for U.S. policymakers on how to improve U.S.-China cybersecurity relations, alter China's risk calculus to deter negative behavior in cyberspace, and modify norms for operating in cyberspace.

III. UNDERSTANDING CHINA'S NETWORK SECURITY STRATEGY

Xi Jinping's remarks at the first meeting of the Central Network Security and Informatization Leading Small Group (中央网络安全和信息化领导小组, *zhongyang wangluo anquan he xinxihua lingdao xiaozu*) in 2014 signaled a new, high-level prioritization of cyber as a major strategic initiative with political, economic, and military implications and also indicated the relative importance of network security on the Chinese political agenda. Xi's speech also noted that the central government perceives network security and informatization as two major components of both national security and national development.[8]

Network security and informatization fit into this calculus similarly: a secure and modern network would simultaneously mitigate threats to CCP rule and also ensure domestic stability, economic growth and national security. Linking national security with national development allows China's central government – namely, the Chinese Communist Party – to manipulate interpretation of high-level directives favorable to continued CCP legitimacy. Approaching these issues in a comprehensive manner allows the CCP to justify controlling major elements of policymaking and implementation for the interest of national security.[10] These mainly domestic priorities manifest in foreign policy, with China promoting the adoption of international norms and rules that do not impinge upon its domestic agenda, such as sovereignty in cyberspace and non-interference in domestic affairs. As China attempts to advance its interests at a policy-level, China and the People's Liberation Army (PLA) have also been planning for the possibility of cyber conflict in the future.[11]

This report represents one of the first open source assessments of China's network security strategy. Western open source analysis of China's network security strategy, doctrine, and systems has been sparse due to four primary impediments: First, Western analysis has devoted significant resources to understanding what China is doing in the cyber domain, but discourse relating these activities to broader phenomena in China's national security strategy has been limited.[12] Second, the secretive nature of the issue makes it difficult for analysts to find much open source material on China's network security strategy. Third, the development of several initiatives on network security strategy occurred after Xi Jinping took control of major leadership posts in 2012. As analysts continue to decode Xi's leadership style, objectives, and strategic direction in this space, they are still discerning his specific outlook on cyber issues. And fourth, national-level implementation of a network security strategy is hampered by bureaucratic overlap and fragmentation.

> *"Efforts should be made to build our country into a network powerhouse."*[7]
>
> XI JINPING

While China's network security policy is driven from high-level directives, the implementation of these policies can conflict, overlap or be unevenly executed by the many actors in this space (refer to the stakeholder chart on page 15 for a map of the numerous actors involved). As PLA Major General Wu Jiangxing, an academic at the Chinese Academy of Engineering and Dean of PLA Information Engineering University, explained in a 2013 interview, "China has not yet formed systems, institutions, laws and policies to support a comprehensive multi-dimensional information security system."[13] Indeed, the fragmented state of China's network security strategy, as represented in the

What is "informatization"?

"Informatization," also known as "informationization" or 信息化 (*xinxihua*), refers to a holistic framework that aims to modernize and transform an industrial society into an information society through the development of information and communications technology (ICT) industries and applications; information resources, infrastructure, and security; talent; and legal elements.[9]

disjointed nature of its administrative bodies and managing organizations, further obscures its leaders' true intentions from international view.[14]

Definitions of "Cybersecurity" Diverge from U.S. Concepts

In order to examine China's network security strategy properly, it is first important to understand gulfs in how China and the United States define cybersecurity/network security and other related terminology. As mentioned previously, in Chinese literature there currently exists no formal, authoritative terminology for "cyber," "cybersecurity," or other terms stemming from the word "cyber," though the Chinese government and scholars have adapted to its usage in English-language media.[15] Instead, China uses "information security" and "network security" to refer to similar concepts. Western scholars should recognize the differences and implications for each of the terms to include or infer cyber connotations.

Government, academic, and military literature relevant to the "cyber" domain often refer to "network"-related terminology (网络, *wangluo*). Parallels to English-language terminology include the use of the term "network space" (网络空间, *wangluo kongjian*) to refer to "cyberspace" (赛博空间, *saibo kongjian*) and the term "cyber operations" parallels the PLA term "network warfare" (网络战, *wangluo zhan*). PLA literature currently positions "cyber" concepts within the "information operations" domain (信息作战, *xinxi zuozhan*), although "information operations" also encompasses a broad range of other concepts in computing, psychological operations, and the electromagnetic spectrum.[16]

In Chinese literature there currently exists no formal, authoritative terminology for "cyber," "cybersecurity," or other terms stemming from the word "cyber," though the Chinese government and scholars have adapted to its usage in English-language media.

The PLA has formal definitions of network protection, network warfare, and information security. Based on the definitions highlighted below, this report argues that China's network security strategy incorporates the "use of information...to influence or control the direction of an opponent's decision-making activities"[17] to serve offensive and defensive goals.[18] These interpretations are broader than U.S.-equivalent initiatives on cybersecurity.

These definitions support the argument that the Chinese strategy for network security encompasses not only controls and regulation of information and network assets, but also their employment to serve national (i.e., domestic) objectives beyond pure defense or use in warfare. The United States' equivalent to a cyber strategy, the Comprehensive National Cybersecurity Initiative, established in January 2008, is more

DEFINITIONS

NETWORK WARFARE

The PLA's military dictionary defines "network warfare" (网络战, *wangluo zhan*) as: "also known as network confrontation. The destruction of the adversary's network of information systems and network information, the undermining of effectiveness of the adversary's use of its capabilities, while protecting one's own network of information systems and information in cyberspace. [19]

NETWORK PROTECTION

The PLA's military dictionary defines "network protection" (网络防护, *wangluo fanghu*) as: "to protect one's own information network system and data and taking preventative measures and actions to keep information safe, effective and functioning; includes network isolation, access control, intrusion detection, attack traceback, etc."[20]

INFORMATION DEFENSE

The PLA's military dictionary defines "information defense" (信息防御, *xinxi fangyu*) as: "also known as information protection. Ensuring the stable operation of one's own information systems, information security and the correct decisions and measures taken. Information defense includes electronic defense and network protection."[21]

INFORMATION OFFENSE

The PLA's military terms dictionary defines "information offense" (信息进攻, *xinxi jingong*) as: "information attacks. The utilization of information warfare technology to interfere and sabotage enemy information operations and information systems. Important tactics include electronic attack and network attack. The purpose is to affect and weaken the enemy's information acquisition, transmission, processing and utilization decisions."[22]

INFORMATION SECURITY

The PLA defines "information security" (信息安全, *xinxi anquan*) as: "The protection of information collection, processing, transport, and use from disruption, destruction or theft; the protection of normal use of information by its legitimate owners. Information security includes information content security, information systems security, information infrastructure security, information exchange security and information security awareness."[23]

limited in scope: It focuses on network defense and strengthening defensive capabilities at a technological and human capital level.[24]

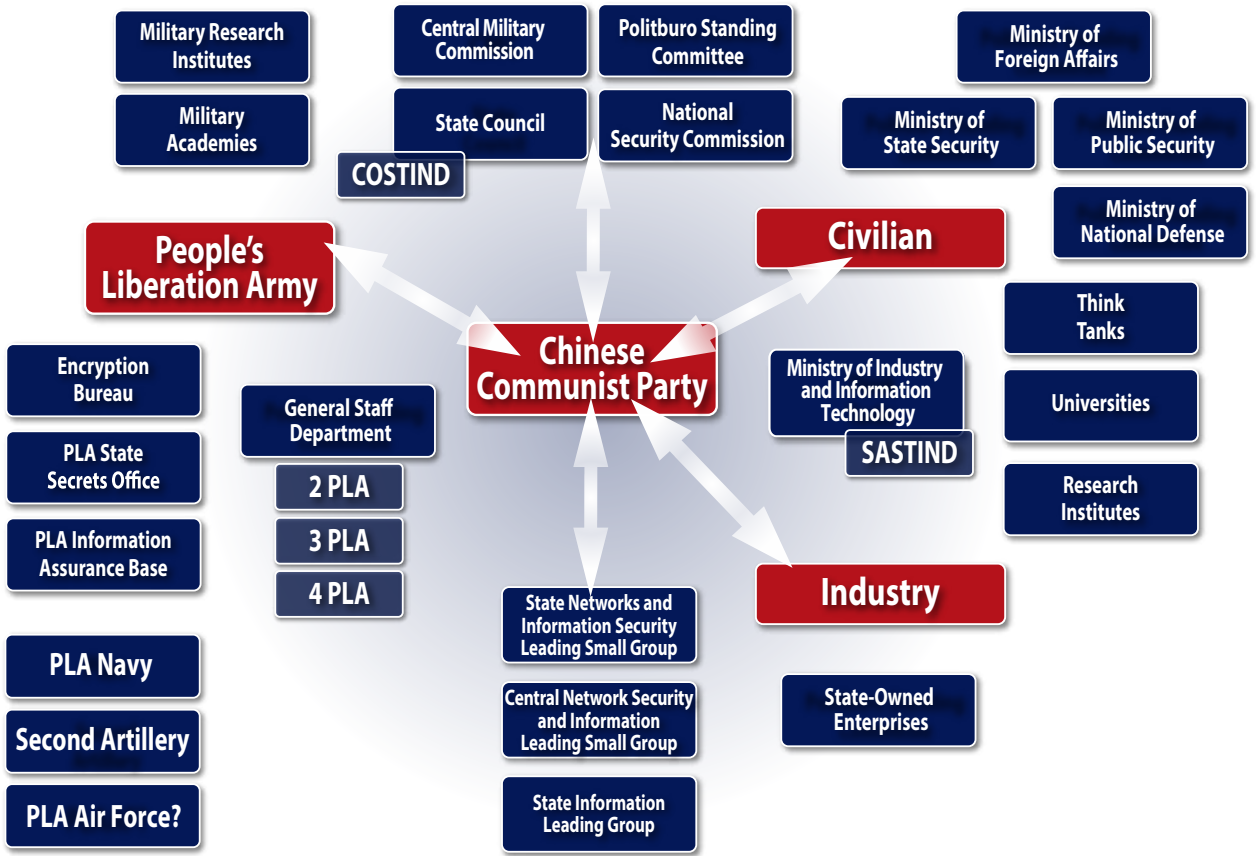
STAKEHOLDERS IN CHINA'S NETWORK SECURITY STRATEGY AND POLICY

The likely stakeholders in formulating and implementing network security are represented in Figure 1 below. [25] While not comprehensive, both the figure and list below serve as an indication that Chinese efforts to influence or execute network security represent an array of likely competing sectors and interests.

Stakeholders include:

- High-level decisionmakers
  - » Politburo Standing Committee
  - » Central Military Commission
  - » The State Council
  - » Commission for Science, Technology and Industry for National Defense (COSTIND) [before it dissolved in 2008, part of its duties went to SASTIND]
  - » Civilian government agencies (e.g., Ministry of Industry and Information Technology (MIIT), Ministry of State Security (MSS), Ministry of Public Security (MPS))
- State Administration for Science, Technology and Industry for National Defense (SASTIND)
- State Secrets Bureau
- State Encryption Bureau
- Party and State Leading Groups and Leading

FIGURE 1: STAKEHOLDERS IN CHINA'S NETWORK SECURITY



Small Groups (e.g., Central Network Security and Informatization Leading Small Group; State Informatization Leading Group; State Network and Information Security Coordination Small Group)

- National Security Commission
- The People's Liberation Army (e.g., General Staff Department (GSD) 2nd Department, GSD 3rd Department, GSD 4th Department, Encryption Bureau, State Secrets Office, intelligence departments of the PLA Navy, PLA Air Force and Second Artillery, PLA Information Assurance Base)
- Government-affiliated academic and research institutions (e.g., Chinese Academy of Engineering, Chinese Academy of Sciences, Central Party School)
- PLA academic institutions such as Academy of Military Science, PLA Information Engineering University, PLA University of Foreign Languages
- Academia and think tanks (Peking University, Tsinghua University)

Piecing Together China's Network Security Strategy

The advancements in China's network security from around 1986 to the present under the helm of Xi Jinping and his predecessors Jiang Zemin and Hu Jintao are noteworthy. To operationalize priorities set by China's leaders over the past three decades, the central government has been supporting domestic innovation of information technology and network weapons, modernizing and professionalizing its military, conducting cyber espionage of foreign entities for economic and military

TABLE 1: MAJOR HIGH-LEVEL CCP GROUPS ON NETWORK SECURITY

NAME	YEAR ESTABLISHED	SIGNIFICANCE
State Informatization Leading Group	1993, reinstituted in 2001, though no evidence of meeting between 2008 and January 2014	Staffed by high-level representatives of the central government and military, the group promulgates strategic guidance and advises senior political leaders on informatization, R&D, personnel, and information security policies The Leading Group did not meet between 2008 and January 2014; reasons are unclear but may be related to an absence of clear leadership or guidance
State Network and Information Security Coordination Small Group	2003	Staffed by senior government and military representatives, this small group focuses in particular on information security
National Security Commission	2013	With Xi Jinping at the helm, this group is a high priority for the Xi and other senior officials and focuses on domestic security concerns, of which network security is a consideration
Central Network Security and Informatization Leading Small Group	2014	Similarly with the National Security Commission, this group is important because of Xi Jinping's involvement and indicates the prioritization of network security in national security considerations

purposes, controlling discourse on the Internet for political stability, and maintaining leverage in bilateral and multilateral cyber relationships through information operations.

The focus on information technology and the promotion of network security technologies have roots in national-level initiatives begun in 1986 (establishment of State Economic Information Management Leading Small Group), 1999 and 2001 (establishment and re-establishment of State Informatization Leading Group), and 2003 (establishment of State Network and Information Security Coordination Group). These groups were tasked with developing indigenous information technologies and considering their implementation in a national security context.[26]

Momentum gathered in the late 1990s and early 2000s. For example, an initiative spearheaded by former President Jiang Zemin in 2001 and upheld by former President Hu Jintao during his tenure, the "integration of informatization and industrialization" (两化融合, *lianghua ronghe*),[27] promoted an integrated approach to IT development that attempted to turn China's historical disadvantages into strengths by rapidly "leapfrogging" over once-superior competitors. It was during this time that the CCP leadership also began to speak about national security and economic security as a reinforcing pair.[28]

In 2003, China – specifically the State Informatization Leading Group – released "Document 27: Opinions for Strengthening Information Security Assurance Work" (《国家信息化领导小组关于加强信息安全保障工作的意见》, *guojia xinxihua lingdao xiaozu guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian*), which set policy direction and strategic guidance on issues of information security, cryptography, research and development, personnel training, and public awareness.[29] While this document gained traction in paving the way for initial network security initiatives in China, and experts believe

that the Leading Group created frictions with other agencies because of the strong policy views held by bureaucrats in the Leading Group.[30]

As policies and stakeholders addressing network security grew, strategic direction for policy became more diversified, including input from the State Council, Central Committee (including Politburo Standing Committee and Central Military Commission), and Leading Small Groups (informal consultative bodies that advise the Politburo and State Council). The establishment of a National Security Commission (中央国家安全委员会, *zhongyang guojia anquan weiyuanhui*) in 2013 was also significant: It once again underscored the importance of security to the central government, as well as the government's inclusion of a broad swath of topic areas within its understanding of national security, including the economy and science and technology (S&T).[31] The National Security Commission has been widely viewed by analysts as a domestically focused committee specializing in social and political domestic stability, rather than a foreign policy body akin to the United States' National Security Council.[32]

In 2012, the State Council issued a new policy opinion to promote the development of Chinese information technology and information security.[33] While the 2012 opinion is in many senses a continuation of the 2003 opinion, emphasizing the dynamic monitoring of the Internet, critical infrastructure development, and the promotion of leadership and management of information security, the 2012 opinion also for the first time ties developments in information security to citizens' economic and social livelihoods and betterment. This broader scope implies that China has expanded its information security purview from "safeguarding national security information" to also include "promoting stable and rapid economic development and social harmony and stability."[34]

Among the Leading Groups and Leading Small Groups, the groups that regularly provide policy guidance on network security include:

- The State Informatization Leading Group (国家信息化领导小组, *guojia xinxihua lingdao xiaozu,* SILG);
- The State Network and Information Security Coordination Small Group (国家网络与信息安全协调小组, *guojia wangluo yu xinxi anquan xietiao xiaozu*, SNISCSG);
- The Central Network Security and Informatization Leading Small Group (中央网络安全和信息化领导小组, *zhongyang wangluo anquan he xinxihua lingdao xiaozu*).

While much remains obscure about the nature and activities of the various groups, the presence of high-level politicians within them indicates that they likely play a key role in guiding national strategy. The Central Committee of the Communist Party of China and the State Council initially formed the State Informatization Leading Group in 1993, and then reconstituted it in 2001 to provide leadership on the promotion of informatization and on the safeguarding of state information security.[35] Scholars have observed that the SILG did not meet between 2008 and 2014, which may be indicative of an absence of clear leadership or guidance.[36] MIIT manages the group and carries out specific tasks related to implementing informatization.[37]

The SNISCSG was formed as a subgroup of SILG; it focuses on network and information security and facilitates the promotion of information security protection systems and information security management and operation.[38] SNISCSG is chaired by Li Keqiang, and the small group drafted China's national civilian network security strategy ("Document 27") and approved major network security-related policies and national strategies. The SNISCSG disbanded in 2008 and was reconstituted in 2009, though "there is no public record of meetings since then."[39] Then, in February 2014, China announced the establishment of a Central Network

TABLE 2: INFLUENTIAL LITERATURE IN CHINA'S NETWORK SECURITY STRATEGY

DOCUMENT TITLE	ACTOR	YEAR WRITTEN	SIGNIFICANCE
Military Strategic Guidelines	People's Liberation Army	1956, 1980, 1993	Authoritative documents that represent the PLA's strategic priorities and objectives in modernization, force structure and organization; provides insight on how the PLA would wage war
"Document 27"	State Council	2003	Outlined China's national civilian network security and information security strategy
"National Informatization Development Strategy, 2006–2020"	Communist Party Central Committee and State Council	2006	Indicates priorities of central government arm that is responsible for information security, telecommunications, the Internet, and the research and development of electronic and information technology products; this plan highlights investment in protection of government information systems
The Science of Military Strategy	Academy of Military Science	Latest edition: 2013	Strategic thought on how the PLA would prepare for, prevent, and wage war
White Paper: The Diversified Employment of China's Armed Forces	Chinese government (civilian and military)	2013	Authoritative documents that represent both the PLA and civilian government on China's domestic and national security policies, stipulates national security interests in cyberspace and the possibility of deployment of military forces in cyberspace
"Opinion on Further Strengthening Military Information Security Work"	Xi Jinping, Central Military Commission	2014	Sets forth the guidelines, basic principles, key tasks, and support measures for military information security work

Sources: CPC Central Committee and State Council, "Guojia xinxihua lingdao xiaozu guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian [Opinions for Strengthening Information Security Assurance Work]," September 9, 2003; CPC Central Committee and State Council,*2006–2020 nian guojia xinxihua fazhan zhanlüe [2006–2020 National Informatization Development Strategy]*, March 19, 2006, http://www.gov.cn/gongbao/content/2006/content_315999.htm; Academy of Military Science Strategic Research Department, *The Science of Military Strategy,* (Beijing: Military Science Publishing House, 2013); Information Office of the State Council, "White Paper: The Diversified Employment of China's Armed Forces," April 2013, http://eng.mod.gov.cn/Database/WhitePapers/; and "Jing Xi Jinping zhuxi pizhun zhongyang junwei yinfa 'guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian' [Chairman of the Central Military Commission Xi Jinping approved the issuance of 'Opinion on Further Strengthening Military Information Security Work']," *Jiefangjun bao* [PLA Daily], October 7, 2014, http://news.xinhuanet.com/mil/2014-10/07/c_1112726181.htm.

Security and Informatization Leading Small Group, headed by President Xi Jinping and Premier Li Keqiang.[40] Though not much has been revealed about the groups' exact contributions to network security, both Chinese sources and Western observers have noted that they are domestically oriented.[41]

Further, at the Eighteenth National People's Congress in 2012, former President Hu Jintao underscored network security as a matter of "great importance."[42] The Eighteen Party Congress' Third Plenum in 2013 also displayed unprecedented thought on network security, advocating for strategic planning, safeguarding national networks and increasing R&D funding for technology development.[43] Further spurred by Edward Snowden and the disclosure of National Security Agency (NSA) programs, the government has ramped up efforts to procure domestic computer security products for central

TABLE 3: CHINESE JOURNAL ARTICLES SEARCH RESULTS FOR KEY TERMS

TERM	2009	2010	2011	2012	2013
信息战争, ***xinxi zhanzheng,*** **information warfare**	5,260	6,789	7,359	10,335	11,336
信息战略, ***xinxi zhanlüe,*** **information strategy**	53,119	57,004	59,627	73,760	75,196
网络战争, ***wangluo zhanzheng,*** **network warfare**	2,514	3,517	4,006	6,099	6,971
网络战略, ***wangluo zhanlüe,*** **network strategy**	29,478	32,470	34,872	45,765	47,707
赛博安全, ***saibo anquan,*** **cybersecurity**	40	66	84	107	108
赛博空间作战, ***saibo kongjian zuozhan,*** **cyberspace operations**	76	104	145	157	165

Source: China National Knowledge Infrastructure, http://www.global.cnki.net/kns50/single_index.aspx.

government and military use, among other means of preparation for cyber conflict.[44] President Xi's June 2014 speech at the Chinese Academy of Sciences and Chinese Academy of Engineering annual conference also made clear that the central government will continue to prioritize innovation in core technologies.[45]

While China has never publicly issued any formal strategic doctrine for cyber or military applications of information technology, it has published Military Strategic Guidelines (军事战略方针, *junshi zhanlüe fangzhen*) that provide authoritative directives for defense policy and military modernization. Although the full text of these guidelines is unavailable in open source literature, they are known to align with other Chinese policy documents from the same era in their references to the need to prepare to "fight local wars under high-tech conditions" – terms that imply the importance of information technology in Chinese operational plans.[46]

Additionally, authoritative texts on military strategy, such as the Academy of Military Science's *The Science of Military Strategy* have had an influence on China's network security strategy and policy, though it is unclear how closely the military follows the principles outlined in the book's latest edition. Chapters in *The Science of Military Strategy* detail the evolution and development of high-tech local war, observations about its characteristics, and strategic guidance on how to approach high-tech local wars.

Most recently in October 2014, Xi Jinping and the Central Military Commission (the highest military policymaking body in command and control of the PLA) released a document with guiding

ideology, basic principles, and priorities for the PLA: "Opinion on Further Strengthening Military Information Security Work" (《关于进一步加强军队信息安全工作的意见》, *guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian*). The opinion provided guidelines and basic principles for military information security, and stressed the development of PLA defensive capabilities, as well as their ability to fight and win a war.[47]

In the 2013 White Paper, *The Diversified Employment of China's Armed Forces*, China refers to its right to "protect… national security interests in outer space and cyber space," though also mentions that "[w]e will not attack unless we are attacked; but we will surely counterattack if attacked."[48] China continually emphasizes its defensive posture in all aspects of warfare, including network security (exercising a concept originally coined by Mao Zedong called "active defense, " which "is based on the premise of striking only after the enemy has struck, but will employ offensive operations at all levels of war and at all stages of conflict."[49]). However, in practice, the actual balance of offensive versus defensive actions of China's computer network operations forces is unknown. Reports such as *APT1* and *Axiom Threat Actor Group Report* by U.S. cybersecurity firms Mandiant and Novetta Solutions, respectively, have both indicated a sophisticated level of network attack operations used against government, industrial, commercial, and even political targets from PLA-affiliated entities, although China has continually denied these accusations.[50]

The increase in Chinese civilian and military research on network security over the years reinforces Chinese leadership's prioritization of formulating and funding research into network security technologies and strategies, as noted by a steady increase in the number of academic journal articles published in Table 3.[51] Major topic areas highlighted on previous page have seen a range of 40 to 277 percent increase in just four years between 2009 and 2013. Note also, on previous page, how "cyber" terminology is not particularly prominent in Chinese academic literature, reflective of the broader terminology distinctions from Western parallels. The table below indicates the extent of each term's usage in Chinese: Search results for "cyber"-related terminology pale in comparison to "network"- or "information"-related search terms.

IV. EXPLAINING CHINA'S MOTIVATIONS IN CYBERSPACE

Based on authoritative statements on network security and on China's observed behavior, China's network security strategy is, just as with its overall strategy, primarily driven by the goal of prolonging the power of the Chinese Communist Party, and domestic concerns maintaining internal stability, curbing social and political unrest, and promoting economic growth.[52]

Drivers can be observed through three main lenses: economic, political, and military. China's network security strategy aspires to protect and promote its domestic economy, allows sufficient latitude for maintaining domestic security through information control measures, and promotes military development, providing direction for both defensive and offensive measures. Announcements by Xi Jinping in 2013 to strengthen military involvement in domestic security concerns, and Hu Jintao's "New Historic Missions" for the PLA both support the argument that issues such as network security are primarily a domestic concern to maintain CCP rule and safeguard China's national interests.[53]

China's foreign policy furthers these same goals, for it attempts to convince the international community to conform to Chinese norms on network security. Further, by engaging the international community, China wishes to signal to other countries that it is a responsible and cooperative actor on technology issues. China has expressed willingness to conform to some norms on behavior in cyberspace, but these may be only at face value to avoid further scrutiny from international actors. Parallel examples of this behavior can be seen in other areas of Chinese foreign policy: China's accession to United Nations Convention on the Law of the Sea (UNCLOS). While it is a signatory to the regime, China has also cited major reservations and failed to observe critical clauses.[54]

China's network security strategy is, just as with its overall strategy, primarily driven by the goal of prolonging the power of the Chinese Communist Party, and domestic concerns maintaining internal stability, curbing social and political unrest, and promoting economic growth.

Economic: Hacking and Cyber Crime

The economic component of China's network security strategy has two main drivers: ensuring continued economic growth and deterring domestic cybercriminal activity. First, as China's economic growth rate declines and China's population ages, maintaining economic stability for a country of 1.3 billion people is a major concern.[55] China attempts to ensure domestic economic growth and maintain domestic firm competitiveness against global rivals in part by conducting cyber economic espionage.[56]

Industrial cyber espionage, where countries and non-state actors exfiltrate large amounts of industrial economic information including trade secrets, research and development, and products, occurs at a massive scale in China. While a dollar amount on the losses to the U.S. economy are impossible to count, FBI Director James Comey said in a recent interview that it costs the United States "billions."[57] The U.S. Office of the National Counterintelligence Executive (NCIX) described Chinese cyber actors in a report about foreign spies as "the world's most

active and persistent perpetrators of economic espionage."[58] Admittedly, the difficult nature of measuring the level of these impacts limits our knowledge of the true extent of cybercrime and cyber espionage by China.[59]

The economic component of China's network security strategy has two main drivers: ensuring continued economic growth and deterring domestic cybercriminal activity.

Despite what top U.S. officials have alleged, China in fact conducts economic espionage not simply to collect "information that's useful to them so they don't have to invent," but also because it would bolster indigenous innovation, domestic industry, and research and development.[60] The demand for economic growth is pressing enough for China to resort to approaches such as intellectual property theft to garner it.

The United States has repeatedly requested that China cease economic industrial espionage, insisting that China's behavior falls outside of recognized espionage norms. The United States argues that (1) despite the Edward Snowden leaks on U.S. government espionage, its own espionage activity falls within the realm of acceptable behavior for national security purposes, and (2) it is not acceptable state behavior to bestow stolen foreign intellectual property upon domestic companies. China counters U.S. statements, in part by pointing out incidents where the United States has had questionable grounds for espionage.

In February 2013, Mandiant released a report, *APT1*, accusing an alleged PLA unit (Unit 61398) of the General Staff Department in Shanghai of committing large-scale industrial cyber espionage against U.S. targets. According to the report, the CCP likely sponsored Unit 61398 to fulfill national objectives.[61] A report released in October 2014 by Novetta Solutions about a state-sponsored threat group they named Axiom complements these findings. The report argues that Axiom is "responsible for directing highly sophisticated cyber espionage operations" against government agencies, manufacturers, and firms that are of strategic economic interest, including environment, space and aerospace, energy, information technology and telecommunications.[62]

The United States, in the 2013 and 2014 Department of Defense (DOD) Annual Reports on China's military and security developments, publicly declared that cyber espionage and intrusions "appear[ed] to be attributable directly to the Chinese government and military."[63] China refuted (and continues to refute) these accusations, insisting that the country does not support "any hacker activity," and cited its own victimization by network attacks in an attempt to distance itself from the attacks.[64]

There currently exist few incentives for China to cooperate meaningfully with more developed nations on curbing intellectual property theft, cybercrime and other criminal issues that occur across borders. In the realm of economic and industrial espionage, whether or not the actions of third party actors are state-sponsored, it is without question that China's domestic economy benefits from the troves of data, technology, and information it receives from these sources.[65] As long as the perceived risks of exfiltrating large amounts of sensitive economic and military data remain low, China will not likely cease these activities. Some of these risks would include incurring substantive economic costs (e.g., sanctions, loss of

business from abroad), political repercussions (e.g., cessation of diplomatic ties), or military retaliation, though these punitive actions are currently unlikely because they would also drastically affect U.S. domestic interests such as the economy.

The Chinese government worries that unrestricted Internet access or uncontrolled information or dissent might pose a significant risk to the Chinese communist regime's stability and hold on power.

China's second concern is domestically focused on hacking and criminal activity within its own borders. China claims that its economy can be severely hampered by hacking and cybercrime, which target corporations, banks, and individuals for real asset theft (i.e., bank accounts and credit cards), virtual asset theft (e.g., identity theft), abuse of Internet resources and services (e.g., abusing vulnerabilities in Internet services and providers for profit), and black hat[66] sales in providing cyber criminals with viruses, attack tools, and training.[67] Western observers claim persuasively that China experiences high levels of cybercrime due in part to rampant use and distribution of pirated technology, which, among a host of other issues, makes it difficult for security updates and patches to reach users and creates vulnerabilities for criminals to exploit.[68]

Another level of complexity in defending against cybercriminal activity in China, as Li Yuxiao, Director of the China Internet Governance Research Center at Beijing University of Posts and Telecommunications (BUPT) highlights, is the rise of mobile technology and lack of risk awareness or defensive measures.[69] A recent report by China's National Computer Virus Emergency Response Center indicated that 54.9 percent of computers in China are infected with viruses, and that 1,367 out of 2,714 government portals examined in 2013 reported security loopholes.[70] With 591 million Internet users in China, and the magnitude with which individuals and corporations conduct business and commerce electronically, China is particularly vulnerable to cybercrime.[71] China exerts spotty scrutiny to the economic problem: It exhibits complacency or even direct government culpability in some circumstances (e.g., international economic industrial espionage) while combating the issue in others (e.g., identity theft and other related criminal activity).[72]

Political: Information Management and Dissemination

China also employs or sanctions cyber activity (e.g., limits to information access on the Internet or social media and networking sites) for the protection of domestic political stability. For example, the Chinese government is preoccupied with "revisionist organizations," "separatists, extremists, splittists," and Western imperialist forces, thus screening Internet and social media and promoting propaganda to counter these forces.[73] As of October 2014, official Chinese media reported that Beijing had "nabbed some 30,000 suspects involved in cyber crimes in an online crackdown that began in 2011." Over the past three years, the Beijing Public Security Bureau noted that it deleted 17 million "illegal" online messages, and detained 50 suspects "implicated in terrorism activities."[74] Project these trends from Beijing's Public Security Bureau on a national level, and the magnitude of online censorship and arrests would be notable and alarming.

The Chinese government worries that unrestricted Internet access or uncontrolled information or dissent might pose a significant

Network operations "are expected to play an important role" in military scenarios involving Taiwan, other territorial or maritime conflicts or the United States.

risk to the Chinese communist regime's stability and hold on power. To mitigate some of this risk, China has implemented measures such as requiring "Real Name Registration" for social media (e.g., microblogs in 2011[75] and instant messaging services in 2014[76]) and mobile phones in 2013.[77] Allegedly instituted to "protect web users' interests and [improve] credibility on the web," the rules also aim to limit "information that leaks state secrets, damages national security and interests, and instigates ethnic resentment, discrimination, or illegal rallies that disrupt social order."[78] China's use of terminology – by couching network security under information security – allows the country to focus on threats not just to its security, but also to its stability.[79] China's take on information security grants the government agency to conduct information management (i.e., controlling information and communication technologies, and filtering information or censoring speech) to limit threats to the regime.

The Axiom report indicates that Chinese actors similarly use malware to monitor or infiltrate domestic targets of particular political importance, such as pro-democracy non-governmental organizations, political dissidents in China or universities in Hong Kong.[80] China also resorted to information management during the Hong Kong protests that started in late-September 2014, when activists in Hong Kong were concerned about Beijing's role in their electoral politics and their prospects for genuine democracy in the region. In addition to information control on media platforms from broadcast news to social media updates, China also employed a mobile remote access trojan (mRAT) called Xsser mRAT, which extracted large amounts of information from infected mobile phone users, including "SMS, email, and instant messages, location data, usernames and passwords, call logs and contact information."[81] The desire for information indicates Beijing's desire to understand and manage the protests.

In foreign affairs, the Chinese government also employs non-state actors to make (or at least does not prevent them from making) "credibly signal coercive threats" to disagreements or conflicts with other states.[82] The connection to the state is blurry, though there has been a correlation between a bi- or multilateral dispute and the incidence of malicious cyber activity against the adversary. For example, Japan reported surges in cyber intrusions on government websites and systems after maritime territorial disputes. In September 2012, Japanese government sites were attacked after it was announced that Japan bought three islands in the disputed Senkaku Diaoyu Island chain.[83] China also has an unconfirmed, but suspected connection to non-state actors who commit acts of economic, industrial, and military cyber espionage. The ambiguous line between Chinese government actors and state-sponsored actors in this realm makes it particularly difficult for outside law enforcement, policymakers, and intelligence communities to attribute blame.[84]

China therefore proposes a distinct method of cyber governance that diverges from Western notions of protective measures, arguing for sovereignty in cyberspace, which would allow China to "control" Internet traffic within its borders. While the Western notion of cyberspace encompasses an open, free flow of information across borders, China's language on cyberspace specifically employs the word "sovereignty," implying China's ability to control its

own Internet and administer what happens within its own borders. This debate manifests in bilateral meetings and international institutions, where states with an interest in controlling information such as China and Russia argue for "sovereignty" over their domestic networks.

Military: Network Applications in Warfare and National Defense

Chinese discourse on the use of network and information technology in the military has existed for decades, but the major turning point in China's approach to information technology and information warfare arose from the United States' employment of advanced military technology in the Gulf War.[85] China has since strongly emphasized the importance of information and communications technology for the future of warfighting, aspiring to prevail in "local wars under informatized conditions by 2050."[86]

Foundations for considering China's network strategy are rooted the PLA's broader strategic literature, such as the Military Strategic Guidelines (军事战略方针, *junshi zhanlüe fangzhen*) and *The Science of Military Strategy* (战略学, *zhanlüe xue*), government initiatives, such as Hu Jintao's New Historic Missions (新的历史使命, *xinde lishi shiming*), and the National Defense White Papers.

In these texts, military strategists have explored strategies to exploit the network domain in both offensive and defensive scenarios. Because of different strategic cultures, military literature does not clearly distinguish between defensive and offensive measures, and thus what the United States or other foreign actors deem offensive may be interpreted as defensive by China. The principle of "active defense," for example, which Mao Zedong referred to as warfare that "consists of the alternate use of the defensive and offensive," is one that continues to stoke analytic debate among U.S. policy and academic communities.[87]

As can be implied from PLA terminology and definitions of conditions for information security, China's military network strategy has components intended for both peacetime and in times of war, including both domestic scenarios and foreign contingencies. The Chinese interpretation of network security not only includes regulation of information and network assets, such as Internet content within its realm of authority, but also considers military conflict with adversaries, as indicated by China's acceptance of United Nations (U.N.) international law in the cyber realm and its response to major U.S. strategic shifts in cybersecurity (e.g., the establishment of Cyber Command). As China scholar Michael Swaine argued, civilian and military elites both share support for "pragmatic, development-oriented policies designed to sustain or expand social order, regime unity, social prosperity and national power and prestige."[88]

Network operations "are expected to play an important role" in military scenarios involving Taiwan, other territorial or maritime conflicts, or the United States.[89] Chinese strategists have hypothesized that with informatization "a new pattern of cyberized war is going to appear" and the People's Liberation Army is aware of potential applications of information technology in a wartime scenario such as in information warfare (i.e., attacking an adversary over network connections) and in command, control, communications, computer, intelligence, surveillance, and reconnaissance (C4ISR) operations.[90] Chapters in *The Science of Military Strategy* discuss the evolution and development of high technology use in war and the importance of the information domain to national security and development interests.[91] The recently updated 2013 *Science of Military Strategy* dedicates an entire section on conflict in the network domain and discusses types of military conflict in the network domain (network reconnaissance, network attack and defense operations, and network deterrence) and ways to prepare for potential military conflict.[92]

The PLA's role in network security relates closely to two other major elements of China's network security strategy: economics and politics. It is important to understand that the PLA by nature is a party military (i.e., for the CCP), not a state military, like that of the United States, which serves to protect the nation regardless of who is in power. This has implications for the PLA's objectives and functions. As outlined in former President Hu Jintao's "New Historic Missions," the primary goal of the PLA is to provide an important guarantee of strength for the party to consolidate its ruling position, tying its operations to CCP political objectives.[93] The secondary goals of the PLA in Hu's "New Historic Missions" include providing strong security guarantees for national development and the safeguarding of national interests. China's national interests concern both political and economic objectives that are domestically driven (though potentially with international implications). For this reason, foreign observers see PLA involvement in (1) utilizing computer network operations for political objectives and (2) conducting cyber industrial espionage of industrialized nations for economic gain. Evidence from *APT1*, the Axiom report, and the installation of malware on 2014 Hong Kong protesters' mobile phones links the PLA with CCP economic and political objectives.

While China alleges that its activity to ensure network security – including military preparation for cyber conflict – is defensive in nature,[94] Western sources imply that neither observed Chinese behavior in cyberspace nor its military capability buildup reflect China's stated position.[95] Authoritative U.S. government documents often describe China as "using its computer network exploitation capability to support intelligence collection against the U.S. diplomatic, economic, and defense industrial base sectors that support U.S. national defense programs."[96] Mandiant's *APT1* report states: "APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations… The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan."[97] The Axiom report reinforces this finding: Its actions "fit in particularly well with China's strategic interests and with their most recent Five Year Plans …in 2006 and 2011."[98] Concurrent with its network intrusions, references to "elite, specialized network warfare forces" in the *Science of Military Strategy* indicate that military leaders are actively cultivating a human capital base for network attacks for both offensive and defensive strategies and capabilities.[99]

V. CHINA'S INTERPRETATION OF U.S. ACTIVITY IN CYBERSPACE

As China cultivates its own network security infrastructure, it also spends time studying foreign actors' cyber capabilities and strategies. China considers U.S. cybersecurity strategy to be hypocritical and threatening to Chinese interests: Chinese analysts have highlighted how the United States uses its network and information technology to interfere in the internal affairs of other nations, and how U.S. hegemony in the network domain endangers China's political, network, cultural, and military security.[100]

Each of the cases highlighted below – the U.S. declaration of cyberspace as a new domain of warfare in July 2011; the Snowden intelligence leaks in May and June 2013; and the U.S. Department of Justice indictment of five PLA officers for economic espionage in May 2014 – indicate that regardless of the avenues pursued to change China's behavior (military, diplomatic, and criminal, in these instances), U.S. behavior modification efforts that threaten the existence of the CCP are likely to provoke undesirable reactions.

Although there has historically been a degree of tumult in the U.S.-China relationship, the degree of interdependence between the two nations means that both cooperative and conflicting interactions are to be expected. Over the past several years, the United States has confronted China on several occasions about transparency and cyber intrusions allegedly aimed at exfiltrating U.S. commercial and military data. Efforts to resolve these differences have stalled with U.S. classified intelligence leaks from former U.S. government contractor Edward Snowden – which revealed extensive surveillance and espionage programs that included Chinese targets – and Chinese discontent over the Department of Justice indictment of five PLA hackers.[101]

In response to the indictment, China resolutely denied any connection with hacking and suspended the U.S.-China Cyber Working Group (CWG), which had been convened only months earlier to dispel mistrust and promote bilateral engagement on cyber issues.[102]

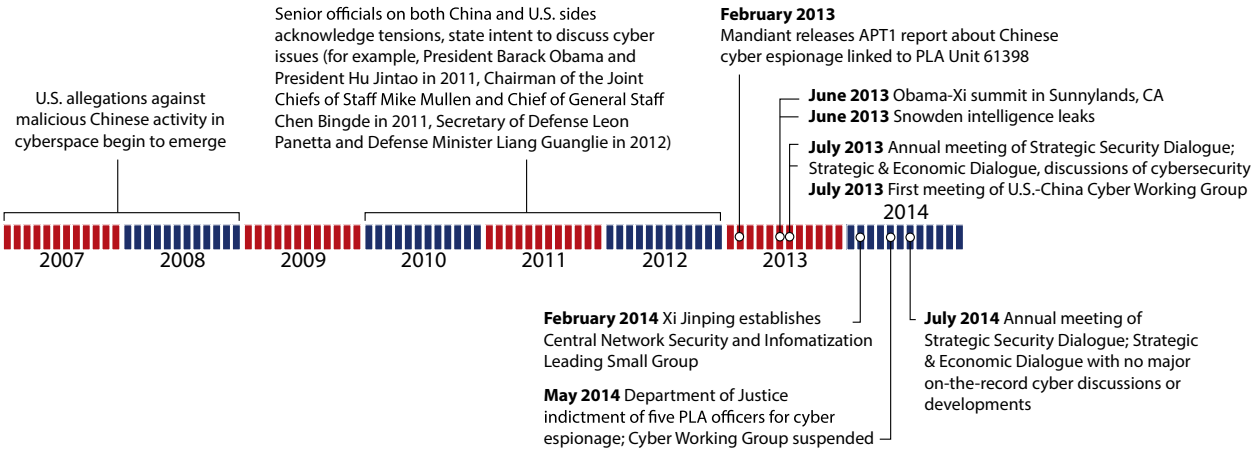
The Effect of U.S. Declaration of Cyberspace as a New Domain of Warfare

The United States' establishment of U.S. Cyber Command (CYBERCOM) in June 2009[103] and consequent declaration of cyberspace as a new domain of warfare in July 2011[104] has changed the contours of the global battlefield. Cyber Command is a joint sub-unified command under U.S. Strategic Command (STRATCOM) to direct military cyberspace operations and defend military networks. CYBERCOM shares its commander/director with the civilian National Security Agency (NSA), which provides the NSA with intelligence, administrative, and logistical support.[105]

Responses from Chinese media to this development have been scathing. A July 2011 editorial in the state-run *People's Daily* interpreted it as a destabilizing progression towards a new "Cold War mindset" that would "threaten world peace." The editorial posited that cyberspace "will become a new international battlefield" marked by an unavoidable cyber arms race.[106] Other editorials have advocated for just such a race in response, to ensure that China does not fall behind. In December 2011, a *China Defense Daily* editorial listed objectives key to an effective command system for cyber war mobilization in China:[107]

- Develop a centralized command structure that integrates the military, state, organizations, industry, and even individuals;
- Train military and civilian personnel in network warfare; modeling off similar structures in the United States, Britain, and South Korea, the PLA should also form network warfare units, cyber armies, and cyber reserve units;

FIGURE 2: TIMELINE OF MAJOR EVENTS IN THE U.S.-CHINA CYBER RELATIONSHIP, 2007–2014



- Utilize the full range of offensive and defensive measures for higher effectiveness; and
- Have a strong grasp of indigenous technologies, but also conduct further research and development into new offensive weapons

While shunning the U.S. development as an escalatory step towards cyber conflict, China has simultaneously taken steps to emulate similar developments in its own military. Academic studies at institutions affiliated with the PLA (e.g., Harbin Institute of Technology) have been devoted to studying the development and what the implications are for further research in cybersecurity and cyber war. [108]

The Effect of the Snowden Intelligence Leaks

During May and June 2013, Edward Snowden released troves of information on the NSA's programs, which included the PRISM project – a clandestine electronic surveillance program that collected global communications data. The leaks reversed momentum towards what could have been a breakthrough in U.S.-China cyber relations: Enough pressure had been mounted against China for industrial cyber espionage that an agreement between Presidents Xi Jinping and Barack Obama during their June 2013 summit would have implicitly found China culpable.[109]

China's Foreign Ministry spokespeople and state-sponsored media used the Snowden disclosures to turn the narrative around, pointing out U.S. hypocrisy on the issue, despite apparent differences between U.S. collection of intelligence and Chinese collection of industrial secrets. China's Foreign Ministry spokesperson Hua Chunying said that the Snowden leak "shows once again that China falls victim to cyber attacks."[110] China's employment of misinformation and denial in the wake of the Snowden leaks have allowed China to avert blame for cyber espionage, to turn blame towards the United States, and to continue its espionage operations without major repercussions.[111]

The Effect of U.S. Department of Justice Indictment of PLA Officers

Despite evidence to the contrary, China resolutely denies any malicious cyber activity against the United States and U.S. industries. To signal its dissatisfaction with China's behavior, the U.S. Department of Justice (DoJ) indicted five PLA officers for economic cyber espionage against U.S. companies in May 2014.[112] The United States government chose to pursue the matter through

DoJ to indicate the criminality of the activity (as opposed to taking action through the DOD or the State Department, which would have placed cyber espionage in the military or diplomatic realm). Despite this consideration by the United States, China responded with fury: refuting the charges as fictitious, absurd, and a serious violation of basic norms of international relations.[113] China suspended the bilateral Cyber Working Group, "banned Windows 8 from being installed on government computers, ordered state-owned enterprises to cut ties with U.S. consulting companies," and declared its intent to vet IT products.[114]

There have been no marked changes in Chinese behavior (i.e., cessation of cyber espionage activity or acknowledgement of culpability of espionage), though Chinese state-sponsored media has – as it did in the Snowden case – tried to turn the blame towards the United States. In addition to painting itself as a victim of U.S. hacking activities, China has accused the United States of violating "basic norms governing international relations," though it has not specified which norms were violated.[115]

The failure of the U.S. indictment to deter Chinese cyber espionage underscores that it will take time to advance norms of appropriate behavior in cyberspace, especially in cases where doing so threatens the interests of the CCP. There will be short-term obstacles, such as the current freeze in bilateral cyber relations. Still, the U.S. decision to pursue the indictment through DoJ set a powerful precedent establishing cyber espionage as criminal behavior – powerful enough to merit delaying formal bilateral relations on cyber issues.

China's Position on Cybersecurity in International Institutions

Because international norms and law have yet to codify computer network operations and cyber activity, Chinese investment and activity may set the course for relevant international trends.

Recently, China has modified its previously held views that the laws of armed conflict do not apply to the cyber realm.[116] As a member of the 15-member U.N. Group of Governmental Experts (GGE) – a body whose mandate is to study and build norms in the information space – China agreed in a June 2013 report released by the GGE that the U.N. international law should guide state behavior in the cyber domain.[117]

The report states that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful, and accessible [information and communication technology] environment."[118] China also agreed to the norm that "states must meet their international obligations regarding internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts. States should seek to ensure that their territories are not used by non-state actors for unlawful use of [information and communication technologies]."[119]

China's acceptance of the applicability of international law to cyberspace indicates one instance of conformity to Western norms. However, there are other sections of the report that maintain a fierce Chinese commitment to state sovereignty over ICT-related activities.[120] China reinforced this view at a December 2013 China-South Korea Internet Roundtable Conference, where Lu Wei of China's State Internet Information Office referenced the U.N. Charter and extended its concept of state sovereignty into cyberspace.[121] Similarly, Li Yuxiao of BUPT has applauded international cooperation to solve issues of cybersecurity, but he has also argued that "there are differences between countries, so it is impossible for all countries to do everything in the same style. Every country has its own problems in Internet security. It is unfair for one country to criticize others according to its own policies."[122]

On October 23, 2013, the Chinese Delegation on Information and Cybersecurity used its remarks to the 68th U.N. General Assembly to chastise unnamed nations for "[developing] cyber military capabilities and [threatening] others with preemptive strikes" and employing ICT tools to "interfere in other countries' internal affairs." The Chinese delegation argued that state activity in cyberspace (referred to as the "information space" in the document) should "adhere to the principle of balance between freedom and law," and avoid "[undermining] other countries' political, economic and social stability as well as cultural environment."[123] Such rhetoric closely reflects China's long-held suspicions of international institutions, linked to deeply ingrained historical and political anxieties. As other China observers have noted: "Even as China has accepted change, the perpetuation of collective memories about past violations of Chinese sovereignty, coupled with ongoing concerns about the fragility of Beijing's rule over China, has made Chinese acquiescence especially tenuous and contingent."[124]

Limited Traction for U.S.-China Cyber Cooperation

Despite its aversion to perceived sovereignty infringements, China has taken some limited steps towards becoming more transparent about its cybersecurity position. Bilateral fora, such as the (currently suspended) U.S.-China Cyber Working Group, were indicative of a willingness to engage in dialogue, even if resulting actions remain elusive. We can expect this trend to continue for the foreseeable future, unless major shifts in politics (e.g., changes in U.S. approaches to engagement/conflict with China) or incentives change China's domestic and foreign policy risk calculus and objectives.

Currently, however, through its public conduct and strategic positioning, China has largely been able to shape U.S. perceptions on cyber issues and to garner traction in the international sphere with other like-minded nations. Based on its understanding of U.S. objectives in cyberspace and its apt assessment of U.S. vulnerability post-Snowden, the Chinese central government has thus far found it easy to avoid collaborating with the United States. China has three main strategic reasons for resisting change.

Through its public conduct and strategic positioning, China has largely been able to shape U.S. perceptions on cyber issues and to garner traction in the international sphere with other like-minded nations.

First, pursuing a collaborative and transparent relationship would run counter to the Chinese government's priorities. For example, the United States requests that China lessen its restrictions on civilian access to Internet, which would threaten the central government's objective to maintain political stability through control of online information and discourse.[125]

Second, China has observed that the United States has remained eager to collaborate and share information about its cyber strategy without guaranteed reciprocation. For example, prior to U.S. Defense Secretary Chuck Hagel's visit to China in April 2014, the Obama Administration briefed the Chinese military leadership on "the Pentagon's emerging doctrine for defending against cyberattacks against the United States" and its use of "cybertechnology against adversaries, including the Chinese" to alleviate potential concerns of conflict escalation between the two

states.[126] These earnest efforts went unreciprocated, yet Pentagon officials, such as Rear Admiral John Kirby, have continued to "stress to the Chinese that we in the military are going to be as transparent as possible…and we want the same openness and transparency and restraint from them."[127] Under the guise of "mutual transparency," China has effectively secured access to sensitive U.S. information while offering little in return.

Third, the United States lost significant moral high ground after the Snowden intelligence leaks, which gave China ammunition to delay or refuse any requests to modify its behavior in cyberspace. Numerous statements from official Chinese sources verify this. For example, in protest against the DOJ indictments of five PLA officers for hacking, a *Xinhua* article said, "The United States filed ungrounded commercial cyber espionage charges against five Chinese military officers, despite its own flawed record in surveillance."[128] The Ministry of Foreign Affairs said that the indictment came from the "hacking empire"[129] and was a gross violation of norms that "jeopardizes China-U.S. cooperation and mutual trust."[130]

VI. CONCLUSION

Tensions run deep in the U.S.-China bilateral cyber relationship. The United States and China have fundamentally different conceptions of cyber/network security, which influences the strength and depth of cyber relations and affects broader bilateral dynamics.

The primary driver for China's network security strategy formulation remains the maintenance of CCP governing power. China's burgeoning network security strategy has economic, political, and military manifestations, and is closely linked with other national security priorities (e.g., territorial integrity, domestic political and social order, economic growth, and military modernization) that contribute to the consolidation of CCP power. Senior U.S. officials have also recognized this trend: Director of National Intelligence James Clapper testified before the Senate Foreign Relations Senate Select Committee on Intelligence on January 29, 2014 that "China's cyber operations reflect its leadership's priorities of economic growth, domestic political stability, and military preparedness."[131]

Despite high-level guidance and strategic direction from Xi Jinping and senior civilian and military officials, however, overlapping bureaucratic priorities and competing stakeholder interests across regions and functionalities in China's network security space hinders more robust implementation of China's network security strategy. While China faces setbacks and obstacles, the United States nonetheless must continue to improve defenses against malicious cyber activity conducted by China.

The United States should formulate a strategy that both significantly hampers China's pursuit of disruptive peacetime cyber activities (e.g., economic espionage) and creates a message strong enough to reach the top levels of the Chinese bureaucracy, where any policy change is most likely to originate. The effect of such changes will almost certainly be partial rather than total: China's attitudes and actions will inevitably take time to modify, as the country's underlying incentive structure is unlikely to change substantively in the near term. However, these interactions could allow for greater insight into China's strategic decisions and policymaking process.

The United States must be aware that China has been actively promoting an alternative approach to cyberspace that runs counter to the dominant Western norm. As China attempts to alter the authority a country is afforded within its own cyber domain, China has also signed onto regimes about the application of international law in the cyber realm. China's superficial compliance to norms allows it more autonomy and legitimacy in the international arena, while also affording it the leeway to promote international positions that align with its core network security objectives (e.g., sovereignty over networks within one's borders).

While we can expect that China will continue to emphasize sovereignty and attempt to elicit reinforcing responses from other nations against the U.S.-dominant norms on cyber issues, the United States could leverage smarter policymaking to offset these trends. Similarly, despite seemingly intractable differences, as data about China's network security strategy continue to emerge, U.S. policymakers can craft policies that shape Chinese behavior over time based on a better understanding of China's network security infrastructure, drivers, perspectives, and objectives. Recommendations to decrease tension and misunderstanding in the U.S.-China cybersecurity relationship will be released in a policy brief in early-2015.

ENDNOTES

1. Gerry Shih, "China's Internet chief accuses U.S. of hacking but says talks 'unhindered'," *Reuters*, October 30, 2014, http://www.reuters.com/article/2014/10/30/china-cybersecurity-idUSL4N0SP2QE20141030.

2. James A. Lewis, Director and Senior Fellow, Technology and Public Policy Program, "Asia: The Cybersecurity Battleground," Statement to the Subcommittee on Asia and the Pacific, Foreign Affairs Committee, U.S. House of Representatives, July 23, 2013, http://csis.org/files/attachments/130723_jimlewis_testimony_v2.pdf; An Gang, "Striking a Balance," *Beijing Review*, July 17, 2014, http://www.bjreview.com.cn/world/txt/2014-07/13/content_629274.htm; and Andrew Rafferty, "Cybersecurity threatens US-China relationship, White House official says," *NBC News*, March 11, 2013, http://usnews.nbcnews.com/_news/2013/03/11/17273068-cybersecurity-threatens-us-china-relationship-white-house-official-says.

3. The term "China" will refer to the Chinese government, the Chinese Communist Party (CCP), and Beijing, and terminology will be varied throughout the piece for readability.

4. Strategy is defined here as an actor's plan (either military or non-militarily) to achieve political goals. For further elaboration, see Carl von Clausewitz, "Chap 1." in *On War,* trans. J.J. Graham (London: N. Trubner, 1873).

5. Wang Yukai, "Zhongyang wangluo anquan yu xinxihua lingdao xiaozu de youlai ji qi yinxiang [The Origins and Influence of the Central Network Security and Informatization Leading Small Group"], *Zhongguo Gongchandang Xinwen Wang* [*Communist Party of China News Network*], March 3, 2014, http://theory.people.com.cn/n/2014/0303/c40531-24510897.html.

6. National Initiative for Cybersecurity Careers and Studies, Glossary definition of "cybersecurity," http://niccs.us-cert.gov/glossary#cybersecurity.

7. "Xi Jinping: Ba woguo cong wangluo daguo jianshe chengwei wangluo qiangguo [Xi Jinping: Efforts should be made to build our country into a network powerhouse]," *Xinhua*, February 27, 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538788.htm.

8. Ibid.

9. See Xiaofan Zhao, "Practice and Strategy of Informatization in China," October 18, 2006, http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan025040.pdf.

10. Shen Dingli, "Framing China's National Security," *China-US Focus*, April 23, 2014, http://www.chinausfocus.com/peace-security/framing-chinas-national-security/.

11. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (May 2013), http://www.defense.gov/pubs/2013_china_report_final.pdf.

12. Some examples of Western analysis include: Kenneth Lieberthal and Peter W. Singer, *Cybersecurity and U.S.-China Relations* (Washington: Brookings, February 2012); Michael D. Swaine, "Chinese Views on Cybersecurity in Foreign Relations," *China Leadership Monitor* no. 42 (Fall 2013); and Timothy L. Thomas, "Chapter 20: Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: National Defense University Press and Potomac Books Inc., 2009).

13. Deng Wenhao, "Jiefangjun shaojun: Wangluo zhan weixie shen yu hedan, zhongguo shang wu wangjun" ["The Threat of Network Warfare Worse Than Threat of Bombs, China Has No Cyber Army"], *Nanfangwang* [*Southcn*], December 9, 2013, http://news.southcn.com/z/2013-12/09/content_86717999.htm.

14. "We Are Probing Each Other, All the Time," *New Perspectives Quarterly*, 30 no. 3 (Summer 2013), http://www.digitalnpq.org/archive/2013_summer/03_mcconnell.html.

15. For example, state news outlets such as *Xinhua* use the term "cybersecurity" and "network security" interchangeably in their English-language publications.

16. Quanjun junshi shuyu guanli weiyuanhui [PLA Military Technology Management Committee], *Zhongguo renmin jiefangjun junyu (quanben)* [*The People's Liberation Army Military Terminology (Complete)*], Beijing: junshi kexue chubanshe (2011), 259.

17. Timothy Thomas, "Nation-State Cyber Strategies: Examples from China and Russia," in *Cyberpower and National Security,* eds. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington: National Defense University Press, 2009).

18. The following definitions were all translated from Chinese. PLA Military Technology Management Committee, *Military Terminology*, 50.

19. Ibid., 286.

20. Ibid., 287.

21. Ibid., 262.

22. Ibid., 261-62.

23. Ibid., 253.

24. The White House, *The Comprehensive National Cybersecurity Initiative,* http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf.

25. Jimmy Goodrich, "Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, Report from workshops held at the University of California, San Diego (April 2012), 5-6, http://igcc.ucsd.edu/assets/001/503568.pdf.

26. Wang Yukai, "Zhongyang wangluo anquan yu xinxihua lingdao xiaozu de youlai ji qi yinxiang [The Origins and Influence of the Central Network Security and Informatization Leading Small Group]," *Zhongguo Gongchandang Xinwen Wang* [*Communist Party of China News Network*], March 3, 2014, http://theory.people.com.cn/n/2014/0303/c40531-24510897.html.

27. For more information about this initiative, please see the Ministry of Industry and Information Technology's website dedicated to it at http://www.miit.gov.cn/n11293472/n11293877/n12244385/.

28. Jiang Zemin, "Lun zhongguo xinxi jishu chanye fazhan [On China's Information Technology Industry Development]," *Xinhua*, April 22, 2009, http://news.xinhuanet.com/newscenter/2009-04/22/content_11232665_1.htm.

29. CPC Central Committee and State Council, "Guojia xinxihua lingdao xiaozu guanyu jiaqiang xinxi anquan baozhang gongzuo de yijian [Opinions for Strengthening Information Security Assurance Work]," September 9, 2003.

30. See Wang Yukai, "The Origins and Influence," 2014, and Jimmy Goodrich, "Chinese Civilian Cybersecurity: Stakeholders, Strategies, and Policy," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, Report from workshops held at the University of California, San Diego (April 2012), 5-6, http://igcc.ucsd.edu/assets/001/503568.pdf.

31. "Zhonggong shiba jie zhong quanhui gongbao (quanwen) [Communiqué of the Third Plenary Session of the 18th Central Committee of the CPC (Full Text)]," *China.org.cn*, November 12, 2013, http://www.china.org.cn/chinese/2014-01/16/content_31213800.htm.

32. Samantha Hoffman and Peter Mattis, "Inside China's New Security Council," *The National Interest*, November 21, 2013, http://nationalinterest.org/commentary/inside-chinas-new-security-council-9439.

33. Guowuyuan bangongting [State Council], "Guowuyuan guanyu dali tuijin xinxihua fazhan he qieshi baozhang xinxi anquan de ruogan yijian" ["State Council Opinion on Vigorously Promoting the Development of Informatization and Effective Protection of Information Security"], 2012, http://www.gov.cn/zwgk/2012-07/17/content_2184979.htm.

34. State Council, Opinion on Vigorously Promoting the Development of Informatization and Xue Ruihan, "Jianli jianqian guojia wangluo he xinxi anquan chang xiao jizhi [Establish and improve the national network and information security long-term mechanisms]," *Renmin Wang* [*People's Daily Online*], April 17, 2014, http://leaders.people.com.cn/n/2014/0417/c347621-24909496.html.

35. Guojia xinxihua zhuanjia zixun weiyuanhui [Advisory Committee for State Informatization], "Guojia xinxihua lingdao xiaozu" ["State Informatization Leading Group"], http://www.acsi.gov.cn/en/.

36. Wang Yukai, "The Origins and Influence," 2014.

37. Guowuyuan bangongting [State Council], *Guowuyuan yishi xietiao jigou shezhi* [*Advisory and Coordinating Organs under the State Council*], http://www.gov.cn/zwgk/2008-04/24/content_953488.htm.

38. Gonganbu, Guojia baomiju, Guojia mima guanli weiyuanhui bangongshi, he guowuyuan xinxihua gongzuo banggongshi [Ministry of Public Security, State Secrecy Bureau, National Committee on Password Management, and State Council Informatization Office], *Guanyu yinfa "Guanyu xinxi anquan dengji baohu gongzuo de shishi yijian de tongzhi* ["*Notification Regarding Implementation Opinions for Information Security and Other Protective Measures*]," September 15, 2004, http://oi.pku.edu.cn/xxaq/xxaqdjbh/22572.htm.

39. Jimmy Goodrich, "Chinese Civilian Cybersecurity," 5-6.

40. "Zhongyang wangluo anquan he xinxihua lingdao xiaozu chengli: cong wangluo daguo maixiang wangluo qiangguo [Central Internet Security and Informatization Leading Small Group Established: From a Networked Country towards a Networked Strong Country]," *Xinhua*, February 27, 2014, http://news.xinhuanet.com/politics/2014-02/27/c_119538719.htm.

41. "Xi Jinping leads Internet security group," *Xinhuanet*, February 27, 2014, http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm; and Hoffman and Mattis, "Inside China's New Security Council."

42. "China to speed up full military IT application: Hu," *Renmin Wang* [*People's Daily Online*], November 8, 2012, http://english.people.com.cn/90785/8010620.html.

43. Xue Ruihan, "Establish and improve the national network and information security long-term mechanisms."

44. Cai Yawei, "Zhongshi xinxi anquan jianshe wangluo qiangguo [Focusing on Information Security to Become a Cyber Power]," *Huicong 360*, September 17, 2014, http://info.it.hc360.com/2014/09/171112789285.shtml.

45. "Li Qing, "Xi Jinping chuxi zhongguo kexueyuan di shiqi yuanshi dahui, zhongguo gongchengdi shierci yuanshi dahui kaimu hui bing fabiao zhongyao jianghua" ["Xi Jinping attends the Chinese Academy of Sciences 17th Conference and Chinese Academy of Engineering's 12th Conference, delivers important speech," *Xinhua*, June 9, 2014, http://news.xinhuanet.com/politics/2014-06/09/c_126597413.htm.

46. Jiang Zemin, Guoji xingshi he junshi zhanlüe fangzhe [The Global Situation and Military Strategic Outline] in *Jiang Zemin wenxuan* [*Jiang Zemin Anthology*] (Beijing: Renmin chubanshe, 2006).

47. "Jing Xi Jinping zhuxi pizhun zhongyang junwei yinfa 'guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian [Chairman of the Central Military Commission Xi Jinping approved the issuance of 'Opinion on Further Strengthening Military Information Security Work']," *Jiefangjun bao* [*PLA Daily*], October 7, 2014, http://news.xinhuanet.com/mil/2014-10/07/c_1112726181.htm.

48. Information Office of the State Council, "White Paper: The Diversified Employment of China's Armed Forces," April 2013, http://eng.mod.gov.cn/Database/WhitePapers.

49. Dennis J. Blasko, "Chapter 3: The Evolution of Core Concepts: People's War, Active Defense, and Offshore Defense," in *Assessing the People's Liberation Army in the Hu Jintao Era*, eds. Roy Kamphausen, David Lai, and Travis Tanner (Carlisle, PA: Strategic Studies Institute, 2014), 81.

50. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units," (Mandiant, February 18, 2013), http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf and Novetta Solutions, "Operation SMN: Axiom Threat Actor Group Report," (Novetta, October 2014), http://www.novetta.com/files/9714/1446/8199/Executive_Summary-Final_1.pdf.

51. This conclusion is reached based on an analysis of both civilian and military institution research trends conducted via The China National Knowledge Infrastructure databases, an electronic platform that integrates significant Chinese knowledge-based information resources. Since much of China's research into network security technologies have dual-use purposes, making the distinction between civilian and military research particularly difficult.

52. "Zhonggong zhongyang guanyu quanmian shenhua gaige ruogan zhongda wenti de jueding [CPC Central Committee decision on deepening reform]," *Renmin Wang* [*People's Daily Online*], November 15, 2013, http://politics.people.com.cn/n/2013/1115/c1001-23559207.html; Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014* (June 5, 2014), 17, http://www.defense.gov/pubs/2014_DOD_China_Report.pdf; and Murray Scot Tanner, "China's Social Unrest Problem," Statement to the U.S.-China Economic and Security Review Commission, May 15, 2014, http://www.uscc.gov/sites/default/files/Tanner_Written%20Testimony.pdf.

53. "Jing Xi Jinping zhuxi pizhun zhongyang junwei yinfa 'guanyu jinyibu jiaqiang jundui xinxi anquan gongzuo de yijian [Chairman of the Central Military Commission Xi Jinping approved the issuance of 'Opinion on Further Strengthening Military Information Security Work']," *Jiefangjun bao* [*PLA Daily*], October 7, 2014, http://news.xinhuanet.com/mil/2014-10/07/c_1112726181.htm and James Mulvenon, "Chairman Hu and the PLA's 'New Historic Missions'," *China Leadership Monitor* no. 27 (Winter 2009), 2, http://media.hoover.org/sites/default/files/documents/CLM27JM.pdf.

54. M. Taylor Fravel, "China's Strategy in the South China Sea," *Contemporary Southeast Asia*, 33 no. 3 (2011), 292–319.

55. "Growing China to contribute more to Asia development: Xi," *Xinhua*, October 29, 2014, http://news.xinhuanet.com/english/china/2014-10/29/c_133752083.htm.

56. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace: Report to Congress on Foreign Balance Economic Collection and Industrial Espionage, 2009-2011*, October 2011, 7–8, http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf.

57. FBI Director James Comey, interview by Scott Pelley, *60 Minutes,* October 5, 2014, http://www.cbsnews.com/news/fbi-director-james-comey-on-threat-of-isis-cybercrime/.

58. Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Economic Secrets in Cyberspace,* i.

59. Ibid.

60. Comey, *60 Minutes*.

61. Mandiant, "APT1," 2.

62. Novetta Solutions, "Axiom Threat Actor Group Report," 4 and 9.

63. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* and Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2014*.

64. Ministry of National Defense of the People's Republic of China, Regular News Conference Hosted By Senior Colonel Geng Yansheng, February 28, 2013; and "Mei zaici chaozuo wangluo weixie; Zhuanjia: Wumie zhongguo diu meiguo lian ['America again speculates about Chinese cyber threat; Expert: The United States loses face in slandering China']," *Xinhua*, October 30, 2014, http://news.xinhuanet.com/yzyd/mil/20141030/c_1113037076.htm.

65. For more information about this, see William Hannis, James Mulvenon, and Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation* (New York: Routledge, 2013).

66. "Black hat" refers to hackers who "[violate] computer security for little reason beyond maliciousness or for personal gain." From Robert Moore, *Cybercrime: Investigating High Technology Computer Crime* (Burlington, MA: Elsevier, 2011), 25.

67. Zhonghua renmin gongheguo guowuyuan [PRC State Council], *Zhongguo hulianwang zhuangkuang* [*The Status of China's Internet*], June 8, 2010, http://www.gov.cn/zwgk/2010-06/08/content_1622866.htm; and Cai Mingzhao, Minister of the State Council Information Office of China, "Making Joint Efforts to Maintain Cybersecurity" (Fourth World Cyberspace Cooperation Summit, Stanford University, November 5, 2013), http://www.chinausfocus.com/peace-security/making-joint-efforts-to-maintain-cyber-security/.

68. Author interview with China experts in Washington area, December 11, 2013. For more information on how pirated software and technology could increase cybersecurity risks, see John F. Gantz et al., "The Dangerous World of Counterfeit and Pirated Software: How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations ... and the Resultant Costs in Time and Money," White Paper no. 239751 (IDC, March 2013), 3–4, http://www.computerworld.com.pt/media/2013/03/IDC030513.pdf.

69. Li Yuxiao, "Cyberspace Security and International Cooperation in China," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, Report from workshops held at the University of California, San Diego (April 2012), 5-6, http://igcc.ucsd.edu/assets/001/503568.pdf.

70. "China's computer virus infections up first time in 5 years," *Xinhua,* September 16, 2014, http://news.xinhuanet.com/english/china/2014-09/16/c_133647807.htm.

71. Zhongguo Hulianwangluo Xinxi Zhongxin [China Internet Network Information Center], "CNNIC fabu di 32 ci 'Zhongguo hulianwangluo fazhan zhuangkuang tongji baogao' [CNNIC Publishes the 32nd "Statistical Report on China's Internet Development], July 17, 2013, http://www.cnnic.cn/gywm/xwzx/rdxw/rdxx/201307/t20130717_40663.htm.

72. Author interviews with former and active duty U.S. military officers, Cambridge, MA, December 2013; and interview with Department of Defense official, Washington, December 2013.

73. For examples of this language as justification for Chinese government restrictions of civilian use of Internet, see China (and Russia)'s UN General Assembly proposal for an International Code of Conduct for Information

Security: Zhonghua Renmin Gonghe Guo [Ministry of Foreign Affairs of the People's Republic of China], "Xinxi anquan guoji xingwei zhunze" ["International Code of Conduct for Information Security]," http://www.fmprc.gov.cn/mfa_chn/ziliao_611306/tytj_611312/zcwj_611316/t858317.shtml.

74. "Beijing police nab 30,000 suspects in cyber crime crackdown," *Xinhua*, October 9, 2014, http://news.xinhuanet.com/english/china/2014-10/09/c_133702753.htm.

75. "Beijing requires real names in microblog registration," *Xinhua*, December 16, 2011, http://news.xinhuanet.com/english/china/2011-12/16/c_131310381.htm.

76. "China regulates instant messaging services," *Xinhua*, August 7, 2014, http://news.xinhuanet.com/english/china/2014-08/07/c_133539676.htm.

77. "Real name registration starts for mobile phone network," *Xinhua*, September 1, 2013, http://news.xinhuanet.com/english/china/2013-09/01/c_132681732.htm.

78. "Beijing requires real names in microblog registration."

79. For references to China's use of information security and cybersecurity to encompass information management, see "Statement by the Chinese Delegation on Information and Cybersecurity at the Thematic Debate at the First Committee of the 68th Session UNGA," (New York, October 2013), http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf.

80. Novetta Solutions, "Axiom Threat Actor Group Report," 15.

81. Shalom Bublil, Daniel Brodie, and Avi Bashan, "Lacoon Discovers Xsser mRAT, the First Advanced Chinese iOS Trojan," *Lacoon blog*, September 30, 2014, https://www.lacoon.com/lacoon-discovers-xsser-mrat-first-advanced-ios-trojan/.

82. Jeffrey Kwong, "State Use of Nationalist Cyber Attacks as Credible Signals in Crisis Bargaining," in *China and Cybersecurity: Political, Economic, and Strategic Dimensions*, Report from workshops held at the University of California, San Diego (April 2012), 5-6, http://igcc.ucsd.edu/assets/001/503568.pdf.

83. Agent France-Presse, "Chinese cyber attacks hit Japan over islands dispute," *The Globe and Mail*, September 19, 2012, http://www.theglobeandmail.com/news/world/chinese-cyber-attacks-hit-japan-over-islands-dispute/article4553048/.

84. Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Washington: U.S.-China Economic and Security Review Commission, 2012), 11, http://origin.www.uscc.gov/sites/default/files/Research/USCC_Report_Chinese_Capabilities_for_Computer_Network_Operations_and_Cyber_%20Espionage.pdf.

85. See James Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, eds. James Mulvenon and Richard Yang (Washington: 1999).

86. See Information Office of the State Council, People's Republic of China, "China's National Defense in 2006," December 29, 2006, available at http://www.fas.org/nuke/guide/china/doctrine/wp2006.html.

87. Perspectives about how China employs "active defense" vary widely in the analytical community. See the following article for an acknowledgement of the debate: Alexander Chieh-cheng Huang, "Transformation and Refinement of Chinese Military Doctrine: Reflection and Critique on the PLA's View," in *Seeking Truth From Facts: A Retrospective on Chinese Military Studies in the Post-Mao Era*, eds. James Mulvenon and Andrew Yang (Arlington, VA: RAND Corporation, 2001).

88. Michael D. Swaine, "China's Assertive Behavior Part Three: The Role of the Military in Foreign Policy," *China Leadership Monitor* no. 36 (2012), 4.

89. Hannas, Mulvenon, and Puglisi, *Chinese Industrial Espionage*, 221.

90. Peng Guangqian and Yao Youzhi eds., "Chapter 20: Rise of the High-Tech Local War and Its Historic Status," in *The Science of Military Strategy,* Academy of Military Science Strategic Research Department (Beijing: Military Science Publishing House, 2005), 406.

91. Academy of Military Science Strategic Research Department, *The Science of Military Strategy* (Beijing: Military Science Publishing House, 2013), 188.

92. For discussions of strategy in the network domain, see: Academy of Military Science Strategic Research Department, *The Science of Military Strategy*, 188–197.

93. Mulvenon, "Chairman Hu and the PLA's 'New Historic Missions'," 2.

94. Ministry of Foreign Affairs, "Foreign Ministry Spokesperson Hua Chunying's Regular Press Conference on May 7, 2013," May 8, 2013, http://www.fmprc.gov.cn/eng/xwfw/s2510/t1038551.shtml.

95. U.S.-China Economic and Security Review Commission, *2013 Annual Report to Congress* (November 2013), 258.

96. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013*, 36.

97. Mandiant, "APT1: Exposing One of China's Cyber Espionage Units."

98. Novetta Solutions, "Axiom Threat Actor Group Report," 10.

99. Academy of Military Science Strategic Research Department, *The Science of Military Strategy*, 196–197. For a deeper discussion of China's network attack human capital development, see Joe McReynolds, Leigh Ann Ragland, and Amy Chang, "The Swordsmiths: The Human Capital Ecosystem Underlying the PLA's Network Weapons Development," conference paper presented at UC San Diego annual Study of Innovation and Technology in China conference, August 10, 2014.

100. Zhuang Lin and Si Huijing, "Meiguo wangluo anquan zhanlüe de shizhi [The essence of American network security strategy]," *Guofang Keji* [*National Defense Science and Technology*], no. 4 (2013); Wu Zecheng, "Meiguo wangluo baquan dui zhongguo guojia anquan de yinxiang ji duice [Influence of U.S. network hegemony on China's national security and countermeasures],"

Guofang Keji [*National Defense Science and Technology*], no. 1 (2014), and Liu Dan and Bi Mingxin, "Surveillance Programs Reveal U.S. Hypocrisy," *Xinhua*, June 14, 2013.

101. David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *The New York Times*, March 22, 2014, http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html; "China's Xinhua news agency condemns US 'cyber attacks'," *BBC News*, June 23, 2013, http://www.bbc.com/news/world-asia-23018938.

102. "China suspends cyber working group activities with U.S. to protest cyber theft indictment," *Xinhua*, May 20, 2014, http://news.xinhuanet.com/english/china/2014-05/20/c_126520553.htm.

103. U.S. Strategic Command, "Fact Sheet: U.S. Cyber Command," August 2013, http://www.stratcom.mil/factsheets/2/Cyber_Command/.

104. Karen Parrish, "Lynn: Cyber Strategy's Thrust is Defensive," *American Forces Press Service*, July 14, 2011, http://www.defense.gov/news/newsarticle.aspx?id=64682.

105. CYBERCOM and NSA are two distinct U.S. organizations with different rights and responsibilities.

106. Yu Xiaoqu, "US playing dangerous game with 'cyber deterrence'," *Renmin Wang* [*People's Daily Online*], July 26, 2011, http://english.people.com.cn/90001/90780/91343/7452284.html.

107. "Jiasu zhenghe hanwei 'quanwei guotu' de dongyuan liliang [Accelerating the Integration of Defending Multidimensional Homeland' Mobilizing Force]," *Zhongguo Guofang Bao* [*China Defense Daily*], December 22, 2011, http://www.mod.gov.cn/mobilize/2011-12/22/content_4330110.htm.

108. For an example of an academic paper, see: Zhang Hongtao et al., "Review of Research State and Development Direction of Cyberspace," *Journal of Harbin Institute of Technology* (May 2011), http://en.cnki.com.cn/Article_en/CJFDTOTAL-HRBG201105004.htm.

109. The White House, Office of the Press Secretary, "Press Briefing By National Security Advisor Tom Donilon," *The White House,* June 8, 2013, http://www.whitehouse.gov/the-press-office/2013/06/08/press-briefing-national-security-advisor-tom-donilon.

110. Ministry of Foreign Affairs of the People's Republic of China, "Foreign Ministry Spokesperson Hua Chunying's Remarks," June 23, 2013, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1052673.shtml.

111. Comey, *60 Minutes*.

112. Department of Justice Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," May 19, 2014, http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

113. Ministry of Foreign Affairs of the People's Republic of China, "China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel," May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml

114. Xiao An, "The 'Achilles' heel' in the China-US relationship," China.org.cn, June 4, 2014, http://www.china.org.cn/opinion/2014-06/04/content_32566808.htm.

115. "China suspends cyber working group activities with U.S. to protest cyber theft indictment," *Xinhua*, May 19, 2014, http://news.xinhuanet.com/english/china/2014-05/20/c_126520553.htm.

116. U.S.-China Economic and Security Review Commission, *Roundtable: U.S.-China Cybersecurity Issues* (Washington: July 11, 2013), 34.

117. Experts were from fifteen countries: Argentina, Australia, Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and the United States of America.

118. United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," A/68/98 (United Nations General Assembly, June 24, 2013), 8, http://www.un.org/ga/search/view_doc.asp?symbol=A/68/98.

119. Ibid.

120. Ibid.

121. Lu Wei said, "信息服务可以跨越国界，但网络空间不能没有主权 [Information services cross borders, but cyberspace cannot live without sovereignty.]" From "Anquan jueding chengbai, fazhan yinling weilai [Safety Determines Success or Failure, Developing Future Leadership]," *Xinhua*, December 10, 2013, http://news.xinhuanet.com/world/2013-12/10/c_125838121.htm.

122. Li Yuxiao, "Cyberspace Security and International Cooperation in China," in *China and Cybersecurity*, 4.

123. Statement by the Chinese Delegation on Information and Cybersecurity at the Thematic Debate at the First Committee of the 68th Session UNGA (New York, October 2013), http://www.un.org/disarmament/special/meetings/firstcommittee/68/pdfs/TD_30-Oct_ODMIS_China.pdf.

124. Allen Carlson, "More Than Just Saying No: China's Evolving Approach to Sovereignty and Intervention Since Tiananmen," in *New Directions in the Study of Chinese Foreign Policy,* eds. Alastair Iain Johnston and Robert S. Ross (Stanford: Stanford University Press, 2006), 235.

125. Thomas Lum, Patricia Moloney, and Matthew Weed, "China, Internet Freedom, and U.S. Policy," R42601 (Congressional Research Service, July 13, 2012); Keith Bradsher, "China Toughens Its Restrictions on Use of the Internet," *New York Times,* December 28, 2012, http://www.nytimes.com/2012/12/29/world/asia/china-toughens-restrictions-on-internet-use.html.

126. David E. Sanger, "U.S. Tries Candor to Assure China on Cyberattacks," *The New York Times*, April 6, 2014, http://www.nytimes.com/2014/04/07/world/us-tries-candor-to-assure-china-on-cyberattacks.html.

127. Ibid.

128. "China Voice: Cooperation should prevail over rifts in Sino-U.S. ties," *Xinhua*, May 28, 2014, http://news.xinhuanet.com/english/china/2014-05/28/c_133367441.htm.

129. "China rejects U.S. accusation of cyber attacks," *Xinhua*, June 10, 2014, http://news.xinhuanet.com/english/china/2014-06/10/c_133397601.htm.

130. Ministry of Foreign Affairs, "China Reacts Strongly to US Announcement of Indictment Against Chinese Personnel," May 20, 2014, http://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2535_665405/t1157520.shtml.

131. James R. Clapper, Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, U.S. Senate, January 29, 2014, http://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf.

About the Center for a New American Security

The mission of the Center for a New American Security (CNAS) is to develop strong, pragmatic and principled national security and defense policies. Building on the expertise and experience of its staff and advisors, CNAS engages policymakers, experts and the public with innovative, fact-based research, ideas and analysis to shape and elevate the national security debate. A key part of our mission is to inform and prepare the national security leaders of today and tomorrow.

CNAS is located in Washington, and was established in February 2007 by co-founders Kurt M. Campbell and Michèle A. Flournoy. CNAS is a 501(c)3 tax-exempt nonprofit organization. Its research is independent and non-partisan. CNAS does not take institutional positions on policy issues. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Center for a New American Security
1152 15th Street, NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org
www.cnas.org

Production Notes

Paper recycling is reprocessing waste paper fibers back into a usable paper product.

Soy ink is a helpful component in paper recycling. It helps in this process because the soy ink can be removed more easily than regular ink and can be taken out of paper during the de-inking process of recycling. This allows the recycled paper to have less damage to its paper fibers and have a brighter appearance. The waste that is left from the soy ink during the de-inking process is not hazardous and it can be treated easily through the development of modern processes.

Center for a
New American
Security

STRONG, PRAGMATIC AND PRINCIPLED
NATIONAL SECURITY AND DEFENSE POLICIES

1152 15th Street, NW
Suite 950
Washington, DC 20005

TEL 202.457.9400
FAX 202.457.9401
EMAIL info@cnas.org

www.cnas.org

PRINTED WITH SOY INK

Printed on Post-Consumer Recycled paper with Soy Inks