Preface

If you are holding this report in your hands or viewing it on your computer screen, you have come upon something unusual. In a time when heated verbal and written exchanges between our two countries are the norm for most topics related to cyberspace, the tone of this report is an exception. In a time of escalating mistrust, this report reflects some measure of cooperation, teamwork and a commitment to a shared goal. In a time when most can only see a grim, downward spiral of recrimination when it comes to all things cyber, this report is the product of cooperation and offers some hope for an improved relationship between China and the U.S.

Neither of us, nor any of our team members, is naive concerning the existing concerns that our two countries have about each other in cyberspace. Both of us recognize that the Internet is an evolving vehicle that has brought – and continues to bring – great benefit for the development of China, the U.S. and the world. It also brings with it many new societal challenges. In this first engagement, we managed to achieve trust and cooperate on a common, concrete problem.

Both of us want to thank the subject matter experts, whose names are listed on the next page. These individuals devoted significant time and expertise to this process, and this important step toward international cooperation in cyberspace would not have been possible without them.

KARL FREDERICK RAUSCHER
Leader, U.S. Experts Group
Chief Technology Officer
& Distinguished Fellow
EastWest Institute

Bell Labs Fellow
New York City

ZHOU YONGLIN
Leader, China Experts Group
Director
Network & Information Security Committee
Internet Society of China

Head, CNERT/CC Operations Department
Beijing

Rauscher and Yonglin at
EWI Worldwide Security Conference
Brussels, February 2010

Contents

The New York Times

By THE EDITORIAL BOARD

May 25, 2013

Preventing a U.S.-China Cyberwar

When President Obama and President Xi Jinping of China have their first meeting next month in California, addressing the issue of China's cyberattacks on American institutions will be an important priority. Both nations need to take steps to avoid drifting into an all-out cyberwar.

Despite Beijing's denials, there is little doubt that Chinese hackers have taken aim at a range of government and private systems in the United States, including the power grid and telecommunications networks. In February, a report by the computer security firm Mandiant detailed how hackers working for the People's Liberation Army of China had gained access to data from American companies and government agencies. Earlier this month, a Pentagon report explicitly accused the Chinese military of the attacks.

With the evidence of their activities mounting, Chinese hackers went silent for three months, but, they now seem to have resumed their attacks. A report last week by the Commission on the Theft of American Intellectual Property, a private group led by two former Obama administration officials — Dennis Blair, who was the director of intelligence, and Jon Huntsman Jr., an ambassador to China — said that hacking costs the American economy more than $300 billion a year and that China was responsible for 70 percent of the theft of corporate intellectual property and trade secrets.

While there are concerns about military-related incursions, the focus of most public discussion surrounds hacking into business and industry. The commission's report spoke of the risk of "stifling innovation" in America and elsewhere if hackers in China are able to steal blueprints and negotiation strategies. The Chinese complain that they, too, have suffered cyberattacks. That could offer some basis for cooperating with Washington on norms of behavior. China recently agreed to an Obama administration proposal to create a working group on cyberissues.

The commission said the American response was "utterly inadequate" and proposed stronger ways to deter Chinese hacking, like possibly allowing companies to retaliate against attackers with their own counterstrikes.

But before adopting punitive measures, the two nations need to try working together. For example, the EastWest Institute, an independent research group, is working with representatives of many governments, including China and the United States, to develop ground rules for protecting the digital infrastructure. The group's detailed proposal on fighting spam — which carries malware used by hackers — is worth considering by President Obama and President Xi.

China-U.S. Bilateral on Cybersecurity

FIGHTING SPAM TO BUILD TRUST

By KARL FREDERICK RAUSCHER & YONGLIN ZHOU

June 2011