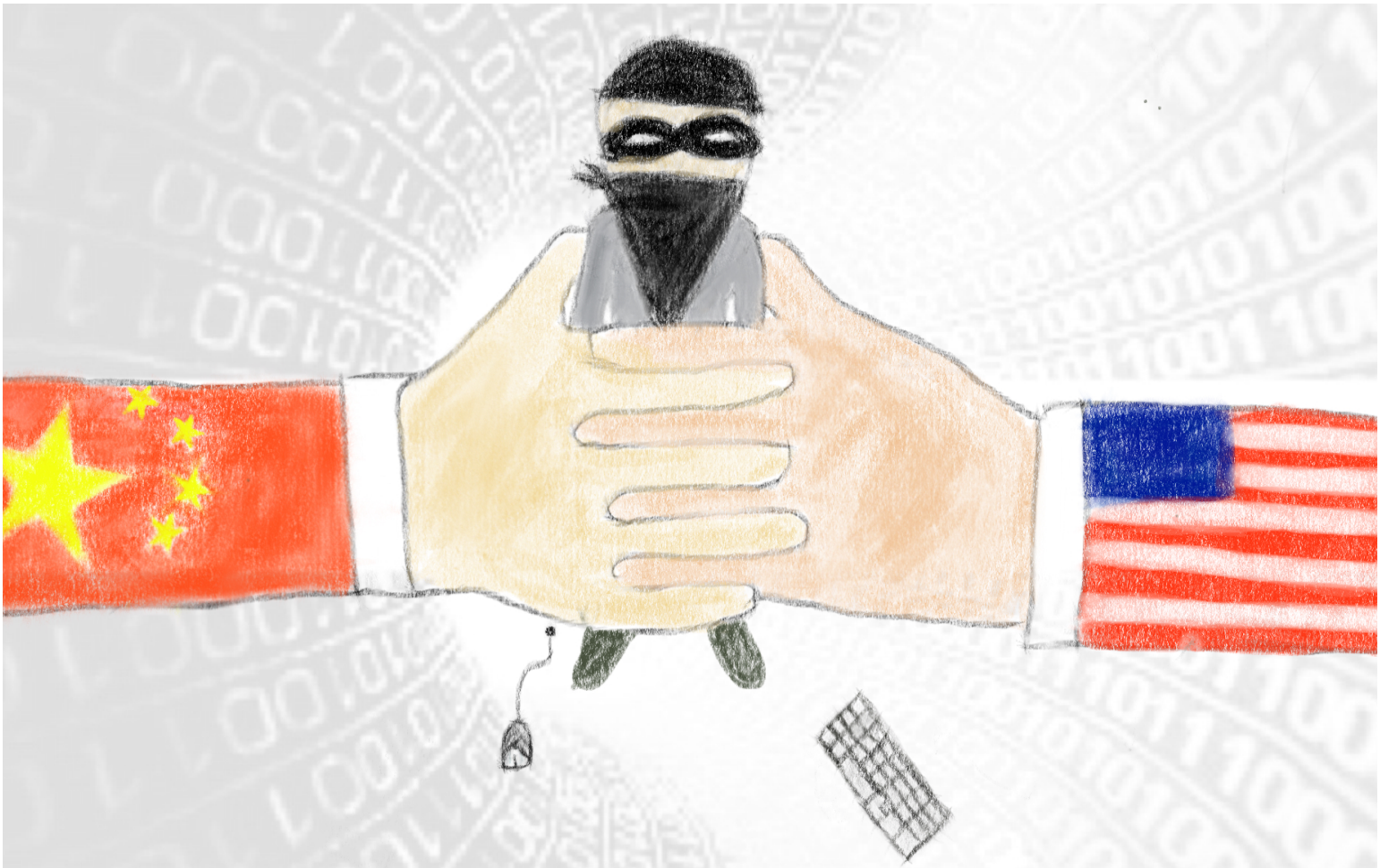


FINAL VERSION OF THE AUTHORS AND EXPERTS GROUP

Presented at the EWI – IEEE World Cyberspace Cooperation Summit Stanford University – November 2013

CHINA-U.S. TRACK 2 BILATERAL ON CYBERSECURITY

FRANK COMMUNICATION & SENSIBLE COOPERATION TO STEM HARMFUL HACKING

EastWest Institute

中国互联网协会

China-U.S. Bilateral on Cybersecurity *Frank Communication & Sensible Cooperation to Stem Harmful Hacking*, Issue 1.2

The primary authors of this document are:
Karl Frederick Rauscher, CTO & Distinguished Fellow, EastWest Institute; Bell Labs Fellow
&
Yonglin Zhou, Secretary General, Information & Network Security Committee, Internet Society of China

Cover Artwork by Yonglin Zhou and Mercy Rauscher

ISBN 978-0-9856824-3-9

The EastWest Institute is an international, non-partisan, not-for-profit policy organization focused solely on confronting critical challenges that endanger peace. EWI was established in 1980 as a catalyst to build trust, develop leadership, and promote collaboration for positive change. The institute has offices in New York, Brussels, Moscow and Washington.

The Internet Society of China was inaugurated in 2001 with a main mission to promote the development of the Internet in China and make efforts to construct an advanced information society. ISC is expected to be a link among the community, to make efforts benefiting the whole industry, to protect Internet user's interests, to push forward industry self-discipline, to strengthen communication and cooperation between its members, to assist and provide support for policy making, and to promote Internet application and public awareness.

For more information about EWI or this paper, please contact:

The EastWest Institute
11 East 26th Street, 20th Floor
New York, NY 10010 U.S.A.

+1 212 824 4100

communications@ewi.info

For more information about the ISC, please contact:

Tower A East, Tianyin Plaza
No. 2-B South Fuxingmen Ave
Beijing, China 100031

+ 86 10 66035712

isc@isc.org.cn

中美非政府层面网络安全对话

China-U.S. Track 2 Bilateral on Cybersecurity

真诚沟通 务实合作
共同抵制黑客攻击活动

Frank Communication & Sensible Cooperation to Stem Harmful Hacking

---

by KARL FREDERICK RAUSCHER & ZHOU YONGLIN

"This report indicates that China and the U.S.
can make joint efforts for a safe and secure cyberspace.
I support concrete actions like this."

蔡名照
Minister Cai Mingzhao
Minister of the Information Office of the State Council
People's Republic of China

"While the U.S and China may approach cyberspace
from different political and cultural vantage points,
both nations have a fundamental stake in an Internet that is secure and trustworthy.
This report frames a way forward that builds trust in a deliberate and verifiable manner.*"*

Michael Chertoff
Chairman & Co-founder of The Chertoff Group
fmr. Secretary, U.S. Department of Homeland for President George W. Bush
fmr. Federal Judge, U.S. Court of Appeals, Third Circuit

"Maintaining the prosperity and development of the Internet is
the fundamental interests of China and the U.S.
China and the U.S. should work together to face the challenges of cyber security.
The report is the outcome of bilateral cooperation;
let us continue to work and make a greater contribution
for the global development of the Internet.*"*

鄔贺铨
WU Hequan
President, Internet Society of China
Member, Chinese Academy of Engineering,
Member, Advisory Committee for State Informatization

"Cybersecurity presents very tough problems and they are not for the faint of heart.
Those wishing to play a part in solving them
either need to lead, follow or get out of the way.
Here is bold leadership.*"*

General James L. Jones (USMC ret.)
fmr. National Security Adviser to President Barack Obama
fmr. Supreme Allied Commander, Europe (SACEUR)

*"**The foundations of meaningful and constructive cooperation***
between China the U.S. and the world
***have been laid down within this authoritative report** on Hacking.*
Karl Rauscher, Yonglin Zhou and their entire team of experts have delivered
***the definitive, global thought leadership work for resolving distrust in cyberspace**."*

Matthew W. Bross
fmr. Global Chief Technology Officer, Huawei
fmr. Global Chief Technology Office,r British Telecom
fmr. Co- founder of Critical Technologies,
Chairman Global Information Infrastructure Forum,
CEO IP Partners

*"Cyberspace security is up to the communications and cooperation among major countries, otherwise it's unimaginable. **This report offers joint efforts to make concrete rules and norms of conducts for a safe and secure cyberspace."***

石现升
SHI Xiansheng
Deputy Secretary General, Internet Society of China

*"It is a **refreshing and astoundingly clear proposal.**"*

Roger Hurwitz
Research Scientist, Massachusetts Institute of Technology (MIT)
Computer Science and Artificial Intelligence Laboratory,
Senior Fellow, Canada Centre for Global Security Studies

*"An **excellent contribution to science diplomacy.**"*

John Savage
An Wang Professor of Computer Science, Brown University
fmr. Jefferson Science Fellow, U.S. State Department

*"This report **demonstrates a practical plan** for the development of Cybersecurity between China and the U.S., which is a noticeable improvement in cyber-law studies."*

刘德良
LIU Deliang
Director, Asia-Pacific Institute for Cyber-law Studies
Professor of Law at the Law School,
Beijing Normal University

*"A **refreshing approach to building bridges** in cyber."*

Catherine Lotrionte
Director, Institute for Law, Science & Global Security, Georgetown University
fmr. Counsel and Director, U.S. President George W. Bush Foreign Intelligence Advisory Board
fmr. Assistant General Counsel, Central Intelligence Agency

"When Presidents Xi and Obama met in California to discuss the US-China relationship, cyber was one of the main topics on their agenda. Developing rules of the road for cyber will require strong efforts both by governments and non-governmental organizations. This report is ***an important step in the right direction.****"*

Joseph S. Nye, Jr.
Harvard University Distinguished Service Professor
fmr. Dean, John F. Kennedy School of Government, Harvard University
fmr. Assistant Secretary of Defense for International Security Affairs for President Bill Clinton
fmr. Deputy Under Secretary of State for Security Assistance, Science and Technology
fmr. Chair, National Intelligence Council

"Cybersecurity can be advanced only through trust without borders. This report provides a ***much-needed blueprint*** *for establishing trust between two major counties."*

谭刚
Gang Tan
Assistant Professor, Computer Science and Engineering, Lehigh University
Security of Software (SOS) Lab
National Science Foundation Award Recipient

*"****Brilliant!*** *Yonglin and Karl built* ***a bridge for technologists*** *of China and the U.S. that will make the world more secure."*

赵良
ZHAO Liang (Richard)
Chief Strategy Officer, NSFocus
Senior Fellow, EastWest Institute
Founder and Board Member, Greater China Cloud Security Alliance;

"This report ***demonstrates how to 'change the game'*** *in cyber to one of finding common ground for improving the security of an efficient Internet."*

Greg Shannon
Chief Scientist, CERT Program at Carnegie Mellon University's
Software Engineering Institute
Department of Defense Federally Funded Research and Development Center

---

A comment on the predecessor to this report, *Fighting Spam to Build Trust* (Rauscher & ZHOU, 2011):

"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****."*

-The New York Times
The Editorial Board in *Preventing a U.S. China Cyberwar,* 25 May 2013

Foreword

The cybersecurity issue is not only a hot topic as a global trend, but also a prominent factor in the overall China-U.S. relationship, indeed even now escalated to the bilateral presidential agenda. The invisibility of hacking incidents, serious damage to victims and the lack of frank and effective communication between China and the U.S. on these issues have significantly lowered trust between the two countries on cybersecurity.

Information and communications technology (ICT) is vital to the security of both countries and the global community. If we cannot solve the cybersecurity issue, the world will have a less bright future. Personalities on both sides of the Pacific have increasingly called for efforts to turn this situation around. On this point, China and the U.S. have a great responsibility, as do other countries. Working together in this area is vital to the future of the world.

Both China and the United States have a deep respect for each other: as cultures, as economic partners, as political forces and as competitors. While it is hard to build a good relationship, it is easy to destroy one. Many people are needed to construct a good relationship between two countries; but a few malicious actors are sufficient to break it. Our countries need wise people to work together on cyber problems. The success of our previous report *Fighting Spam to Build Trust* is an example of what can be achieved. We are not just speaking about those who can discuss the problem, but those capable of moving it towards practical solutions. This report meets these tremendous challenges in a straightforward fashion to a seemingly intractable problem, harmful hacking. It offers actionable recommendations and voluntary best practices that are the output of some of the finest minds of both nations.

We believe that this report will be a constructive factor as both sides come to grips with taking action on this complex issue of cybersecurity risks. This policy and technical study by top experts from both China and the United States is an attempt to begin to change the situation. In order to do this, we have to be honest with ourselves. Harmful hacking involves a complex set of issues. But it can be broken down into component parts as shown here in these pages.

This has been a two-year long cooperative effort by scores of top professionals. It presents an objective examination of the current situation and problem. It also provides practical guidance that can change the course, placing us on a path to a brighter future for Chinese, Americans and others around the world. We encourage leaders of government and industry to take this guidance seriously and move with urgency in pressing forward with renewed, and always cautious, cooperation in fighting harmful hacking in international cyberspace.

Everyone knows that our two countries have a cybersecurity problem; it is now time that they know that we are also capable of devising solutions. We call on others to join this most important effort.

John Edwin Mroz
President & CEO
EastWest Institute

WU Hequan ［邬贺铨］
President, Internet Society of China
Member, Chinese Academy of Engineering,
Member, Advisory Committee for State Informatization

A cautious climber can capture hundreds of cicadas and a careful captain can sail thousands of miles.
- Ancient Chinese Proverb

Be sure you put your feet in the right place, then stand firm.
- Abraham Lincoln

Preface – *"What's Next?"*

Our government hallways, our media arenas and our burgeoning blogosphere, have been, for some years now, echoing the hacking story over and over again . . . another accusation of hacking . . . another denial . . . another claim of hypocrisy . . . another argument . . .

We all understand the problem.
So, what's next?

Can the two largest economies in history work this out? Or are we destined to head down the path of an ever-widening chasm? This report is about taking the next step. Carefully. Firmly.

Neither of us, nor any our contributors, are naïve to the overarching national security interests, dire economic consequences and profound social impacts that hang in the balance with the cybersecurity conundrum that now influences the China-U.S. relationship. However, neither are we convinced that we have given this situation our best shot.

This paper presents eight actionable recommendations that, if implemented, would alter the course of the crisis in the relationship, placing it on a track of cautious trust and expanding cooperation.

This is our second time in collaborating on an important China-U.S. bilateral on cybersecurity. Both of the recommendations presented in our last bilateral report, *Fighting Spam to Build Trust*, have not only been implemented, but they are also institutionalized by the international Messaging, Malware and Mobile Anti-Abuse Working Group (M^3AAWG) and others. We are excited about the prospects for these new recommendations and encouraged by our colleagues' enthusiasm to get started on their implementation.

We are both very grateful to each of the subject matter experts and stakeholders who have contributed to this report (following pages). Their service to their countries and to making the world a better and safer place is something their organizations and families can be proud of. This list is evidence that we are not only bridging gaps between China and the United States, but also between government and industry, politicians and scientists, lawyers and engineers, and those comfortable with the status quo and those driving for improvements. But the most important bridge we can build is one between hostility and friendship. Best wishes to all of those we respectfully challenge in these pages with facing some hard truths and stepping up to action.

Sincerely,

Karl Frederick Rauscher
Chief Technology Officer & Distinguished Fellow,
EastWest Institute

Chairman Emeritus, IEEE CQR

Bell Labs Fellow

Yonglin Zhou
Secretary General,
Information & Network Security Committee,
Internet Society of China

Director, Department of Science & Technology, CNCERT

Contributors

The following individuals served as subject matter experts during the development of this report. Their contributions from their respective fields of experience as a stakeholder, a corporate manager or technical expert were essential to the analysis, conclusions and guidance presented herein. Contributors may not agree with all the observations made in the document, but all agree that it presents an important framework for going forward. In addition to those listed below, there were an equal number of contributors with equal stature whose names are not included for various reasons.

Andrew Bach
Chief Architect, Financial Services - Juniper Networks
Ffmr. Global Head of Network Services, NYSE Euronext

Merritt Baer
Independent Consultant, Merritt Rachel Baer, LLC
fmr. Legislative Fellow, United States Senate
Harvard Law School

Frank Biller
Managing Vice President, Hitachi Consulting
fmr. Group Vice President,
Verizon Enterprise Integration Services

Matthew W. Bross
fmr. Global Chief Technology Officer, Huawei
fmr. Global Chief Technology Officer, British Telecom
Chairman Global Information Infrastructure Forum
Co-Founder, Critical Technologies
CEO, IP Partners

Matt Carothers
Senior Security Architect, Cox Communications

陈利军
CHEN Lijun
Business Executive, Division of Network Safety,
Network Operation and Maintenance Department,
China United Network Communications Group Co.,Ltd
中国联合通信有限公司

Michael Chertoff
Chairman & Co-founder of The Chertoff Group
fmr. Secretary, U.S. Department of Homeland
for President George W. Bush
fmr. Federal Judge, U.S. Court of Appeals, Third Circuit

Erin Nealy Cox
Executive Managing Director, Stroz Friedberg, LLC
fmr. Assistant United States Attorney, U.S. Dept. of Justice

Bryan Cunningham
Principal, Bryan Cunningham Law
fmr. Deputy Legal Adviser to National Security Advisor
Condoleezza Rice under U.S. President George W. Bush
fmr. Founding Vice-Chair, American Bar Association
CyberSecurity Privacy Task Force
fmr. Senior CIA officer under U.S. President Bill Clinton

David Fagan
Partner, Covington and Burling, LLP
Author on Foreign Direct Investment

高峰
GAO Feng
Chief Engineer of Standardization,
ZTE Corporation
中兴通迅股份有限公司

James "Gib" Godwin
Founder and President of BriteWerx
fmr. Rear Admiral, U.S. Navy Naval Air Systems Command
and Space and Naval Warfare Systems Command

Stuart Goldman

Lifetime Bell Labs Fellow

fmr. Chair, Alliance for Telecommunications Industry Solutions Network Interconnection and Interoperability Forum

胡珀

HU Po

Safety Technical Manager,

Web Security and Information Security,

Tencent Inc.

腾讯公司

Roger Hurwitz

Research Scientist,

Massachusetts Institute of Technology (MIT)

Computer Science and Artificial Intelligence Laboratory,

Senior Fellow, Canada Centre for Global Security Studies

姜朋

JIANG Peng (Patrick)

VCERT Director,

Computer Emergency Response Service，

Venustech

北京启明星辰信息安全技术有限公司

刘德良

LIU Deliang

Director of Asia-Pacific Institute for Cyber-Law Studies

Professor of Law at the Law School,

Beijing Normal University

北京师范大学

刘紫千

LIU Ziqian

Senior Engineer,

China Telecommunications Corporation

中国电信集团有限公司

Catherine Lotrionte

Director, Institute for Law, Science & Global Security,

Georgetown University

fmr. Counsel and Director, U.S. President George W. Bush Foreign Intelligence Advisory Board

fmr. Assistant General Counsel, Central Intelligence Agency

Royal Hansen

Managing Director, Information Risk, Goldman Sachs

马欢

MA Huan

Engineer, Department of Science and Technology,

The National Computer network Emergency Response Technical Team Coordination Center of China

(CNCERT/CC)

国家互联网应急中心

Bernard Malone III

Senior Engineer, Windstream Communications

Systems Engineering Advisory Council Member,

University of Arkansas at Little Rock

Executive Vice President Operations / Founding Member,

Wireless Emergency Response Team (WERT)

Ramses Martinez

Director, Yahoo! Security Team

fmr. Director of Information Security, VeriSign, Inc.

fmr. Director Malicious Code Operations Group,

iDefense/Verisign Inc.

Patrick McDaniel

Professor of Computer Science and Engineering,

Pennsylvania State University;

Co-director of the Systems and Internet Infrastructure Security Laboratory (SIIS)

Nirmal Mody
Manager, Customer Protection Specialist, Comcast Cable

Joseph S. Nye, Jr.
fmr. Dean, John F. Kennedy School of Government,
Harvard University
fmr. Assistant Secretary of Defense
for International Security Affairs,
fmr. Chair, National Intelligence Council
fmr. Deputy Under Secretary of State for Security
Assistance, Science and Technology

Wayne Pacine
Senior Interagency Project Analyst,
Federal Reserve Board of Governors
Chair, Treasury Department's GETS Committee;
Co-chair (with the DHS), GETS/WPS User Council;
Co-chair (with the FCC), Priority Services Work Group

Audrey Plonk
Global Security and Internet Policy Specialist, Intel
Corporation
fmr. Consultant, Department of Homeland Security National
Cyber Security Division,
Booz Allen Hamilton

钱小斌
QIAN Xiaobin
Director of Enterprise Network Security TMG,
Huawei Technologies Co., Ltd.
华为技术有限公司

Tom Quillin
Director of Cyber Security Technology and Initiatives,
Intel Corporation

Lt. Gen. Harry D. Raduege, Jr. USAF ret
Senior Counselor to The Cohen Group & Chairman,
Deloitte Center for Cyber Innovation
fmr. Director, Defense Information Systems Agency
fmr. Commander, Joint Task Force –
Global Network Operations

Chris Roosenraad
M3AAWG Co-Chairman;
Director of Systems Engineering, Time Warner Cable;
Co-vice chairman, The Messaging, Malware and Mobile
Anti-Abuse Working Group

Dominic Ruffolo
Director 2, Prodt Development Engineering,
Comcast Corporation

Marcus Sachs
Vice President, National Security Policy, Verizon
fmr. Director, Communications Infrastructure Protection,
White House
fmr. Director, SANS Internet Storm Center
ret. Major, United States Army

John Savage
An Wang Professor of Computer Science, Brown University
fmr. Jefferson Science Fellow, U.S. State Department

Greg Shannon
Chief Scientist for the CERT Program at Carnegie Mellon
University's Software Engineering Institute, Department of
Defense federally funded research and development center

石晓虹
SHI Xiaohong
Vice President,
Qihoo 360 Technology Co. Ltd
奇虎 360 科技有限公司

Justin Somaini
Chief Trust Officer, Box
fmr. Chief Information Security Officer, Yahoo!
fmr. Chief Information Security Officer, Symantec

Andy Steingruebl
Sr. Manager, Internet Standards, PayPal Inc.
Board Member, National Cyber Security Alliance & Online
Trust Alliance

Eliza Strickland

Associate Editor, IEEE Spectrum

Columbia University Graduate School of Journalism

Fred Stringer

System Engineer - Network Architect,

AT&T Chief Security Office

苏志胜

SU Zhisheng

Network Security Manager,

Network Operation and Maintenance Department,

China Telecommunication Co. Ltd.

中国电信集团有限公司

谭刚

TAN Gang

Assistant Professor, Computer Science and Engineering,

Lehigh University, Security of Software (SOS) Lab

National Science Foundation Award Recipient

谭晓生

TAN Xiaosheng

Vice President,

Qihoo 360 Technology Co.,Ltd

奇虎 360 科技有限公司

Julie Taylor

SVP/Operations Manager, SAIC

VP Deputy Operations Manager, Science Applications

International Corp.

Meredith Walker

Economist, MMW Research

North Texas Crime Commission, Cybercrime Committee

fmr. Federal Reserve Banks of New York and Dallas

China specialist and Grandniece of AVG Flying Tiger

王怀州

WANG Huaizhou (Joe)

Director, Innovation Center, NQ Mobile Inc.

网秦科技有限公司

王慧

WANG Hui (Sophia)

Engineer, Department of Science and Technology,

The National Computer Network Emergency Response

Technical Team Coordination Center of China

(CNCERT/CC)

国家互联网应急中心

王明华

WANG Minghua

Director of Operation Department,

The National Computer Network Emergency Response

Technical Team Coordination Center of China

(CNCERT/CC)

国家互联网应急中心

魏来

WEI Lai

Project Manager, Department of Networks,

China Mobile Communications Corporation

中国移动通信集团有限公司

Bill Woodcock

Founder and Research Director, Packet Clearing House

Trustee, American Registry for Internet Numbers (ARIN)

Jody Westby

CEO and Founder, Global Cyber Risk LLC

Adjunct Distinguished Fellow, Carnegie Mellon CyLab

Chair, American Bar Association Privacy

& Computer Crime Committee

fmr. Director of Domestic Policy,

U.S. Chamber of Commerce

Rebecca Wexler

Independent Documentary Filmmaker
Co-founder of the ISP Yale Visual Law Project
Yale Law School

Jason Zabek

Manager Customer Safety, Cox Communications
fmr. Senior Abuse Engineer/Team Lead - Customer Safety,
Cox Communications

吴建强

WU Jianqiang

Security Manager,
Sohu.com Inc.
搜狐公司

张明

ZHANG Ming

Associate Research Professor, LL.D.,
China Institutes of Contemporary International
Studies(CICIR)
中国现代国际关系研究院

徐原

XU Yuan

Engineer, Operation Department,
The National Computer Network Emergency Response
Technical Team Coordination Center of China
(CNCERT/CC)
国家互联网应急中心

赵良

ZHAO Liang (Richard)

Chief Strategy Officer,
NSFOCUS Information Technology Co., Ltd
北京神州绿盟信息安全科技股份有限公司

杨满志

YANG Manzhi

Chief Technology Officer,
Eversec (Beijing) Technology Co., Ltd.
恒安嘉新（北京）科技有限公司

赵闽

ZHAO Min

Safety Technical Director,
Jinshan Technology Co. Ltd.
金山网络技术有限公司

Acknowledgements

Special recognition and sincere appreciation is here expressed:

to the **many volunteers, financial sponsors** and **in-kind contributors,**
whose devotion to making the world a safer and better place makes this work possible.

to **C.H. Tung** and **Joel Cowan,**
for their personal interest and invaluable insights into the Sino-American relationship.

to **Michael O'Reirdan, Chris Roosenraad** and **Jerry Upton,**
for their contributions in the planning of worldwide outreach for the 'Fighting Spam to Build Trust' recommendations of the preceding bilateral report.

to **SHI Xiangsheng,**
for continuous encouragement and support.

to **Peter Castenfelt,**
for his intellectual rigor and invaluable insights on international relations.

to **Kaiser Kuo,**
for his exceptional perspective and passion for bridging two cultures.

to **Greg Austin,**
for his continuous support and encouragement of the China-U.S. bilateral program.

to **ZHAO Liang (Richard), Lu Lan** and **Jane Lu,**
for their special role in providing advice.

to **Nadiya Kostyuk**,
for her research and operational support.

to **Merritt Baer, Matt Carothers, Bryan Cunningham, David Fagan, Franz-Stefan Gady, Stu Goldman, Bernie Malone, Mercy Rauscher, Grace Rauscher**, **John Savage,** and **Sarah Stern,**
for their editing, proofreading and quality control.

to, **David Firestein**, **Piin Fen-Kok, Alison Kung and Euhwa Tran,**
for their experience, insights and dedication regarding the China-U.S. relationship.

to **CAI Mingzhao, HUANG Chengqing, LIU Zhengrong,**
James L. Jones and **John Edwin Mroz,**
for their vision that opened the door for this opportunity.
.

and finally, to our wider community of respective stakeholder confidants in Beijing and Washington, D.C.
whose appreciation for Track 2 innovation confirms the value of accomplishments like this.

Table of Contents

List of Definitions

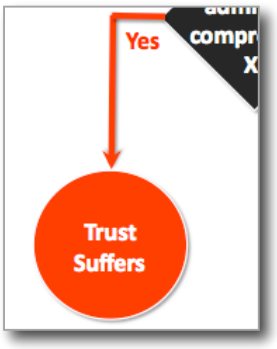
List of Figures

List of Tables

1. Executive Summary

The 'hacking' issue is a *serious challenge* for the future friendship and the prosperity of China and the United States.

Unlike superpowers before, history's two largest economies are intimately intertwined and mutually reliant in cyberspace. Information and communications technology (ICT) is pervasively applied to medical care and social life, industry and trade, research and education, and law enforcement and national security, to name a few. The technologies that China and the United States are now so reliant upon are rapidly advancing in both the power they wield and the complexity they bring, thus making us more and more vulnerable. China and the United States are mutually reliant upon ICT products that are made by each other. While the U.S. has a unique grasp of the technology supply chain with its research and development leadership in core software and hardware platforms, China is catching up. They are so close in their integrated reliance on each other, that each can easily do harm to the other—*devastating* harm. Unfortunately, in the past years, China and the U.S. have seen the trust in their relationship suffer. The current situation is thus one of growing instability for China and the U.S. with regard to cybersecurity.



Arising from a variety of motivations, including crime, politics and curiosity, a growing number of harmful activities are conducted in the cyberspace we are so much relying upon. Such harmful hacking threatens the safety and prosperity of the world. From a pure numbers perspective, the networks of China and the U.S. have many Internet Protocol (IP) addresses, and thus have many potential sources of malicious activity, as well as many potential targets. Among all written and spoken words on the subject, the suspicions and blames have taken on the strongest voice for the relationship of China and the U.S. Yet we know that such an approach can never solve such difficult problems. On the contrary, such accusations and arguments have fueled escalations so that the relationship is now strained, making even routine dialogue apprehensive, rather than comfortable and confident.

Presidents Obama and Xi have placed cybersecurity on their bilateral agenda, and front and center is the issue of damaging hacking.[1] The problems include the exfiltration of commercially sensitive data, access into operations of critical infrastructure and national security assets, the militarization of cyberspace, unequal scrutiny of behaviors in cyberspace and the dependence on the other's systems in its critical infrastructures. The joint problem statement was agreed as:[2]

> For China and the United States, the following are unacceptable: (i) the **perceived core beliefs** of each other for what is permissible behavior in cyberspace, (ii) the **proliferation of compromises** being

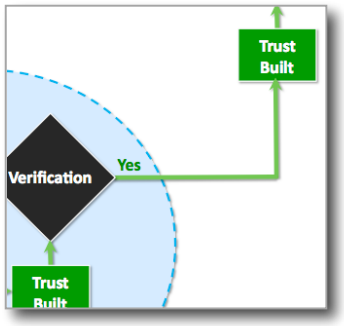
[1] *Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting*, Sunnylands Retreat, Rancho Mirage, California, 8 June 2013.
[2] Section 2.2, *Problem Description*.

made to each other's assets in cyberspace, and (iii) the **unsettled dispositions of identified incidents** of compromises that have affected each other's assets.

What is common is that neither side is comfortable with the policies and practices of the other. Both sides also recognize that harmful hacking is not just a China-U.S. issue, as it is of global concern.

This report was prepared to help these two countries get out of this predicament. This report was prepared through the agility of a track 2 bilateral approach, with the insights of over 150 volunteer subject matter experts with profound experience and knowledge of policy, technology, business and law, as relevant to cybersecurity. Facilitated by the Internet Society of China (ISC) and the EastWest Institute (EWI), this research report answers two questions:

1. *How do we build trust between China and the U.S. in cyberspace?*
2. *What practical countermeasures can we take to improve the safety of cyberspace?*



This report submits ten immediately actionable Recommendations, which if implemented, will establish practical conversations and relationships that can slow the rate of destabilization around this subject, and with continued application then reverse the trend's direction to one that is favorable (Section 4).

Together, the first four recommendations support a Total Trust Management (TTM) system that assures a reliable assessment (Figure 1). With this system in place, genuine trust can thrive and each party can have confidence in their assessment. This system will also detect when either party is demonstrating behavior that is *not* trustworthy, and likewise enable a party to have confidence in its judgment that there is insufficient evidence that their interests are being protected. The system deliberately removes the gamesmanship of political doublespeak. This will confront political operations that employ euphemistic, ambiguous and obscure language to address difficult situations. But the seriousness of the present China-U.S. crisis dictates that we can no longer afford the luxury of such diversions for our limited mindshare, resources and time.

The TTM system is equally applicable for a wide range of topics, including international cooperation in fighting crime, international cooperation in tracking down malicious hackers, protection of humanitarian interests, protection of commercial intellectual property and norms of behavior in cyberspace. The first set of recommendations can be summarized as:

- **Recommendation No. 1** ***Stated Policy***
  The first step to building trust is setting expectations. This first recommendation calls on governments, businesses and other organizations to state clearly their interests and practices in cyberspace.

- **Recommendation No. 2** ***Policy Deployment***
  Once policy is stated, the second step in building trust can begin: moving from words to actions. This recommendation calls on governments, businesses and other organizations to deploy the policies they espouse.

- **Recommendation No. 3** ***Performance Measurement***

Once policy is stated and deployed, then the third step in building trust can begin: engaging stakeholders who perceive an apparent failure in policy or its deployment. This recommendation calls for cooperation in analyzing incidents of failed policy or its deployment.

- **Recommendation No. 4** ***Corrective Action***
  The response to failures in stated policy or its deployment are a key indicator of an organization's trustworthiness, whether it be a govenement agency, a business, or otherwise. Corrective actions are tangible ways that show serious commitment to stated policy.[3]

Each party is evaluated based on adherence to its stated policy and plan of action.[4] If implemented, these recommendations will clear the air. Stakeholders will have confidence in each other based on their observations from a pattern of what is said, done and seen. This cycle of meaningful dialogue and engagement will in turn produce tangible progress at various levels in confidence building and risk reduction, with the aim of producing an upward spiral of reinforcing cooperation and trust.

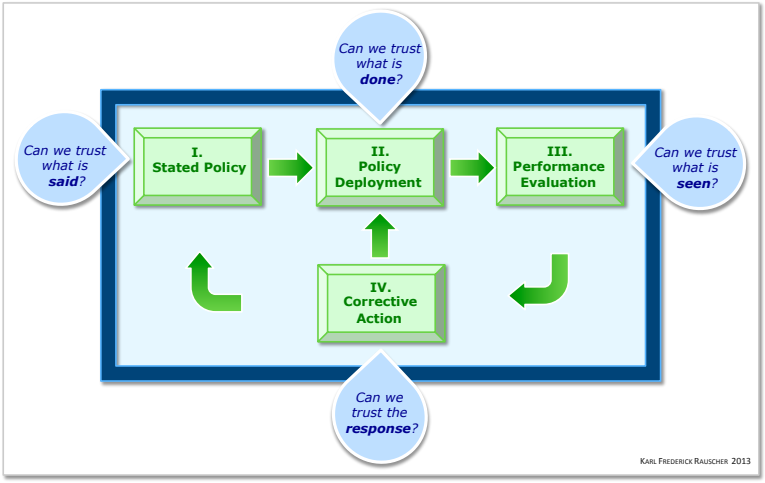


Figure 1. Total Trust Management Model, with Trust Questions.

The simple truth is that the essential 'asks' in these first four recommendations are actually quite *basic*. Yet, the present day China-U.S. crisis over hacking is evidence of how these *basics* have been neglected. In the unfortunate case where either one or both sides is unwilling to commit to these basics, discussions on more advanced subjects can be delusional; giving a false sense of safety for which there is no foundation. Thus the TTM system can help inform both parties and stakeholders of a status of good health, improving health, deteriorating health, or bad health. The TTM system is an alternative to brinkmanship, i.e. deterioration of confidence that is reinforced by the negative cycle of non-cooperation and misinformation.

An element of the analysis was the Landscape of Interests in Cyberspace framework, which enabled focused analysis of three primary interests, and their interactions (Figure 2, Section 2.4.1, *Landscape of Interests*). By examining the interests, we categorize the information systems into seven groups. Different groups have different involvement with

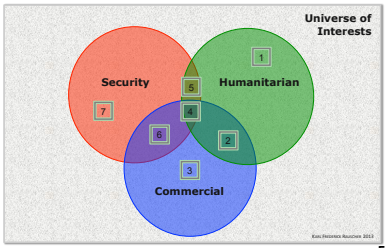


Figure 2. Landscape of Interests in Cyberspace.[5]

[3] i.e., Recommendation No. 4, *Corrective Action*, anticipates regular needs to adjust Stated Policy and Policy Deployment plans.
[4] At its core, the TTM system described above is an empirical method of arriving at the truth, but one that allows for human imperfections along the way.
[5] Rauscher, Karl Frederick, *Written Statement for the United States Congress House Committee on Foreign Affairs, Hearing on "Asia: The Cyber Security Battleground"*, 23 July 2013.

cybersecurity. One major conclusion from this analysis includes agreement that humanitarian assets in cyberspace deserve special protection. A second major conclusion is that governments, businesses and other entities with national security missions, should acknowledge the higher risk of international espionage when doing so.

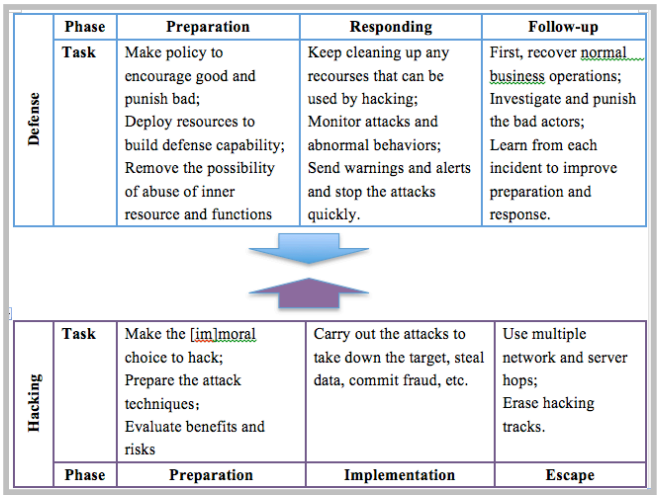


Figure 3. Model of Harmful Hacking and Defense.

Another element of the analysis was the Model of the Harmful Hacking and Defense, which helps present the countermeasures to improve the security and address the attacks.

Based on the above analysis, another six recommendations were developed to provide additional guidance that compliments the first set of recommendations by emphasizing specific critical areas requiring special attention:

- **Recommendation No. 5** ***Separate Critical Humanitarian Assets***
  This recommendation calls for qualified humanitarian entities to articulate their interests and to seek separation of their assets in cyberspace.

- **Recommendation No. 6** ***De-Clutter Espionage Expectations***
  This recommendation acknowledges the expectation that national security-oriented assets, because of their potential for hostility, are elevated as targets for espionage by foreign interests. This factor suggests a differentiation between incidents experienced by national security interests and other entities.

- **Recommendation No. 7** ***Summon a Roundtable of Subject Matter Experts***
  This recommendation calls on world-class subject matter experts from both countries to create a new mode of collaboration, and as a resource for objective analysis and assessment. Joint China-U.S., objective assessments of the situation will be an alternative to the assessments offered by journalists, the marketing literature of commercially-vested interests and solely to government agencies with competing political agendas.

- **Recommendation No. 8** ***Continuous Approach Status Indicator***
  This recommendation calls for a provisional capability to monitor, assess and report on the status of each of these crucial components. It will provide a reliable, independent assessment of the health of the dialogue and cooperation.

- **Recommendation No. 9** ***Prepare Sufficiently, React Quickly and Summarize Seriously***
  This recommendation calls for transformation of the harmful hacking responses from one that is primarily reactive to one that is proactive, and includes setting goals that define sufficient preparation and response.

- **Recommendation No. 10** ***Launch Parallel Bilateral Collaboration on Government and Industry Levels***
  This recommendation calls for industry level collaboration to supplement the new cooperation undertaken at the governmental level. Industry technical expertise and business insights are required to combat the harmful hacking that is out of control.

This report also presents voluntary Best Practices, which provide complimentary support to the Recommendations (Section 5). The Best Practices development was informed by the Eight Ingredient Framework and intrinsic vulnerability analysis (Section 2.5.2) and the Lifecycle of a Hack (Section 2.5.3).

This bilateral report can be summarized statistically as follows:

1		Common purpose to reverse the hacking that is harming our countries
2		The number in a series of bilateral reports[6]
10		Recommendations
80		Key Observations from analyses
100		Voluntary Best Practices
>150		Contributing subject matter experts and stakeholders
>2,000		Years of combined experience of contributing experts and stakeholders
>100,000		Analysis points with determinations made

This report is *not* a typical policy paper, nor are its ideas "in the sky." Rather, it is a document that includes the practical, "down to earth" guidance essential for solving the harmful hacking problem. The character of this report may be more likened to that of a musical score for a symphony orchestra, where distinct contributions are called for from a diverse range of talents; if each performs in harmony with the other, the results are awesome. Those who care about the cyber relationship, and those who care about the security and prosperity of the cyberspace, are encouraged to read and reference this report.

[6] Rauscher, Karl Frederick, Zhou, Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting Spam to Build Trust*, EastWest Institute and Internet Society of China: 2011.

Give me six hours to chop down a tree and I will spend the first four sharpening the axe.
- Abraham Lincoln

When the wind of change blows, some build walls, while others build windmills.
- Ancient Chinese Proverb

2. Introduction

This section provides background information regarding the motivation, scope and methodology of this study. In the following pages the reader can learn the answers to the central questions: *Why was the study undertaken?*, *What was covered in the study? How was the study conducted?* Additional information is interwoven throughout this introduction regarding *who* contributed to the study, and *when* and *where* the study took place.

2.1 Motivation

The motivation for this study has been brewing for most of the past decade. We review here the most important aspects of the impetus for action.

2.1.1 A Profoundly Serious Subject

First, we answer the question: *Why this subject?* The simple truth is that **"hacking" is a profoundly serious subject for modern society**. Hacking is at the core of the broader cybersecurity concern that is established as a critical priority for societies around the world, both economically developed and economically developing. The integral role of information and communications technology (ICT) is pervasive, intensifying in many dimensions—social, enterprise, critical infrastructure and military, to name a few. Hacking jeopardizes the integrity of each of these dimensions, and thus the safety, stability and security of people around the world. The intrinsic vulnerabilities of cyberspace being what they are, there are many opportunities for hacking to cause harm.[7]

The hacking conundrum is particularly problematic when the offending and offended parties reside in different nation-states, having different histories and cultures. The incongruence in some values and practices impedes solutions. This geopolitical border challenge brings us to the next motivation for this study.

2.1.2 The Stakes are High for China and the United States

So why do we focus on China and the United States? Another simple truth is that **there are no two countries for which the stakes related to hacking are greater than for China and the United States.** As Taiwan, which U.S. General Douglas MacArthur referred to as 'an unsinkable aircraft carrier', is China's biggest point of tension with the U.S., hacking has for several years been the biggest point of tension for the U.S. with China.[8] American government leaders are claiming that Chinese hackers are

[7] Rauscher, Karl. F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal Homeland Security Special Issue, Volume 9, Number 2, 2004.
[8] MacArthur, Douglas, Message on Formosa, 17 August, 1950.

responsible for "billions of dollars" when "industrial secrets are stolen."[9] Yet at the time of this report's writing, allegations of the U.S. National Security Agency (NSA) operations and related cooperation with U.S. companies, raises Chinese concerns regarding U.S. policies and practices affecting its public information systems.

It is clear that the integral role of ICT is even more critical for the two largest economies in the history of this planet. Both China and the United States (i) have **heightened reliance** on cyberspace, economically and otherwise, (ii) are **leading producers** of the technology that each other and the rest of the world depend upon, (iii) have **advanced capabilities** given their leadership role in ICT, and (iv) are **uneasy** with the influence that each other wields in cyberspace.[10] Thus both China and the U.S. find the situation unacceptable, as do many other countries. It directly follows that the security of cyberspace is integral to the stability, peace and security of both countries, and to the world.

2.1.3 A Breakthrough Is Needed Now

To date, solutions from both the public and private sectors to this hacking problem have been insufficient. This brings us to the next aspect of motivation and a third question: *Why undertake this study now?* At present there is an unmistakable inflection in the perceived priority of this subject for China and U.S. relations.[11] There is also a realization that the limited progress of conventional approaches seems to many experts to be insufficient. Moreover, the outlook for the future production of these conventional approaches is similarly disappointing. Thus, a breakthrough is needed. Indeed, **without a breakthrough soon, the present course is fraught with near term hazards**. Unlike the Taiwan conundrum, which both countries have learned to accommodate in international relations, the new tension is acute and destabilizing as it is only becoming more central to economic and political priorities for both countries.

2.1.4 An Abundance of Caution

Having presented the motivation for this study in a straightforward fashion, it is worth pausing to recognize that not all parties are supportive of pursuing genuine bilateral collaboration addressing the hacking problem between these two countries. Just as there are avid supporters for genuine China-U.S. collaboration from throughout the realms of politics, academia, business and the public at large (Section 2.3.1, *Subject Matter Expertise and Stakeholders*), there are also skeptics from across this same landscape. Their resistance is rooted primarily in mistrust of the other country.[12] Such perspectives are firmly held by individuals who are presumed to be exceptionally well informed.[13]

Skeptics of these contrarians attribute some portion of the resistance to personal political ambition, commercial exploitation, or other interests that conflict with the goal of stabilizing the situation.[14] In the final sum however, it is underscored here that the gravity of the combined motivation factors from above

[9] U.S. President Barack Obama, *Transcript: President Obama's Exclusive Interview With George Stephanopoulos*, ABC News, 13 March 2013.
[10] For (iii) Experts Survey Question No. 7. Key Observation No. 5, *U.S. Leading China in Cybersecurity*, Section 3.1.
[11] Key Observation No. 19, *A Window of Opportunity*, Section 3.1; Key Observation No. 20, *Government Working Groups Are Underway*, Section 3.1.
[12] Key Observation No. 44, *Reluctance to Cooperate on Combating Hacking Is Reinforced by Distrust*, Section 3.2; Key Observation No. 45, *West Cautious of East*, Section 3.2; Key Observation No. 46, *East Cautious of West*, Section 3.2.
[13] Hayden, Michael, former Director, U.S. National Security Agency and former Director, Central Intelligence Agency: *"I understand the Chinese espionage effort against the West. As an intelligence professional, I stand back in awe at the breadth, depth, sophistication and persistence of the Chinese espionage campaign against the West. . . . They have a much broader definition of legitimate espionage to include intellectual property, commercial trade secrets, and the negotiating positions of private entities."* Joye, Christopher, *Transcript: Interview with former CIA, NSA chief Michael Hayden*, Australian Financial Review, The, 19 July 2013.
[14] Key Observation No. 21, *Cybersecurity Is a Growing Market*, Section 3.1; Key Observation No. 22, *Funding Attracts Interest*, Section 3.1; Key Observation No. 42, *Cybersecurity Brings the Influence of Insidious Interests*, Section 3.2.

outweigh the objections to collaboration, though the later, as well as the internal appreciation of the respective national security interests of team members, informs the former to use an abundance of caution.

2.1.5 Objectives

The purpose of this study is to create practical mechanisms and provide concrete best practices between the Chinese and U.S. industries that will form a bridge over which sensible trust between China and the United States can be fostered and the online environment can be improved dramatically (Figure 3). This effort is a part of a larger bilateral program that seeks to optimize the contour of cooperation between the two countries (Figure 5). At the practical level, a measure of success is whether tangible operational changes can be made in the behaviors of both countries. The measures of success for this endeavor are whether or not the recommendations put forth (Section 4) are effective in impacting the hacking issue between China and the United States by either: (Objective I) *slowing* the rate of decline in the health of the relationship; or better, (Objective II) *stopping* the decline in the health of the relationship; or, most desirable, (Objective III) *reversing* the direction from a declining health to an improving health (Figure 4).[15]

Figure 4. Building Sensible Trust and Safe Cyberspace on a Bridge of Practical Measures.

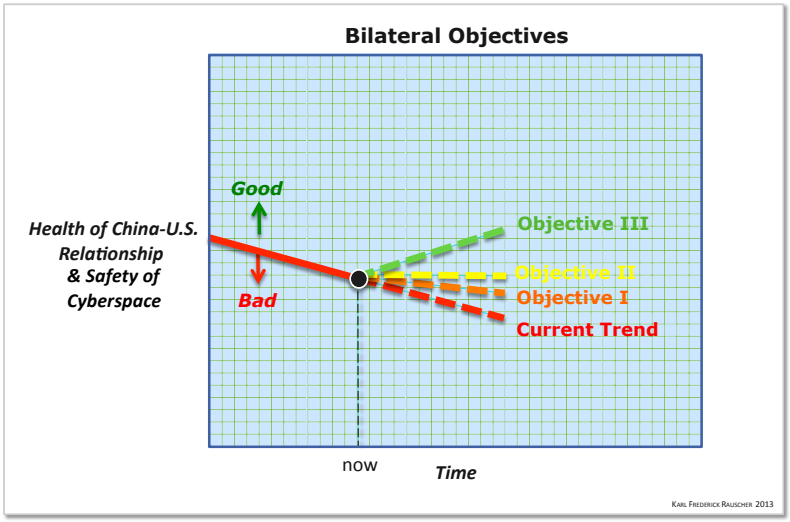
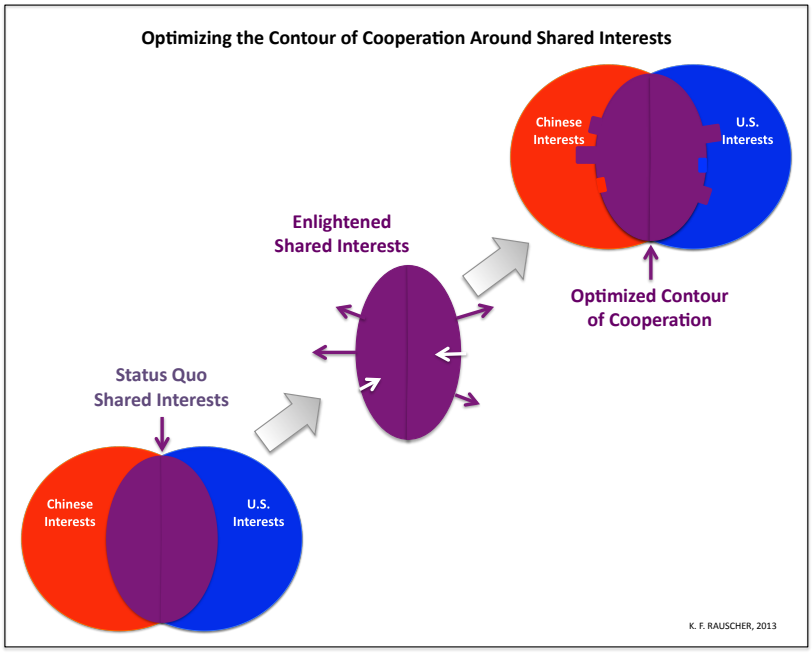


Figure 5. Bilateral Objectives for Impacting the Health of the China-U.S. Relationship and the Safety of Cyberspace.
Objective I = *slow* the rate of decline
Objective II = *stop* the decline (better)
Objective III = *reverse* the direction (most desirable)

[15] Key Observation No. 58, *Three Levels of Success*, Section 3.3.

The contributors to this study are not naïve regarding the very real and significant differences in the interests of their two countries, or of the associated dangers when large powers are at odds with each other, as history can well attest. However, solutions to the current predicament that are based on a major overhaul of ideological or political regimes have a low probability of success. On the contrary, the objective of this body of work is to be achieved by focusing on real, tangible steps toward progress to actually make cyberspace better for all of us. These are bold because they break new ground, but reasonable because they are well researched and feasible. Figure 6 suggests how the objective of trust building for the issue of hacking can be achieved through focused collaboration on well-defined, incremental steps.



- First, the U.S. and China have both shared and unshared, or simply, different interests. This is what makes the world so interesting and dangerous.
- Second, regarding the shared interests, there is potential for cooperation, however the current environment of growing mistrust impedes straightforward understanding of each other's interests.
- Third, the contour of cooperation can be optimized if we (a) extend cooperation into new areas based on enlightened understanding of actual shared interests, and (b) pull back cooperation where shared interests are not, after careful examination, in reality enjoyed.
- Fourth, an optimized contour of cooperation of shared interest can reset the tone for discussions, giving both sides the confidence that the relationship can improve as steps of new cooperation are taken. As we have found with the success of the fighting spam work, we can now move into arenas of higher complexity and higher consequence.

Figure 6. Optimizing the Contour of Cooperation around Shared Interests.[16]

The practical measures take the form of specific "Next Steps" and "Measures of Success" that are detailed for each of the eight recommendations (Section 4) and in the form of voluntary Best Practices (Section 5). The application of these practical measures can be achieved by the organizations called upon to take action. The incremental enactment of these practical steps will in turn have an effect of incremental trust building, step by step.

[16] Rauscher, Karl Frederick, *Written Statement for the United States Congress House Committee on Foreign Affairs, Hearing on "Asia: The Cyber Security Battleground"*, 23 July 2013. docs.house.gov/meetings/FA/FA05/20130723/101186/HHRG-113-FA05-Wstate-RauscherK-20130723.pdf .

2.2 Problem Description

Both China and the U.S. find the current situation regarding hacking as unacceptable. However, each country sees the problem differently.

UNILATERAL PROBLEM STATEMENTS

As seen in America . . .

For the United States, the primary aggravation in cyberspace is the theft of its **private sector intellectual property** (IP). IP theft includes, but is not limited to, propriety information of companies, software and hardware designs and digital media content. Another weighty area of irritation is unauthorized foreign access into the control systems of U.S. **national critical infrastructure** such as energy grids. The primary concern here is that such access could cause intentional or unintentional disturbances to the operation of critical infrastructure, which could result in loss of life and severe economic consequences. A third area of complaint is foreign access into **national security assets** of the U.S. military. As the world's technology leader and for its unique status of influence, the U.S. believes it is the target of a disproportionate amount of compromising efforts in cyberspace from many sources, and often identifies the above described malicious activity as emanating from Chinese communications networks.

As seen in China . . .

For China, there are four distinct cybersecurity concerns in cyberspace. One major concern is the **increasing militarization** of cyberspace, and it sees the United States as the most aggressive actor that is contributing to this dangerous global trend, inciting a cyber arms race. The second major concern is that the **U.S. has control over** most of the core resources of the Internet, such as the root DNS servers, and China relies on the U.S. too much for ICT software & hardware. So the U.S. can easily disable China in cyberspace. The third concern is that a great number of systems from the government, Internet service providers, critical information systems and academy research institutes, etc., have been **broken into and secretly controlled** by IP addresses appearing to come from U.S. networks. The fourth major concern is the **underground hacking economy**, which include source IP addresses that appear to be emanating from American networks.

On one hand, *if unresolved,* the current trajectory of the above-described problem(s) puts the stability of the China-U.S. relationship in increasing jeopardy. On the other hand, *if resolved*, the aggregate solutions could enhance the many beneficial areas the two countries presently enjoy as economic partners and can serve as a role model for other nation-states facing similar problems with each other.

A bilateral consensus problem statement extracted from these two perspectives was formed and is presented here.

BILATERAL PROBLEM STATEMENT

For China and the United States, the following are unacceptable:

(i) the **perceived core beliefs** of each other for what is permissible behavior in cyberspace,
(ii) the **proliferation of compromises** being made to each other's assets in cyberspace, and
(iii) the **unsettled dispositions of identified incidents** of compromises that have affected each other's assets

Therefore, China and the United States desire to solve their shared relationship problem with solutions to each of the specific elements of the Bilateral Problem Statement. There are three distinct components of the Bilateral Problem Statement:

I. **The perceived core beliefs for what is acceptable behavior in cyberspace**
II. **The proliferation of compromises to assets in cyberspace**
III. **The unsettled dispositions of identified incidents**

On one hand, the policy aspect of each of these three elements is apparent as the "core beliefs" (from I), the "compromises of assets" (from II) and the rhetoric around "unsettled dispositions" (from III) are powerful factors in the China-U.S. political relationship. On the other hand, the technical aspects of these problems is also quite evident, noting that the "behavior in cyberspace" (from I), that "compromises" (from II) and "incidents" (from III) are each ultimately technical realities that generally require in-depth technical skills. Therefore the solutions to these three related, yet distinct, elements of the problem necessitate an integration of policy and technical expertise and experience. Each party seeks policy-sound and technically sound agreements with the other on expectations for behavior in cyberspace as well as mechanisms for reporting and investigating cyber incidents identified by either party. The combined eight Recommendations (Section 4) and 100 Best Practices (Section 5) provide such needed, integrated solutions.

The key to addressing the first part of the problem, *perceived core beliefs for what is acceptable behavior in cyberspace (*I), is clarification of policies, alignment of these policies with practices and avoiding hypocritical statements where one party is blaming the other for practices that itself engages in.[17] If beliefs, and therefore policies, are not exactly in agreement, stability can still be achieved if reasonable expectations can be set for the handling of such areas of incongruence.

The second part of the problem, *the proliferation of compromises to assets in cyberspace* (II), is addressed by Best Practices countermeasures that span the hacking lifecycle, including addressing the motivations of malicious hackers, leveraging stakeholder incident detection, joint analysis in source identification and countermeasure development and application.

[17] For example, state-on-state espionage is tolerated under international law. At the same time both China and the U.S. seek to protect their commercial and state cyberspace-dependent infrastructure from compromises that damage operations or the value of proprietary data.

The third part of the problem, *unsettled dispositions of identified incidents* (III), relies upon new joint collaboration that is undertaken by subject matter experts that are confirmed as being objective, not having a conflict of interests.

In addition to these problem statement components, there are many facets of the problem that cut across many dimensions. From the many insights gleaned throughout this study, the most essential are captured in Key Observations, Section 3.

2.3 Observations

Studious observation is essential for advancing one's understanding, whether it is of another culture or of a lingering problem, such as bilateral distrust over harmful hacking. To observe means "to see" or "to notice", and is distinct from interpretation. Thus the observations made in this report are *not* the opinions of the contributors, though some include observations of opinions, such as those gleaned from a survey.

Section 3 includes 80 key observations that were collected during the study as reference points that are critical to grasping the problem and for deriving solutions.

2.4 Scope

Cyberspace is a vast field with many topics and discussions. In this section we describe the boundaries within which this study was conducted.

The scope of this study passes through many dimensions—linguistic, technical, moral, political, legal, and business, to name a few. Thus a description of the scope requires discussion of a varied array of parameters. This section reviews the scope of study in order to provide a crisp outline of what was covered and what was not. By and large the scope was broadly inclusive, i.e. the nature of the study was to be open to all potential factors of significance that were encountered.

2.4.1 Type of Potential Targets

The scope of this study included the primary core interests that both American and Chinese experts raised throughout its undertaking, namely, humanitarian, commercial and security (Figure 7, *Landscape of Interests in Cyberspace*). Each of these interests was accepted as unequivocally legitimate for both countries. As such, respect for each is carried forth throughout this report and were integral in shaping its guidance. These three core interests have exceptional status among the universe of interests because of the powerful influence they wield in societies for countries around the world.

Humanitarian

The humanitarian interest was driven by concerns for the daily safety of the general public, that is, the average, and even the least influential, members of our societies. These individuals could be harmed by hacking activities that impair their sustenance-yielding livelihood, their health care, or other essentials. Offending hacking activities could span the spectrum of directness from being tightly targeted at their personal affairs, to being indirect, or collateral, such as affecting critical infrastructure. Of the three interests, this humanitarian area was where the most commonality was shared.

The intended meaning of the term "humanitarian" in this report derived from that worked out in the Geneva and Hague Conventions of War. Thus it deals with medical care, cultural, and

spiritual assets.[18] It is envisioned that it can also extend to education, food, water and disaster relief. In this way, existing principles of agreement are leveraged, being carried into cyberspace. See Figure 7, *Landscape of Interests in Cyberspace*, Categories 1, 2, 4 and 5.

Definition 1. **humanitarian:**
concerned with human well being

Commercial

Protecting, supporting and enhancing commercial interests were major priorities for both countries. Aspects of commercial interests were diverse and encompassed free market access in each other's countries, cooperating in fighting crime and protecting intellectual property. The commercial interests are above board and transparent. The U.S. participants frequently raised concerns about the theft of intellectual property. Of the three interests, this commercial area was emphasized relatively more by the United States participants.

This category includes both for-profit as well as not-for-profit organizations, when the latter is chartered with supporting industry interests. See Figure 7, *Landscape of Interests in Cyberspace*, Categories 2, 3, 4 and 6.

Definition 2. **commercial:**
concerned with earning money

Security

Finally, the security interests of both countries were also regarded as necessary priorities for both countries to pursue. Interests in regard to security include the scopes of both national security and local law enforcement, as well as the functions of providing for it, protecting it, and maintaining its competitiveness with potential adversaries. Of the three interests, the security interest, and in particular, the stopping crime aspect, was emphasized relatively more by China. China also expressed concerns about national security interests, particularly in light of the stated U.S. government military doctrine to maintain dominance in cyberspace.[19]

While the primary focus in this report is national security, law enforcement interests, including at the local level, are also included in the "security" category. See Figure 7, *Landscape of Interests in Cyberspace*, Categories 4, 5, 6 and 7.

Definition 3. **security:**
concerned with making people or things safe

[18] A useful set of examples can be found in: Geneva Convention I, 1949, Annex 1, Articles 1-13, Hague Convention IV, 1907, Articles 27-28, 54.

[19] "*As Airmen, it is our calling to dominate Air, Space, and Cyberspace*." Secretary of the Air Force Michael Wynne and Chief of Staff General T. Michael Moseley, *Dominant Air, Space, and Cyberspace Operations*, Air & Space Power Journal, Spring 2007.

In the law enforcement domain, keeping people and property safe includes protecting youth, intellectual property and user personal information. In the national security sense, this definition of "making people or things safe" includes at times belligerent activities broadly defined. These activities include intelligence gathering, reconnaissance, as well as offensive and defense operations.

Each of these core interests played an important role in the methodology described in Section 2.5 below.[20]

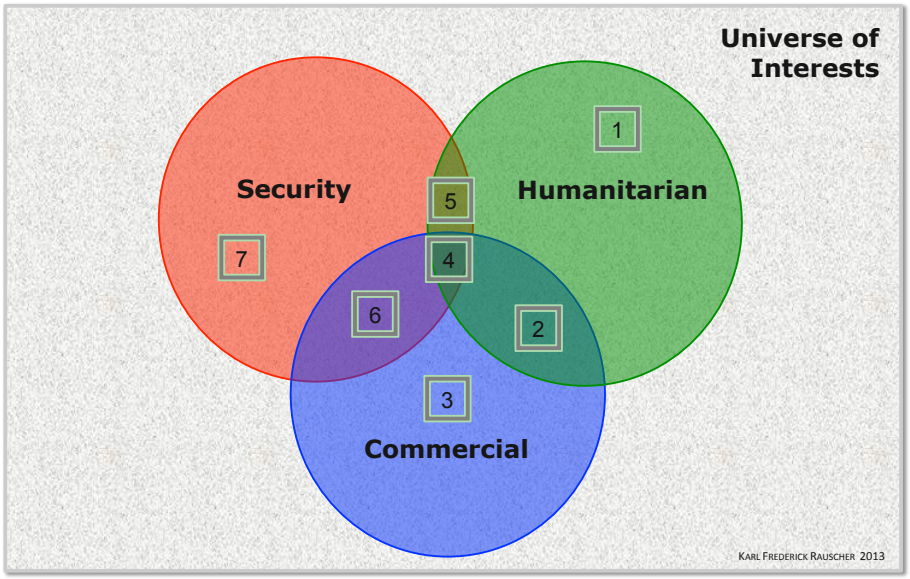


Figure 7. Landscape of Interests in Cyberspace ('KLIC' - re-shown here from Section 1)**.**[21]

It is important to note that "interests" are distinct from an organization type (Table 1). For an example, the fiduciary responsibility of for-profit and non-profit organizations providing similar services have some fundamental differences. Likewise, a commercial entity that steps into the arena of making products that support belligerent functions is distinct from those that do not in significant ways (see Recommendation No. 5, *De-Clutter Espionage Expectations*).

- **Category 1 Entities:** **Humanitarian**
  Entities whose interests are purely humanitarian, are non-profit and who avoid taking part in any security function.

- **Category 2 Entities:** **Humanitarian + Commercial**
  Entities whose interests are humanitarian, are for-profit and who avoid taking part in any security function.

- **Category 3 Entities:** **Commercial**

[20] The authors recognize that there may be other important interests in addition to the three emphasized here. However, the sense has been, with review across a wide diversity of stakeholders, that these are the chief areas of concern.
[21] Rauscher, Karl Frederick, *Written Statement for the United States Congress House Committee on Foreign Affairs, Hearing on "Asia: The Cyber Security Battleground"*, 23 July 2013. 'Karl's Landscape of Interests in Cyberspace' (KLIC).

Entities whose interests are for-profit and who avoid taking part in any security function.

- **Category 4 Entities:** **Humanitarian + Commercial + Security**
  Entities whose interests are humanitarian, are for-profit and who perform a security function.

- **Category 5 Entities:** **Humanitarian + Security**
  Entities whose interests are humanitarian and who perform a security function.

- **Category 6 Entities:** **Commercial + Security**
  Entities whose interests are for-profit and who perform a security function.

- **Category 7 Entities:** **Security**
  Entities whose interests are to perform a security function.

Table 1. Entity Type Mapping to Interests – Examples.

Category	Examples	Humanitarian	Commercial	Security
1	non-profit disaster relief organization synagogue, temple, church military hospital			
2	for-profit hospital pharmaceutical company private museum art gallery			
3	an Internet service provider a passenger airline a bank			
4	food supplier an airport or energy grid chemical weapon antidote distributor			
5	international banned weapons inspectors international affairs policy institute dual use ambulance fleet			
6	drone developers defense contractor for fighter jets networked solider technology supplier			
7	command and control center intelligence agency military force			

Other Interests

Having reviewed these three interests considered as proper influencers for China-U.S. agreements, standards, policies and regulations (ASPR) in addressing the hacking situation, we turn to interests considered improper for such high consequence deliberation. These other interests are very real, and while some of them are legitimate at a micro level for individuals or organizations, their presence in international discussions can be toxic to meaningful collaborative progress. Conducting the study necessitated

recognition of the reality of these interests and their potentially corruptive sway. Without such acknowledgement progress could be held hostage, bias could be unknowingly endorsed or attitudes, words and behaviors of some parties would be misunderstood.[22]

Contrary to the transparency of the humanitarian, commercial and national security interests that are mutually accepted as legitimate, the presence of improper interests is typically downplayed or hidden, with the result that it is often ignored. These interests include the **personal career ambitions** of those in charge of policy, such as that of elected or appointed politicians. Other interests include **nontransparent business designs**, such as those that exploit the misperception of a problem, which they may even have had a hand in shaping. Still other interests include **controlling internal government turf**, where competing agencies jockey for position in an emerging field with growing budgets and many fresh opportunities. These examples by no means complete a comprehensive list, but serve to illustrate the diversity and tangible potency of interests that could be factors, particularly at a tactical level.

Caution Against Harmful Hacking of Any Sort

Having distinguished between humanitarian, commercial and security interests, a more general statement is offered here. All harmful hacking breaks laws for all types of organizations (humanitarian, commercial and security). There are local laws in place in both China and the United States against hacking into any entity. Furthermore, there are international laws against harming humanitarian interests and commercial interests.[23] Throughout human history, there have always been attacks on enemy's systems, especially when there is a hostile relationship. But in cyberspace we still would like to say "no" to hacking into even security-related assets for these reasons:

1. The Internet and information systems are usually connected and may influence each other; i.e. when a small part of a system in the Internet infrastructure is affected it could cause a larger scale impact. Thus you cannot control the collateral damage. An example of this is evident with a virus that can spread indiscriminately.

2. In the process of hacking into a security system, you can accidentally "trip" causing, for example, a weapon to detonate.

3. For current ICT technologies it is very hard to determine the real identity of attackers, and thus any reaction could be misdirected to the wrong entity (e.g. false flag).

2.4.2 Definitions

The most significant of all scoping issues was defining "hacking," which was the initial label used to describe the subject matter for this initiative. Very soon after commencing the study, there was a realization that "hacking" is an imperfect term. Indeed, the word "hacking" was sufficiently ambiguous to render it unsuitable for effective discussion at the deeper level undertaken here in this study (see *Intrinsic Vulnerability Analysis*, Section 2.5.2)

Evidence of the ambiguity of the term 'hacking' in the context of cyberspace is apparent when one seeks clarification around simple questions like:

1). *Is hacking inherently wrong?*
2). *Does hacking include only passive access, or also active control?* and,
3). *Is it hacking if it is war?* or, *is it war if there is hacking?*

[22] Key Observation No.42, *Cybersecurity Brings the Influence of Insidious Interests*, Section 3.2.
[23] IHL.

This first question brings us to two very different value orientations of the term. On the one hand, the common practice among political leaders, journalists and the public at large has a clearly negative connotation, where *a moral offense* has been committed.[24]

On the other hand, the technical community, which certainly can't be ignored as cyberspace is their turf after all, has a practice of focusing on the *skill* associated with hacking as one of value and, moreover, is generally indifferent toward the moral nature of its use.[25]

From a solely moral outlook, the two practices of use for the word "hacking" reviewed above seem diametrically opposed. And because the chief distinguishing elements (i.e. moral offense and valued skill) is such a potent aspect for both communities, but most particularly for the former, it at first appears that a consensus agreement may be unreachable. However fortunately, a semantic decomposition of the essential elements of both usages yielded a tight articulation of meaning that serves both communities.

Analysis of a wide range of uses of the term, were resolved with the generation of the following four definitions.

Definition 4. hack (verb):
(a) to gain access (b) to an asset (c) in cyberspace
(d) without the presumed required knowledge (e) or official credentials.

Definition 5. hacking (verb):
(a) an act (b) of gaining access (c) to an asset (d) in cyberspace
(e) without the presumed required knowledge (f) or official credentials.

Definition 6. hack (noun):
(a) a specific incident (b) of gaining access (c) to an asset (d) in cyberspace
(e) without the presumed required knowledge (f) or official credentials.

Definition 7. hacker (noun):
(a) an individual (b) skilled in the art (c) of gaining access (d) to assets
(e) in cyberspace (f) without the presumed required knowledge
(g) or official credentials.

Note that these definitions accommodate both the behaviors that are widely judged as morally wrong, such as hacking another person's computer and extracting personal financial data, and behaviors that are esteemed for their creativity in the technical community, such as bypassing a constraint in a software program to provide or enhance functionality.

Another useful term is "compromise."

Definition 8. compromise (noun):
a change that makes something worse and that is not done for a good reason.[26]

[24] See Appendix D, *Discussion on the Meaning of the Term "Hacking"*, for examples.
[25] Ibid.
[26] Merriam-Webster Dictionary, merriam-webster.com.

Definition 9. compromise (verb):
to damage or weaken something.

For the China-U.S. relationship in cyberspace, the essence of the *concern* are acts that **gain access to data or assets in cyberspace in order to monitor or extract information or control assets.** This is the real problem that both countries object to. Thus while the term "compromise" focuses more on the impact, the term "hacking" refers more to the initial penetration. Both are used in this report.

Harmful hacking causes damage as asset in cyberspace, or to the people or systems that depend on it. Harmful hacking includes, but is not limited to, webpage defacement, phishing, intrusions, etc.[27] Harmful hacking is defined thus as:

Definition 10. harmful hacking (adjective, verb):
(a) an act (b) of gaining access (c) to an asset (d) in cyberspace
(e) without the presumed required knowledge (f) or official credentials
(g) that causes damage (h) to the asset (i) or an associated asset.

Appendix D, *Discussion on the Meaning of the Term "Hacking"*, provides a more detailed analysis of the meaning of the term "hacking".

2.4.3 Path of Hacking Behavior

As a bilateral, the focus of this effort was on interactions between China and the United States. Thus the two primary concerns were when a hacker from within one country was hacking the other (Table 2, *Scope of Source-Target Engagements*). However, as hacking can be something that is done with a cloak to disguise one's identity and location, situations where a hacker from within another (third) country was making it appear that either the U.S. or China was the source of a hack, were also included.

Table 2. Scope of Source-Target Engagements.

		TARGET		
		China	**U.S.**	**Other Countries**
SOURCE	**China**	*	in scope	out of scope
	U.S.	in scope	**	out of scope
	Other Countries	*	**	out of scope

*out of scope unless the source was made to appear to be from the U.S.
**out of scope unless the source was made to appear to be from China.

Internal hacking was an important concern that was raised by Chinese team members throughout the study. While not a direct focus, it is recognized that the Recommendations (Section 4) and voluntary Best Practices (Section 5) will benefit efforts to prevent hacking incidents, and ameliorate their impact should they occur, whether they come from with a country or any other (third) country.

[27] An early working definition presented by the Chinese experts: "Hacking is malicious activity conducted through ICT media, targeting direct or in-direct online systems and users, with the goal of modifying, destroying or stealing the information, or disturbing or stopping the normal running of a system or normal operation of users."

2.4.4 Governing Rules

The rules of governments (e.g., treaties, laws, regulations, directives, etc.) were considered within the scope, but not with automatic presumed authority for two reasons. First, there is a wide range of views as to the applicability of the existing rules of the physical world to cyberspace.[28] On one side of this spectrum is the view that the existing rules that have served the world prior to the arrival of cyberspace are mostly or completely transferable to it. For this perspective, legal precedents occupy and define what many others see as a vacuum of order and agreement. On the other side of this spectrum, there is a view that the virtual world of cyberspace is something new and its own new rules should apply, many of which have yet to be created.

A second reason for not presuming the authority of legal precedents is jurisdictional complexity. There are several aspects of this complexity that impede direct application, each is a case where jurisdictional assumptions cannot be assumed:

- Simple bi-domain: differences between Chinese and American national laws
- Multi-domain: distributed command and execution across multiple countries

As the number of legal precedents is seemingly unending, the considerations of legal precedents were limited. Nevertheless, legal arguments were given serious debate when raised. Areas where legal precedent was most embraced were those where extensive analysis was performed on the applicability of existing rules to cyberspace. One example of this was international humanitarian law.[29]

In the solution space, both Chinese and American experts agreed that enhanced legal structure is needed to support the investigation and prosecution of crimes in cyberspace, including those committed across borders.[30]

2.4.5 Timeframe

The scope of the study included the complete range of time orientations, namely: past, present and future. Insights were gleaned from the *history* leading up to modern times, most notably through the team's combined more than 2,000 years of experience in ICT, security, international relations or pertinent law. Examples such as specific malicious exploits, legal case studies and policy decisions were examined for relevance. In addition, the *present situation* was central to the analysis as many of the Key Observations (Section 3) bear out. Statements of politicians and other items in the news, as well as trends in offenses being carried out in cyberspace, were all part of the analysis conducted. But most importantly, this effort's goals were tied to the *future*, i.e. ways forward that enhance the stability, safety and security of cyberspace. The best corroborated with the details integrated into the presentation of the recommendations, specifically, suggested next steps and measures of success (Section 4). In summary, no limits were placed on information based on its orientation with time.

Another aspect of the time domain is whether there is present a mode of peace or of war.[31]

[28] 45% of respondents indicated that cyberspace is a truly new society that deserves its own new rules or a partly new society that deserves some of own new rules, Interactive polling results, EWI-IEEE First Worldwide Cybersecurity Summit, Dallas, 2010. 50% of respondents indicated that cyberspace is an arena where a new society really does exist and different rules should apply or is realized in part and mostly different rules should apply, EWI Worldwide Security Conference 7, Brussels, 2009. Pirate Parties are rallying around reform of copyright regulation as it affects digital media and patent law as it affects software, expansion of the right to anonymity in communication, Pirate Parties International, http://www.pp- international.net/ .

[29] Over 750 articles of the Laws of War were analyzed in: Rauscher, Karl Frederick, Korotkov, Andrey, *Russia-U.S. Bilateral on Critical Infrastructure Protection - Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute, February 2011. A later complimentary analysis provided extensive legal review: Schmitt, Michael, N., *Tallinn Manual on the International Law Application to Cyber Warfare*, Cambridge University Press, 2013.

[30] Key Observation No. 28*, Cyber Crime Laws – Overview*, Section 3.1.

[31] Key Observation No. 37, *Hacking May Lead to War,* Section 3.2.

2.4.6 Cyberspace

The scope of this study is also bound by cyberspace. In this section we discuss key aspects of cyberspace such as network types, technology types, data types and information system types. But first we introduce a definition of cyberspace:

> **Definition 11. cyberspace (noun):**
> **is an electronic medium through which information is created, transmitted, received, stored, processed, and deleted.**[32]

A more technical discussion of cyberspace recognizes that it is made of specific ingredients (Section 2.5.2).

Network Types

One of the more technical aspects of the scope was the type of networks to be included in the study. All assets in cyberspace, such as computers, databases, mobile phones, remotely controlled weapons and airplanes are connected, either temporarily or continuously, through some type of network. Quite simply, all network types were included, i.e. fabrics, medium, access control, latency, connectivity, as well as next generation networks:

- Access Control:[33] public, private and closed
- Control Path:[34] in-band and out-of-band
- Connectivity:[35] continuous, intermittent and discrete
- Fabrics:[36] legacy circuit-switched, data and hybrids
- Latency:[37] real time, near real time and non-real time
- Medium:[38] wire line, coaxial, fiber optic, wireless and free space optics
- Spatial Size:[39] Near Field Communications (NFCs), Body Area Networks (BANs), Near-me Area Networks (NANs), Personal Area Networks (PANs), Campus Area Network (CANs), Metropolitan Area Networks (MANs), Local Area Networks (LANs), Wide Area Networks (WANs), Internet Area Networks (IANs)

Technology Types

All information and communications technologies were included. Thus any technologies associated with the network types outlined immediately above are covered. Technologies include communication platforms, protocols and standards. Some of these technologies are inclusive of others.[40] The nature of the discussion

[32] Rauscher, Karl Frederick and Yaschenko, Valery, *Russia-U.S. Bilateral on Cybersecurity - Critical Terminology Foundations*, EastWest Institute and Information Security Institute of the Moscow State University, 2011.

[33] *Access Control* concerns privileges needed to be part of the network, i.e. is it open to any member of the *public* (which may include a subscription fee); or do *private* interests control access to it such as for a home, office or enterprise network; a *closed* network has additional restrictions such as being dedicated to particular limited functions or using proprietary protocols.

[34] *Control Path* refers to whether the network signals that control traffic are sent within the same path as the payload (e.g., like the Internet), or whether they are separated (e.g., like the plain old telephone service (PSTN)).

[35] *Connectivity* refers to the time association of the network with its nodes, i.e. always communicating or with periodicity or at unpredictable intervals.

[36] *Fabric* refers to the multiplexing architecture, i.e. space, time, frequency, etc.

[37] *Latency* refers to the relation of communication transmit and receive events relative to time, i.e., fully real-time duplex like the PSTN, or non-real time like email services.

[38] *Medium* refers to the physical medium that will transport the signals.

[39] *Spatial Size* refers to the approximate physical span of a network, e.g., city, global, etc.

[40] Asynchronous Transfer Mode (ATM), Broadband Wireless Access (BWA), Data Over Cable Service Interface Specification (DOCSIS), Code Division Bluetooth, Multiple Access (CDMA), Ethernet Globalization Protocols (E6), File Transfer Protocol (FTP), Global System for Mobile communication (GSM), Hyper Text Transfer Protocol (HTTP), Secure Hyper Text Transfer Protocol (HTTPS), Intelligent

assumes the use of proprietary, and unknown in the public domain, protocols; these too are standards, even if of a restricted application, and are included by nature of their being part of the ASPR of cyberspace.

Data Types

The scope includes all forms of electromagnetically or optically transmitted or stored data, i.e. at rest, in motion and being processed. Thus the intellectual property assets in databases are included, as is information being passed in a conversation from Country A to Country B that traverses the communications infrastructure of Country C. The scope also includes the full range of data ownership: personal or family information such as medical or financial records, commercial intellectual property and other business information like contracts and contacts, and military secrets and other operational defense information.

Information System Types

The scope also included all types of information systems. These are systems that create, transmit, receive, store, process, and delete data. These include tablets, personal, laptop and mainframe computers; switches, routers, gateways and other networking systems; thumb drives, networked databases, cloud and other storage systems; devices, switches routers gateways, etc. service control points, processing systems.

2.5 Methodology

This section summarizes the structure and approaches of the study, using as departure points: (a) the bilateral objectives for establishing tangible mechanisms of cooperation and thereby impacting the health of the China-U.S. relationship (Section 2.1.5, Figure 4), (b) both the unilateral and bilateral problem statements (Section 2.3), and (c) the first principles that enable new bilateral cohesion (Key Observation No. 14, *Common Principles*). Key components of methodology are reviewed here that include the assemblage and coalescence of subject matter experts and stakeholders, the scientific and engineering rigor that simultaneously anchored the confidence with original analysis and elevated the intellectual grasp of the subject matter, the openness to frank discussions for all issues as demonstrated in a joint survey that team members participated in, and quality control in developing the report's guidance.

It should not escape notice that, as with the predecessor of this China-U.S. bilateral, *Fighting Spam to Build Trust,* the methods used to produce this report were also fundamentally different in deliberate ways. Most notably, this report, in contrast to the existing body of literature (a) is a bilateral with the strong representation from both sides, (b) does not permit a point to be unchallenged by Chinese or American critics (i.e., political or public relations doublespeak does not survive), and (c) is driven by the scientific and engineering fundamentals that form the hard limits and also point toward the limitless potentials, which are the true character of cyberspace.

2.5.1 Subject Matter Expertise and Stakeholders

A bilateral endeavor involving the world's two largest economies, which has profound economic and national security implications, which is escalating in the wrong direction of growing distrust, and which takes on a highly complex and technology-oriented subject, *requires the support of an unconventionally intense assemblage of expertise and experience*.

Network (IN), Internet Protocol (IP), IP Multimedia Subsystem (IMS), Long Term Evolution (LTE), Network Time Protocol (NTP), Next Generation Networks (NGN), Post Office Protocol (POP), Secure File Transfer Protocol (SFTP), Secure Shell (SSH), Secure Socket Layer (SSL), Session Initiation Protocol (SIP), Signalling System 7 (C7, SS7), Simple Mail Transfer Protocol (SMTP), Synchronized Optical Networking (SONET), Synchronized Digital Hierarchy (SDH), Telnet Telephone Network (TTN), Third Generation Wireless (3G), Time-Division Multiplexing (TDM), TLS Transport Layer Security (TLS), Wireless Fidelity (WIFI) IEEE 802.11, Wireless Local Area Network (WLAN), Worldwide Interoperability for Microwave Access (WIMAX) IEEE 802.16, Universal Mobile Telecommunications Service (UMTS).

A partial list of the combined experts and stakeholders consulted throughout this study is provided in the front pages of this report (*Contributors*).[41] The expertise spans many disciplines, including science and engineering, business and management, legal and policy, military and security, and media and academia. The 2013 worldwide media attention on U.S. intelligence programs, is even more reason, why non-government participants are supporting this grass-roots effort to build trust in the area of cybersecurity. The combined years of experience of the aggregated China and U.S. team members is well over two thousand years.

The challenge of this study also required cross-discipline interaction of the disciplines, i.e. one expert's thoughts about how a problem was handled or miss-handled by another type of experts could be confirmed or corrected in interactive sessions.

2.5.2 Intrinsic Vulnerability Analysis

A chief distinction of this study from the vast array of policy-related literature available in the public domain is that it integrates science and engineering. Specifically, its methodology was grounded in scientific fundamentals and engineering principles that greatly strengthen the confidence associated with constraints, limitations and opportunities. This section briefly reviews the scientific and engineering principles applied in the course of the study.

The Eight Ingredient (8i) Framework of Information and Communications Technology (ICT) Infrastructure was utilized to inform the technical analysis conducted as part of this study of hacking (Figure 8).[42]

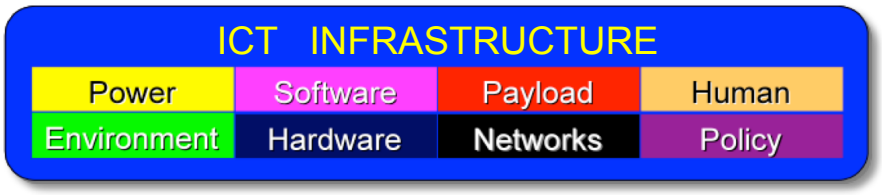


Figure 8. Eight Ingredient (8i) Framework.[43]

The 8i Framework introduces the complete set (i.e. 8) of ingredients necessary for cyberspace. Of great significance, is that each of the eight ingredients has a finite set of intrinsic vulnerabilities.

> The 8i Framework is a systematic and comprehensive framework that a) consists of the ingredients that make up communications infrastructure, b) includes all of these ingredients, c) specifies the 8 ingredients of environment, power, hardware, software, network, payload, ASPR (Agreements, Standards Policy and Regulations; abbreviated as Policy) and human. This framework is used for understanding and mastering vulnerabilities, identifying disciplines, decomposing attributes, preparing for new technologies, and other studies that support network, security, and emergency preparedness.[44]

[41] Some subject matter experts preferred not to be identified in this study. For example, reasons given included an individual not wanting personal expert opinions to be associated with their company or the complexity of approval associated with active government employees.
[42] Rauscher, Karl F., *Proceedings of 2001 IEEE Communications Society Technical Committee Communications Quality & Reliability (CQR) International Workshop*, Rancho Bernardo, CA, USA, 2001. Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.
[43] Ibid.
[44] ATIS Telecom Glossary, www.atis.org .

It follows that the ingredient and associated intrinsic vulnerability approaches have key benefits, including providing (i) the necessary rigor within the technical domain, (ii) an accurate sense of completeness, and (iii) method of examining the direct realities of cyberspace.[45] In contrast, the overwhelming majority of technical analysis provided on the subject of hacking is largely high application-specific and reliant on models of historic analogy and anecdote.

The format of this report does not provide for a thorough discussion of the ingredients and intrinsic vulnerabilities.[46] Immediately below, a brief description is provided for each ingredient, along with a subset of intrinsic vulnerabilities and an example of a strategic asset and compromise (Tables 3 thru 10). Of significance, the 8i Framework served in a central capacity in the technical analysis that underpinned the predecessor of this Report, *Fighting Spam to Build Trust*.

Environment

The Environment ingredient is the physical location of other ingredients, and includes buildings, trenches where cables are buried, space where satellites orbit, locations of microwave towers and cell sites, and the floor of the ocean. The intrinsic vulnerabilities of the Environment ingredient include being identifiable, accessible, subject to surveillance and remotely managed. While not thought of as a high technology aspect of cyberspace, it is essential, and if compromised can impair the function of systems.

An example compromise of the Environment ingredient that can expose a critical operation to malicious activity is shown in Table 3.

Table 3. Environment – Example Compromise.

Ingredient	Strategic Asset	Compromise
Environment	data center building	through remote management, influence accessibility

Power

The Power ingredient is the electrical supply for hardware, and includes four basic components: the distribution plant, the battery plant, the generator plant, and the grounding system. The intrinsic vulnerabilities of the Power ingredient include distribution plant - loss of connectivity, distribution plant - loss of potential, battery plant - critical fuel characteristics, battery plant - load limitations, battery plant - interface limitations, battery plant - chemical damage and generator plant - load limitations. As power is essential to the operation of hardware, its compromise can leave systems inoperable or even permanently damaged.[47]

[45] Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security*, Bell Labs Technical Journal, Volume 11, Issue 3, 2006.

[46] Additional publications that expound on the 8i Framework and intrinsic vulnerability approach include international policy applications with China, Europe, Russia, the United States and Global scopes: Rauscher, Karl, F., *European Commission-Sponsored, Availability And Robustness Of Electronic Communications Infrastructures (ARECI) Report*, March 2007. Rauscher, Karl Frederick, *Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report, The*, IEEE: 2010. Rauscher, Karl Frederick, Korotkov, Andrey, *Russia-U.S. Bilateral on Critical Infrastructure Protection - Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace*, EastWest Institute, February 2011. Rauscher, Karl Frederick, Zhou, Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting spam to Build Trust*, EastWest Institute and Internet Society of China: 2011.

[47] Krock, R., Rauscher, K., Runyon, J., Hayden, P., *Intrinsic Vulnerabilities of the Power Systems Supporting Communication Networks and Expert Strategies for Defense*, Bell Labs, 2007.

An example compromise of the Power ingredient that can disable a targeted individual or a large segment of a network operator's customer population is shown in Table 4.[48]

Table 4. Power – Example Compromise.

Ingredient	Strategic Asset	Compromise
Power	mobile phone	through battery load limitations, drain battery

Hardware

The Hardware ingredient includes equipment frames, semiconductor chips, electronic circuit packs and cards, and metallic and fiber optic transmission cables. The intrinsic vulnerabilities of the Hardware ingredient include logical design, physical damage, temperature range dependency, field force influence – electric, electromagnetic, adverse radiological interaction and aging.

An example compromise of the Hardware ingredient that could enable a malicious entity to perform a wide range of clandestine operations is shown in Table 5.

Table 5. Hardware – Example Compromise.

Ingredient	Strategic Asset	Compromise
Hardware	semiconductor chip	through logical design, manipulate machine language execution

Software

The Software ingredient includes the programs that provide both the functionality and the fault management capabilities. Software includes the development and test loads, version control and management, chain of control deliver and stored software releases. The intrinsic vulnerabilities of the Software ingredient include the ability to control (render a system in an undesirable state, e.g., confused, busy), mutability of deployed code (patches), accessibility (during development, distribution, rootkit to control kernal/core), logical errors, discoverability of intelligence (reverse engineer, exploitable code disclosure) and incompatibility (with hardware, with other software).

An example compromise of the Software ingredient that could perform diverse stealth operations within networks is shown in Table 6.

Table 6. Software – Example Compromise.

Ingredient	Strategic Asset	Compromise
Software	network element software program	through a temporary patch, introduce temporary capture and transmit functions

[48] This example could be device-dependent, thus users with non-targeted hand set models would not be impacted.

Network

The Network ingredient includes the configuration of nodes and their interconnection; network topologies and architectures; various types of networks, technology, synchronization, redundancy, and physical and logical diversity; and network design, operation and maintenance. The intrinsic vulnerabilities of the Network ingredient include capacity limits, points of concentration (congestion), points or modes of failure, complexity, interconnection (interoperability, interdependence, conflict), uniqueness of mated pairs, automated control (i.e. via software), accessibility (air, space, metallic or fiber) and border crossing exposures.

An example compromise of the Network ingredient that could impair the operation of a critical function of a commercial operation (e.g., bank, airline retail store) is shown in Table 7.

Table 7. Network – Example Compromise.

Ingredient	Strategic Asset	Compromise
Network	enterprise call center	through a point of concentration, exceed ingress network capacity limitations[49]

Payload

The Payload ingredient includes the information transported across the infrastructure; traffic patterns and statistics; information interception; and, information corruption. It includes both normal data transport and signaling and network control traffic. The intrinsic vulnerabilities of the Payload ingredient include extremes in load, corruption, interception, emulation, encapsulation of malicious content, authentication (miss-authentication), insufficient inventory of critical components, and encryption (prevents observability).

An example compromise of the Payload ingredient that can wreak havoc on the proprietary operations of an organization (e.g., business, government, etc.) is shown in Table 8.

Table 8. Payload – Example Compromise.

Ingredient	Strategic Asset	Compromise
Payload	organization email system	through encapsulation of malicious content, penetrate a firewall with a hidden program[50]

Human

The Human ingredient includes the human involvement throughout the entire lifecycle of activities related to the ICT infrastructure and devices (design, implementation, operation, maintenance and decommissioning); intentional and unintentional behaviors; limitations; education and training; human-machine interfaces; and, ethics and values. People have a vital role in the design, testing, implementation, monitoring, maintenance and repair of ICT systems and devices. The intrinsic vulnerabilities of the Human ingredient include physical (limitations, fatigue), cognitive (distractibility, forgetfulness, ability to deceive, confusion), ethical (divided loyalties, greed, malicious intent) and human-user environment interaction.

An example compromise of the Human ingredient that could result in impaired operations or loss of sensitive information is shown in Table 9.

[49] i.e., Distributed Denial of Service attack (DDoS).
[50] i.e. a Trojan.

Table 9. Human – Example Compromise.

Ingredient	Strategic Asset	Compromise
Human	international gateway	through ethical – divided loyalties, provide remote access credentials to hostile actor

Policy

Agreements, Standards, Policies and Regulations (ASPR) is a term used to refer to the complete set of inter-entity arrangements that are necessary for entities to anticipate the behavior of each other. These entities may be governments, companies, individuals or machines. These arrangements include national and international standards; federal, state and local regulations or other legal arrangements; or any other agreement between entities - including industry cooperation and agreements and other interfaces between entities. ASPR provides the necessary mechanisms used to anticipate, improve and control the behaviors of entities that design, develop, implement, operate and evolve communications networks. ASPR is abbreviated here as 'Policy'. The intrinsic vulnerabilities of the Policy ingredient include lack of ASPR (agreements, standards, policies, regulations), conflicting ASPR, outdated ASPR, unimplemented ASPR (complete or partial), interpretation of ASPR (mis- or multi-), inability to implement ASPR, pace of development, inflexible regulation, predictable behavior due to ASPR, ASPR dependence on misinformed guidance, ASPR ability to infuse vulnerabilities and inappropriate interest influence in ASPR.

An example compromise of the Policy ingredient that could jeopardize the vitality of a business' future is shown in Table 10.

Table 10. Policy – Example Compromise.

Ingredient	Strategic Asset	Compromise
Policy	commercial intellectual property	through lacking ASPR, extract massive amounts of information

The above summary provided a brief review of the eight ingredients that are essential for cyberspace. In addition, examples were provided for how each could be compromised to cause harm.

The key "take aways" from the above analysis are that (i) there are a wide range of types of compromises that can be performed in cyberspace, i.e. across no less than eight ingredients, (ii) in addition to known types of hacking that we have learned about from experience, there exist latent failure modes, that have yet to be exercised, (iii) and that therefore, in order for policies to have future-proof effectiveness in improving international cooperation in this area, the complete set of possibilities needs to be considered—both those with which we are familiar, and those for which we are not.

The voluntary Best Practices of Section 5 provide a beginning suite of countermeasures across each of the eight ingredients.

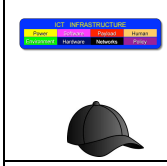
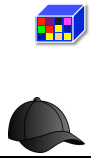
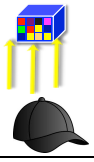
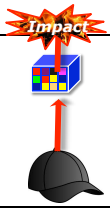
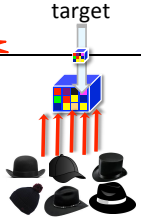
2.5.3 The Life Cycle of a Hack

One helpful perspective of hacking that was employed in the study was a timeline over which a hack would exist. Specifically, the 'life cycle of a hack' was used to examine each phase (Table 11). Understanding the

characteristics of each phase of this life cycle provided insights into the types of countermeasures that are most effective.

The discussion below describes the sequential phases of a hack in what is perhaps its simplest form. In reality there are many (e.g., millions) of probes and hacks underway at any given time, and they are often coordinated and very sophisticated. Thus the key value of discussing the simple form of the hack lifecycle is to appreciate its distinct phases, which are later used to build a systematic approach to stem it via Best Practices (Section 5).

Table 11. Life cycle of a Hack.

Victim View Phases						
Design	Deployment	Monitoring	Compromised	Response	Counter-measure	Repeat
8 ingredients with intrinsic vulnerabilities	transition from lab to field	detect	prevent, detect	isolate, report	counter-measures at target	*cycle repeats*
						
motivation training resources	aligns with motivation	search for 'softness'	successful compromise	leverage, transfer, expand to similar targets	counter-measures at origin	*cycle repeats*
Preparation	Selection	Probe	Hack	Propagation	Defeat	Repeat
Hacker View Phases						

Preparation Phase

The lifecycle of a hack begins with a *preparation phase* that is characterized by motivation, training and resources. Best Practices for this phase focus on the motivations such as curiosity, financial rewards, peer recognition and other notoriety. The Best Practices also address the resource aspect by providing guidance for organizations to perform due diligence in preventing their members from misusing their resources for harmful hacking (Section 5.1).

There are four general types of hackers, namely individuals (and in particular youth), organizations, governments and machines (via software programs). Basically, anyone can be a hacker. The use of low cost script kiddies enables a novice to employ an application that is developed with high hacker skills.[51] The motivations of these diverse sources are not completely decipherable, but there do tend to be some common themes.

[51] IEEE Spectrum, *Two Face of Hacking, The,* July 2011. Verton, Dan, *Black Hat Highlights Real Danger of Script Kiddies Reckless probing by amateurs could actually be helping cybercriminals,* ComputerWorld, 23 July 2011. Protalinski, Emil, *15-Year-Old Arrested for Hacking 259 Companies*, ZDNet, 17 April 2012.

It is important to understand the primary motivations of hackers as best as possible. A beginning approach is to accept that there can be four primary types of influences on hackers, namely: positive and internally controlled, positive and externally controlled, negative and externally controlled and negative and internally controlled (Figure 9).

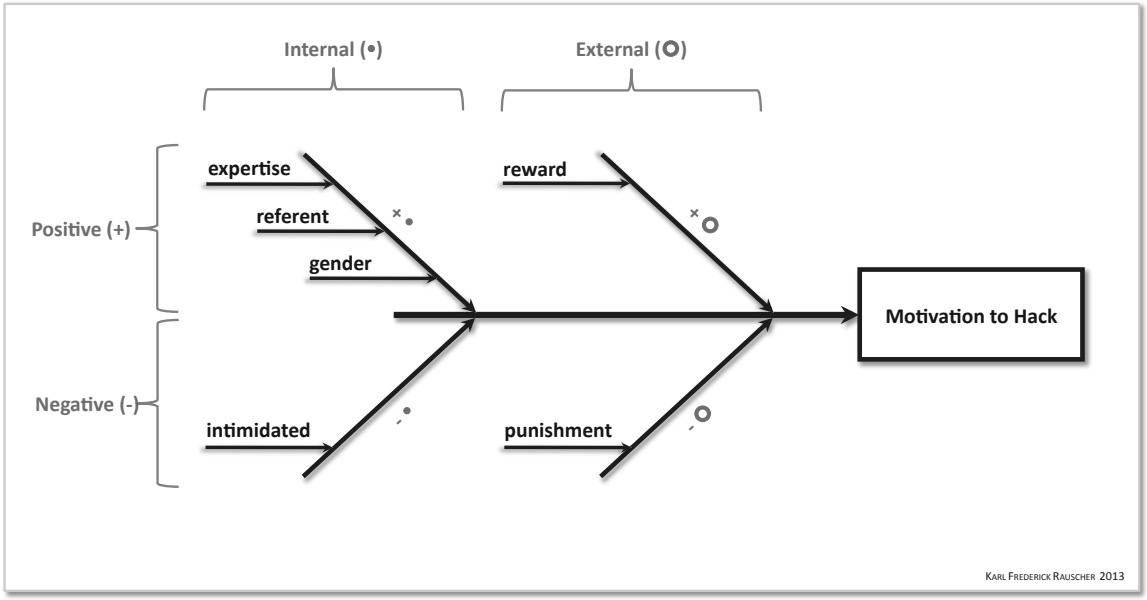


Figure 9. Ishikawa Diagram of Primary Hacker Influencers.

Positive and internally controlled influences are active when the individuals are, within themselves, inspired to action. They are satisfying curiosity where there is internal belief that the expertise gleaned is of value or there is a desire to be like someone such as a respected peer or hero. It is also possible that there may be an internal gender-related motivation, as hackers are predominantly male.[52]

Positive and externally controlled influences are active when rewards are the goal. Rewards can be financial, notoriety and career advancement, the latter of which would apply for those in certain types of belligerent organizations. The reward can also be achieving a particular objective for an ideological campaign.

Negative and externally controlled influences are active when there is punishment for not performing. This coercion could be used on highly skilled or knowledgeable individuals such as those extracted from a targeted environment. The human intrinsic vulnerability of having divided loyalties can be exercised on such individuals by causing harm to them, their family members, or others.

Negative and internally controlled influences are active when one allows oneself to be intimidated, i.e. where an individual has an internal fear of a consequence, which may not be real.

[52] J. Oquendo, J., *Insiders, Outsiders and Hackers Oh My!*, infiltrated.net, 2013. Adam, A.E., *Hacking into Hacking: Gender and the Hacker Phenomenon*, Information Systems Research Centre, University of Salford, Volume 33 Issue 4, December 2003.

The most cost effective way to deal with hacking is at the beginning of the cycle, i.e. the motivation. It is encouraging to know that some hackers can be converted.[53]

For the victim, there is a corresponding *design phase* that begins with the building blocks of eight ingredients (Section 2.5.2), each of which have intrinsic vulnerabilities. Thus it is known from the start that any application or system will be susceptible to being compromised. Best Practices for security are important during the *design phase*. Best Practices for this *design phase* are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Selection Phase

The next progression of the lifecycle of a hack is a *selection phase* that is characterized by a search to align motivation with a target, i.e. curiosity with a new challenge, or a financial reward with a source of monetary potential. When an attractive target is discovered, it creates a potential for a future hack. Best Practices for this phase focus on discouraging hackers from causing harmful compromises first of humanitarian interests, and second of commercial interests (Section 5.2).

For the victim, there is a corresponding *deployment phase* that begins with the first introduction of an application or system within a specific restricted environment or even in the wide-open environment of the Internet, i.e. "in the wild." As a transition is made from a controlled lab environment to a "real world" environment, care is given to any early indication of a major problem. The transition typically occurs only once developers believe that sufficient testing has been conducted to confirm that the application or system is ready to perform its intended function. Best Practices for quality control and stress testing are important during the *deployment phase*. Best Practices for this *deployment phase* are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Probe Phase

The next progression of the lifecycle of a hack is the *probe phase* that is characterized by attempts to find susceptibility in the application or system. Each of the eight ingredients is a potential avenue of opportunity. Best Practices for this phase focus on detecting probes in transport networks and trying to stop them at their source (Section 5.3).

For the victim, there is a corresponding *monitoring phase*. The Best Practices for this phase are similar to those for the *probe phase*, however here the detection takes place at the target. Best Practices for this *monitoring phase* are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Hack Phase

The next progression of the lifecycle of a hack is the *hack phase* and is when the hack actually takes place, meaning that an application or system is compromised. This means that "a specific incident of gaining access to an asset in cyberspace without the presumed required knowledge or official credentials" has occurred.[54] Depending on the compromise, the hack may enable the hacker to gain additional specific advantages. These include gaining additional access and control, conducting additional probes from within, assigning elevated privileges, conducting extensive internal surveillance of the organization and move to parallel systems and applications. Best Practices for this phase focus on identifying the relevant location, resources and individuals and stopping the perpetrations in advance (Section 5.4). Best Practices also include strategies to attract hackers to avenues where they can be foiled (e.g., "honeypots").

[53] Companies cited examples of individuals who were converted from black hat to white hat hackers through financial bounties for bugs found. Notes from the interactive session on Non-State Actors, IEW-IEEE Third Worldwide Cybersecurity Summit, New Delhi, 2013.
[54] Definition 6: hack (noun).

For the victim, there is a corresponding *compromised phase*. This means that "a change that makes something worse and that is not done for a good reason" has occurred.[55] The Best Practices for this phase are focused on rapid detection of an incident and capturing information such as the destination of any outbound messaging from the target (i.e., that may contain sensitive information being infiltrated). Best Practices are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Propagation Phase

The next progression of the lifecycle of a hack is the *propagation phase* that is characterized by attempts to utilize the value associated with a successful hack. This utilization often involves propagation to others in the hacker community, to other similar applications or systems and to other organizations deploying such applications or systems. The reasons for propagation may be to impress peers, to multiple opportunities for greater financial reward, to gain notoriety, or to advance some ideological cause, among others. Best Practices for this phase focus on exposing the sources of the hack insight by examining these channels or propagation (Section 5.5).

For the victim, there is a corresponding *response phase*. The Best Practices for this phase are focused on isolating the impact of incidents, capturing information about the incidents that can support digital forensics and providing accurate reports of what happened to trusted partners who can lend assistance in the investigation and mitigating actions. Best Practices for this *response phase* are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Defeat Phase

The next progression of the lifecycle of a hack is the *defeat phase* that is characterized by the successful hack being effectively defeated. Best Practices for this phase focus on defeating the hack at the origination end, and also accommodating variations of the hack such as location, resources, individuals and methodology (Section 5.5).

For the victim, there is a corresponding *countermeasure phase*. In this phase there has been some sort of compromise. The Best Practices for this phase are focused defeating the hack at the target end, and usually involve some sort of hardening of application or system defenses. Those Best Practices that address an entire class of hacks are more beneficial over the long run than those developed to only respond to a narrow specific hack. Best Practices for this *countermeasure phase* are deferred to work envisioned for the mutual cooperation described in Recommendation No. 7.

Repeat

Once these phases are complete, both the hacker and victim start the process over again. Of course this cycle can be underway for numerous hacks at any given point of time, each progressing at its own pace and therefore bring at different phases at any given point in time.

Key "Take Aways"

The above analysis provided a brief review of the lifecycle of a hack, from both the views of a malicious agent and of a victim.

The key "take aways" from the above analysis are that (i) there are separate phases of the hacking process, each of which has distinct characteristics and opportunities, (ii) the distinct characteristics of each phase

[55] Definition 8: compromise (noun).

provides opportunities for different types of countermeasures to be applied for both incident prevention and impact amelioration, and (iii) there are some countermeasures for which sharing insights can have a risk for the sharing party and therefore require that the "shared with" party be vetted as a trusted entity for such collaboration.

The voluntary Best Practices of Section 5 provide a beginning suite of countermeasures across each of the eight ingredients.

The Model of Harmful Hacking and the Defense

In order to develop countermeasures against harmful hacking, we need to examine hacking and defense together (Figure 10). For each phase of the hacking process, the hacker performs some tasks. If the countermeasure is not effective in focusing on these tasks and constraining them, then the hacker will proceed to the next step. Thus the defense side loses a game and has to work hard in the next game if it exists. That means more cost of human resources and capital. But if the countermeasure is very effective, then the hacker will be defeated. Not only the cost is saved but also the damage is avoided.

From the hacking perspective, the first phase is "Preparation". In this phase, the hacker needs to think whether "to be a bad guy or not." If outside factors can influence a decision to be good, which the countermeasures need to be, then the hacker will not go on. Otherwise, the hacker will continue to prepare with the tools and resources for the attack. So the defense side needs to prepare themselves with effective security devices like anti-malware gateway, firewalls, etc. For those potential internal hackers, organizations should build necessary capability to ensure that the organizations' resources and the functions can not be accessed by unauthorized persons and that all operations are be supervised.

For the second phase, the hacker will take all means to carry out the attack on attractive targets. Some attacks may make use of resource of botnets, vulnerabilities or malware hosts. So from the defense view, all the organizations should work together to clean up the resources for malicious use. Furthermore, the defense side should have certain capabilities to detect hacking and take quick actions to stop it. In addition, the defense should give timely alert to help others better prepare.

For the last phase, the hacker will try best to hide and escape. So the hacker may make use of many hops on a network, or erase the logs on targets' host. For the defense side, the number one priority is to recover the business operation. Then a very careful investigation should be taken to find out the problems and to locate the hacker. A very strict punishment can make other hackers know there will be very serious consequences for their actions. Finally, an organization should conduct a carefully correction once they have learned from incidents.

	Phase	Preparation	Responding	Follow-up
Defense	Task	Make policy to encourage good and punish bad; Deploy resources to build defense capability; Remove the possibility of abuse of inner resource and functions	Keep cleaning up any recourses that can be used by hacking; Monitor attacks and abnormal behaviors; Send warnings and alerts and stop the attacks quickly.	First, recover normal business operations; Investigate and punish the bad actors; Learn from each incident to improve preparation and response.

Hacking	Task	Make the [im]moral choice to hack; Prepare the attack techniques; Evaluate benefits and risks	Carry out the attacks to take down the target, steal data, commit fraud, etc.	Use multiple network and server hops; Erase hacking tracks.
	Phase	Preparation	Implementation	Escape

Figure 10. The Model of Hacking and Defense.

2.5.4 Experts Survey

An important element of this bilateral study was the openness amongst the participants. It was essential that members felt comfortable with expressing any sort of view and also being able to ask questions of others, especially hard or uncomfortable questions. This openness was fostered in private consultations, virtual meetings and face-to-face meetings. The subject that were raised not only matched that found in the most sharp criticisms in the public domain, but, with the expertise that team members had, went even further into the deeps and to the edges of these issues. Team members appreciated the candor and willingness to discuss these topics.

One aspect of the process was the use of an experts' survey. A survey was created that enabled multiple people to answer the same questions. The survey results gave insights into some of the strongest opinions held as well as to the variety of opinions on important topics.

Highlights of the survey results are distributed throughout Section 3, *Key Observations*. A more complete summary of the survey is found in Appendix B.

People's minds are changed through observation and not through argument.

- Will Rogers

To investigate a problem is, indeed, to solve it.

- Mao Zedong

3. Key Observations

This section contains a subset of the observations made during this study. Those included here are critical to understanding the primary factors that shaped the development of the guidance provided in the eight Recommendations (Section 4) and 100 Best Practices (Section 5).

This section contains 80 observations that are presented in three categories:

- Seeing the Current Situation (31)
- Understanding the Problem (26)
- Exploring the Solution Space (23)

The first category includes observations about the present circumstances. The second category provides analysis of some of the more dynamic factors having influence on the problem and that therefore must be dealt with. The third category identifies avenues for breakthroughs, and lays the groundwork for feasible ways forward.

It is emphasized here that these are observations, and *not* interpretations, though some of the observations are of established opinions of a group of individuals as noted. The presentation of critical opinions is a form of active listening.

Great doubts, deep wisdom. . . small doubts, little wisdom.

- Ancient Chinese Proverb

Apparently there is nothing that cannot happen today.

- Mark Twain

3.1 The Current Situation

This section includes 31 observations of the static situation. The insights presented here cover a wide range of subjects such as statistics, technology, business, politics and culture. These initial observations demonstrate the rich diversity of factors that are essential to appreciating the current situation between China and the United States in cyberspace.

1. China Doubles U.S. Online Population

China has the biggest online population in the world, more than doubling the next closest country, which is the U.S. Combined, the online populations of China (~600 million) and the U.S. (~260 million) make up almost one third (~30%) of the Internet users worldwide (Figure 10).[56] The countries have the two largest netizen populations in the world. About 80% of the U.S. population is online, compared to about 40% of China's.[57]

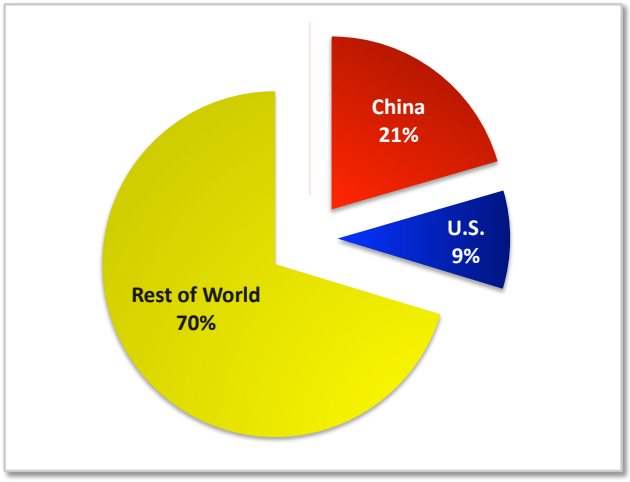


Figure 11. Netizen Populations.

[56] International Telecommunications Union (ITU), 2012 Statistics.
[57] For relative comparison, the populations (and percentage of world's population) of these same categories are: China: 1.4 billion (19%); U.S.: 0.32 billion (4%) and Rest of the World 5.5 billion (76%).

2. U.S. Has the Most Popular Global Services on the Internet

The most popular Internet services with worldwide reach are American. Examples include Facebook (>1 billion users), Twitter (>0.5 billion users) and Google (>0.5 billion users). China has emerging social networking services such as Weibo (>0.5 billion), WeChat (>0.4 billion), but these are primarily Chinese user base.

3. Made in China

China is the world's leading manufacturer, and the U.S. is second.[58] Many American technology companies rely on China for outsourced hardware manufacturing. China is a major manufacturer of ICT equipment (network elements, end user devices, etc.).[59] Over one quarter of China's most promising small businesses belong to the ICT sector.[60]

4. U.S. Making the Core Technology

The U.S. tends to depend on China for technology with lower intelligence and lower control functions, such as system integration and manufacturing. Whereas China depends on the U.S. for relatively higher intelligence and higher control functions, such as software operating systems and core hardware semiconductor platforms.

5. U.S. Leading China in Cybersecurity

Experts from both sides agree that the U.S. has an advantage over China in cybersecurity.[61] However Chinese expertise is growing and is expected to look very different in a decade or less. American expertise is also increasing.

6. China's Goal of Self-Reliance in Core Technologies

The Ministry of Science and Technology provided insights in its 12th Five-Year Plan (2011-2015) regarding domestic companies being expected to achieve breakthroughs in technologies such as major cloud computing equipment, core software and supporting platforms.[62]

7. China Views United States as a Likely Aggressor in Cyberspace

Chinese experts rated the U.S. as the country in the world that is most likely to launch a cyber war.[63] The U.S. was followed, in order by: Israel, North Korea, China, and Russia.

[58] Annual outputs for China are ~$2.9 trillion versus the U.S. ~$2.43 trillion, United Nations National Accounts Main Aggregates Database, 2013.

[59] Shenzhen-based Huawei is the largest network equipment manufacturer in the world. *Who's afraid of Huawei?, The rise of a Chinese world-beater is stoking fears of cyber-espionage*. *Techno-nationalism Is Not the Answer*. The Economist, 4 August 2012. *Who's afraid of Huawei?*

[60] *Ninth Up-and-Comers List* by Forbes China, January 2013.

[61] This observation is of the participants of the study. An 'experts survey' was taken of 75 Chinese and 12 Americans. 85% of respondents indicated that the U.S. is a greater threat to China than vice versa or that China needs more assistance form the U.S. than vice versa, Experts Survey Question 12: *What do you think the mutual influence of China and US to each other on cyber security?* Austin, Greg, *China's Cyber Weakness*, The Global Journal, 5 April 2013.

[62] The Ministry of Science and Technology 12th Five-Year Plan (2011-2015).

[63] Experts Survey, Question 8.

8. U.S. More Advanced in Tactics

The Chinese experts consider the U.S. more advanced in cyberspace.[64] This includes capabilities such as launching an attack, conducting clandestine operations, detecting a probe or defending against an attack.

The U.S experts agreed with this assessment, but acknowledge that China's expertise and capabilities in cyberspace are very respectable and advancing at a rapid pace. China is aware of its relative position on the growth curve and is committed to developing evermore advanced capabilities.[65]

9. Tracing Back to the Real Hacker is Difficult

It is very difficult to be certain about the attribution of a hacking incident. It is rare in a real public network environment, such as the Internet, that even an expert analyst can be certain of the origination and identity of an electronic message. This is due to the intrinsic vulnerabilities of electronic messaging, namely corruption, interception, emulation, and authentication (i.e. miss-authentication).[66]

This difficulty is exacerbated when the transmission path of a probe or hack crosses international borders as it becomes much harder to achieve the cooperation necessary to analyze incidents. Sophisticated hackers, particularly those with ill intentions, are adept at disguising their identities, physical location, and affiliation, often employing sophisticated technology to confuse those attempting to attribute their activities. One must always be aware that a perpetrator may be counting on an analyst to believe that the obtainable origination details that have been gathered are the actual ones, when in reality the perpetrator may be one or more levels deeper in sophistication, and thereby able to trap an analyst in a false sense of confidence.[67]

10. Expanding Enterprise Examinations

Governments are expecting companies that provide critical infrastructure systems to be more transparent. One example of a company's operations being scrutinized is the Chinese technology giant Huawei, which though ranking as the largest network equipment supplier in the world, has been unable to gain the trust of security-focused lawmakers and defense officials in the United States, and has been all but shut out of the world's largest market.[68]

While American communications firms have not received the same treatment in China to date, a Chinese state-owned newspaper has suggested that eight U.S. technology companies pose a threat to China's security.[69]

11. Many Damages from Hacking

Hacking causes a wide variety of damage. Costs from hacking can include the loss of valuable information, direct financial hit, harmed reputation (as when a web site is altered), degraded services, disruption of business continuity, and mistrust of electronic systems and the Internet community in general.[70] Hacking

[64] Experts Survey, Question 7.
[65] Fei, Gao, *China's Cybersecurity Challenges and Foreign Policy*, Georgetown Journal of International Affairs, International Engagement on Cyber – Establishing Norms and Improving Security, 2011.
[66] Payload Ingredient, Section 2.5.2, *Intrinsic Vulnerability Analysis.*
[67] There can also be simple mistakes made in the analysis as was the case with the Korea Communications Commission. Kim Sam, *South Korea Misidentifies China as Cyberattack Origin*, AP, 22 March 2013. Menn, Joseph, *Hacker 'Mercenaries' Linked to Japan, South Korea Spying: Researchers*, Reuters, 26 September 2013.
[68] Meyer, David, *Don't Trust Huawei and ZTE, US Congressional Committee Warns*, ZDNet, 8 October 2012. Lee, Cyrus, *Huawei Fed Up, Tells US Critics 'Shut Up'*, ZDNet, 19 July 2013.
[69] Huanqiu, the Chinese language version of Global Times, named U.S. companies: Cisco, IBM, Google, Qualcomm, Intel, Apple, Oracle, and Microsoft, 6 June 2013.
[70] Lewis, James and Baker, Stewart, *Economic Impact of Cybercrime and Cyber Espionage, The,* Center for Strategic Studies, July 2013. Blair, Dennis, C., Huntsman, Jon, M. Jr., *The IP Commission Report – The Report of the Commission on the Theft of Intellectual Property*, The National Bureau of Asian Research, May 2013.

may cause large-scale faults of critical online infrastructure that may cause further and longer disorder for society.

12. Official Statement: The U.S. Has Stated Its Principles

The U.S. has announced its strategy for cyberspace that emphasizes the following principles [emphasis added per]:

- Upholding Fundamental Freedoms
- **Respect for Property**
- **Valuing Privacy**
- **Protection from Crime**
- **Right of Self-Defense**
- Global Interoperability
- **Network Stability**
- Reliable Access
- Multi-stakeholder Governance
- **Cybersecurity Due Diligence**[71]

At least six (in bold) of these principles are related directly to hacking, namely respect for property, valuing privacy, protection from crime, right to self-defense, network stability and cybersecurity due diligence. In addition, the U.S. strategy has also emphasized the need for international norms of behavior in cyberspace.

13. Official Statement: China's 5 Principles of Peaceful Co-Existence

China has announced that its diplomacy is guided by five key principles (emphasis added):

- mutual **respect for sovereignty** and territorial integrity
- mutual **non-aggression**
- **non-interference in each other's internal affairs**
- **equality** and mutual benefit, and
- **peaceful co-existence**[72]

Hacking can involve each of these principles, since it can (i) involve the critical infrastructure (sovereignty), (ii) be used to initiate an attack (non-aggression), (iii) spread ideology through hacktivism (internal affairs), (iv) be performed asymmetrically when one party has an advantage or different practice (equality) and (v) trigger an escalated conflict (peaceful co-existence).

14. Common Principles

This bilateral's research and collaboration were accompanied by a hunt for shared "first principles", i.e. foundational propositions of value that are irreducible to more elemental notions. These first principles provided the essential cohesion for cooperation throughout the study, and enabled the production of its guidance.

The following ten simple principles were agreed to by both Chinese and American participants as being highly relevant to the international hacking discussion.

[71] Office of the President of the United States of America, *International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World,* The White House, May 2011.

[72] Qingmin, Zhang, *China's Diplomacy*, China Intercontinental Press, 2010, p. 82.

- **Open Communication and Sensible Cooperation**
  Maintaining frank dialogue and seeking common ground when there are differences in order to keep forward progress in negotiations is important and requires diligence and a long-term view.[73]

- **Responsibility for Actions**
  Individuals, organizations and governments should be held accountable for their behaviors, and in particular for those actions that have affected others negatively.[74]

- **Ownership of Property**
  The ownership of property should be respected. The alternatives to respecting property ownership are degrading to the time and talents of individuals, the prolonged result of which are decay in social structure and delay in economic progress.[75]

- **Conflict Avoidance (Non-Aggression)**
  Peace is more desirable than war or other forms of conflict between nation-states. The social, economic and other consequences of escalated conflict, including all-out war, are highly undesirable.[76]

- **Self Defense**
  Nation-states have the right to defend themselves. This defense includes preparing for possible threats, anticipating emerging and future threats and developing and updating capabilities to respond to belligerent attacks made against it.[77]

- **Respect for National Network Sovereignty in Cyberspace**
  Taking adverse actions against each other's networks is unacceptable during peacetime. International cooperation is important to reduce risk and enhance security.[78]

[73] Cooperation includes the use of available technologies (e.g., filter fake-source-IP traffic).

[74] In response to hacking that causes harm, when an individual is confirmed as being the perpetrator, the prosecution of justice, aside from cooperation across jurisdictional boundaries, is relatively straightforward. For situations when a government or other organization is accused of the offense, it becomes more complicated. In these situations, questions arise such as*: Was the behavior sanctioned by the organization?* and if not, *Was due diligence performed to prevent the offensive behavior?* Thus, an opportunity discovered in this bilateral process was for the mutual development of voluntary best practices of due diligence for organizations to implement (see Recommendation 2, *Policy Deployment*, Section 4.2 and *Best Practices*, Section 5).

[75] A necessary quality of respecting property ownership is protecting it. Protecting property requires prohibiting and punishing its theft. Indeed ownership, or at least rightful control, is a prerequisite for theft to be a crime. Both China and the U.S. recognize that individuals, organizations and governments can be the legal owners of property. Prior to legal reforms introduced in the period from 2003 to 2007, the Chinese social structure was oriented primarily around collective property ownership. Today, China's property law recognizes three types of property ownership: state, collective and private. Property can be in the form of *tangible physical assets*, such as land, precious metals and machinery, as well as in the form of *intangible intellectual assets*, such as software programs, media content and industrial designs. Intangible assets tend to be more difficult to reach agreements on and protect and due to their abstract nature and ease to copy and transfer. Nevertheless, both China and the United States have codified its protection, the former acknowledging that its system is in relatively early stages.

[76] Participants observed that while this principle is true in general, there are exceptions, including protection against, and defense from, cyberattack. Some worry about conflicting interests, i.e., individuals and organizations that benefit from conflict. These could include government operational units that gain real-world experience that cannot be achieved with "offline" training, private sector firms that sell products and services for commercial gain and political leaders who are able to leverage crises. Another exception is when a nation-state or people find conditions unacceptable, and see conflict with a controlling entity as a means to improve their condition.

[77] Self defense particularly in cyberspace has historically been undertaken primarily by government ministries or departments of defense, however, increasingly, private sector companies and non-government organizations are considering roles that they can play to protect themselves. One example of this is launching counterattacks on the sources of Distributed Denial of Service (DDoS) attacks.

[78] "Further progress in cooperation at the international level will require actions to promote a peaceful, secure, open and cooperative ICT environment. Cooperative measures that could enhance stability and security include norms, rules and principles of

- **Improvements Are Good**
  Doing something better is good. Improvements solve problems, with the potential to improve the quality of life for many. Human creativity is at the core of improvement, and should be encouraged. Creativity can be promoted by rewarding it.[79]

- **Promote the Development of the Internet**
  Countries should not hinder the development of the Internet in other's countries. All should work to close the 'digital divide' and to support capacity building.

- **Combat the Hacker Underground Hacker Economy**
  Crime needs to be detected and prosecuted in order to protect the economic stability of civilization.

- **Service Disruptions Should Be Avoided**
  Keeping online services operational is important for the safety, stability and security of individuals in the modern world, and will only become more so in the foreseeable future.

15. Lack of Trust

The China-U.S. relationship in cyberspace suffers from a lack of trust. This is a complex environment, where businesses have extensive contractual relationships with companies from both countries playing important roles in the other's success. Moreover, our economies depend upon each other for stability and prosperity. It is clear that there are many bright spots of cooperation in the world of international business. However at the highest political levels and in the attitudes of the general populations, the situation appears to be worsening. In general, neither side is comfortable with what it believes about the other.[80]

16. Ever-Lower Expectations for Cooperation

Many people do not have confidence that the China-U.S. relationship can improve with regard to cybersecurity. Few people expect improvement in the short term. Others believe that the China-U.S. cybersecurity problem will be worse in the near future and that significantly improved long term trust between the two countries is unlikely.[81]

---

responsible behaviour by States, voluntary measures to increase transparency, confidence and trust among States and capacity-building measures. . . . States must meet their international obligations regarding internationally wrongful acts attributable to them." UN Group of Governmental Experts (GGE) … United Nations A/68/98*General Assembly Distr.: General, 24 June 2013.

[79] When rewards are in place, innovation thrives, as a healthy race of competition ensues. Examples in the arena of this bilateral include the mutually agreed to voluntary Best Practices (Section 5). Others include the way to teach voluntary Best Practices to the technical community.

[80] The highest responses from Chinese experts to the multi-vote question *"What do you think are the problems and obstacles in the China-U.S. cooperation on cyber security?"* were:
1. *"Serious lack of trust in politics and deviation in knowledge as well as understanding between each other." (53 out of 75)*
2. *"The China-U.S. cooperation is heavily influenced by political factors. The cooperation on Non-government level and industry level are much neglected and weakened." (36 out of 75)*
3. *"The U.S. has an absolute advantage and does not really need to carry out reciprocal cooperation with China. They only hope that China is in accordance with their wishes." (36 out of 75)*
Experts Survey, Question 13.

[81] There are many examples of caustic statements that go to the core of a lack of trust. E.g., Xinhua News Agency quoted Col. Wang Xinjun, a researcher at the Academy of Military Sciences of the Chinese People's Liberation Army saying that the accusations levied against China in the DoD report were "groundless" and "irresponsible." The Xinhua article concluded in a similar tone, arguing that the false accusations will have a negative impact on the U.S.-China military cooperation. Hou Qiang, *"Pentagon's Cyber Attack Accusations Irresponsible: Expert*," Xinhua, 7 May 2013. Joye, Christopher, *Transcript: Interview with former CIA, NSA chief Michael Hayden,* Australian Financial Review, The, 19 July 2013.

17. Trust Is a Watershed

The situation now is critical. We are at a crossroads. One way leads to more peace and prosperity, the other to more conflict and difficulty. We are in this together and it is therefore either a "win-win" or a "lose-lose."

The entirety of the China-U.S. relationship does *not* rest on the hacking issue. However it is a major issue at this time and it is therefore fitting to look at the bigger picture to understand the larger consequences for this issue's resolution or escalation to further instability. The potential consequences if the current, growing mutual mistrust cannot be reversed may be severe for our two countries, both in cyberspace and the physical world.

> Trust and Trustworthiness are concepts that are at the basis of human experience. We use them intuitively and their assessments are invariable context dependent. But when we transpose these concepts to a digital environment, we can easily run into trouble.
>
> The introduction of digital technology has revolutionized human communication and cooperation by introducing a new intermediary of a complex set of technology-based "institutions" (including networks, digital services, data bases, social networks). In dealing with trust between human actors we must therefore also consider the aspect of trust (or confidence) in this technology infrastructure.[82]

At stake for China and the United States are missed opportunities and negative repercussions for a diverse set of interests that are vital for both countries. Table 12, *The Trust Watershed and Consequences*, offers 24 examples of these consequences for eight areas.

[82] Bus, Jacques, *Societal Dependencies and Trust: Modern Societies' Dependency on ICTs and the Internet, Section 3.1 of The Quest for Cyber Peace*, International Telecommunications Union, January 2011, pp 18-19.

Table 12. The Trust Watershed and Consequences.

	Opportunities Lost	Repercussions Encountered
Technological[83]	reduced cost of system components reliability and security interoperability	increased cost of system components inefficiencies and incompatibilities decreased reliability and security
End User Experience[84]	enhanced user experience increased reliability and security reduced cost of products and services	diminished user experience decreased reliability and security increased cost of products and services
Economic	opened access and expanded free trade competitive markets benefits of scaling	closed access and reduced free trade anticompetitive markets benefits of scaling
Business[85]	more opportunities larger customer base strategic enabling partnerships	fewer opportunities smaller customer base blocked strategic partnerships
Political	resources applied to safety and stability improved stability on a central issue role model for other countries	distraction from other priority issues growing instability on a central issue propaganda consumes resources
Military	decreased risk of escalation increased meaningful dialogue cooperation in defining norms for behavior	increased instability arms race in cyberspace elevated risk of escalation
Cultural	mutual benefits from more understanding mutual respect for differences healthy competition	bipolarity from less understanding disrespect for differences unhealthy rivalry
Legal[86]	prosecuted crime strengthened cooperation in investigations greater IP and critical infrastructure protection	unprosecuted crime IP theft and other crimes thrive insufficient cooperation in investigation

[83] Examples cited derive from cooperation, or lack of cooperation, in standards development organizations (SDOs).
[84] These are a directly attributable to the technological progress or lack thereof.
[85] The near term direct revenue affected is in the order of magnitude range of $10 to $100 billion annually; indirect affects expected in other markets are of a similar level (based on private consultation of the authors).
[86] Both sides agree there exists a subset of crimes that both countries can agree to cooperate on. *Chinese Police Chief Vows International Cooperation in Fighting Internet Crimes*, People's Daily, 31 August 2011.

18. Returning Rebukes

China and the United States both accuse the other of improper behavior in cyberspace. In these censures there is an implied justification of the source.

Table 13. Returning Rebukes – Examples.

"What is absolutely true is that we have seen a steady ramping up of cybersecurity threats. Some are state sponsored. Some are just sponsored by criminals ... and billions of dollars are lost to the consequences. You know, industrial secrets are stolen. Our companies are put into competitive disadvantage. You know, there are disruptions to our systems that, you know, involve everything from our financial systems to some of our infrastructure. And this is why I've taken some very aggressive executive actions. ... that will protect people's privacy and civil liberties, but will also make sure that our overall system, both public and private, are protected from these kinds of attacks. Well, we've made it very clear to China and some other state actors that, you know, we expect them to follow international norms and abide by international rules. And we'll have some pretty tough talk with them. We already have. What we don't want is a situation analogous to 9/11– not where we have, you know, obviously the same level of destruction and loss of life. But you could see situations where we are surprised by major system disruptions. You know, our air traffic control system affected." - U.S. President Barack Obama[87]	"It is well known that actually the U.S. is the "hackers' empire", which has had a lot of cyber espionage targeting not only hostile countries but also allies in political, military, scientific, commercial and other fields. In recent years, it has strengthened its cyber attack as an instrument to overthrow the regimes of other countries. Since the day the Internet was invented the United States has been preparing for cyber war and has set many records in this area. The U.S. is the first country to establish cyber army. In 1998, the U.S. army issued the Joint Doctrine for Information Operations. According to reports the U.S. cyber army has more than 50,000 troops. It has a considerable network arsenal in which more than 2,000 cyber weapons are stored. The U.S. is the first country to convert the cyber space into warfare. In the Quadrennial Defense Review Report issued in 2010, it put the cyberspace on par with land, sea, air and space for the first time. Then cyberspace became the fifth domain of warfare, according to the Strategy for Operating in Cyberspace issued by the U.S. in July 2011." - The People's Daily, a publication of the Central Committee of the Communist Party of China (CCPC) [88]
"Promoting the 'China military threat theory' can sow discord between China and other countries, especially its relationship with neighbouring countries, to contain China and profit from it. [The U.S. is] trumpeting China's military threat to promote its domestic interest groups and arms dealers . . . US arms manufacturers are gearing up to start counting their money." - Senior Colonel Geng Yansheng, PLA Defense Ministry[89]	"China is using its computer network exploitation (CNE) capability to support intelligence collection against the US diplomatic, economic, and defense industrial base sectors that support US national defense programs. In 2012, numerous computer systems around the world, including those owned by the US government, continued to be targeted for intrusions, some of which appear to be attributable directly to the Chinese government and military." - U.S. Office of the Secretary of Defense[90]

[87] Obama, Barack, *Transcript: President Obama's Exclusive Interview With George Stephanopoulos*, ABC News, 13 March 2013.
[88] Chun, Yao, *Defaming China Cannot Cover US Evil Acts,* People's Daily, 9 May 2013.
[89] People's Liberation Army Daily, August 2013.
[90] *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, U.S. Office of the Secretary of Defense, 2013.

19. A Window of Opportunity

At present there is an unmistakable inflection in the perceived priority of this subject for China and U.S. relations.[91] The subject has been on the agenda for presidential talks, signifying that both leaders are willing to speak about the subject.

"What both President Xi and I recognize is that because of these incredible advances in technology, that the issue of cybersecurity and the need for rules and common approaches to cybersecurity are going to be increasingly important as part of bilateral relationships and multilateral relationships. . . . And it's critical, as two of the largest economies and military powers in the world, that China and the United States arrive at a firm understanding of how we work together on these issues."

- U.S. President Barack Obama[92]

"We need to pay close attention to this issue and study ways to effectively resolve this issue. And this matter can actually be an area for China and the United States to work together with each other in a pragmatic way. . . . By conducting good-faith cooperation we can remove misgivings and make information security and cybersecurity a positive area of cooperation between China and the U.S."

- PRC President Xi Jinping[93]

20. Government Working Groups Are Underway

The governments of China and the U.S. began working groups to increase cooperation on cybersecurity.[94] The early outcomes of the initial meetings were characterized as follows:

Cyber Working Group: Welcomed the first meeting of the Cyber Working Group (CWG) under the SSD, and commented positively on the candid, in-depth, and constructive dialogue. The two sides had an in-depth discussion on issues of mutual concern and decided to take practical measures to enhance dialogue on international norms and principles in order to guide action in cyber space and to strengthen CERT (Computer Emergency Response Team) to CERT coordination and cooperation. The two sides will also discuss additional cooperative measures in future meetings. Both sides recognized the CWG as the main platform for bilateral talks on cyber issues, agreed to have sustained dialogue on cyber issues, and agreed to hold the next meeting by the end of this year.

CNCERT/CC and US-CERT Consultation: Decided to hold consultations between the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT/CC) and the United States Computer Emergency Readiness Team (US-CERT) to enhance cooperation between the two entities.

Law Enforcement Cooperation: Decided to continue efforts to deepen and improve law enforcement cooperation to address issues of mutual concern, especially through the Joint Liaison Group on Law Enforcement Cooperation (JLG). In accordance with discussions at the tenth plenary session of the JLG in

[91] "*America must also face the rapidly growing threat from cyber-attacks. We know hackers steal people's identities and infiltrate private e-mail. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, and our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy.*" U.S. President Barack Obama, State of the Union Address, 2013.

[92] *Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting*, Sunnylands Retreat, Rancho Mirage, California, 8 June 2013.

[93] Ibid.

[94] *U.S.-China Strategic and Economic Dialogue Joint Opening Session*, U.S. State Department, 10 July 2013. *Remarks With Chinese Foreign Minister Wang Yi Before Their Meeting*, U.S. State Department, 19 September 2013.

> Guangzhou in December 2012, the two sides decided to . . . intellectual property rights, cyber crime, and child pornography as priority areas in the coming year . . .[95]

21. Cybersecurity Is a Growing Market

There are specialized security businesses that rely on the general cybersecurity problem, as this is the core problem space they provide products and services for. Their role may be in the incident prevention, detection, forensics, defense, attribution, etc.

Based on publicly available marketing materials, the China-U.S. component is a major aspect of this landscape.[96]

22. Funding Attracts Interest

Cybersecurity is one of just a few areas in the present economy that is experiencing growing funding. As a result it receives more attention from those who seek to be part of the funding stream. This includes those who would manage funds, receive funds directly or receive funds indirectly.[97] The net effect is that there is increased competition for being part of this new segment of the economy.

23. The Trade-off for Covert Operations

Organizations involved in belligerent clandestine activities in cyberspace prioritize the avoidance of unwanted exposure. There is a trade-off for plausible deniability however, as the value of this activity may be paid for with a cost to other organizations, as they may be suspected as being more involved in operations than they may be (e.g., high tech businesses may lose access to markets).

24. U.S. Behavior – Interpreted by Chinese Experts

The resistance of the U.S. Government to the use of Chinese equipment supplier Huawei in the U.S. critical infrastructure, and its active lobbying with other countries with which it has close ties, spurred Chinese experts to consider whether they should apply the same approach regarding having similar American equipment in their networks.

> "I recognise the danger of implants and backdoors in telecommunications networks. Beyond that, just a foreign firm gaining the intimate knowledge they would get by helping build a telecommunications network is a sufficient "first-principles" national security problem to give you serious pause before you even consider the presence of backdoors.
>
> But frankly, given the overarching national security risks a foreign company helping build your national telecommunications networks creates, the burden of proof is not on us. It is on Huawei.
>
> Listen, I fully admit: we steal other country's secrets. And frankly we're quite good at it. But the reason we steal these secrets is to keep our citizens free, and to keep them safe. We don't steal secrets to make our citizens rich. Yet this is exactly what the Chinese do."[98]

---

[95] U.*S.-China Strategic and Economic Dialogue Outcomes of the Strategic Track*, U.S. Department of State, 12 July 2013.

[96] The following language can be found on the web sites of commercial security firms: "*APT1: Exposing One of China's Cyber Espionage Units"* (mandiant.com); *"China – the Elephant in the Room"* from *World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks,* 2013, p. 5 from on fireeye.com.

[97] State-operated Chinese media criticizes the interests of the U.S. military establishment: *". . . the Pentagon issued … annual report to Congress on Chinese military developments, claiming some of the cyber attacks on U.S. government and defense industry originated from Chinese government and military. By the report the U.S. also set up an imaginary enemy so as to get more financial support and legal basis for its cyber army expansion."* Chun, Yao, *Defaming China Cannot Cover U.S. Evil Acts*, People's Daily, 9 May 2013.

[98] Remarks from the former Director of the National Security Agency (NSA) and former Director of the Central Intelligence Agency (CIA); Joye, Christopher, *Transcript: Interview with former CIA, NSA Chief Michael Hayden*, Australian Financial Review, The, 19 July 2013. The unsubstantiated claims of Edward Snowden cited include: *"We hack network backbones - like huge Internet routers,*

Some Chinese experts think that China should have a similar policy. The possibility of the Chinese coming to this conclusion seems to have escaped the calculations of some decision-makers in the U.S. government, i.e. with possible repercussions of massive long-term high technology market share loss, extending beyond China, should a symmetrical policy be applied.[99]

25. China Suspicions of U.S. Network Gear

Some Chinese experts have suspected for several years that Cisco routers have a payload capture and send back software functionality that is performing U.S. national security functions.[100]

26. Previous Argument Is Less Convincing

Chinese experts are increasingly skeptical of U.S. hardware and software manufacturers. Their trust has eroded since the revelation of NSA activities. For example, the previous argument made by a major U.S. software manufacturer that it would be "crazy" for business to put back doors in products, is less convincing.[101]

27. Different Approaches

Chinese experts believe that their country's reaction to the combined revelations by a former top U.S. intelligence official and of a former U.S. national security contractor were much more calm than the U.S. response has been to much less certain information. American experts agree that there has been a more calm approach by Chinese politicians, though the arm of state-run media appears to have been their surrogate for criticisms.

The understanding of this difference by the Chinese is that their culture emphasizes the need to improve and therefore they focus on their vulnerability as the primary problem. The Chinese further underscore their need to improve themselves rather than rely upon others to keep them safe. On the other hand, Americans view their vulnerability more as something that is necessary and expect behaviors that do not take advantage of the weaknesses.

28. Cyber Crime Laws – Overview

Both the United States and China are developing laws and regulations to deal with cyber crimes. These laws need to be further developed as technology advances. Table 14 provides a summary of the substantive criminal law, copyright and related rights, procedural law, jurisdiction and international cooperation. This Table uses a comparison to the Council of Europe Convention for structure. Additional details are provided in Appendix A, *Laws Related to Cyber Crime*.

---

basically - that give us access to the communications of hundreds of thousands of computers without having to hack every single one . . ." Snowden Says US Targets Included China Cell Phones, South China Morning Post, 28 September 2013.

[99] Ibid.

[100] Private consultations with Chinese subject matter experts. Custer, C., *Chinese Media: Snowden Says Cisco Helped the US Spy on China*, Tech in Asia, 19 June 2013. Custer, C., *Report Says Cisco, Other US Companies Pose Threat to Chinese Information Security*, Tech in Asia, 28 November 2012.

[101] *"Would Microsoft put back doors in its products to help particular governments? It was interesting because there were very logical arguments why that would be the craziest thing to do. If you put a back door in a widely deployed product it will be discovered and when it is discovered you are immediately out of business not just in foreign countries but in every country in the world, because no one wants to run products like that. But notwithstanding the logic of that reality, governments wanted more transparency."* Remarks from Scott Charney, at EWI's Second Worldwide Cybersecurity Summit, London, June 2011.

Table 14. Legal Coverage Comparison.

China[102]	Council of Europe Framework	United States
	Section 1 (Articles 2 thru 9)	
Criminal Law of the People's Republic of China Arts. 252, 285, 286, 287, 363, 364, 367	**Substantive Criminal Law** illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography	18 U.S.C. § 1029 18 U.S.C. § 1030 (2) (1) – (5), 18 U.S.C. § 1343 18 U.S.C. §1831 18 U.S.C. § 2511 18 U.S.C. §2512 18 U.S.C. §2251 18 U.S.C. §2252 18 U.S.C. §2252A
	Section 2 (Articles 10 thru 13)	
Copyright Law of the People's Republic of China Arts. 1, 3, 9, 10, 11, 20, 22, 23, 24, 27, 29, 30, 31, 32, 33, 34 Criminal Law of the People's Republic of China Arts. 217, 218, 220	**Copyright and Related Rights** offences related to infringements of copyright and related rights, attempt and aiding or abetting, corporate liability, sanctions and measures	17 U.S.C. §506 18 U.S.C. §2 18 U.S.C. §1029 (b) 18 U.S.C. §1030 (c) (e) 18 U.S.C. §2251 (d) 18 U.S.C. §2252 (b) 18 U.S.C. §2252A (b) 18 U.S.C. §2319
	Section 2 (Articles 14-21)	
Regulation on Internet Information Service of the People's Republic of China: Art. 14; Working Rules of Interim Regulation of International Networking of Computer Information Network: Art. 19; Regulations on Internet Surfer Service Sites: Art. 10; Provisions for the Administration of Internet Electronic Bulletin: Arts. 14, 15; Criminal Procedure Law of the People's Republic of China: Art. 116; People's Procuratorate Rules of Criminal Procedure: Arts. 188, 192 Procedural Rules for Criminal Cases by Public Security Organs: Arts. 57, 58; State Security Law of the People's Republic of China: Art. 10; People's police Law of the People's Republic of China: Art. 16 State Security Law of the People's Republic of China: Art. 10 People's Police Law of the People's Republic of China: Art. 16	**Procedural Law** scope of procedural provisions, conditions and safeguards, expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of stored computer data, real-time collection of traffic data, interception of content data	Common law has a complex system of safeguards that meet the requirements of the Convention on Cybercrime 18 U.S.C. §2511 18 U.S.C. §2513 18 U.S.C. §2703 (f) 18 U.S.C. §2703 18 U.S.C. §2704 18 U.S.C. §3121-3127
	Section 3 (Article 22)	
Copyright Law of the People's Republic of China: Arts. 6, 7, 8, 9, 10, 11, 12	**Jurisdiction**	No single clause implementation. In general federal criminal jurisdiction is conferred by an element of interstate or foreign commerce or communication.
	Chapter III (Articles 23-35)	
Extradition Law of the People's Republic of China Arts. 3, 4, 5, 7, 8, 9	**International Cooperation** extradition, general principles relating to mutual assistance, spontaneous information, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, confidentiality and limitation on use, expedited preservation of stored computer data, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, trans-border access to stored com data with consent of where publicly available. mutual assistance in the real-time collection of traffic data, mutual assistance regarding the interception of content data, 24/7 network	Agreement Between the Government of the United States of America and the Government of the People's Republic of China on Mutual Legal Assistance in Criminal Matters

[102] Hong Kong has a few exceptions in its regional legislation. Those exceptions were not reflected in this table.

29. Deeply Integrated, But with Mixed Reliance

The United States and China are deeply integrated in their mutual dependence on each other for ICT. However, the reliance is not uniform in terms of the types of functions being delegated to each other. The U.S. tends to depend on China for lower intelligence and lower control technology functions, such as system integration and manufacturing. Whereas China depends on the U.S. for relatively higher intelligence and higher control functions, such as software operating systems and core hardware semiconductor platforms.

30. The Military Puts an Unexpected Color on a Cyberspace 'Domain'

Cyberspace is a very important virtual place for many social, economic and other transactions. It is often perceived by netizens as a place for a virtual community. Many governments, on the other hand, see it as a place where their rules should be extended. Furthermore, the military considers cyberspace a new place for battle.

Some industry members object to the military's designation of cyberspace as a fifth common, or domain, akin to land, water, air and space. The objection was raised from the sentiment that it is industry that designs, builds and operates the networks that is, in essence, the embodiment of cyberspace.[103] Thus, unlike land, water, air and space, which were not created by man, cyberspace is a frontier that is being built, piece by piece, and has an owner; i.e. there are no "open waters" in cyberspace. Thus if a belligerent operation is taking place, it is taking place on someone's property.

The implication of this observation is that the militarization of cyberspace has the effect of bringing substantial risk to the assets (i.e. networks, systems, etc.) that are otherwise built for commercial purposes. Such language is a verbal possession of the property of others, apparently initiated by the U.S.

31. Both Highly Reliant on ICT

Both China and United States recognize that their social safety, economic stability and national security are now highly reliant on the integrity of ICT. Therefore it is in the mutual interests of both countries to reduce harmful hacking.

[103] For much of the world, 80-95% of communications network are privately (or 'industry') –owned and operated.

Three feet of ice were not frozen in a day.

- Ancient Chinese Proverb

3.2 Understanding the Problem

This section includes 26 observations that are essential for coming to grips with the real problem—including those of perception. These insights are captured here because any viable solution to harmful hacking must consider these. The insights presented here cover a wide range of fields, including technology, business, politics and military.

32. Flawed Practice of Engaging with Each Other

The current practice of engagement between the two countries is one of repeated cycle:

"hacked entity accuses suspected offender –> accused offender denies –> accused offender accusing original back …"

This method of engagement is fundamentally flawed in several ways, including:

(a) the accuser has incomplete information about the originating source

(b) the accuser prefers to protect methods of discovery, and

(c) therefore avoids cooperation with the accused

(d) there is an error-prone translation from technical realities, which is an exegetical hermeneutic, to political inference, which is an eisegetical hermeneutic; and

(d) there are political necessities to deny embarrassing incidents

When a flawed system is exercised, failures are experienced, as is the case here. Thus the most convincing evidence that the currently employed engagement system is flawed comes from the mounting empirical evidence of the (lack of) results achieved from its repeated use. Figure 14, *Verdict-Initiated Decision Tree* (Section 4) breakdowns the paths to failure that are observed when this engagement system is used. Indeed there seems little, if any, suggestion that this approach is improving the situation. On the contrary, the dialogue is producing further escalation and instability.

Understanding the limited utility of such a flawed system of engagement is the first step in moving toward a solution (See Section 4.0.1, *Innovation 1. A New Engagement Methodology: Decision Tree Optimized for Trust-Building (DTOT)).*

There is a realization that the limited progress of these conventional approaches is insufficient. Moreover, the outlook for the future production of these conventional approaches is similarly.[104]

33. Different Motivations of Harmful Hacking Makes Combating It Difficult

There are several different motivations for harmful hacking. One motivation is that the hackers are interested in hacking technology and they want to test their skills online with other systems. Sometimes they want to "show off" to others. A second motivation is that some hackers want to use their skills for illegal financial gain and they think such action is easy to do and with very low risk of being detected and punished. A third reason that motivates some hackers is to attract attention to their ideology (e.g., politics, religion). A fourth motivation for some hackers is to just follow the instruction of their organizations, which is to carry out missions of a government authority. In this case, it is part of an operation of cyber war or cyber conflict between countries.

[104] Rauscher, Karl Frederick, *Fresh Tracks for Cybersecurity Policy Laterals Updating the Track 1 -Track 2 Paradigm to Tracks κ, ε and φ*, IEEE Proceedings of the Third Worldwide Cybersecurity Summit, New Delhi, 2012.

The diversity of motivations makes combating the hacking problem more difficult, as many countermeasures are needed. A method of generating effective countermeasures to hacking is to apply Ishikawa Analysis to the motivation types.[105]

34. Repeating Distrust – Non-cooperation Cycle

The lack of trust between China and the U.S. in cyberspace hinders technical cooperation in specific areas like harmful hacking, i.e. collaborating on tracking down the sources of an incident. This lack of cooperation in turn feeds the distrust, and so on.

A powerful counterforce is needed to breakthrough this downward spiral.

35. Hacking Provides Much Leverage

Hacking can make use of a relatively very small set of resources to have highly leveraged effects on governments and businesses. Even one person with one computer can do much damage.

36. Hacking Opportunities Grow Dramatically

In the coming years, hacking opportunities are expected to grow. Reasons include many more services being provided by the Internet, systems becoming more complex and the introduction of Internet Protocol version 6 (IPv6), the number of targets open to being hacked will grow exponentially. Appliances, vehicles, and possibly nanotechnology, will be networked and therefore exposed to malicious attempts of access and control. Also, the number of netizens will continue to grow. Each of these netizens are potential hackers, or their systems are potential resources that can be controlled by hackers. The new growth areas, mostly in developing countries, are ripe areas for hackers to take advantage of.

37. Hacking May Lead to a War

Cyberspace lends itself to being a place where conflict can take place. Indeed many countries are developing capabilities to use in such scenarios. A major concern is that a perceived attack in cyberspace could trigger an escalation that leads to a war (Table 15).

Given the concern about a trigger, it is important to understand the differences in the acceptability of hacking different interests. For the most part, hacking was considered *particularly inappropriate* against humanitarian interests independent of the peace-war mode context. As for hacking into commercial interests, it was recognized that the peace mode or war mode context would be quite significant. In fact, many experts are concerned that hacking into commercial interests could be a trigger that causes an escalation, i.e. a transition into more conflict, up to and leading a war. Conversely, a reduction in hacking of commercial interests may have the favorable affect of improving stability and moving from a state of war or other escalated conflict toward peace. Nevertheless, during a mode of war, the hacking of commercial interests is expected to greatly intensify. Finally, the hacking of security interests during peace or war was considered, typically, as conventional practice of covert espionage, which breaks local laws, but for which there is no international law against it.[106] It is expected that during a war, the hacking would greatly intensify.

[105] Section 2.5.3, *Lifecycle of a Hack* and Figure 8, *Ishikawa Diagram of Primary Hacker Influencers.*

[106] Military to military dialogue may suggest that certain types of hacking activities would be unacceptable and would therefore result in retaliation. One such example may be hacking into the control systems of nuclear weapons.

Table 15. Hacking Acceptability Relative to Peace-War Modality.

Mode	Humanitarian	Commercial	Security
Peace	Unacceptable	Unacceptable	Expected
Transition	Unacceptable	*Trigger*	*Trigger*
War	Unacceptable	**Expected with Intensity**	**Expected with Intensity**
Transition	Unacceptable	*Olive Branch*	*Olive Branch*
Peace	Unacceptable	Unacceptable	Expected

38. There Are Secret Government Operations in Cyberspace

Some government agencies and corporations are uncomfortable with being transparent about their practices. For government agencies engaged in national security-related operations in cyberspace, the reasons given for obscurity include concern that disclosure could raise unwanted awareness of clandestine practices, compromise the methods being used, or trigger unnecessary public alarm.[107] In the corporate world, it is a widely accepted and even presumed practice for marketing departments to emphasize the most desirable aspects of a product or service in the eyes of the consumer, and de-emphasize, or even avoid, mention of what the consumer would consider a trade-off for the value proposition. The reasons here include sales strategies, protecting business interests and risk avoidance.

39. Some Policies and Practices Are Not Popular

When policies are not popular there is temptation to provide misinformation about them to make them more appealing. This is a trade-off for short-term gain in (unwarranted) trust at the expense of long term (warranted) mistrust.[108] An example of this that occurred during this bilateral study took place in a U.S. Senate Intelligence Committee hearing, in a brief exchange between Senator Ron Wyden and the Director of National Intelligence, James Clapper:

Sen. Wyden: *Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?*

Director Clapper: *No sir.*

Sen. Wyden: *It does not.*

Director Clapper: *Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly.*[109]

[107] http://www.dni.gov/index.php/newsroom/testimonies .
[108] Healy, Jason, *Time to Split the Cyber 'Deep State' of NSA and Cyber Command*, Huffington Post, 2 October 2013.
[109] Greenberg, Andy, Watch Top U.S. Intelligence Officials Repeatedly Deny NSA Spying On Americans Over The Last Year (Videos).

Three months later, Clapper released a statement that admitted that the NSA was collecting telephony metadata on millions of Americans telephone calls.[110]

40. Political Speech Is Too Often Unclear

When there is a potential for the interests of two or more parties to clash, judicious word selection is wise. However too often policy statements are optimized for the certain aspects of diplomacy and legal protections, and neglect the most fundamental need to communicate with clarity, i.e. there is diplomatic or delicate doublespeak. The results are *policy statements that avoid saying what needs to be said plainly*, are too long and whose meaning is out of grasp for many of those needing to read them. A very familiar example of this practice is the "End User Legal Agreement", or EULA, which typically is written at a readability level that exceeds the average population reading skills level.[111] Examples of dazzling statecraft can found in the many highly nuanced statements that cloak accusations and threats, and that imply that there are different operating practices between the speaker and the subtly judged guilty party.

The skills used to produce these statements have doubtless forestalled many acute concerns that were pressing at the moment. However in the long run, they have too often missed the opportunity for simple, clear communication.

41. Hacking Violates Sovereignty and Commercial Interests

The issue of respect for the sovereignty over nation-states and for commercial interests was raised in the context of foreign governments monitoring the commercial communications networks of other countries.

While it is expected that the security agencies of a government would monitor the traffic being transported on the communications networks within their own jurisdiction, the same practice on communications networks of other countries is met with firm opposition by both the offended government and the industry.

42. Cybersecurity Brings the Influence of Insidious Interests

There are some interests that are generally accepted as harmful for genuine trust building because of the bias they bring to the table. These interests can have a significant impact on how this China-U.S. relationship is viewed and shape the language of the dialogue, and even influence which actions are more likely to be undertaken. Most of these interests are legitimate at a micro level for individuals or organizations. However their presence in international discussions can be counterproductive, and even improper. In an earnest effort to build some improved level of trust, these interests are best not ignored.

- **Business interests that benefit directly or indirectly from the problem:**
  - includes security firms that specialize in products or services that are purchased to address some aspect of the perceived problem
  - they serve a valuable function in applying expertise to protect national interests
  - for such enterprises, a dramatic change in the landscape of the problem would be disruptive to existing planning and strategy.[112]

- **Personal career ambitions:**
  - includes those in charge of policy related to the subject, both elected and appointed politicians and staff, as well as some corporate leadership

[110] Clapper, James, R., *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, 6 June 2013.
[111] Rauscher, Konrad M., *The Digital Shrink Wrap Dilemma - When We Don't Necessarily Agree with Agreements, But Agree to Them Anyway*, Proceedings of the IEEE-EWI Third Worldwide Cybersecurity Summit, New Delhi, 2012.
[112] This specific type of business is a special case of the general "commercial" interest organizations, where there is no immediate conflict of interest.

- sometimes it can be safer to meet the relatively lower expectations of the status quo, i.e. the problem is unsolvable; rather than expressing an alternate view to popular positions, which requires strong leadership because it is too risky at a personal level
- expressing a view that is a reversal of a previously taken public position can be intellectually disruptive and requires repositioning.

- **Staking out turf in a rare area with growing budgets and many fresh opportunities:**
- includes internal government competition for control over various aspects cybersecurity subject
- the behaviors of organizations affect the inclusion (or exclusion) of competing agencies, and thus competencies critical to the multi-disciplinary aspects of the problems.

These examples by no means complete a comprehensive list, but serve to illustrate the diversity and tangible potency of interests that could be factors, particularly at a tactical level.

43. Politics Influences Cooperation for the Hacking Problem

Many of the Chinese and American experts agreed that political factors have great influence on addressing the hacking problem. Politics can make cooperation better or worse. The cooperation to date has suffered. Technical cooperation is essential to solving the problem, but requires political support to enable it. The technical community typically believes that it can solve much of the problem if bilateral cooperation was better supported.[113]

44. Reluctance to Cooperate on Combating Hacking Is Reinforced by Distrust

Because it is a firmly held belief by some leaders that any improved genuine trust between China and the United States in cyberspace is impossible, any perceived progress is considered misplaced trust that must be corrected. This environment in turn rewards those who reinforce the status quo, i.e. that nothing can be done. This becomes a self-fulfilled prophecy.

45. West Cautious of East

A critical mass of Americans with expertise relevant to this subject of hacking believe it is inherently dangerous for their country to trust the Chinese, believing that Western culture is vulnerable to misplacing trust in Eastern cultures where agreements may be perceived to be made from a Western view, but not upheld over time.

46. East Cautious of West

A critical mass of Chinese with expertise relevant to this subject of hacking believe it is inherently dangerous for their country to trust Americans, believing they be taken advantage of with emerging American technology and social networking applications.

47. Suspicion of U.S. End the East's Expansion

Chinese political and business leaders and educated citizens believe that the design of U.S. foreign policy is to contain or confront China's economic and political expansion. Therefore the American criticisms of China regarding hacking are believed to be a part of this design.

[113] "Politics" was part of largest response (43%) to Expert Survey Question No. 13, *What do you think are the problems and obstacles in the China-U.S. cooperation on cyber security? (53 out of 75)*

48. Americans Challenged by Their Competitor

The previous generation of Americans was primarily concerned with the communist political doctrines of China (and that of the Soviet Union). Today's generation however, recognizes that China has in many ways become more like itself, and now has a different problem. This new problem is that of a competitor in strategic global economic markets, like ICT.

49. Potential Cyber Arms Race

The U.S. military has proclaimed as aspirational doctrine "superiority" and "dominance" in cyberspace.[114] The Chinese perceive U.S. military ambitions as signaling an unwelcome militarization of cyberspace. Many countries are developing their military capabilities in cyberspace, including standing up special units to conduct cyber operations.

50. Suspecting Espionage

Both China and the U.S. have detected that their sensitive and confidential information has been stolen online. Furthermore, both China and the U.S. believe that the other is accessing their state secrets via cyberspace. The victim country cannot appeal to international law to accuse a cyber spy in another country. Unlike the physical world where a spy can be captured in and prosecuted for breaking local laws, the remote location of a cyber spy in another country prevents similar protection of national sovereignty.

51. Both Americans and Chinese See the Other as Source of Much Hacking

American and Chinese companies are seeing hacking efforts on a daily basis that are believed to be emanating from each other's networks.[115] Many of these incidents are associated with intellectual property theft, and thus are a serious concern for these commercial interests.

52. U.S. Blames Chinese Government

A significant number of U.S. experts, politicians and other influencers have concluded that hacking activity that is observed to be originating from Chinese networks is likely sanctioned by the Chinese government.

53. China Implies U.S. Is Major Source of Hacking of Chinese Networks

Based on reports from the technical community, China is more and more stating publicly that a major source of hacking in its networks originates from American networks.[116]

54. CERT-CERT Cooperation is Lacking

Cooperation between the China and U.S. CERTs is far from sufficient.

55. Practical Collaboration Hindered by Visa Screeners

[114] *National Military Strategy of the United States of America*, *The,* Office of the Chairman of the Joint Chiefs of Staff, Washington, DC. 2004.
[115] http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16001&view=map .
[116] *Annual Report - National Computer network Emergency Response Technical Team /Coordination Center of China – People's Republic of China*, 2012.

Chinese cybersecurity experts complain of having their U.S. visa applications rejected. Conversations they relay of their interactions (e.g., the questions they are asked) indicate that the U.S. consular staff clearly do not understand basics of the Internet and are their rejecting their involvement in collaborative activities in the U.S. Some Chinese contributors to this study did not want their names to be included in this report due to their concerns that the U.S. government may see their involvement in this technical-political discussion as a reason to restrict their entrance into the U.S. for future technical conferences.

56. Investigation of Cross-Border Attacks Usually Requires Joint Cooperation

Cooperation among two or more countries is difficult due to language, time zones and practices, among other factors. This essential cooperation is even further hindered when there is lack of trust between parties. Countries seldom conduct joint investigations and thus each side lacks data and confidence in conclusions, and investigations are inefficient.

57. American Businesses Affected by U.S. Government Policies

Netizens can view government authority not only with respect, but also with some suspicion because of the unequal status – i.e. checks and balances. Netizens are particularly concerned when these authorities have policies and practices that are not aligned. The U.S. government came under sharp criticism from American businesses for its communications failures regarding polices that required cooperation from U.S. Internet companies with global operations.[117]

> "It's our job to protect everyone who uses Facebook. It's our government's job to protect all of us, our freedom and the economy. They did a bad job at balancing this.
>
> Frankly I think the government blew it–communicating the balance of what they were going for here with this.
>
> (They said) don't worry, we're not spying on any Americans. Wonderful, that's really helpful for companies trying to work with people around the world. Thanks for going out there and being clear. I think that was really bad."[118]
>
> - Mark Zuckerberg, CEO, Facebook

Companies can be impaired by policies of their government, i.e. hurting their development in other countries where there is suspicion of the extent of their operations.

In addition, businesses who value their customers' trust can be inhibited from being more transparent by government authorities.[119] The following statements from Yahoo's CEO underscores the force of government obligations on companies.

> "If you don't comply, it is treason," Mayer said when asked why she couldn't just spill details of requests by U.S. spy agencies for information about Yahoo users.
>
> "We can't talk about it because it is classified," she continued. "Releasing classified information is treason, and you are incarcerated. In terms of protecting our users, it makes more sense to work within the system."[120]

American experts observed that the public debate that is taking place between business and government may produce a healthy result, if new, corrected policy statements are acceptable and the associated revised policy deployment practices are consistent with the stated policies. This can be a way for other countries around the world to see how the debate on these issues can lead to improvements.

---

[117] Timberg, Craig and Nakashima, Ellen, *Amid NSA Spying Revelations, Tech Leaders Call for New Restraints on Agency,* The Washington Post, 1 November 2013.

[118] Comments at the TechCrunch Conference San Francisco.
Geron, Tomio, *Mark Zuckerberg: U.S. Government 'Blew It' On NSA Issue*, Forbes, 11 September 2013.

[119] Zuckerberg said he believes people deserve to know more about government programs and said Facebook is pushing for more transparency. Gallagher, Billy, *Zuckerberg Says The "Government Blew It" On The NSA Scandal,* TechCrunch, 11 September 2013.

[120] Chapman, Glenn, *Yahoo CEO Fears Defying NSA Could Mean Prison*, Yahoo News, 12 September 2013.

To have principles, first have courage.

- Ancient Chinese Proverb

Always bear in mind that your own resolution to succeed

is more important than any other.

- U.S. President Abraham Lincoln

3.3 The Solution Space

The section includes 21 insights on the way forward. Some of the insights may appear to only give a small advantage, but combined together, they offer a way forward that is fashioned in the bold recommendations of Section 4.

58. Three Levels of Success

Given the instability and decline of trust that presently defines the China-U.S. relationship there are actually three levels of success (Figure 5, *Bilateral Objectives for Impacting the Health of the China-U.S. Relationship*). Each of these is meaningful, with progressive degrees of significance:

(a) *slowing* the rate of escalation,

(b) *stopping* the escalation, or most desirably, or

(c) *reversing* the direction from an escalation to a de-escalation

Given what may hang in the balance for both sides, even the least of these accomplishments, a slowing of the rate of worsening, is a meaningful impact at this time.

59. A "Win-Win" Is Wise

The best outcome for a resolution of the current situation is where both China and the U.S. can benefit from greater trust in their relationship, increased stability of the same and greater protections for their respective commercial and humanitarian interests. A "win-win" would most likely also be a "win" for much of the rest of the world.

60. An Uphill Path to Improve the Harmful Hacking Situation

Both China and the U.S. will have to work hard to build trust. This will involve government, business and other organizations. The present instability suggests that nothing can be taken for granted.

61. Varied Responsibility for Response to Hacking Behavior

Who should respond to hacking behavior? The responsibility for responding to a hacking incident depends on several factors. One of these factors is the hacker, i.e. a country, organization or individual. Though the source of a hack is rarely known with a high degree of certainty. Therefore, the attacked entity is also a factor for determining who should respond. The necessary response for all types of hacking incidents requires the combined effort of government, companies and individuals (Figure 11, *Responsibility for Response*).

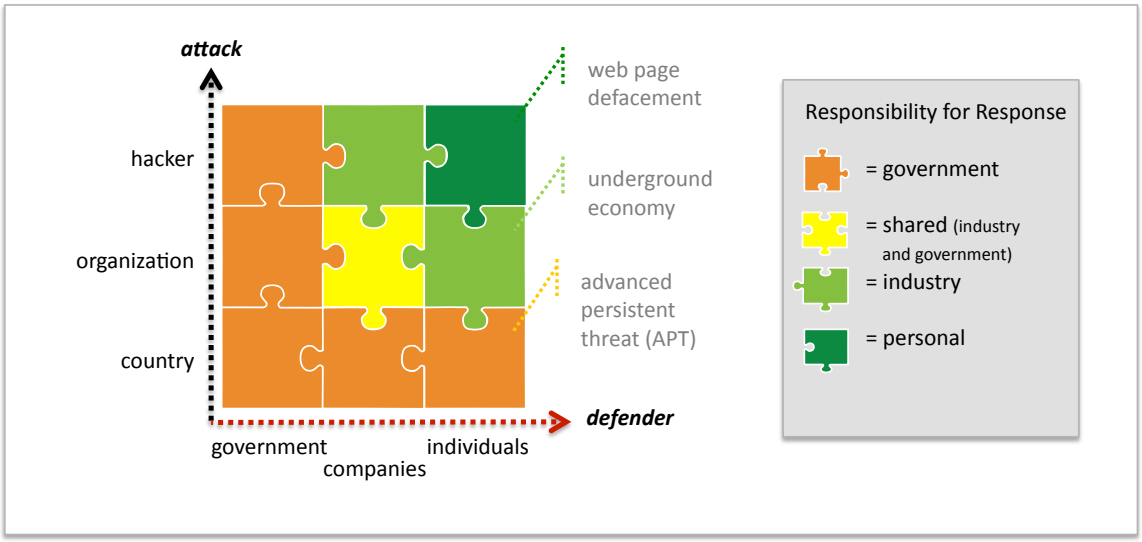


Figure 12. Responsibility for Response.[121]

62. Effect As an Indicator of Response

How is the response level to hacking behavior best determined? Three aspects best determine the level of response to hacking incidents: (i) the type of hacking source, (ii) the type of target and (iii) the effects of the hacking behavior. The basic principle is that the response level should be proportional to the level of perceived threat. Three examples help to illustrate this:

A. If the hacker is an individual and the targets are individuals with the effects being relatively small, this situation is likened to a single individual becoming sick and individual treatment is sufficient.

B. If the hacking source is an organization and the targets are individuals with the effects being relatively small, this situation is likened to a contagious flu, which has some national concern to contain and treat those affected.

C. If the hacking source is a nation-state and the targets are individuals with the effects being moderate, this situation is likened to a highly contagious disease that is difficult to treat, that requires a much stronger national response.

More formal hacking sources (i.e. governments) and bigger effects will result in greater levels of response being called for. Figure 12, *Effect Influence on Response*, presents a partial view of how the additional dimension of effect can be a factor in the determination of an appropriate response.

[121] Source: CNCERT.

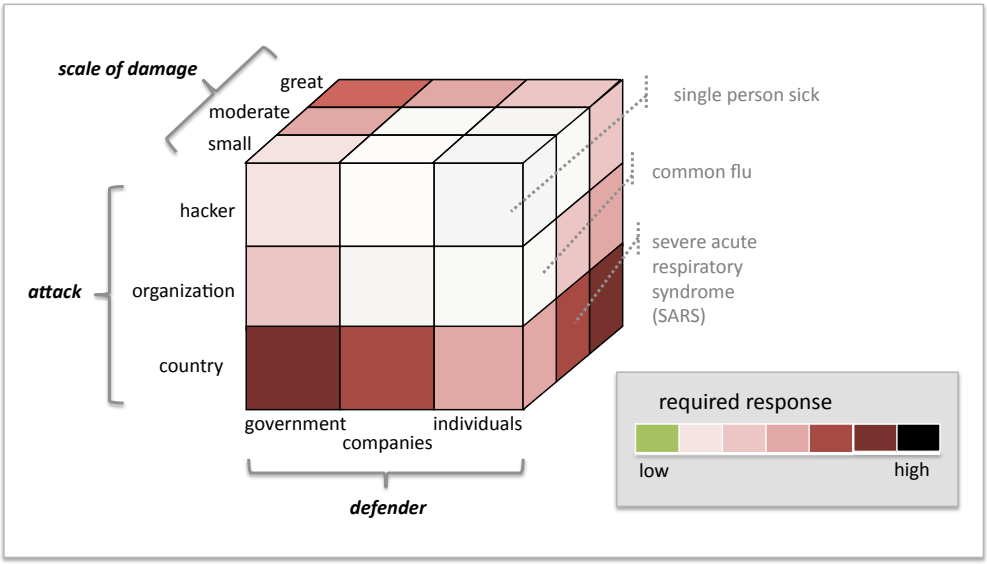


Figure 13. Effect Influence on Response.[122]

63. Humanitarian Interests Deserve Special Protection from Hacking

Both Chinese and American experts agree that purely humanitarian interests such as those defined in International Humanitarian Law (IHL) deserve special protection in cyberspace, as they do the physical world.[123] Thus the first category of entities to be protected from being compromised consists of those organizations with a stated and practiced policy to perform purely humanitarian (medical, cultural and spiritual) functions with their assets in cyberspace.

64. National Security Functions Are Conventional Targets for Espionage

National security-oriented assets are, because of their potential for hostility, elevated as targets for espionage by foreign interests. This is conventional practice of statecraft for thousands of years. Thus they should expect to be the target of hacking activities and should provide stronger defenses against hacking, especially for weapons of mass destruction.

This reality suggests a differentiation between hacking incidents experienced by entities with national security interests and other entities without such interests. Moreover, because the former should expect espionage, their objections should not express the same level of surprise and disapproval, as would a humanitarian or commercial interest.

65. Alignment of Words and Actions

What government and business leaders say and what their respective organizations do needs to be aligned. Without this alignment, trust is fleeting at best, and otherwise out of grasp for the China-U.S. relationship.

[122] Idem.
[123] *Geneva Convention, The, The Geneva Conventions of 1949 and Their Additional Protocols*, Geneva, 1949. *Geneva Protocol, The; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, Geneva, 1925. *Hague Convention, The Hague Convention of 1899 and 1907* The Hague.

66. No Substitute for Corrective Action

Making necessary adjustments to Stated Policies and Policy Deployment plans is hard, but necessary. There is no substitute for effective corrective action to prevent future incidents that are similar to those experienced by stakeholders, and to ameliorate their impact should they occur again.

67. Trust is a Two-Way Street

In order for China and the United States to build genuine trust with each other, there must be relative symmetry in respect, expectations, accountability and willingness to cooperate.

68. Repeating Trust-Cooperation Cycle

Incremental, tangible steps of cooperation such as meaningful dialogue, sharing of Best Practices, teaming up in investigations and prosecutions of crime, in turn create trust, which in turn fosters more cooperation. Such a continued positive cycle can lead to an upward spiral of trust and cooperation. The first steps can be cautious and measured to protect the concerns and interests of both parties.

69. More Technological Independence May Be a Safe Option for China and U.S.

The high degree of reliance that both China and the United States have upon each other's technologies in their critical infrastructure may be too much. The present mutual reliance upon each other's technology is at the core of distrust. Sometimes a relationship does not have good standing because it is in a dangerous place for both sides. The weight of the interests of the two largest economies in history requires substantial support. If there is not enough support, the situation may be like standing on ice that is too thin.

More stability could actually be achieved if there were a backing off of dependencies. This does not mean an extreme position of isolationism, but rather that those few most irritating issues be taken off the table, perhaps temporarily for a trial period. This is not the desired path, as better trust is the preferred 'win-win' that maximizes prosperity for both China and the U.S., but such a pull back is an alternative to the present path of destabilizing distrust.

It could be that the demands of intense technological interdependencies have been achieved too rapidly, outpacing the ability for the two countries to develop genuine trust and appreciation for each other's interests.

70. Areas of Interest for Cooperation - Government

Chinese and American experts provided input on ideas for future collaboration that spanned the government, military and industry. Suggestions for government cooperation included crime, terrorism, market access, technical conferences, joint simulated exercises and legislative research and analysis.[124] Possible topics for military dialogue included strategy discussions, agreements for non-aggression and joint development of weapons that could defend cyberspace; Chinese experts provided these specific suggestions for cooperation in the military.[125]

[124] Experts Survey, Item 15: "Please make specific recommendations on the cyber security cooperation between China and the U.S. at the government level."
[125] Experts Survey, Item 16: "Please make specific recommendations on the cyber security cooperation between China and the U.S. at the military level."

Suggestions for industry cooperation included improving CERT interactions, real-time collaboration to track incidents, research on vulnerabilities, joint emergency response capabilities, strategies for dealing with transnational DDoS attacks, and more technical conferences.[126]

71. Good News Can Be Good

Media reporting of cooperation between China and the U.S. can be helpful in two distinct ways.[127] First, more expansive coverage that includes good examples of cooperation can change general expectations and those expectations in turn build up some mental constraints among individuals and organizations against hacking the other party. Secondly, positive examples can help change the incentive structures within particular organizations, so that individuals can get rewarded for cooperating rather than doing the opposite of that.

72. The Lifecycle of Harmful Hack Gives Insights for Solutions

Each of the phases of the lifecycle of a hack (Section 2.5.3, Table 11) has distinct characteristics that can be used to inform countermeasures for that specific phase.[128]

73. Science Diplomacy

Both Chinese and American experts who are trained in science, technology, engineering and mathematics (STEM) believe that they can make progress in cooperating in ways that politicians cannot.

74. Surface Tension Barrier for Technical Cooperation

For technologists, the next steps for improving cooperation between the two countries involves getting past some initial resistance, like "surface tension", but it is not considered so hard that it should prevent those determined to succeed. There are two major difficulties that must be overcome:

A. Separation

Separations are the first major set of difficulties, such as **language** and **time zone**, which is from 12 to 15 hours ahead of most of the U.S. The former is increasingly less a problem as Chinese bilingual skills increasingly include English. There are countless examples of successful China-U.S. business partnerships that demonstrate effective communication, though it is a distinct necessity here that specific highly skilled subject matter experts overcome this challenge.

The latter difficulty, time zones, is also managed by global businesses on a regular basis, and so is achievable here.

Culture is relatively less of an issue between the two countries.

B. Risk

Given the heated rhetoric of political leaders, and possible reality of most of what is alluded to, technologists on both sides are hesitant about what they might otherwise naturally do to engage with peers in their professional community. The first of two major risk concerns they face are **increasing their organization's vulnerability** by inadvertently providing insights as to the sources and means by which they are discovering and analyzing incidents. If transferred to adversaries, such information could enable more sophisticated compromises that could attempt to avoid learned detection capabilities. Unlike the first risk concern, the second is political and deals with perception, i.e. **uncertainty about the appropriateness of cooperating** with the "other country." After all there is so much bad news in the media, is it a good thing to

[126] Experts Survey, Item 17: "Please make specific recommendations on the cyber security cooperation between China and the U.S. at the industry level (including CERTs/CSIRTs and other social institutions)."
[127] Key Observation No. X, *Light Some Candles*, Section 3.3.
[128] The Best Practices of Section 5 are focused on these distinctions and are arranged by phases of a the lifecycle of a hack.

> do what would normally be done in these circumstances and solve these problems? What is the right thing to do?

Once the difficulty of getting past these issues is resolved, there are readily identifiable methods of improving cooperation to investigate incidents, determine their causes and agree to and enact specific countermeasures to address them.

75. Real Problem Solvers Needed

Both Chinese and American experts felt strongly that the technical community, specifically network operators, service providers and application developers, were the most capable of solving hacking problems. However, they need the support and encouragement of their respective governments to develop healthy peering relationships where problems of malicious activity can be jointly detected, investigated and reported.

76. Information Channels

In the United States, much of what the general population, and even those technically savvy, "know" about cybersecurity, and hacking specifically, is learned from the media. Therefore, the media shapes our perceptions and understanding, whether right or wrong. Thus it is easy for our understanding to be clouded, since we don't have a more direct access channel to the facts, such as raw data associated with a specific incident, that we know is incomplete and requires some interpretation.

The Chinese experts felt they had a similar experience as what the Americans described above, for both the general population and technical community.

77. Good Examples Need to Be Highlighted

The power of a positive media storiy can have an enormous effect and, especially when it is true, it can become contagious. Examples of successful cooperation between China and the U.S., such as the Federal Bureau of Investigation (FBI)— are too few and far between:

> Meng Jianzhu, State Councilor and Minister of Public Security, made the remarks at a meeting held to mark an operation conducted in cooperation with the United States Federal Bureau of Investigation (FBI) in June that resulted in the arrests of more than 10 individuals distributing online child pornography in the two countries.
>
> 'Although China and the U.S. have different judicial systems and cultural values, the two sides share a common view in crime-fighting,' Meng said."[129]

Industry stakeholders who have positive experiences in working with China could, as appropriate, provide greater awareness of specific instances of constructive cooperation.[130]

78. More Interaction Online Between the Expertise of Two Sides Can Achieve More Mutual Benefits

Chinese experts have observed from the interactions of technical communities in virtual and other forums, that people of Western cultures tend to be more open to share key information in their discussion of problems and thus have more productive conversations where answers can emerge. In contrast, the Chinese experts observed that most people of the East (Japan, Korea, China, etc.) tend to be more conservative and to share less insights in collaborative conversations with industry peers (maybe due to the language barrier). Thus, they do not maximize the benefits of social network-type technical collaborations. The key learning

[129] *Chinese Police Chief Vows International Cooperation in Fighting Internet Crimes*, People's Daily, 31 August 2011.
[130] The authors point out that team members suggested that this bilateral is an example of a story that cuts across the grain of the present narrative and public awareness of it is important for a more complete picture to be drawn.

here is that since there do exist cultural differences between the West and the East, more daily bilateral interaction on the Internet can help the two sides to achieve more mutual benefits.

79. More Open Markets Will Naturally Facilitate Cooperation in Technical Communities

Chinese experts observe that because major Chinese technology firms are excluded from the U.S. market, the normal course of cooperation that would occur is ended before it has a chance to begin. The evidence they point to is the greater access of U.S. companies and experts to Chinese markets.

The key observation here is that more open markets will precipitate more interaction, which will precipitate more understanding, which will precipitate more cooperation, which will precipitate more trust, which will precipitate real, tangible results in stopping hacking.

Both sides will benefits in both markets from progress in this direction.

80. Sharing Minimal Incident Data in Mutual Investigations Has Minimal Risk and Is Very Helpful

The most essential information needed to support collaboration on cross-border hacking source analysis does not require the victim to give up sensitive source and methods information. The minimum information includes such details as a time stamp, the destination IP address and port, the source IP address and port and the characteristics of the attack.

Both Chinese and American companies have data from hacking incidents they believe are from each other's networks. If cooperation in tracing back to the sources produces results that are of value, then the investment of resources will be worth continuing. Initially, working on actual hacking incidents will be a priority over working on detected probing.

Cybersecurity presents very tough problems and they are not for the faint of heart.
Those wishing to play a part in solving them either need to lead, follow or get out of the way.
- General James L. Jones (USMC ret.)

Cyberspace should be a field where China and the United States
can enhance mutual trust and boost cooperation.
- Foreign Minister Wang Yi

4. Recommendations

This report presents eight (8) immediately-actionable recommendations that, if implemented, will establish tangible China-U.S. cooperation to improve the safety, stability and security of cyberspace.[131] This China-U.S. cooperation will in turn change the current direction of declining health in the China-U.S. relationship regarding cybersecurity, by *slowing the rate* of decline, *stopping* the decline and *reversing the direction* to become one that is of improving health (Figure 5, *Bilateral Objectives for Impacting the Health of the China-U.S. Relationship).*[132] These recommendations are bold and will require hard work, yet they are firmly sound in respecting the interests of both nation states and their respective commercial industries and societies.[133]

These recommendations are also **symmetrical** in that they apply equally to China and the United States.[134] Furthermore, these recommendations seek **completeness** in covering the actors of influence, i.e. guidance is submitted not only to those large roles of government and industry, but also to non-government, non-commercial, philanthropic organizations with a much smaller, yet consequential impact.[135] Within this suite of recommendations there is even consideration for how to engage and challenge the hacking community itself for greater good. In these recommendations stakeholders can be other countries, companies or even the general public.[136]

How the Recommendations Address the Current Situation

These recommendations address the current situation in numerous different ways from the status quo, but three innovations are worth emphasizing here: [137]

1. **A new engagement methodology: Decision Tree Optimized for Trust-Building (DTOT)**
2. **A new system of verification: Total Trust Management (TTM) System**, and
3. **A new framework for the Landscape of Interests in Cyberspace (KLIC)**

[131] Recommendations Nos. 1 through 4 actually include three recommendations each, with specific direction to government, commercial and humanitarian organizations. Thus the number of recommendations tracked in implementation will actually be twelve (12) from these first four and sixteen (16) total.
[132] Key Observation No. 58, *Three Levels of Success*, Section 3.3.
[133] Key Observation No. 59, *A 'Win-Win' Is Wise*, Section 3.3; Key Observation No. 60, *An Uphill Path to Improve the Harmful Hacking Situation*, Section 3.3.
[134] Key Observation No. 12, *Official Statement: The U.S. Has Stated Its Principles*, Section 3.1; Key Observation No. 13, *Official Statement: China's Principles of Peaceful Co-Existence*, Section 3.1; Key Observation No. 14, *Official Statement: Common Principles,* Section 3.1; Key Observation No. 67, *Trust is a Two-Way Street*, Section 3.3.
[135] Key Observation No. 61, *Varied Responsibility for Response to Hacking Behavior*, Section 3.3; Key Observation No. 62, *Effect As an Indicator of Response,* Section 3.3; Key Observation No. 63, *Humanitarian Interests Deserve Special Protection from Hacking,* Section 3.3; Key Observation No. 64, *National Security Functions Are Conventional Targets for Espionage,* Section 3.3.
[136] Key Observation No. 11, *Many Damages from Hacking*, Section 3.1; Key Observation No. 37, *Hacking May Lead to War*, Section 3.2; Key Observation No. 17, *Trust is a Watershed*, Section 3.1.
[137] The recommendations took into account the full range of critical observations made in Section 3.1, T*he Current Situation*, and Section 3.2, *Understanding the Problem*.

Each of these key innovations is discussed below.

4.0.1 Innovation 1. A New Engagement Methodology: Decision Tree Optimized for Trust-Building (DTOT)

One of the most significant observations of this study was that there has been a flawed practice of engagement.[138] Up until now, the entry point for the discussions took the relationship down paths where trust suffers (Figure 14, *Verdict-Initiated Decision Tree*).[139] In contrast, the Recommendations presented here call for a change from initiating engagements that begin with accusations, to starting engagements that are more frank and sensible, with surgical-like focus on verifiable steps that can lead to trust building.[140] Together, these Recommendations provide direction toward a cautious examination of the core verifiable elements of trust, i.e. *what is said, done and observed* (Figure 15, *Decision Tree Optimized for Trust Building*).[141]

> In the new approach, the entry question is "*Do you have a policy against (or for) this?*"
>
> A. If "*yes*", good . . . and trust is built.
> B. If "*no, but corrective action will be taken to remedy the problem*", then this too is good, . . . and trust is built.[142]
> C. Only if the answer is "*no*", and there is insufficient effort to correct the situation, . . . then trust suffers.
>
> The next step is then to ask the same regarding policy deployment, and then performance evaluation, and so.[143]

Suspicions, Accusations and Reality

To better understand this problem, Figure 13 (*Managing Suspicions Regarding Incidents*) introduces the possibilities when a party expresses their suspicions about the perpetrator of a hacking incident. When an entity (i.e. a government, company or individual) is accused of hacking a system, there are two distinct elements that can be either true or false in the accuser's statement.

Consider the example of Entity A making the accusation "*Entity B committed compromise X*". There are four possibilities involving the permutations of the following two parameters:

- Did the event of compromise X take place?
- Was it Entity B that committed compromise X?

The key takeaway from this analysis is that since there are four logical possibilities that can be true in reality, *a system is needed that can handle all possibilities in a way that minimizes distrust and trust when not warranted, and that maximizes trust and distrust when appropriate*.

[138] Key Observation No. 32, *Flawed Practice of Engaging with Each Other*, Section 3.2.
[139] Key Observation No. 15, *Lack of Trust*, Section 3.1; Key Observation No. 16, *Ever-Low Expectations for Cooperation*, Section 3.1; Key Observation No. 18, *Returning Rebukes*, Section 3.1; Key Observation No. 34, *Repeating Distrust – Non-cooperation Cycle*, Section 3.2; Key Observation No. 44, *Reluctance to Cooperate on Combating Hacking Is Reinforced by Distrust,* Section 3.2; Key Observation No. 52, *U.S. Blames Chinese Government,* Section 3.2; Key Observation No. 53, *China Implies U.S. Is a Major Source of Hacking of Chinese Networks,* Section 3.2; *Flawed Practice of Engaging with Each Other,* supra n 138.
[140] Key Observation No. 40, *Political Speech Is Too Often Unclear*, Section 3.2.
[141] Key Observation No. 63, *Alignment with Words and Actions*, Section 3.3.
[142] Key Observation No. 43, *Politics Influences Cooperation for the Hacking Problem*, Section 3.2; Key Observation No. 66, *No Substitute for Corrective Actions* Section 3.3.
[143] Key Observation No. 66, *No Substitute for Corrective Actions* Section 3.3.

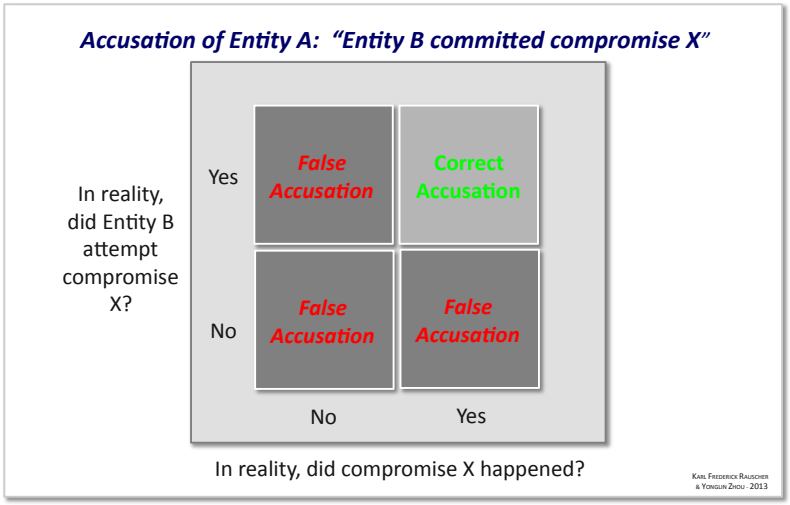


Figure 14. Managing Suspicions Regarding Incidents.

The Current Situation: Paths that Lead to Distrust

Given that the current China-U.S. relationship is filled with accusations, it is worth studying how this approach plays out. Figure 14 (*Verdict-Initiated Decision Tree*) provides a flow chart of the possible paths for an engagement that begins with accusations can traverse. Referring to Figure 14, each path has its own characteristics, but arrives at the same final disposition:

- Disposition W: Trust suffers because A confirms B as dangerous
  AND B admits it is dangerous.
- Disposition X: Trust suffers because A believes B is dangerous.
- Disposition Y: Trust suffers because A (falsely) believes B to be dangerous
  AND B agrees.[144]
- Disposition Z: Trust suffers because A (falsely) believes B to be dangerous
  AND B is falsely accused
  AND B is not believed.

Disposition W warrants distrust. Disposition X also does, but with less certainty. Of importance is the fact that the engagement process as shown does not offer an opportunity to change the disposition for either of these cases. Thus, the key take away here is that for all of the final dispositions, *trust suffers*.

Another conclusion is that the only way that trust can be achieved for both parties is when the conditions are such that (a) no compromises are being made and (b) no accusations are made. Neither of these conditions holds for the present China-U.S. hacking situation.[145] Rather the opposite trends are being observed.[146]

[144] e.g., there are times when multiple terrorists groups claim responsibility for an incident, apparently in an attempt to gain perceived power.
[145] Key Observation No. 18, *Returning Rebukes*, Section 3.1; Key Observation No. 34, *Repeating Distrust – Non-cooperation Cycle*, Section 3.2.
[146] Key Observation No. 15, *Lack of Trust*, Section 3.1; Key Observation No. 16, *Ever-Low Expectations for Cooperation*, Section 3.1.

What is missing in the above (and our current) situation, is frank communication (Dispositions W, X and Y) and sensible cooperation that could dispel the inaccurate dispositions (e.g., for X, Y and Z).

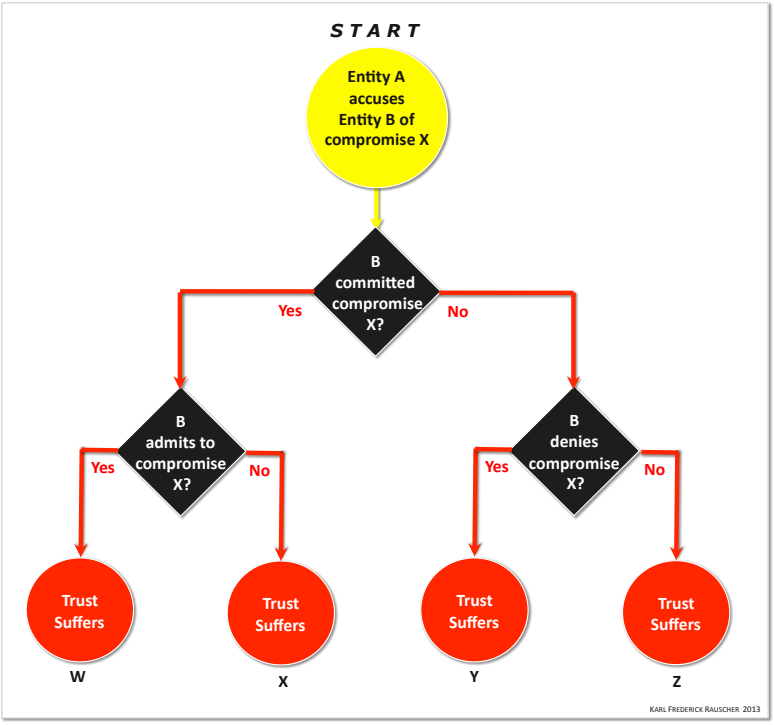


Figure 15. Verdict-Initiated Decision Tree (VIDT).

The following summary statistics provide insights into the effectiveness of the *VIDT* approach depicted in Figure 14:

4 **Total distinct paths**
0 Paths leading trust building
4 Paths leading to distrust

2 **Total number of verification points**
0 Opportunities to build trust for all paths
2 Steps needed to detect non-trustworthiness for all possible paths[147]

The Solution

This report introduces an alternative, the Decision Tree Optimized for Trust-Building (DTOT), to the current practice of engagement taking place between China and the U.S (Figure 15). In contrast to the verdict-oriented accusations that define the present situation, this alternative approach offers a distinct entry point and subsequent guidance for managing suspected harmful hacking. The value of this different approach is that it (i) enables a high degree of confidence in whether or not trust is warranted and (ii) it provides multiple opportunities to improve the situation and build verifiable trust.

[147] i.e. the "Yes" that leads to Disposition "W" and the "Yes" that leads to Disposition "Y"; note that Disposition "X" lacks a detection step.

The entry point for the new approach is a question directed at the suspected offender: *"Do you have a policy against committing compromise X?"* The response to this question determines whether (a) trust can be warranted now, (b) trust can be built with corrective action, or (c) distrust is warranted (Loop 1).

The second stage (Loop 2) presents a similar question and opportunity for response, but this time it is about whether the stated policy is being deployed: *"Have you deployed your policy against X?"* The response to this question determines whether (a) trust can be warranted now, (b) trust can be built with corrective action, or (c) distrust is warranted.

The third stage (Loop 3) presents a similar question and opportunity for response, but this time it is about whether cooperation will be offered to investigate an incident that appears as evidence that either the stated policy or the policy deployment have failed: "*Will you cooperate to investigate X?"* The response to this question determines whether (a) trust can be warranted now, (b) trust can be built with corrective action, or (c) distrust is warranted.

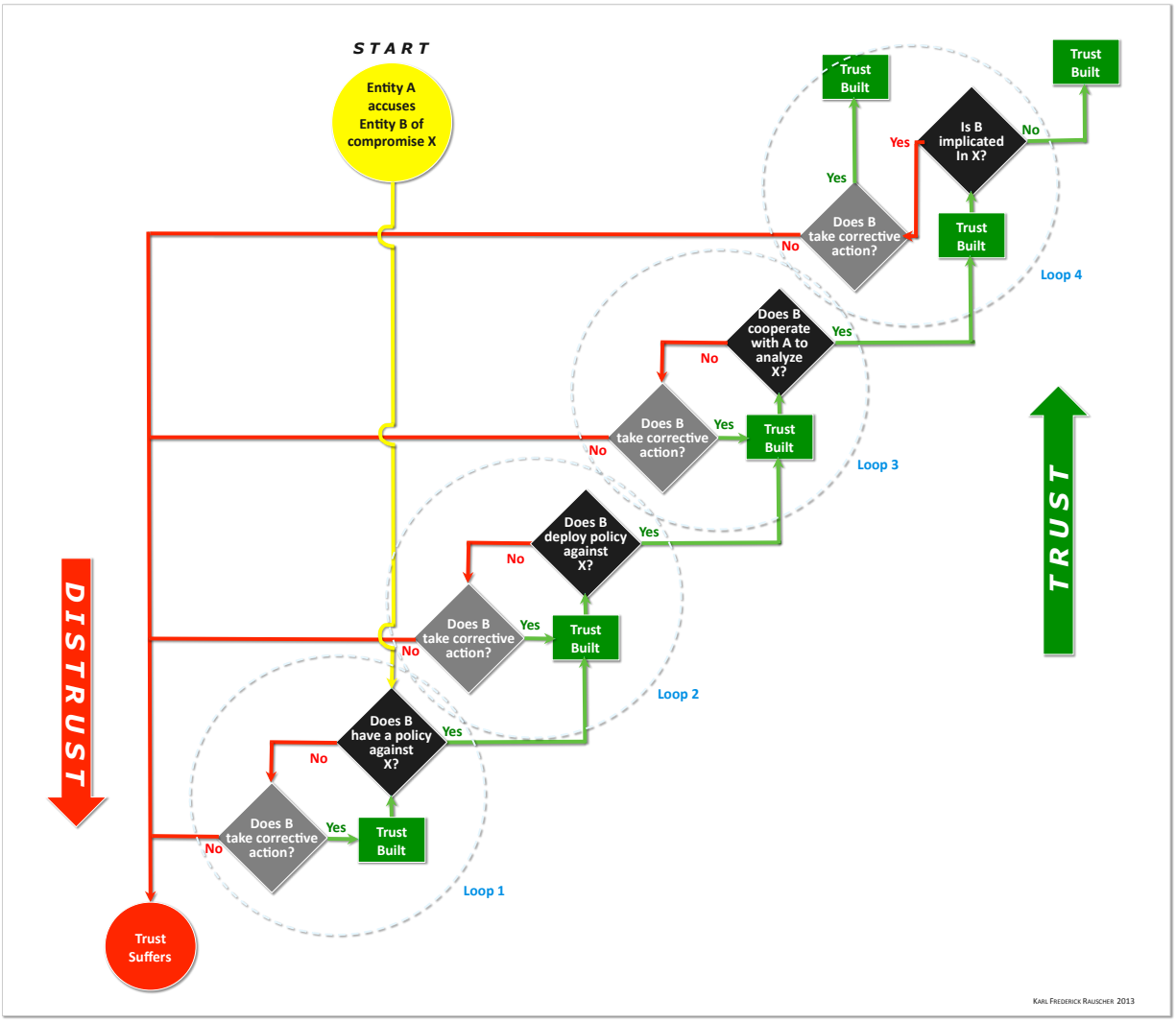


Figure 16. Decision Tree Optimized for Trust-Building (DTOT).

The fourth stage (Loop 4) presents a slightly different question and opportunity for response. This time it is about whether the objective evidence that is gathered from a joint investigation implicates the accused party in being responsible for compromise X: "*Are you responsible for X?"* The response to this question determines whether (a) trust can be warranted now, (b) trust can be built with corrective action, or (c) distrust is warranted.

The major value offered with the DTOT approach is that it enables trust to be built in a way that elevates the confidence of verification. The DTOT methodology essentially interlinks four key loops, each of which includes a critical verification and an opportunity for corrective action should the verification fail (Figure 15).

This new approach can handle the full range of possible situations, including both the true and false incidents outlined in Figure 13. It illustrates how essential frank communication is to the dialogue and how important sensible cooperation is in making corrective action and cooperating in joint investigations.

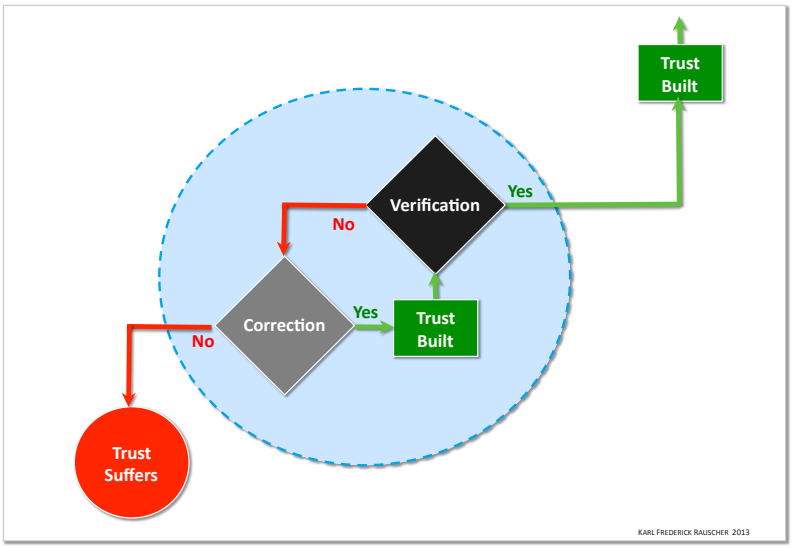


Figure 17. DTOT Verification and Correction Loop.[148]

There are 31 possible logical paths that can be taken in the DTOT approach that is presented in Figure 15. Each of these paths is presented in Table 16, *Logical Paths for DTOT*.

Once entered, each loop provides exactly three ways out. Two of these build trust, while the other confirms that trust is unwarranted. The further one goes in the process, i.e. from one loop to another, the more significant and noticeable is a departure from the trust-building mode. However, experts and stakeholder still expect that even in highly trusting relationships, there may be times when the path taken is the one that does not build trust. For example, a country or company may find it undesirable to cooperate in an investigation that it knows is embarrassing to its stature or reputation, or when the possibility of information leakage could cause further harm. It is expected at any given time there will be multiple activities underway when DTOT is being followed, and thus it is not necessary that every verification be passed in order for the general trend of trust building to thrive.

[148] Доверяй, но проверяй (doveryai, no proveryai), a Russian proverb translated "Trust, but verify," was often quoted by U.S. President Ronald Reagan in the context of diplomacy with the Soviet Union. In the September 2013 negotiations that yielded the Russia-U.S. agreement to dispose of Syria's chemical weapons U.S. Secretary of State John Kerry suggested that this phrase needed an update to "Verify and Verity."

When combined with frank communication and sensible cooperation, the *DTOT Verification and Correction Loop* and the objective nature of technical analysis can cause a powerful reversal in the deteriorating relationships in cybersecurity, including that which China and the U.S. now find themselves.

Table 16. Logical Paths for DTOT.

Path	Have Good Policy?	Deploy the Policy?	Cooperate in Investigation?	Implicated in Causing Incident?	Disposition
A	Yes	Yes	Yes	No	**Trust**
B	Yes	Yes	Yes	Yes & TCA*	**Trust**
C	Yes	Yes	Yes	Yes & No TCA	**Distrust**
D	Yes	Yes	No & TCA	No	**Trust**
E	Yes	Yes	No & TCA	Yes & TCA*	**Trust**
F	Yes	Yes	No & TCA	Yes & No TCA	**Distrust**
G	Yes	Yes	No	n.a.	**Distrust**
H	Yes	No & TCA	Yes	No	**Trust**
I	Yes	No & TCA	Yes	Yes & TCA*	**Trust**
J	Yes	No & TCA	Yes	Yes & No TCA	**Distrust**
K	Yes	No & TCA	No & TCA	No	**Trust**
L	Yes	No & TCA	No & TCA	Yes & TCA*	**Trust**
M	Yes	No & TCA	No & TCA	Yes & No TCA	**Distrust**
N	Yes	No & TCA	No	n.a.	**Distrust**
O	Yes	No	n.a.	n.a.	**Distrust**
P	No & TCA	Yes	Yes	No	**Trust**
Q	No & TCA	Yes	Yes	Yes & TCA*	**Trust**
R	No & TCA	Yes	Yes	Yes & No TCA	**Distrust**
S	No & TCA	Yes	No & TCA	No	**Trust**
T	No & TCA	Yes	No & TCA	Yes & TCA*	**Trust**
U	No & TCA	Yes	No & TCA	Yes & No TCA	**Distrust**
V	No & TCA	Yes	No	n.a.	**Distrust**
W	No & TCA	No & TCA	Yes	No	**Trust**
X	No & TCA	No & TCA	Yes	Yes & TCA*	**Trust**
Y	No & TCA	No & TCA	Yes	Yes & No TCA	**Distrust**
Z	No & TCA	No & TCA	No & TCA	No	**Trust**
AA	No & TCA	No & TCA	No & TCA	Yes & TCA*	**Trust**
AB	No & TCA	No & TCA	No & TCA	Yes & No TCA	**Distrust**
AC	No & TCA	No & TCA	No	n.a.	**Distrust**
AD	No & TCA	No	n.a.	n.a.	**Distrust**
AE	No	n.a.	n.a.	n.a.	**Distrust**

**TCA = Taking Corrective Action*

The following summary statistics provide insights into the effectiveness of the *Decision Tree Optimized for Trust Building* depicted in Figure 15:

31 Total distinct paths
16 Paths leading trust building
15 Paths leading to distrust[149]

[149] There four decisions that lead to distrust: 1) Do not state policy; 2) Do no deploy policy; 3) Do not cooperate with stakeholders for investigations (at least for some); and 4) D not take corrective action.

124 Total number of verification points
98 Opportunities to build trust for all paths
15 Steps needed to detect non-trustworthiness for all possible paths

The contrast between the VIDT and DTOT approaches is striking. The key differences are the number of verification points, number of opportunities to build trust and available opportunities for stronger confidence in concluding that trust is not warranted (Figure 17, *Rich Environment for Trust Building*). The authors note that this approach is aligned well with a recently coined phrase "verify and verify."[150]

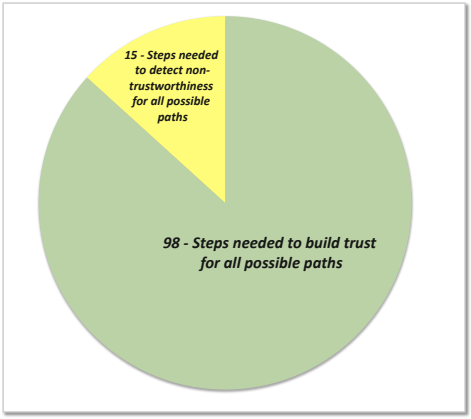


Figure 18. Rich Environment for Trust Building.

4.0.2 Innovation 2. A New System of Verification: Total Trust Management (TTM)

Another key factor in shaping these recommendations is the Total Trust Management Model (TTMM). The first four recommendations (Nos. 1 through 4) combine to form a tight system. This system is depicted in Figure 18, *The Total Trust Management Model*.

- **Recommendation No. 1 Stated Policy**
- **Recommendation No. 2 Policy Deployment**
- **Recommendation No. 3 Performance Measurement**
- **Recommendation No. 4 Corrective Action**

These steps are equally applicable for a wide range of topics, including international cooperation in fighting crime, international cooperation in tracking down malicious hackers, protection of humanitarian interests, protection of commercial IP and norms of behavior in cyberspace.

[150] Доверяй, но проверяй (doveryai, no proveryai), a Russian proverb translated "Trust, but verify," was often quoted by U.S. President Ronald Reagan in the context of diplomacy with the Soviet Union. In the September 2013 negotiations that yielded the Russia-U.S. agreement to dispose of Syria's chemical weapons U.S. Secretary of State John Kerry suggested that this phrase needed an update to "Verify and Verify."

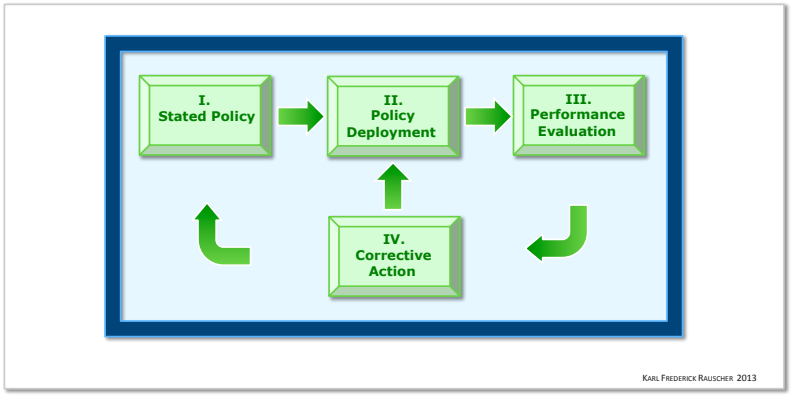


Figure 19. The Total Trust Management Model.

In this TTM system, there are four fundamental tasks outlined for each party to fulfill in order to build genuine trust.

I. Stated Policy

The first step in building trust is setting expectations. When an organization sets expectations it states its principles, its courses of action, and the behaviors it will sanction. These policy statements may be acceptable or unacceptable to stakeholders. If they are acceptable, then it means that the policy commitments are sufficiently clear and complete, and that they set expectations that, if fulfilled, would satisfy the interests of the stakeholder. On the other hand, deficiency in any of these areas could be cause for a stakeholder to find a policy statement unacceptable.

It is unlikely that policy statements will be either perfectly articulated the first time, or achievable as desired due to various factors. Thus it is important that the policy development process be receptive to feedback that can be used to improve stated policies.

For the application of this principle for harmful hacking in the China-U.S. relationship, see Recommendation No. 1, *Stated Policy*.

II. Policy Deployment

Once it is confirmed as Stated Policy, and once it sufficiently satisfies the interests of stakeholders, then the second step in building trust can begin. Policy statements need to be moved from words to actions. Policy Deployment involves strategic planning to combine intelligence, organization and resources toward the aim of achieving the goal (i.e. policy).

Like policy statements, no Policy Deployment will be perfect. Such constraints as limited resources, human error and unanticipated challenges will be some of the factors that can spoil plans from achieving the policy realization goal. Therefore it is critical that the Policy Deployment planning process be receptive to feedback that can used to improve it.

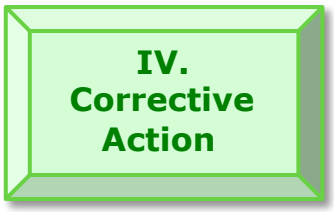
For the application of this principle for harmful hacking in the China-U.S. relationship, see Recommendation No. 2, *Policy Deployment*.

III. Performance Measurement

Once Policy Deployment is underway for Stated Policy, then the third step in building trust can begin. This third step is Performance Measurement. Stakeholders, as well as others, may detect failures in policies. Associated with such failures are both quantitative and qualitative information. Quantitative information such as incident frequency, duration and impact can be measured and reported. Qualitative information includes data associated with the incident. Forensics can be used with this data to better understand the cause of an incident.

For the application of this principle for harmful hacking in the China-U.S. relationship, see Recommendation No. 3, *Performance Measurement*.

IV. Corrective Action



The insights gleaned from failures in Stated Policy or Policy Deployment can be useful in learning about what can be improved. There are two types of countermeasures. First, and most important, there are countermeaures that can prevent similar incidents from occurring in the future. The second type of countermeasures are those that ameliorate the impact of future similar incidents, should they occur.

Both the Stated Policy itself and the Policy Deployment plans designed to realize it, are places where countermeasures can be applied. Given the nature of Stated Policy, it is generally more significant to make adjustments there.

For the application of this principle for harmful hacking in the China-U.S. relationship, see Recommendation No. 4, *Corrective Action*.

As some readers will observe, this integrated system borrows key breakthrough leadership concepts from the Japanese Hoshin Kanri (direction control) and the Deming cycle methodologies.[151]

The simple truth is that the essential "asks" being made in these first four recommendations are actually quite *basic*. Yet these basics are essential for genuine trust. In fact, the authors respectfully submit that most organizations would benefit from implementing these recommendations regardless of the present China-U.S. concern. Benefits from investing in the implementation of these recommendations include enabling increased trust of citizens and consumers in their brands and preempting future public relations disasters, when expectations and reality collide. However, as detailed in the "required commitment" section provided for each recommendation, there is new clarity and discipline expected of all actors. But encouragingly, these requests are reasonable.

A System Built on Frank Communication and Sensible Cooperation

This system is designed to prevent cheating. It is air tight in the sense that there is no way to escape the path of expected communication and cooperation without detection. Consequently frank communication and sensible cooperation are keys for success.[152] Up to this time, too much of the communication has been

[151] Ishikawa, Karoru, *What is Total Quality Control? The Japanese Way*, 1988. William Deming's "Plan-Do-Check-Act"
[152] Key Observation No. 14, *Common Principles*, Section 3.1.

in the form of arguments.[153] As it has been said, "dialogue can mean two people speaking to themselves." A goal of communication in this context has to start including meeting the other party's needs in terms of conveying essential information they need as a stakeholder, e.g., a country needs assurances from a supplier of critical infrastructure technology. As frank communication is not always easy, there is also a need for careful listening.

Together, the implementation of the four TTM recommendations provides assurance of a trustworthiness assessment. That is, with this system in place, when both parties are implementing each of the four recommendations, genuine trust can thrive and each party can have confidence in their assessment.[154] This system will also detect when either party is demonstrating behavior that is not trustworthy, and likewise enable a party to have confidence in its judgment that there is insufficient evidence that its interests are being protected.[155] Thus the TTM system is 'air-tight' in the sense that it detects policy inventory vacancies, inconsistencies between words and actions, and failures in the field. The TTM system deliberately removes the gamesmanship of political doublespeak.[156] For those political operators whose primary means of addressing difficult situations is through the art of using euphemistic, ambiguous and obscure language, this may be uneasy. But the seriousness of the present China-U.S. crisis dictates that we can no longer afford the luxury of such diversions for our limited mindshare, resources and time.

If implemented, these recommendations will clear the air. Stakeholders will have confidence in each other based on what is "said", "done" and "seen"; and then what is "said", "done" and "seen"; and then again, and again . . . At its core, TTM is an empirical method of arriving at the truth, but one that allows for human imperfections along the way.[157]

The present day China-U.S. cybersecurity relationship crisis is evidence for how these *basics* have been neglected.[158] In the unfortunate case where either one or both sides are unwilling to commit to these basics, discussions on more advanced subjects can be delusional; giving a false sense of comfort for which there is no foundation.[159] Thus the TTM can be helpful in informing both parties and stakeholders of a status of good health, improving health, deteriorating health or bad health. The TTM is an alternative to brinkmanship.

Bottom Line: Who Can Be Trusted?

Those can be trusted whose values are tolerable, whose behaviors are consistent with their values, and whose responses to lapses into inconsistent behavior demonstrate accountability through necessary corrections to prevent future lapses and ameliorate their impact.

In summary, the first four recommendations combine to form a tight, disciplined system of values, communication, action, evaluation and response. Together, if implemented, these four recommendations could transform the present decline in China-U.S. relationship health into a positive improvement that is sustainable over the long run.

[153] Key Observation No. 18, *Returning Rebukes*, Section 3.1; Key Observation No. 34, *Repeating Distrust – Non-cooperation Cycle*, Section 3.2.
[154] Key Observation No. 68, *Repeating Trust – Cooperation Cycle*, Section 3.3.
[155] Key Observation No. 69, *More Technological Independence May Be a Safe Option for China and U.S.*, Section 3.3.
[156] Key Observation No. 40, *Political Speech Is Too Often Unclear*, Section 3.2.
[157] i.e., Recommendation No. 4, *Corrective Action*, anticipates regular needs to adjust Stated Policy and Policy Deployment plans. Key Observation No. 73, *Science Diplomacy*, Section 3.3
[158] Key Observation No. 15, *Lack of Trust,* Section 3.1; Key Observation No. 16, *Ever-Lower Expectations for Cooperation,* Section 3.1.
[159] *More Technological Independence May Be a Safe Option for China and U.S.,* supra n 155.

4.0.3 Innovation 3. A New Framework for the Landscape of Interests in Cyberspace (KLIC)

The third new key factor in shaping these recommendations was recognizing the three primary driving interests in cyberspace among the universe of all interests, namely humanitarian, commerce and security. Repeated here for convenience from Section 2.4.1, the KLIC diagram depicts the relationship of these three primary interests (Figure 19). The significance of this diagram is discussed in detail in Section 2.4.1, but emphasized here as it is a significant influence in the development of Recommendations 1-3, 5 and 6.

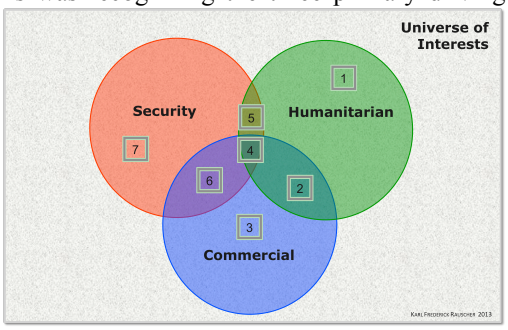


Figure 20. Landscape of Interests in Cyberspace.
(repeated)

Prioritizing Implementation of the Recommendations.

Given that the recommendations below can apply to different types of organizations, the question arises about *where is the most important place to start*? The macro-level China-U.S. cybersecurity relationship is actually a high level simplification of a much more complex aggregation of relationships and various lower levels of granularity and type.[160] There are four primary actors that are challenged to implement the first four recommendations: government organizations (e.g., government agencies), commercial organizations (e.g., businesses and non-profits that promote an industry objective), humanitarian organizations (e.g., those that have a pure involvement in medical, cultural or spiritual matters) and netizens (e.g., organized groups like the Internet Engineering Task Force and individuals). While these types of organizations are actors, these same types of entities are stakeholders of each other. From this stakeholder perspective, it is important to note that there is a variety of types of micro-relationships within the broader China-U.S. macro-relationship that consist of similar and dissimilar organization types.[161] While some of these entities (e.g., humanitarian) are relatively small compared to others (e.g., government), from their operational perspective, the stated and practiced policies of the others can still be very important to them. Table 17 summarizes the types cross-linking of actors and stakeholders with an indicator in each intersection for *how the stakeholder views* the importance of trust in the relationship.[162]

The recommendations emphasize the high importance of each of the stakeholders stepping up to do their part in solving the China-U.S. harmful hacking situation.

[160] Key Observation No. 11, *Many Damages from Hacking,* Section 3.1; Key Observation No. 27, *Trust Is a Watershed,* Section 3.1; Key Observation No. 29, *Deeply Integrated, but with Mixed Reliance,* Section 3.1.
[161] Key Observation No. 61, *Varied Responsibility for Response to Hacking Behavior*, Section 3.3; Key Observation No. 62, *Effect As an Indicator of Response*, Section 3.3.
[162] Ibid.

Table 17. Importance of Trust in Relationship - Stakeholder View.

		ACTORS			
		Governments	Commercial	Humanitarian	Netizens
STAKEHOLDERS	Governments	HIGH	HIGH	Low	MODERATE*
	Commercial	MODERATE	MODERATE	Low	Low
	Humanitarian	HIGH	Low	Low	Low
	Netizens[163]	HIGH	HIGH	HIGH	Low

Recommendations 5 through 10

The remaining recommendations (5 through 10), each provide additional important guidance that compliments the first four recommendations by emphasizing specific critical areas requiring special attention:

- **Recommendation No. 5** ***Separate Critical Humanitarian Assets***

  This recommendation compliments Recommendation No. 1, *Stated Policy*, by enabling policy articulation that distinguishes the treatment of humanitarian interests from national security interests in cyberspace.

  This recommendation also compliments Recommendation No. 2, *Policy Deployment*, by directing the separation of humanitarian assets from national security assets in cyberspace.

- **Recommendation No. 6** ***De-Clutter Espionage Expectations***

  This recommendation compliments Recommendation No. 2, *Policy Deployment*, by clarifying the normal and expected functions of national security–oriented organizations.

  This recommendation also compliments Recommendation No. 3, *Performance Measurement*, by clarifying the expectation that national security-oriented assets are, because of their potential for hostility, elevated as targets for espionage by foreign interests. This factor suggests a differentiation between incidents experienced by national security interests and others.

- **Recommendation No. 7** ***Summon a Roundtable of Subject Matter Experts***

  This recommendation compliments Recommendation No. 3, *Performance Measurement*, by calling on world-class subject matter experts from both countries to come forward for a new mode of collaboration, part of which would support objective assessments of the overall situation between

China and the U.S. and for exceptional incidents that are detected. This recommendation compliments Recommendation No. 4, *Corrective Action*, by serving as a resource for objective analysis and assessment.

- **Recommendation No. 8** ***Continuous Approach Status Indicator***
  This recommendation compliments Recommendation Nos. 1 through 4, by providing a provisional capability to monitor, assess and report on the status each of these crucial components.

- **Recommendation No. 9** ***Prepare Sufficiently, React Quickly and Summarize Seriously***
  This recommendation calls for transformation of the harmful hacking responses from one that is primarily reactive to one that is pro-active, and includes setting goals that define sufficient preparation and response.

- **Recommendation No. 10** ***Launch Parallel Bilateral Collaboration on Government and Industry Levels***
  This recommendation calls for industry level collaboration to supplement the new cooperation undertaken at the governmental level. Industry technical expertise and business insights are required to combat the harmful hacking that is out of control.

Recommendation Presentation

Each recommendation is presented with the essential decision-supporting information to foster its implementation. This information includes the following nine elements:

- **Title** - for identification and a summary.
- **Purpose** – to state the intent in a straightforward manner
- **Background** - to provide the essential elements of the context of the issue being addressed.
- **Recommendation** - to identify who should do what.
- **Required Commitments** – to crisply outline the requirements from critical parties for success.[163]
- **Benefits** – to encapsulate the value proposition for implementing the recommendation.
- **Alternatives and their Consequences** – to outline the other options and likely outcomes.
- **Next Steps** – to offer suggestions for keeping momentum and focus.
- **Measures of Success** – to provide means to objectively evaluate performance.

For additional discussion of the facets of the difficulties being faced and compelling factors for the recommendations, the reader is encouraged to read the other sections of the report. A diagram of the recommendation presentation is provided in Figure 20.

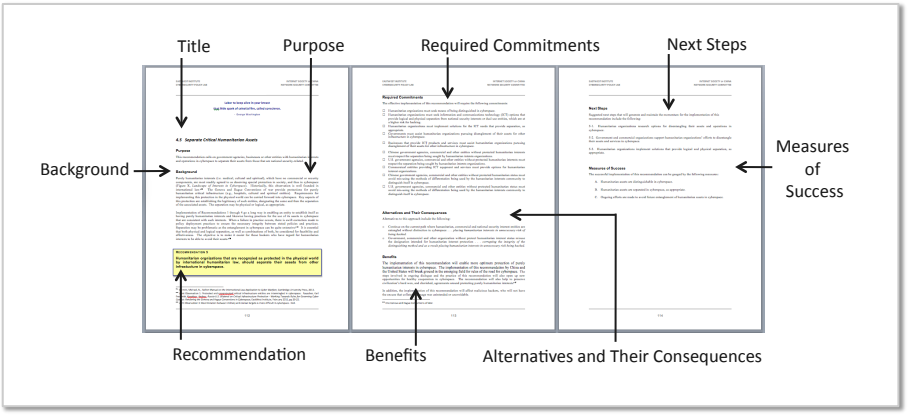


Figure 21. Presentation of Recommendations[164]

[163] Such statements are an example of frank communication.

Whatever America hopes to bring to pass in the world
must first come to pass in the heart of America.
- Dwight D. Eisenhower

To know others, know yourself first.
- Ancient Chinese Proverb

4.1 Stated Policy

Purpose

1 - GOVERNMENT: This recommendation calls on governments to articulate the basic policies that govern the nature of their interests, use of their assets and operations in cyberspace.

1 - BUSINESS: This recommendation calls on commercial organizations to articulate the basic policies that govern the nature of their interests, use of their assets and operations in cyberspace.

1 – OTHER ORGANIZATIONS: This recommendation calls on other organizations to articulate the basic policies that govern the nature of their interests, use of their assets and operations in cyberspace.

Background

In the cybersecurity arena, the China-U.S. relationship suffers from a lack of straightforward communication by government agencies, corporations and other organizations about the issues that matter most.[165] The fact is that the cyberspace operating policies and practices of most government agencies and corporations are too opaque.[166] For many of these organizations, there has been reluctance to being open about some uncomfortable realities.[167] For others, their statements are overly complex. In the place of what should be clear, concise policy statements, there is a barrage of accusations and denials, and even threats.[168]

A significant first step in building trust is stating values and goals in a sufficiently clear and complete manner that will meet the reasonable expectations of stakeholders.[169] However building trust is not the only benefit that a focus on policy statements offers. On the contrary, an unacceptable policy statement can be the first indicator that trust is unwarranted. When the best straightforward formulations of policy statements are unacceptable to critical interests of stakeholders, then the hard reality may be that more stability in the relationship may be achieved through a pulling back of interdependency to areas where trust is achievable.[170]

For a start, an appropriate policy statement for Chinese and U.S. government agencies, businesses, and other organizations is clear about at least 3 critical issues:

1. What are the organization's interests?
2. What is the organization's normal use for its assets in cyberspace?

[164] This method of presenting Recommendations for decision-making was developed by one of the authors while simultaneously serving in advisory capacities for the European Commission and the White House, and observed the low implementation rate of policy recommendations generated by the private sector.
[165] Key Observation No. 40, *Political Speech Is Too Often Unclear*, Section 3.2.
[166] Key Observation No. 38, *There Are Secret Government Operations in Cyberspace*, Section 3.2.
[167] Ibid. Key Observation No. 39, *some Policies and Practices Are Not Popular*, Section 3.2.
[168] Key Observation No. 18, *Returning Rebukes*, Section 3.1.
[169] Key Observation No. 76, *Information Channels*, Section 3.3.
[170] Key Observation No. 69., *More Technological Independence May Be a Safe Option for China and U.S.,* Section 3.3.

3. What, if any, are the explicit conditions for exceptions to (2)?

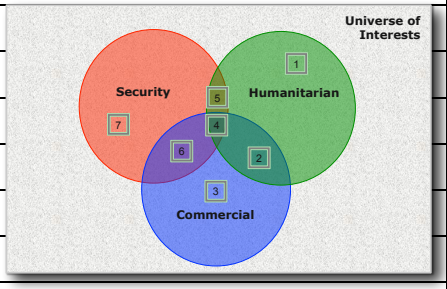
Table 18 provides a sample template that can be used as a checklist for a government, business or other organization. Tables 19 and 20 provide additional consideration for what should be included in policy statements for government agencies and businesses, respectively. These examples are intended to be starting points for internal organization discussions. Additional examples are provided in Appendix C, *Example Templates for Policy Statements*.

An initial reaction from some, particularly those in business and engineering management, is that this recommendation seems so simple - perhaps too simple. *How can we not being doing this?* However, it is quite clear that even businesses, which consistently tend to have more freedom of movement relative to governments, are prevented from stating what they may be required to do, below some level of generality, because of government rules requiring secrecy. This is even true in America, where there is a unique pride on market and social freedoms.[171]

[171] Key Observation No. 57, *American Businesses Affected by U.S. Government Policies*, Section 3.2.

Table 18. Checklist Template for Organization Policy Statements

The Interests of the Organization (select one)	**Example**
☐ 1. Humanitarian[172]	disaster relief
☐ 2. Humanitarian + Commercial[173]	for-profit hospital
☐ 3. Commercial	software company
☐ 4. Humanitarian + Commercial + Security[174]	pharmeceutical lab[175]
☐ 5. Humanitarian + Security	policy think tank
☐ 6. Commercial + Security	defence contractor
☐ 7. Security	defense department
☐ 8. Other	netizen organization



The Organization's Normal Use of Assets in Cyberspace (select one)
☐ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐ 3. Generate a profit for owners
☐ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☐ 7. Engage in belligerent activities
☐ 8. Other (describe)

Explicit Conditions for Exceptions (select all that apply)	**Example**
☐ A. None	
☐ B. In response to lawful government directive in home country	wiretap of suspect
☐ C. In response to lawful government directive in foreign country where operating	investigation
☐ D. In response to lawful government directive in foreign country where *not* operating	
☐ E. In response to government request in home country	
☐ F. In response to government request in foreign country where operating	
☐ G. In response to government request in foreign country where *not* operating	
☐ H. Voluntary assistance in cases where life or human safety are threatened	disaster response[176]
☐ I. Voluntary assistance in cases of a state of national emergency	
☐ J. "Hacking-back" at sources of malicious activity	DDoS attack response
☐ K. Academic research	user behaviors
☐ L. Other (describe)	

[172] see Definition 1, Section 2.4.1, *Core Interests*.
[173] see Definition 2, Ibid.
[174] see Definition 3, Ibid.
[175] i.e. a pharmaceutical company producing antidotes to chemical weapons.
[176] WERT offering of search and rescue capabilities to Sri Lanka in aftermath of 200X Tsunami.

Recent developments are requiring governments and companies to be clearer about their practices.[177] In addition to covering these basic elements, policy statements should include positions on critical outstanding questions, depending on the nature of the organization, such as suggested in Table 19 and Table 20 for governments and businesses, respectively.

Table 19. Checklist Template for Organization Policy Statements – Additional Considerations for *Governments.*

Governments
☐ Acceptability for its citizens to take advantage of vulnerabilities in others' assets in cyberspace
☐ Acceptability for its citizens to steal intellectual property from others in cyberspace
☐ Explicit conditions for interfering in the affairs of vetted and confirmed humanitarian organizations
☐ Use of commercial organizations within its jurisdiction for belligerent missions
☐ Acceptability for its companies to "hack-back" against presumed sources of malicious activity
☐ Prohibition for organization members to misuse assets in cyberspace
☐ Other (describe)

Table 20. Checklist Template for Organization Policy Statements – Additional Considerations for *Businesses.*

Businesses
☐ Storage of statistical data from netizen use
☐ Storage of content data from netizen use
☐ Harvesting of commercial intelligence from netizen use statistics
☐ Harvesting of commercial intelligence from netizen content
☐ Provision of netizen statistical data to third parties
☐ Provision of netizen content data to third parties
☐ Dual use of functionality for belligerent purposes
☐ Prohibition for organization members to misuse assets in cyberspace
☐ Other (describe)

Policy statements should strive to be as accurate as possible. Thus on one hand, caution is warranted in not overstating virtues or achievable objectives. This is because when policy statements are made of which there is no honest intention to fulfill, the long-term results will be further degraded trust.[178] Indeed, the worst scenario is to set expectations for a desirable behavior and then contradict it with actual behaviors (Figure 21, *Policy-Behavior Alignment Options*). This is not the same as policy failures for which corrective action can be taken. As Recommendation No. 4, *Corrective Action*, asserts that in such cases trust can be built.

On the other hand, long-term commitments specified as policies should not be limited to those that can be achievable with existing training and capacity. Government agencies, businesses and other organizations should be informed of what benchmarks have been achieved elsewhere when setting their goals.

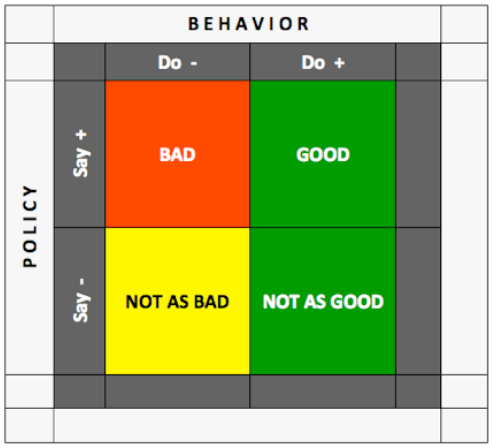


Figure 22. Policy-Behavior Alignment Options
Where "+" is admirable, popular or otherwise approved.
Where "-" is ***not*** admirable, popular or otherwise approved.

[177] Key Observation No. 10, *Expanding Enterprise Examinations*, Section 3.1.
[178] Key Observation No. 65, *Alignment of Words and Actions*, Section 3.3.

Can a stakeholder trust a government, company or other organization? Maybe they should or maybe they should not. The first sanity check is to examine their policy. Stating policy is the first key step of managing trust. This recommendation has three versions (i.e. government, business and other organizations)

RECOMMENDATION 1 – GOVERNMENT

Government agencies should establish expectations for their behavior in cyberspace by articulating their policies governing a) their interests relative to being humanitarian, commercial or national security; b) the use of their assets relative to (a); and c) the explicit conditions for exceptions.

Required Commitments – GOVERNMENT

The effective implementation of this recommendation will require the following commitments:

- ☐ Governments must state the nature of their interests as being humanitarian or national security or some combination thereof.
- ☐ Governments must state the policies for the use of their assets in cyberspace.
- ☐ Governments must provide explicit exceptions to the normal use of their assets.

RECOMMENDATION 1 - BUSINESS

Businesses should establish expectations for their behavior in cyberspace by articulating their policies governing a) their interests relative to being humanitarian, commercial or national security; b) the use of their assets relative to (a); and c) the explicit conditions for exceptions.

Required Commitments - BUSINESS

The effective implementation of this recommendation will require the following commitments:

- ☐ Businesses must state the nature of their interests as being humanitarian, commercial, national security or some combination thereof.
- ☐ Businesses must state the policies for the use of their assets in cyberspace.
- ☐ Businesses must provide explicit exceptions to the normal use of their assets.
- ☐ Governments must remove barriers from businesses to make such statements.[179]

RECOMMENDATION 1 – OTHER ORGANIZATIONS

Non-government, non-commercial organizations should establish expectations for their behavior in cyberspace by articulating their policies governing a) their interests relative to being humanitarian, commercial or national security; b) the use of their assets relative to (a); and c) the explicit conditions for exceptions.

Required Commitments – OTHER ORGANIZATIONS

[179] Key Observations No. 57., *American Businesses Affected by U.S. Government Policies*, Section 3.3.

The effective implementation of this recommendation will require the following commitments:

- ☐ Organizations must state the nature of their interests as being humanitarian, commercial, national security or some combination thereof.
- ☐ Organizations must state the policies for the use of their assets in cyberspace.
- ☐ Organizations must provide explicit exceptions to the normal use of their assets.
- ☐ Governments must remove barriers from organizations to make such statements.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Do nothing regarding policy statements . . . *accepting that a lack of clarity in policies regarding cybersecurity are destabilizing the China-U.S. relationship.*
- Provide new polices but with insufficient content . . . *coming short of meeting the needs of stakeholders for understanding the values and commitments being held.*
- Provide overly nuanced policy statements . . . *unnecessarily complicating the situation and impeding the ability to grow trust.*

Benefits

The implementation of this recommendation will enable a government, business or other organization's beliefs and commitments to be known. Through the process of developing the policy statement, the organization will benefit from the rigor of articulating a careful statement, ideally, feedback from stakeholders, which may include nation-states, companies, and citizens' groups. A clear statement that covers each of the three essential elements specified in the recommendation will begin the process of setting expectations.

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

1-1. Organizations that are critical to the China-U.S. relationships regarding cybersecurity are identified.

1-2. Organizations review their charter, current practices and applicable legal obligations in order to confirm their understanding of: a) their interests relative to being humanitarian, commercial or national security; b) the use of their assets relative to (a); and c) the explicit conditions for exceptions.

1-3. Organizations draft new policy statements, or modify existing ones, to reflect the nature of the organization's interests, their intended practices for the use of their assets in cyberspace, and exception handling.

1-4. Organizations engage stakeholders to learn if the draft language provides sufficient clarity and completeness in what is being written, and refine as appropriate.

1-5. Organizations make their policy statement available to stakeholders, and revise in the future as appropriate, based on future feedback.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Government agencies, businesses and other organizations provide a **clear** policy statements to the public that are **complete**, by covering a) their interests relative to being humanitarian, commercial or national security; b) the use of their assets relative to (a); and c) the explicit conditions for exceptions.

B. Stakeholders have access to these policy statements.

C. The statements are used to set expectations and build trust as they are fulfilled.

D. The policy statements are enhanced, as appropriate, when policy failures are detected.

Men's natures are alike, it is their habits that carry them far apart.

- Confucius

Well done is better than well said.

By failing to prepare, you are preparing to fail.

- Benjamin Franklin

4.2 Policy Deployment

Purpose

2 - GOVERNMENT: This recommendation calls on governments to put into practice what they say in their policy statements.

2 - BUSINESS: This recommendation calls on businesses to put into practice what they say in their policy statements.

2 – OTHER ORGANIZATIONS: This recommendation calls on other organizations to put into practice what they say in their policy statements.

Background

Trust is impossible if words are not backed up with actions.[180] Stated policies have a limited tangible value in communicating beliefs and principles.[181] The tangible value is generated when policies are actually implemented.

Implementation of policies is never perfect; it takes time and furthermore, requires continuous attention and maintenance over time.

Section 5 *Best Practices*, provides voluntary Best Practices that serve as examples of the kinds of countermeasures that organizations can put in place to fulfill stated policy objectives. In this case, the voluntary Best Practices are providing guidance for dealing with rogue members in its midst.

The level of detail of policy deployment plans provided to stakeholders depends on the situation and may range from very limited and at a high level (e.g., "a revised plan has been implemented to address policy deployment failures identified in the field.") to being very granular and specific (e.g., mentioning the name of the person responsible for specific tasks). In general, it is expected that providing more details helps build trust and confidence by conveying that specific appropriate actions are being taken and accountability established. However there are trade-offs and the organizations involved should make determinations based on the sensitivity of the information and feedback of critical stakeholders. Ultimately, it is the experience

[180] Key Observation No. 65, *Alignment of Words and Actions*, Section 3.3.
[181] Key Observation No. 66, *Repeating Trust – Cooperation Cycle*, Section 3.3.

and observations of affected stakeholders that will be the most significant assessment of the effectiveness of Policy Deployment plans and execution.

Can a stakeholder trust a government, company or other organization? Maybe they should or maybe they should not. A second sanity check is to examine the plans to implement their Stated Policy. Policy Deployment is the second key step of managing trust. This recommendation has three versions – one each for government, business and other organizations.

RECOMMENDATION 2 – GOVERNMENT

Governments should develop a policy deployment plan to enact their stated policies for their behavior in cyberspace, apply the necessary resources to implement the plan, and make adjustments to the plan when feedback is received that indicates a need for improvement.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Governments must develop plans that will be effective in implementing their policy commitments for their behavior in cyberspace.
- ☐ Governments must provide the necessary resources to implement these plans.
- ☐ Governments must apply the resources to implement the plans.
- ☐ Governments must receive corrective feedback when presented that indicates a policy deployment failure.

RECOMMENDATION 2 - BUSINESS

Businesses should develop a policy deployment plan to enact their stated policies for their behavior in cyberspace, apply the necessary resources to implement the plan, and make adjustments to the plan when feedback is received that indicates a need for improvement.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Businesses must develop plans that will be effective in implementing their policy commitments for their behavior in cyberspace.
- ☐ Businesses must provide the necessary resources to implement these plans.
- ☐ Businesses must apply the resources to implement the plans.
- ☐ Businesses must receive corrective feedback when presented that indicates a policy deployment failure.
- ☐ Governments must remove barriers from businesses to engage stakeholders on this subject.

RECOMMENDATION 2 – OTHER ORGANIZATIONS

Organizations should develop a policy deployment plan to enact their stated policies for their behavior in cyberspace, apply the necessary resources to implement the plan, and make adjustments to the plan when feedback is received that indicates a need for improvement.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Organizations must develop plans that will be effective in implementing their policy commitments for their behavior in cyberspace.
- ☐ Organizations must provide the necessary resources to implement these plans.
- ☐ Organizations must apply the resources to implement the plans.
- ☐ Organizations must receive corrective feedback when presented that indicates a policy deployment failure.
- ☐ Governments must remove barriers from organizations to engage stakeholders on this subject.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- o Do nothing . . . *expecting that policy statements will be sufficient to accomplish their realization.*
- o Develop a plan, but with ineffective methods . . . *resulting in wasted resources and disappointing performance when the policy is not realized.*
- o Take too long to develop a plan . . . *resulting in delayed deployment and postponed results.*

Benefits

The direct benefit of policy deployment is achieving the results of the stated policy. In addition, the implementation of this recommendation will increase confidence of stakeholders in the seriousness of the policy statements made, enabling trust to grow in critical relationships. In addition, the development and deployment of policy plans will strengthen the maturity of those involved with both policy development as they will realize the practical implications associated with achieving stated goals.

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

2-1 Organizations study existing methods and best practices for achieving the stated objectives.

2-2 Organizations draft a policy deployment plan with sufficient detail to demonstrate that key objectives will be met.

2-3 Organizations implement the policy deployment plan.

2-4 Organizations establish a method of receiving feedback from policy deployment failures in order to make adjustments to the plan or record that will prevent such incidents or ameliorate their impact should they occur again.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Organizations develop a policy deployment plan.

B. Organizations implement their policy deployment plans.

C. Organizations achieve their stated policy.

D. Organizations take corrective actions to improve policy deployment plans when feedback on policy deployment failures is received.

In God we trust, all others must bring data.

- William Edwards Deming

Honest scales and full measure hurt no one.

- Ancient Chinese Proverb

Be not ashamed of mistakes and thus make them crimes.

- Confucius

4.3 Performance Evaluations

Purpose

3 - GOVERNMENT: This recommendation calls on stakeholders to measure the performance of government policy deployments.

3 - BUSINESS: This recommendation calls on stakeholders to measure the performance of business policy deployments.

3 - OTHER ORGANIZATIONS: This recommendation calls on stakeholders to measure the performance of organization policy deployments.

Background

Ideally, policies could be implemented in a straightforward fashion and solve the problems they are intended to address forever. However in the real world, there are many obstacles to policy deployment. Some of these obstacles are known and can be planned for, while others are latent, only to be realized through experience.[182] Naturally, those affected by Policy Deployment failures may be the first to detect them.[183] Thus stakeholders are needed to play an active, constructive role in evaluating the performance of policies and Policy Deployment plans.

On one hand, because the implementation of policies is never perfectly practiced, stakeholders should not be overly sensitive to occasional failures. This is tempting because such failures could provide much fuel for political grandstanding. In fact learning about the policy deployment failures sooner is generally better than finding out later. Therefore, proactive measurement of their performance should be planned for and encouraged.

On the other hand, frequent policy implementation failures should lead to concerns that the Stated Policy is not a serious commitment, or that the Policy Deployment plan is fundamentally flawed or lacks discipline in execution. Performance Evaluation is the ultimate test within the Total Trust Management system.

[182] Key Observation No. 42, *Cybersecurity Brings the Influence of Insidious Interests*, Section 3.2.
[183] Key Observation No. 61, *Varied Responsibility for Response to Hacking Behavior,* Section 3.3.

Key stakeholders of a government, business or other organization's policy, should conduct Performance Evaluations. In addition, the government, business or other organization issuing the policy should also conduct Performance Evaluation of its Policy Deployment. When appropriate, a third party may be an ideal resource for conducting this assessment. Third parties may have competencies and objectivity that is desirable in some circumstances.[184]

Measuring is an essential aspect of improving. It is hard to improve without learning of failures and it is likewise hard to confirm an improvement without comparisons over time. The first part of learning is detecting an incident. Thus stakeholders should be an integral part of this process precisely because they are best able, in many situations, to detect incidents. Exactly what should be measured will depend upon the policy. Some policies will lend themselves to more obvious forms of evaluation, while others will require considerable thought. There will be opportunities for consensus development around forms of Performance Evaluation.

Can a stakeholder trust a government, company or other organization? Maybe they should or maybe they should not. A third, and most significant by far, sanity check is to examine the performance of their policy in the field. Performance Evaluation is the third key step of managing trust. There are three versions of this recommendation (i.e. government, commercial, other organization).

RECOMMENDATION 3 – GOVERNMENT

Stakeholders of governments should periodically evaluate the organizations' behaviors in cyberspace relative to their stated policies, and provide constructive feedback to the evaluated organizations.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Stakeholders must follow through in reporting detected failures of the deployed policies of governments.
- ☐ Stakeholders must be willing to proactively measure the performance of the policy deployments of governments.
- ☐ Stakeholders must be willing to proactively report the performance of the policy deployments of governments.
- ☐ Governments should actively seek to measure the performance of their policy deployment.

RECOMMENDATION 3 - BUSINESS

Stakeholders of the products and services of businesses should periodically evaluate the organizations' behaviors in cyberspace relative to their stated policies, and provide constructive feedback to the evaluated organizations.

Required Commitments

[184] *Cybersecurity Brings the Influence of Insidious Interests,* supra n 182.

The effective implementation of this recommendation will require the following commitments:

- ☐ Stakeholders must follow through in reporting detected failures of the deployed policies of businesses.
- ☐ Stakeholders must be willing to proactively measure the performance of the policy deployments of businesses.
- ☐ Stakeholders must be willing to proactively report the performance of the policy deployments of businesses.
- ☐ Businesses should actively seek to measure the performance of their policy deployment.
- ☐ Governments must remove barriers from businesses to support such cooperation.

RECOMMENDATION 3 – OTHER ORGANIZATIONS

Stakeholders of organizations should periodically evaluate the organizations' behaviors in cyberspace relative to their stated policies, and provide constructive feedback to the evaluated organizations.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Stakeholders must follow through in reporting detected failures of the deployed policies of organizations.
- ☐ Stakeholders must be willing to proactively measure the performance of the policy deployments of organizations.
- ☐ Stakeholders must be willing to proactively report the performance of the policy deployments of organizations.
- ☐ Organizations should actively seek to measure the performance of their policy deployment.
- ☐ Governments must remove barriers from organizations to support such cooperation.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- o Pay special attention to occasional incidents that become escalated . . . *accepting uncertainty regarding the effectiveness of the policy statement and policy deployment plan.*
- o Have overly burdensome measurement requirements . . . *taking on unnecessary costs with minimum return on investment.*
- o Do nothing . . . *accepting uncertainty regarding the effectiveness of the policy statement and policy deployment plan, and most likely, leaving performance evaluation left to journalists' and opponents' subjective assessments.*

Benefits

The implementation of this recommendation will provide an organization and its stakeholders with feedback on how its policy is actually being carried out "in the field." Having measurements of performance increases the intelligence of an organization overall. It also provides early insight into trends that may be emerging; giving an opportunity for early corrective action that can help avoid unnecessary

escalations and damages. Critical for the China-U.S. relationship, it can provide evidence of success or failure in key areas where expectations are set.[185]

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

3-1. Organizations identify potential sources that are capable of objectively detecting policy failure.

3-2. Stakeholders of policy statements prepare to observe the effectiveness of the stated policy.

3-3. Organizations engage potential sources to evaluate the feasibility and objectivity of utilizing their observations for policy deployment performance measurement.

3-4. Organizations and stakeholders select a method of evaluating policy performance that accounts for statistical and similar considerations.[186]

3-5. Stakeholders provide data to the respective organizations.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Stakeholders of an organization's policy are identified.

B. Stakeholders detect policy and policy deployment failures.

C. Stakeholders objectively measure policy and policy deployment failures.

D. Stakeholders objectively report incidents and measurements of policy and policy deployment failures.

E. Stakeholders institutionalize a sustained effort to conduct above functions.

F. Organizations receive the reports of incidents reported from stakeholders.

[185] Key Observation No. 68, *Repeating Trust – Cooperation Cycle*, Section 3.3.
[186] For example, if incident frequency is low, i.e. incidents are rare events, there may be variations (3 incidents this year compared to 1 incident last year) that do *not* indicate a trend, but rather are representative of expected fluctuation. It is critical in such situations to avoid overreactions to misinterpreted trends.

To see what is right, and not to do it,

is want of courage or of principle.

- Confucius

My great concern is not whether you have failed,
but whether you are content with your failure.

- Abraham Lincoln

4.4 Corrective Action

Purpose

4 - GOVERNMENT: This recommendation calls on governments to take corrective action to improve policies and policy deployment plans when either fails.

4 - BUSINESS: This recommendation calls on businesses to take corrective action to improve policies and policy deployment plans when either fails.

4 - OTHER ORGANIZATIONS: This recommendation calls on other organizations to take corrective action to improve policies and policy deployment plans when either fails.

Background

The first three recommendations have started the trust management process by setting expectations through Stated Policy, and then Policy Deployment transformed the words of policies into tangible realities and then Performance Evaluations were made to capture failures that affect stakeholders. The fourth and final step of the trust management process is Corrective Action, which is about making use of the available feedback to create countermeasures to (i) prevent future similar incidents as the reported failures or, (ii) should they occur again, ameliorate their impact.[187]

Corrective Action is hard work.[188] The key elements of effective Corrective Action are (a) making use of the available insights provided by failures, (b) generating effective countermeasures to address the observed failures, (c) the receptivity for change of the policy development and policy implementation planning teams, and (d) the proficiency to manage changes, which includes knowledge transfer and tracking the implementation of specific new practices.

In addition to feedback of failures from stakeholders, Corrective Action should also seek to be informed by internal monitoring capabilities. Ultimately, the Policy Deployment planning capability should benefit from a self-motivated, continuous improvement mindset that is informed by performance evaluations and other feedback from stakeholders as well as from internal monitoring.

Corrective action is always the goal but it may not always be visible. While how an organization openly responds to incidents of Stated Policy or Policy Deployment failures is an indicator of trustworthiness,

[187] Key Observation No. 66, *No Substitute for Corrective Action*, Section 3.3.
[188] Key Observation No. 60, *An Uphill Path to Improve the Harmful Hacking Situation*, Section 3.3.

what is most important in building trust is that corrective action is taken to prevent or ameliorate future, similar failures.

Can a stakeholder trust a government, company or other organization? Maybe they should or maybe they should not. A fourth sanity check is to examine the organization's response to incidents of failure. Corrective Action is the fourth key step of managing trust. This recommendation is presented here in three versions, for government agencies, businesses and other organizations, respectively.

RECOMMENDATION 4 – GOVERNMENT

Governments should receive and act on feedback from stakeholders that evaluates their behaviors relative to stated policies, making appropriate adjustments to policies or policy deployment plans to prevent the classes of failures observed, or ameliorate their impact should they occur again.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Governments must be receptive to both internal and external feedback on their behavior in cyberspace.
- ☐ Governments must be committed to respond with corrective action when behaviors are detected that are not aligned with their policies.

RECOMMENDATION 4 - BUSINESS

Businesses should receive and act on feedback from stakeholders that evaluates their behaviors relative to stated policies, making appropriate adjustments to policies or policy deployment plans to prevent the classes of failures observed, or ameliorate their impact should they occur again.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Businesses must be receptive to both internal and external feedback on their behavior in cyberspace.
- ☐ Businesses must be committed to respond with corrective action when behaviors are detected that are not aligned with their policies.

RECOMMENDATION 4 – OTHER ORGANIZATIONS

Organizations should receive and act on feedback from stakeholders that evaluates their behaviors relative to stated policies, making appropriate adjustments to policies or policy deployment plans to prevent the classes of failures observed, or ameliorate their impact should they occur again.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Organizations must be receptive to both internal and external feedback on their behavior in cyberspace.
- ☐ Organizations must be committed to respond with corrective action when behaviors are detected that are not aligned with their policies.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Deny the reality of objectively reported of Stated Policy or Policy Deployment failures . . . *missing the improve effectiveness of policy deployment and missing opportunities to build trust.*
- Accept the reality of reported incidents, but do nothing . . . *accepting internal and external assessments of problems in policy realization, the loss of confidence as problems go unaddressed, and the likelihood of repeated similar incidents.*
- Have an arm's length engagement with feedback . . . *missing the opportunity for maximum learning for how to be more effective.*
- Take partial corrective action, focusing solely on countermeasures that can prevent similar future incidents . . . *missing opportunity to consider how to ameliorate the impact of future similar events.*
- Take partial corrective action, focusing solely on countermeasures that can ameliorate the impact of similar future incidents . . . *missing opportunity to consider how to prevent the occurrence of future similar events.*

Benefits

The implementation of this recommendation will enable organizations to continuously improve the quality of their policies and policy deployment strategies and methodologies. In the China-U.S. relationship, trust will be built each time one country sees the other taking corrective action to correct a policy or policy deployment deficiency.

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

4-1. Organizations establish capability to receive reports of policy and policy deployment failures.

4-2. Organizations develop capability to research best practices for addressing reported policy and policy deployment failures.

4-3. Organizations develop a process for developing and testing countermeasures to address reported policy and policy deployment failures and track their implementation.

4-4. Organizations track the effectiveness of applied countermeasures.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Organizations receive reports of policy and policy deployment failures.

B. Organizations develop effective countermeasures to address reported policy and policy deployment failures.

C. Organizations apply effective countermeasures to address reported policy and policy deployment failures.

D. Organizations track countermeasure application status.

E. Organizations measure the effectiveness of countermeasures applied to address specific failures.

Labor to keep alive in your breast

that little spark of celestial fire, called conscience.

- George Washington

4.5 Separate Critical Humanitarian Assets

Purpose

This recommendation calls on government agencies, businesses and other entities with humanitarian interests and operations in cyberspace to separate their assets from those that are national security-related.

Background

This report seeks to discourage any harmful hacking to any interests, but history and reality suggest that national security functions and commercial interests will continue to be targets for espionage and crime.[189] Since humanitarian assets should be of less interest to all but the least ethical hackers than other interests, and since they serve important functions for people, there is an opportunity to achieve some special protection for these interests.[190] Specifically, logical or physical separation from likely targets could reduce the danger they are exposed to.

Purely humanitarian interests (i.e. medical, cultural and spiritual), which have no commercial or security components, are most readily agreed to as deserving special protection in society, and thus in cyberspace (Figure 7, *Landscape of Interests in Cyberspace*).[191] Historically, this observation is well founded in international law.[192] The Geneva and Hague Conventions of war provide protections for purely humanitarian critical infrastructure (e.g., hospitals, cultural and spiritual entities). Requirements for implementing this protection in the physical world can be carried forward into cyberspace.[193] Key aspects of this protection are establishing the legitimacy of such entities, designating the same and then the separation of the associated assets. The separation may be physical or logical, as appropriate.

Implementation of Recommendations 1 through 4 would go a long way towards enabling an entity to establish itself as having purely humanitarian interests and likewise having practices for the use of its assets in cyberspace that are consistent with such interests.[194] When a failure in practice occurs, there is swift correction made to policy deployment practices to ensure the necessary integrity between stated policies and practices. Separation may be problematic as the entanglement in cyberspace can be quite extensive.[195] It is essential that both physical and logical separation, as well as combinations of both, be considered for feasibility and effectiveness. The objective is to make it easier for those hackers who have regard for humanitarian interests to be able to avoid their assets.[196]

[189] Key Observation No. 50, *Suspecting Espionage*, Section 3.2; Key Observation No. 64, *National Security Functions Are Conventional Targets for Espionage*, Section 3.2.
[190] Key Observation No. 37, *Hacking May Lead to War*, Section 3.2.
[191] Key Observation No. 63, *Humanitarian Interests Deserve Special Protection from Hacking*, Section 3.3.
[192] Schmitt, Michael, N., *Tallinn Manual on the International Law Application to Cyber Warfare*, Cambridge University Press, 2013.
[193] Ibid.
[194] *Humanitarian Interests Deserve Special Protection from Hacking*, supra n 191.
[195] Joint Observation 1: Protected and nonprotected critical infrastructure entities are intermingled in cyberspace. Rauscher, Karl Frederick and Korotkov, Andrey, *Russia-U.S. Bilateral on Critical Infrastructure Protection - Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace,* EastWest Institute, February 2011, pp 20-22.
[196] Joint Observation 3: Discrimination between military and civilian targets is more difficult in cyberspace. Ibid.

RECOMMENDATION 5

Humanitarian organizations that are recognized as protected in the physical world by international humanitarian law, should separate their assets from other infrastructure in cyberspace to the greatest extent reasonably feasible.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Humanitarian organizations must seek means of being distinguished in cyberspace.
- ☐ Humanitarian organizations must seek information and communications technology (ICT) options that provide logical and physical separation from national security interests or dual-use entities, which are at a higher risk for hacking.
- ☐ Humanitarian organizations must implement solutions for the ICT needs that provide separation, as appropriate.
- ☐ Governments must assist humanitarian organizations pursuing disentanglement of their assets from other infrastructure in cyberspace.
- ☐ Businesses that provide ICT products and services must assist humanitarian organizations pursuing disentanglement of their assets from other infrastructure in cyberspace.
- ☐ Chinese government agencies, commercial and other entities without protected humanitarian interests must respect the separation being sought by humanitarian interest organizations.
- ☐ U.S. government agencies, commercial and other entities without protected humanitarian interests must respect the separation being sought by humanitarian interest organizations.
- ☐ Commercial entitites providing ICT equipment and services must provide options for humanitarian interest organizations.
- ☐ Non-humanitarian organizations should not pretend to be humanitarian organizations in cyberspace.[197]

Alternatives and Their Consequences

Alternatives to this approach include the following:

- o Continue on the current path where humanitarian, commercial and national security interest entities are entangled without distinction in cyberspace . . . *placing humanitarian interests in unnecessary risk of being hacked.*
- o Government, commercial and other organization without protected humanitarian interest status misuse the designation intended for humanitarian interest protection . . . *corrupting the integrity of the distinguishing method and as a result placing humanitarian interests at unnecessary risk of being hacked.*

Benefits

The implementation of this recommendation will enable more optimum protection of purely humanitarian interests in cyberspace. The implementation of this recommendation by China and the United States will

[197] Key Observation No. 65, *Alignment of Words and Actions*, Section 3.3.

break ground in the emerging field of rules of the road for cyberspace. The steps involved in ongoing dialogue and the practice of this recommendation also will open up new opportunities for healthy cooperation in cyberspace. The recommendation also will help to preserve civilization's hard won, and cherished, agreements around protecting purely humanitarian interests.[198]

In addition, the implementation of this recommendation may deter malicious hackers, who will not have the excuse that collateral damage was unintended or unavoidable.

Next Steps

Suggested next steps that will generate and maintain the momentum for the implementation of this recommendation include the following:

5-1. Humanitarian organizations research options for disentangling their assets and services in cyberspace.

5-2. Government and commercial organizations support humanitarian organizations' efforts to disentangle their assets and services in cyberspace.

5-3. Humanitarian organizations implement solutions that provide logical and physical separation, as appropriate.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Humanitarian assets are distinguishable in cyberspace.

B. Humanitarian assets are separated in cyberspace, as appropriate.

C. Ongoing efforts are made to avoid future entanglement of humanitarian assets in cyberspace.

[198] *Geneva Convention, The, The Geneva Conventions of 1949 and their Additional Protocols*, Geneva. *Geneva Protocol, The; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare*, Geneva, 1925. *Hague Convention, The Hague Convention of 1899 and 1907* The Hague.

Blame yourself as you blame others; forgive others as you forgive yourself.
- Ancient Chinese Proverb

4.6 De-Clutter Espionage Expectations

Purpose

This recommendation calls on government, commercial or other entities with national security missions, to acknowledge their reservation of rights to conduct international espionage, and accept the higher risk of international espionage when doing so.

Background

This report emphasizes that all harmful hacking should be discouraged.[199] However, recognizing that there is no commonly accepted international law against espionage, intelligence and defense agencies feel empowered to conduct such activities.[200] In the intelligence field, it is accepted that espionage is necessary. Yet, given that cyberspace is unlike the physical world and hacking can have significant inadvertent effects, technical experts participating in this study urge great caution for any operation carried out by such agencies, given the possibility that widespread harm could be caused by hacking operations.[201]

Governments, companies and other organizations decry compromises of their cyber assets and sometimes even go so far as to specify which countries they blame for incidents.[202] This is understandable as financial loss may occur, intellectual property may be taken, damage done, lives can be put in danger or other harms inflicted.[203] However, the current discussion is unnecessarily muddied when no distinction is drawn between those types of entities that are humanitarian and commercial in interest and operation in cyberspace, and those whose interests and operations are national security-oriented.[204] The later, have for thousands of years, been understood to be legitimate targets of espionage.[205] Thus commercial companies and other organizations whose interests and operations are humanitarian and commercial are endangered when they are associated with 'legitimate' targets of espionage.

Complaints about espionage targeted against government defense institutions and the military industrial complex should be parsed separately from those against humanitarian and commercial entities.[206]

[199] Key Observation No. 11, *Many Damages from Hacking*, Section 3.1.
[200] *Suspecting Espionage*; *National Security Functions Are Conventional Targets for Espionage*, supra n 189.
[201] Systems are often interconnected with each other, malicious code can spread very rapidly, malicious code can spread indiscriminately, a wrong reaction can occur as it is easier for a malicious actor to cloak his identity, a hacker could accidently 'trip' and trigger an unintended consequence. Key Observation No. 23, *The Trade-off for Covert Operations*, Section 3.1. Key Observation No. 28, *Cyber Crime Laws – Overview*, Section 3.1; Key Observation No. 30, *The Military Puts an Unexpected Color on a Cyberspace 'Domain'*, Section 3.1.
[202] Key Observation No. 18, Returning Rebukes, Section 3.1.
[203] *Many Damages from Hacking,* supra n 199.
[204] Key Observation No. 63, *Humanitarian Interests Deserve Special Protection from Hacking*, Section 3.3; Key Observation No. 64, *National Security Functions Are Conventional Targets for Espionage*, Section 3.3.
[205] Key Observation No. 50, *Expecting Espionage*, Section 3.2.
[206] Ibid.

RECOMMENDATION 6

Government and other entities who perform national security-related functions should acknowledge that they are widely recognized as acceptable by their nature as targets in cyberspace for the long-established practice of espionage.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Government and other entities who perform national security-related functions must accept that their nature elevates, and distinguishes them, as target for international espionage.
- ☐ Government and other entities who perform national security-related functions must refrain from mixing their status with that of purely humanitarian and commercial interests.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Continue to make statements as if hacking into a national security entity is basically the same as hacking into a commercial or humanitarian entity . . . *and risk appearing to be disregarding or ignoring the historically accepted practice of espionage in the realm of national security interests, and deny commercial and humanitarian interests the elevated legal protections they should enjoy.*[207]
- Defend and even further proliferate the current practice of mixing condemnations of hacking national security entities with hacking of other interests (e.g., humanitarian and commercial) . . . *opening those making such charges to claims of hypocrisy should the condemning party be exposed itself as conducting national security espionage in cyberspace, resulting in further deteriorated trust.*
- Overstate the acceptability of hacking into national security entities . . . *giving a false impression that such activity is safe and will not be punished to the full extent of the local jurisdictional laws.*

Benefits

The implementation of this recommendation will bring much needed clarity to discussions about the unacceptability of hacking. A more clear focus will enable bilateral agendas to be more realistic. A sense of outrage will be more proportionally applied when humanitarian and commercial interests are compromised in cyberspace. Longstanding protections for purely humanitarian infrastructure will be preserved and extended into cyberspace.

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

6-1. Organizations with national security interests recognize their status as being historically recognized legitimate targets of espionage and, thus, by extension, in cyberspace, as well.

[207] It is generally accepted that there are no international laws prohibiting espionage.

6-2. Organizations with national security interests avoid statements that equate hacking into their systems with hacking into organizations with purely humanitarian or purely commercial interests.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. National security organizations accept their status as distinct from humanitarian and commercial organizations.

B. Condemnations of hacking into national security interests recognize the distinctions between national security interests and purely humanitarian interests.

C. Condemnations of hacking into national security interests recognize the distinctions between national security interests and commercial interests.

D. The media and general public are educated on the distinctions between hacking into organizations with national security interests and organizations with purely humanitarian or commercial interests.

I mistrust the judgment of every man

in a case in which his own wishes are concerned.

- Daniel Webster

Am I not destroying my enemies when I make friends of them?

- Abraham Lincoln

4.7 Summon a Roundtable of Objective Subject Matter Experts

Purpose

This recommendation calls for a joint team of trusted subject matter experts to collaborate in order to provide objective assessments of the overall situation between China and the U.S., as it develops and for specific incidents of exceptional interest.

Background

For China and the United States to accomplish a dramatic turn around with the harmful hacking problem, some striking decisions must be made.[208] One of these decisions is to ensure that the optimum assets are available and being applied. The assets best suited for the tasks ahead are primarily in the categories of:

- the best individuals
- the best tools
- the best data[209]

The latter two items can be obtained on a case-by-case basis with the affected organizations and associated network operators.[210] The first item, however, must be pursued with a firm resolve, as it is uniquely difficult to achieve.[211] The optimum team consists of joint representation (Chinese and American), with required core competencies (advanced technical analysis, innovation in problem solving, international law, etc.) and unquestioned objectivity.[212] The most difficult aspect is the last, as many potentially qualified individuals may be employed by companies that have vested interests in the outcomes or government agencies with conflicting political interests.[213]

The objective is to attract the best minds from both countries.[214] The primary value proposition for these exceptionally talented individuals is the opportunity to collaborate with similar peers who are at 'the top of

[208] Key Observation No. 60, *An Uphill Path to Improve the Harmful Hacking Situation,* Section 3.3; Key Observation No. 74, *Surface Tension Barrier for Technical Cooperation*, Section 3.3.
[209] Key Observation No. 56, Investigation of Cross-Border Attacks Usually Requires Joint Cooperation, Section 3.2.
[210] Data provided for analysis will need to comply with applicable data protection and privacy laws.
[211] Key Observation No. 54, *CERT-CERT Cooperation is Lacking*, Section 3.2; Key Observation No. 55, *Practical Collaboration is Hindered by Visa Screening*, Section 3.2; Key Observation No. 43, *Politics Influences Cooperation for the Hacking Problem*, Section 3.2; Key Observation No. 44, *Reluctance to Cooperate on Combating Hacking Is Reinforced by Distrust*, Section 3.2; Key Observation No. 45, *West Cautious of East*, Section 3.2; Key Observation No. 46, *East Cautious of West*, Section 3.2; Key Observation No. 79, *More Open Markets Will Naturally Facilitate Cooperation in Technical Communities*, Section 3.3.
[212] Key Observation No. 75, *Real Problem Solvers Needed*, Section 3.3; Key Observation No. 42, *Cybersecurity Brings the Influence of Insidious Interests*, Section 3.2.
[213] Key Observation No. 42, *Cybersecurity Brings the Influence of Insidious Interests*, Section 3.2.
[214] Key Observation No. 73, *Science Diplomacy*, Section 3.3.

their game' on the most challenging and high-consequence issues.[215] It is envisioned that participation in the roundtable would be a part-time activity. Given the premium value of such individuals' time, in some circumstances, the participants will require the support of their affiliated organizations (universities, companies, non-government organizations). There may also be a need for funding to cover time and travel, however the source of funding for this activity must also avoid conflicts of interest, both real and perceived.[216]

RECOMMENDATION 7

Chinese and American subject matter experts who are qualified as having the highest caliber command of advanced cyber forensics and who are vetted as being free of commercial and political conflicts of interest, should serve jointly on a roundtable forum to provide objective evaluations of the situation between China and the United States, as it develops, and to provide expertise, objectivity, and stability during escalated incidents.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Qualified subject matter experts from China must step up to serve in the capacity of an objective analyst.[217]
- ☐ Qualified subject matter experts from the United States must step up to serve in the capacity of an objective analyst.
- ☐ Qualified subject matter experts from China must apply their competencies to assess disputed dispositions.
- ☐ Qualified subject matter experts from the United States must apply their competencies to assess disputed dispositions.
- ☐ Qualified subject matter experts from China must make assessments of the status of the quality of stated policies, the effectiveness of policy deployment strategies, the performance of policies and policy deployment plans and the corrective actions.
- ☐ Qualified subject matter experts from the United States must make assessments of the status of the quality of stated policies, the effectiveness of policy deployment strategies, the performance of policies and policy deployment plans and the corrective actions.
- ☐ Qualified subject matter experts from both China and the United States must cooperate with each other in developing principles and practices of operation, conducting analyses, arriving at a level of consensus and making reports.
- ☐ Qualified subject matter experts from both China and the United States must avoid conflicts of interests, in reality and perception, while performing the above tasks.

[215] Open Communications and Sensible Cooperation is a shared 'common principle' for the technical community of both countries. Key Observation No. 14, *Common Principles*, Section 3.1; Key Observation No. 19, *A Window of Opportunity*. Section 3.1; Key Observation No. 32, *Flawed Practice of Engaging with Each Other*, Section 3.2; Key Observation No. 78, *More Interaction Online Between the Expertise of Two Side Can Achieve More Mutual Benefits*, Section 3.3; Key Observation No. 80, *Sharing Minimal Incident Data in Mutual Investigations Has Minimal Risk and Is Very Helpful,* Section 3.3.

[216] Key Observation No. 21, *Cybersecurity Is a Growing Market*, Section 3.1; Key Observation No. 22, *Funding Attracts Interest*, Section 3.1.

[217] The inclusion of qualified subject matter experts from other countries than China and the United States is a viable option.

- ☐ Qualified subject matter experts from both countries must obtain needed support to dedicate their time and cover associated travel costs.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- Continue on the current path . . . *accepting the assessments of the China-U.S. cybersecurity relationship by politicians, commercial firms specializing in cybersecurity products and services and journalists.*
- Create a similar collaborative effort populated with government employees . . . *accepting the potential for bias from the influences to which such individuals are exposed.*[218]
- Create a similar collaborative effort that is populated with employees of commercial organizations that specialize in cybersecurity products and services . . . *accepting the potential for bias from the influence to which such individuals are exposed.*[219]

Benefits

The implementation of this recommendation can provide a breakthrough in the China-U.S. relationship with regard to cybersecurity, resulting in a more accurate and trustworthy assessments of controversial incidents. Cooperation in sharing "missing puzzle pieces" to support analysis will have an immediate and direct impact on genuine trust building. Moreover, the substantive dialogue among these experts can help transform the current disposition from one of accusations and denials to honest reality.

Conversely, failure to cooperate in a proposed joint analysis likely will increase mutual suspicion. Thus the take away value in this situation is one of confirmed untrustworthiness, a clear value for the disappointed party.

This recommendation will also leverage science diplomacy, which is viewed as a more objective discipline; opening enormous potential for trust building on commonly arrived at conclusions.

Next Steps

Suggested next steps to generate and maintain the momentum for the implementation of this recommendation include the following:

7-1. "Roundtable:" A trusted entity is established with the objective to convene qualified trusted entities to conduct joint causes analyses of exceptional cybersecurity compromise incidents.[220]

7-2. "Cyber Knights:" Qualified subject matter experts are recruited to constitute the Roundtable.

7-3. Honor Code: A mutually agreed-upon set of principles is established for the behavior of individuals as well as for the whole.

[218] It is recognized here that all individuals have inherent loyalties that influence them. The distinction between the proposed recommendation and this alternative is a matter of degree. It is reasonable to predict that primary influencing characteristics of some individuals affect them in significant ways. That is, persons with interests that are vested in a government career (or compensation) will typically be exposed to influence that individuals without these interests are not exposed to.
[219] Ibid.
[220] This can be an existing entity that modifies its charter, or a new entity that with a new charter.

7-4. Modus Operandi: A mutually agreed-upon set of practices is established for the operation of the joint collaboration.

7-5. Pilot Study: A test case is designed and utilized for testing the drafted practices.

7-6. Rigor: Based on lessons learned from the test-case exercise, the practices are revised to strengthen effectiveness, as appropriate.

7-7. Standing Up: The joint team of subject matter experts begin to cooperate on analysis, come to consensus conclusions and make reports to stakeholders as agreed.

7-8. Continuous Improvement: Based on lessons learned, the team continues to improve its practices.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. A roundtable of subject matter experts is convened.

B. The roundtable of subject matter experts agrees on principles and practices.

C. The roundtable of subject matter experts commences its operations and produces trusted reports.

D. The China-U.S. relationship is improved through greater confidence in each other's genuine cooperation on cybersecurity concerns brought to each other's attention.

"I heard" is good; "I saw" is better.

- Ancient Chinese Proverb

Honesty is the best policy.

- Benjamin Franklin

4.8 Continuous Approach Status Indicator

Purpose

This recommendation calls for a provisional capability to provide a continuous objective indication of the status of the transition from instability to stability.

Background

In the aviation industry, it is well known that the most dangerous phases of a typical flight mission are the two periods of transition between air and ground, i.e., the take-off and the landing. For the later, it is critical that the pilot be able to confirm that speed and altitude during descent are within an acceptable range to avoid a disastrous miss of the runway by coming down too soon or too late. A Visual Approach Slope Indicator (VASI) is a system of lights on the side near the front of an airport runway that provides critical visual descent feedback and guidance information to a pilot during an approach to land an aircraft (Figure 22).

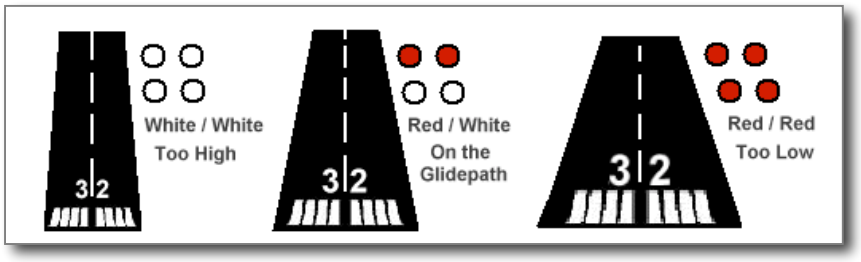


Figure 23. Visual Approach Slope Indicator (VASI) System

As China and the United States seek to transition the health of their relationship regarding harmful hacking from being too highly escalated and unstable to one grounded on shared principles, the VASI system is a highly useful analogy.[221] In this analogy, the landing strip is the *safe ground* – that small, special area where the China-U.S. relationship can find refuge and stability.[222] The parallel of aligning aircraft altitude with the runway is *aligning commitment levels with expectation levels* between countries.[223] The level of commitments must meet the level of expectations. Either the level of expectations or the level of

[221] Key Observation No. 14, *Common Principles*, Section 3.1.
[222] Key Observation No. 15, *Lack of Trust*, Section 3.1.
[223] Key Observation No. 65, *Alignment of Words with Actions*, Section 3.3.

commitments may be too high or too low.[224] The parameters for alignment are taken directly from the Total Trust Management Model (Figure 18):

Stated Policy

- Is the policy statement definition and clarity too low or too high?
- Is the policy statement aiming too low or too high in its commitments?

Policy Deployment

- Is the policy deployment plan detail too low or too high?
- Is policy deployment urgency too low or too high?
- Is policy deployment speed too low or too high?

Performance Evaluation

- Is the performance prioritized too low or too high?
- Is the integrity of the performance evaluation too low or too high?

Corrective Action

- Is the responsiveness of the corrective actions being taken too low or too high?
- Are the effectiveness of the corrective actions too low or too high?
- Is the priority of corrective actions too low or too high?

At present, the China-U.S. relationship with regard to cybersecurity is surmised to be deserving of a '**not aligned for a safe landing**' status assessment for each of the above four key components of the TTM (Figure 23).[225] This assessment is based on the fact that harmful hacking is a top priority issue on the presidential meeting agenda.[226] Hard evidence will be needed to adjust assessments to a status of safety.[227]

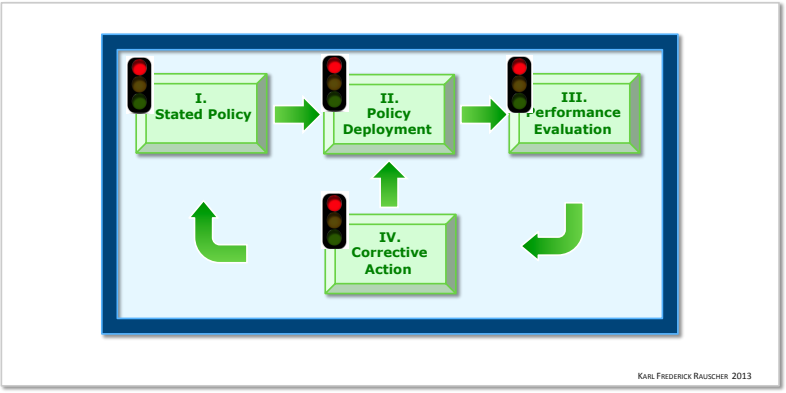


Figure 24. TTM with Traffic Lights.

[224] The natural tendency is for Party A's expectations for Party B to be considered to be reasonable by Party A, but too high by Party B; and, for Party A's commitments to Party B to be considered to be reasonable by Party A, but as too low by Party B.
[225] *Lack of Trust*, supra n 222; Key Observation No. 16, *Ever-Lower Expectations for Cooperation*, Section 3.1; Key Observation No. 18, *Returning Rebukes*, Section 3.1; Key Observation No. 24, *U.S. Behavior – Interpreted by Chinese Experts*, Section 3.1; Key Observation No. 25, *China Suspicions of U.S. Network Gear*, Section 3.1; Key Observation No. 26, *Previous Argument is Less Convincing*, Section 3.1; Key Observation No. 51, *Both Americans and Chinese See the Other as Source of Much Hacking*, Section 3.2.
[226] Key Observation No. 19, *A Window of Opportunity*, Section 3.1; Key Observation No. 20, *Government Working Groups Are Underway*, Section 3.1.
[227] See *DTOT Verification and Correction Loop*, Figure 14.

Another essential point to carry forward from the aviation analogy is that of *continuous feedback* during the critical transition period. The China-U.S. relationship on cybersecurity is at a perilous point, because if expectations are not being met, it is vital to know this immediately so that stakeholders are alerted to the current path not having a safe conclusion, and so that corrective action can be taken promptly.[228] As cybersecurity issues are constantly developing, the continuous 'hands on' monitoring is needed temporarily, until the "plane has safely landed."

The five basic elements of a Continuous Approach Status Indicator (CASI) are listed in the Next Steps further below.

RECOMMENDATION 8

China and the United States should stand up a joint provisional capability for continuous evaluation and status reporting based on stated policy, policy deployment, performance evaluation and corrective action.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ Qualified subject matter experts from China must be willing to serve on a joint provisional task force.
- ☐ Qualified subject matter experts from the United States must be willing to serve on a joint provisional task force.
- ☐ Qualified subject matter experts from the United States must be objective in the assessments they contribute to the joint provisional task force.
- ☐ Qualified subject matter experts from China must be objective in the assessments they contribute to the joint provisional task force.
- ☐ Chinese and U.S. subject matter experts must be willing to make a joint statement of joint health of the relationship.

Alternatives and Their Consequences

Alternatives to this approach include the following:

- o Continue to rely upon the rhetoric of politicians, the opinions of journalists and the messaging of commercial firms to define the health of the China-U.S. relationship regarding cybersecurity . . . *resulting suboptimum support for critical decision-making.*
- o Continue to update assessments of relationship health based on outputs of currently used modes (i.e., immediately above) . . . *resulting in randomly timed intervals.*
- o Create a unilateral relationship health measure that focuses only on the other party's failures . . . *squandering opportunity for trust building.*

[228] Key Observation No. 17, *Trust is a Watershed*, Section 3.1; Key Observation No. 34, *Repeating Distrust – Non-cooperation Cycle*, Section 3.2; Key Observation No. 37, *Hacking May Lead to War*, Section 3.2.

Benefits

The implementation of this recommendation for a CASI will yield a *more accurate* assessment of the status of the relationship than is provided today. A CASI will provide stakeholders with essential *feedback during the critical transition* period when both countries are expressing a willingness to cooperate. Stakeholders of the China-U.S. relationship can be aware of the *current* health status regarding cybersecurity, which is important given the speed at which technological and other developments take place in cyberspace. In addition, the daily contact of Chinese and American subject matter experts on specific critical areas of attention will leverage the untapped potential of the fundamentally more objective *science diplomacy*.

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

8-1. Personnel: A joint team is formed of subject matter experts capable of assessing the alignment status of each of the four components of the TTMM, each of whom is vetted as being objective, free of conflicting political or commercial interests.

8-2. Homework: The joint team conducts research of existing models where multilateral assessments are made for high consequence concerns, in order to determine if existing practice can be transferred.[229]

8-3. Information: The joint team is provided with access to non-public information, as appropriate, that is helpful assessing the status of the TTMM components.

8-4. Venue: A virtual means is set up for team members to collaborate daily.

8-5. Methodology: The team develops a mutually agreed upon method for assessing the alignment of each of the four TTMM components.

8-6. Reporting Framework: The team creates a mutually agreed upon structure and protocol for providing a continuous status.

8-7. Operation: The joint team implements the above elements and provides continuous report status to stakeholders.

8-8. Termination: The CASI capability is stood down once the China-U.S. relationship regarding cybersecurity is stabilized with stated policies, deployed policies, performance evaluations and corrective actions.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures.

A. A CASI capability is established.

B. A joint CASI assessment is made on the health of the relationship.

[229] Examples of potential study targets include United National chemical weapons inspectors, drug and law enforcement cooperation and radio frequency management.

C. A report is issued to stakeholders.

D. This assessment is used to inform critical government and industry decisions.

E. The CASI capability is available continuously.

F. The CASI capability is stood down once the relationship achieves a "healthy" status for an extended period of time. Alternatively, the capability could eventually be stood down if it is determined after an appropriate period of time that the relationship cannot progress out of its unhealthy status due to a lack of commitment from either party.

A fall into a ditch makes you wiser.

- Ancient Chinese Proverb

4.9 Prepare Sufficiently, React Quickly and Summarize Seriously

Purpose

This recommendation calls for the transformation of harmful hacking responses from being primarily reactive to pro-active, and includes setting goals that define sufficient preparation and response.

Background

In recent years, serious cyber attacks happened in not only China and the U.S., but also many other countries. Some of the response and handling of these incidents were successful, while most were not. The main reasons include:

- Insufficient investment into cybersecurity, including capital, human resources, etc.
- The mindset that an attack would be a fluke, makes people think they won't get attacked, or the loss is not large even though they are attacked.
- The existing designs and deployments of security protection systems are not effective enough. There is also a lack of sufficient staff, protection infrastructure, working processes and emergency response plans.
- The analysis of incidents is not carried out earnestly; neither is the discovery procedure for potential threats to security. As a result, few countermeasures are developed to improve the protection.
- On the contrary, hackers persevere at accumulating resources, finding targets and waiting for every chance to take advantage of a vulnerability. They launch attacks as soon as they find appropriate opportunities.

Hence, for the organization who has not prepared well, the response is typically hurry-scurry and full of chaos, which makes it easy for the hacker to succeed in escaping.

By analyzing the model of hacking, a better understanding is achieved of the hacker's methods of preparation, implementation and escape. These insights are used to design defensive countermeasures that are focused on each of these distinct phases.[230] This brings us to Recommendation No. 9.

RECOMMENDATION 9

Chinese and American cybersecurity professionals should shift their focus from one based on being at par with common practices for managing international incidents to a focus that is defined by (a) sufficient preparation, (b) timely response and (c) conclusive post-incident analysis.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

☐ Chinese and American cybersecurity professionals must abandon methods and tools that are not meeting their organizations' or clients' needs.

[230] Section 2.5.3.

- ☐ The cybersecurity industry must agree on benchmarks for performance for key areas like preparation, response and analysis.[231]
- ☐ Cybersecurity professionals must make use of industry performance benchmarks to evaluate and improve their approaches.
- ☐ Government agencies, businesses and other organizations must commit to funding cybersecurity products and services with proven abilities to achieve best-in-class performance benchmarks.

Alternatives and their Consequences

Alternatives to this approach include the following:

- Continue protection oriented around a passive response . . . *suffer from more losses than necessary.*
- Allow hackers to advance in sophistication at a faster rate than defenders . . . *and experience more successful attacks, causing greater inefficiencies in operations.*
- Rely on government regulation to solve the problem . . . *increasing inefficiency and possibly inviting unfunded mandates.*

Benefits

The implementation of this recommendation will improve an organization's protection in cyberspace. Attacks will become more difficult. In addition, users will benefit from continuous improvement.

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

9-1. As appropriate to the degree of trust, China and the U.S. share concepts on shifting the focus from common practices to the best practices for security protection performance for international incidents in terms of (a) sufficient preparation, (b) timely response and (c) conclusive post-incident analysis.

9-2. Government agencies, businesses and other organizations build more pro-active security protection systems.

9-3. As appropriate to the degree of trust, China and the U.S. cooperate on defining benchmarks for security protection system performance for international incidents.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. Security approaches are focused on sufficient preparation, timely response and conclusive post-incident analysis.

B. New policies and standards are developed to measure security performance.

C. Response capabilities are significantly enhanced.

D. Hacking is impeded in terms of having a raised cost and risk for hackers.

[231] Specific areas to be included are maintenance staff, security protection systems, routine security operation regulations, easy to control and feasible emergency response plan, internal control mechanisms, authentication and operation audition mechanism, capable of detecting cyber attacks, system backup and recovery, system logs for incident investigation, strict incident analysis, methods to improve security systems, security protection and emergency response handling.

A people free to choose will always choose peace.

- Ronald Reagan

4.10 Launch Parallel Bilateral Collaboration on Government and Industry Levels

Purpose

This recommendation calls for industry level collaboration to supplement the new cooperation undertaken at the governmental level. Industry technical expertise and business insights are required to combat the harmful hacking that is out of control.

Background

When cybersecurity problems are increasingly prominent, the voices calling for cooperation between China and the U.S. on cybersecurity grow louder. People expect that the governments of China and the U.S. can reach agreements and carry out more tangible cooperation. In recent years, people do see some progress, such as the founding of the China and U.S. joint working group on cybersecurity in 2013.[232] However the general progress of government-level cooperation is expected to be limited for many reasons. In particular the frequent blaming of each other makes cooperation difficult.

Meanwhile, with the rapid development of cyberspace, cross-border hacking is increasing, taking advantage of the lack of China-U.S. cooperation. Requests for assistance are conveyed to government departments via classic diplomatic channels with the hopes that problems can be solved successfully. But this takes a long period of time as a whole. Also, a great number of cross-border attacks have been successfully addressed by operators and organizations (like CERT) on both sides together. Because such cooperation is carried out at a technical level without involving legal and political processes, the speed of progress in such cooperation is very fast.

Since the mutual fundamental distrust between China and the U.S. will not be resolved any time soon, such a problem should not be allowed to be a precondition of moving forward. Rather, a pragmatic approach is to promote the non-government level cooperation for cybersecurity in parallel to the newly initiated government working groups. This brings us to Recommendation No. 10.

RECOMMENDATION 10

American and Chinese information and communications technology industries should supplement governmental cybersecurity working groups by establishing cooperation on concrete measures to address harmful hacking.

[232] Key Observation No. 20, *Government Working Groups Are Underway*, Section 3.1.

Required Commitments

The effective implementation of this recommendation will require the following commitments:

- ☐ The Chinese and U.S. governments must not block its ICT industry from pursuing this engagement.
- ☐ The Chinese and U.S. ICT industries must support cooperation with a critical mass of resources.
- ☐ The Chinese and U.S. ICT industries must be committed to concrete actions.
- ☐ Chinese and U.S. governments must enable subject matter experts to receive visas for the purpose of meeting with peers in each other's countries.

Alternatives and their Consequences

Alternatives to this approach include the following:

- o Continue with only government-level discussions . . . *be limited in solutions and speed.*
- o The influence of political factors further stifles cooperation . . . *making the present situation even worse.*

Benefits

The implementation of this recommendation is expected to facilitate better technical cooperation, in terms of competence and speed in response and analysis. Additional benefits will be to help foster better relationships at the government level for China and the U.S.

Next Steps

Suggested next steps that can generate and maintain the momentum for the implementation of this recommendation include the following:

10-1. The joint industry working groups are formed by a technically oriented neutral facilitator with an appropriate charter.

10-2. A goal is established for long-term cooperation with accountability for concrete measures.

10-3. Initial joint meetings are held with subject matter experts focusing on preparation, response and analysis performance for international incidents.

10-4. Mechanisms are established for briefing the respective government agencies of both countries.

10-5. CN-CERT and U.S.-CERT carry out more specific cybersecurity cooperation.

10-6. Internet operators and companies of both sides carry out concrete technical cooperation.

Measures of Success

The successful implementation of this recommendation can be gauged by the following measures:

A. The joint China-U.S. non-government, technically oriented group convenes regularly.

B. Concrete measures are defined and applied regularly.

C. The government level interactions are supported.

D. Harmful hacking is reduced.

Laws control a lesser person; right conduct controls a greater one.
- Ancient Chinese Proverb

Do you want to know who you are?
Don't ask. Act!
Action will delineate and define you.
- Thomas Jefferson

5. Voluntary Best Practices

This section presents 100 voluntary Best Practices for preventing hacking incidents or for ameliorating their impact should they occur. Governments, businesses and any other organizations operating in cyberspace can all apply these Best Practices. The Best Practices include techniques for ICT equipment and software suppliers, network operators, service providers, social networking enablers, financial services firms and government agencies.

As these voluntary Best Practices are one of several means of influencing organizational behavior, they provide a start for some organizations, depending on the specific policy statements, they implement in Recommendation 2, *Policy Deployment*. The development of additional Best Practices as envisioned by Recommendation 2 further enhances the utility of this initial list.

The format in which Best Practices are presented quickly conveys much information in an easy to understand way (Figure 24, *Best Practice Presentation*). For example, each Best Practice presentation includes a unique identification, shown in the upper left hand corner. Each Best Practice also has a unique title that summarizes its core focus. In order to quickly identify the applicability of each Best Practice, the format includes a color code of the associated ingredients. In addition, the lower left hand corner includes a designation of the types of entities for which the guidance applies. The descriptions of entity categories are repeated here from Section 2.4.1, *Core Interests*.

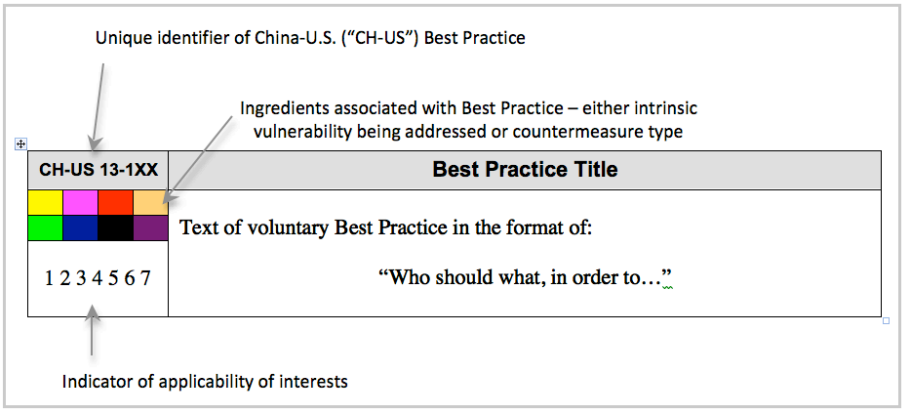


Figure 25. Best Practice Presentation.

Following is a repeated summary of the seven categories that are referenced in the Best Practices presentation.

- **Category 1 Entities: Humanitarian**
  Entities whose interests are purely humanitarian, are non-profit and who avoid taking part in any security function.

- **Category 2 Entities: Humanitarian + Commercial**
  Entities whose interests are humanitarian, are for-profit and who avoid taking part in any security function.

- **Category 3 Entities: Commercial**
  Entities whose interests are for-profit and who avoid taking part in any security function.

- **Category 4 Entities: Humanitarian + Commercial + Security**
  Entities whose interests are humanitarian, are for-profit and who perform a security function.

- **Category 5 Entities: Humanitarian + Security**
  Entities whose interests are humanitarian and who perform a security function.

- **Category 6 Entities: Commercial + Security**
  Entities whose interests are for-profit and who perform a security function.

- **Category 7 Entities: Security**
  Entities whose interests are only to perform a security function.

For some Best Practices, this document describes actors as "organizations with enhanced access to assets in cyberspace." This phrase refers to government, business or other organizations that have special capabilities that could give powerful access or leverage to individuals if used maliciously. Examples of this include communications network operators who have equipment that processes calls and data messaging; equipment suppliers who design and develop software and software with broad applications; and military or law enforcement unites with special training, access or equipment that enables them to perform offensive cyber operations.

Best Practices are organized into sections according to the phase of the Model of Hacking and Defense that they address (Figure 10). The fact that some sections have more Best Practices than others should only indicates that this is the start of a process. In the future, as sensible cooperation and mutual trust develop favorably, it is anticipated that more Best Practices will be issued from a joint team of objective subject experts (see Recommendation No. 7). In addition to those working on this joint cooperation capacity, other subject matter experts are encouraged to help refine those offered here and contribute to future Best Practices.

Table 22 provides an outline of each Best Practices, showing its relationship to the TTMM.

Table 21. Outline of Model of Hacking and Defense.

Hacking	Section	Defense
Preparation	5.1	Preparation
Implementation	5.2	Response
Escape	5.3	Follow-up

Table 22. Voluntary Best Practices Sorted by TTM Stage and Model of Hacking and Defense.

Hacking vs. Defense	Stated Policy	Policy Deployment	Performance Measurement	Corrective Action
Preparation Phases				
Curiosity	**CN-US 13-101**	**CN-US 13-102**	**CN-US 13-103**	**CN-US 13-104**
White Hat Reputation	**CN-US 13-105**	**CN-US 13-106**	**CN-US 13-107**	**CN-US 13-108**
Financial Rewards	**CN-US 13-109**	**CN-US 13-110**	**CN-US 13-111**	**CN-US 13-112**
Prosecution	**CN-US 13-113**	**CN-US 13-114**	**CN-US 13-115**	**CN-US 13-116**
Unauthorized Access	**CN-US 13-117**	**CN-US 13-118**	**CN-US 13-119**	**CN-US 13-120**
Harmful Hacktivism	**CN-US 13-121**	**CN-US 13-122**	**CN-US 13-123**	**CN-US 13-124**
Conflict Screening	**CN-US 13-125**	**CN-US 13-126**	**CN-US 13-127**	**CN-US 13-128**
Pure Humanitarian	**CN-US 13-129**	**CN-US 13-130**	**CN-US 13-131**	**CN-US 13-132**
Commercial	**CN-US 13-133**	**CN-US 13-134**	**CN-US 13-135**	**CN-US 13-136**
Gov. Collaboration	**CN-US 13-137**	**CN-US 13-138**	**CN-US 13-139**	**CN-US 13-140**
Security Team	**CN-US 13-141**	**CN-US 13-142**	**CN-US 13-143**	**CN-US 13-144**
Security System	**CN-US 13-145**	**CN-US 13-146**	**CN-US 13-147**	**CN-US 13-148**
Vulnerability Fixes	**CN-US 13-149**	**CN-US 13-150**	**CN-US 13-151**	**CN-US 13-152**
Incident Resp. Planning	**CN-US 13-153**	**CN-US 13-154**	**CN-US 13-155**	**CN-US 13-156**
Implementation and Response Phases				
Anomaly Monitoring	**CN-US 13-157**	**CN-US 13-158**	**CN-US 13-159**	**CN-US 13-160**
Timely Warning	**CN-US 13-161**	**CN-US 13-162**	**CN-US 13-163**	**CN-US 13-164**
Attack Blocking	**CN-US 13-165**	**CN-US 13-166**	**CN-US 13-167**	**CN-US 13-168**
Source Tracing	**CN-US 13-169**	**CN-US 13-170**	**CN-US 13-171**	**CN-US 13-172**
Clean-up Environment	**CN-US 13-173**	**CN-US 13-174**	**CN-US 13-175**	**CN-US 13-176**
Block Fake IP	**CN-US 13-177**	**CN-US 13-178**	**CN-US 13-179**	**CN-US 13-180**
Joint Analysis	**CN-US 13-181**	**CN-US 13-182**	**CN-US 13-183**	**CN-US 13-184**
Escape and Follow-up Phases				
Recover Business	**CN-US 13-185**	**CN-US 13-186**	**CN-US 13-187**	**CN-US 13-188**
Investigation	**CN-US 13-189**	**CN-US 13-190**	**CN-US 13-191**	**CN-US 13-192**
Incident Summary	**CN-US 13-193**	**CN-US 13-194**	**CN-US 13-195**	**CN-US 13-196**
Law Enforcement	**CN-US 13-197**	**CN-US 13-198**	**CN-US 13-199**	**CN-US 13-200**

5.1 Best Practices for the Preparation Phases of the Hacking and Defense

These voluntary Best Practices are developed for the *preparation phases* of hacking and defense (Figure 10). The first part of these Best Practices focuses on the motivation of a hacker. By understanding motivation, some hackers can be converted.[233]

The remaining Best Practices in this subsection deal with the resources necessary for performing hacks and are intended for organizations that have enhanced access to assets in cyberspace that could provide their members with opportunities to access private data, control the operation of assets or cause unintended consequences through activities undertaken in cyberspace. These practices essentially focus on risk control of inner abuse.

[233] Several companies have reported receiving assistance from hackers in the form of discovered coding errors. Individuals who would have previously exploited the find were now helping with the quality of their product, in return for a coding bug discovery fee. Notes from the interactive session on Non-State Actors, IEW-IEEE Third Worldwide Cybersecurity Summit, New Delhi, 2013.

Guide Curiosity in a Good Direction

A specific example is when a company provides a study and testing environment, including software, hardware and a network to those who have curiosity about hacking technology, to help individuals learn and develop their computer skills, which can enhance their career.

CN-US 13-101	Policies that Guide Curiosity in a Good Direction
1 2 3 4 5 6 7	Organizations should consider establishing policies that guide curiosity in a good direction, in order to replace existing motivations to hack for educational value.

CN-US 13-102	Policy Deployment that Guide Curiosity in a Good Direction
1 2 3 4 5 6 7	Organizations should implement comprehensive plans, including international cooperation aspects that guide curiosity in a good direction, to focus their interests in activities that are equally challenging but have a positive effect on society, in order to replace existing motivations to hack for educational value.

CN-US 13-103	Performance Measurement of Rewards – Curiosity
1 2 3 4 5 6 7	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans for guiding curiosity in a good direction, including international cooperation aspects, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-104	Corrective Action on Curiosity Policy and Deployment
1 2 3 4 5 6 7	Organizations should make use of performance feedback to make corrective actions to hacker curiosity policies and deployment plans, in order to improve the effectiveness of both.

White Hat Recognition

A specific example is when CNCERT provides certificates to individuals who discover and report a serious vulnerability to the supplier. The certificate will improve the peer recognition for the vulnerability discoverer.

CN-US 13-105	Policies for White Hat Recognition
1 2 3 4 5	Organizations should consider establishing policies to influence hackers to use their skills for good by recognizing valuable insights that can improve application, system or organization security, in order to replace existing motivations for peer recognition.

CN-US 13-106	Policy Deployment for White Hat Recognition
1 2 3 4 5	Organizations should implement comprehensive plans, including international cooperation aspects that influence hackers to use their skills for good by recognizing valuable insights that can improve application, system or organization security, in order to replace existing motivations for peer recognition.

CN-US 13-107	Performance Measurement of White Hat Recognition
1 2 3 4 5	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans for recognizing good hacker behavior, including international cooperation aspects, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-108	Corrective Action for White Hat Recognition Policy and Deployment
1 2 3 4 5	Organizations should make use of performance feedback to make corrective actions to white hat recognition policies and deployment plans, in order to improve the effectiveness of both.

Financial Rewards for Good Hackers

A specific example is when a company provides a financial reward to individuals who discover an application vulnerability and report it responsibly to the company that can fix it. This practice is in effect in both China (Alibaba, Tencent QQ) and America (Google, Microsoft).

CN-US 13-109	Policies that Reward Good Hacker Behavior - Financial
1 2 3 4 5 6	Organizations should consider establishing policies to influence hackers to use their skills for good by providing compensation for valuable insights that can improve application, system or organization security, in order to replace existing motivations for financial reward.

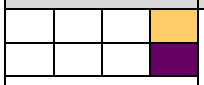
CN-US 13-110	Policy Deployment that Rewards Good Hacker Behavior - Financial
1 2 3 4 5 6	Organizations should implement comprehensive plans, including international cooperation aspects that influence hackers to use their skills for good by providing compensation for valuable insights that can improve application, system or organization security, in order to replace existing motivations for financial reward.

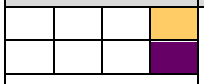
CN-US 13-111	Performance Measurement of Rewards - Financial
1 2 3 4 5 6	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans for rewarding good hacker behavior financially, including international cooperation aspects, in order to determine the effectiveness of the policies and deployment plans.

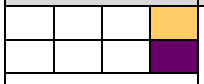
CN-US 13-112	Corrective Action on Financial Rewards Policy and Deployment
1 2 3 4 5 6	Organizations should make use of performance feedback to make corrective actions to financial reward policies and deployment plans, in order to improve the effectiveness of both.

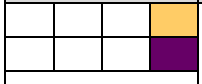
Prosecution of Harmful Hacking

A specific example is when a company prosecutes an individual responsible for harmful hacking in a civil court to recover damages.

CN-US 13-113	Policies that Prosecute Harmful Hacking
 1 2 3 4 5 6 7	Organizations should consider establishing policies that discourage hackers from using their skills to cause harm by prosecuting those who compromise applications, systems or the organization, in order to make use of punishment as a behavior influencer.

CN-US 13-114	Policy Deployment that Prosecute Harmful Hacking
 1 2 3 4 5 6 7	Organizations should implement comprehensive plans, including international cooperation aspects that prosecute those who compromise applications, systems or the organization, in order to make use of punishment as a behavior influencer.

CN-US 13-115	Performance Measurement of Prosecution
 1 2 3 4 5 6 7	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans to discourage harmful hacking with penalties, including international cooperation aspects, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-116	Corrective Action on Prosecuting Harmful Hacking Policies and Deployment
 1 2 3 4 5 6 7	Organizations should make use of performance feedback to make corrective actions to harmful hacking prosecution policies and deployment plans, in order to improve the effectiveness of both.

Unauthorized Access of Organization Resources and Functions

A specific example would be companies that have a disciplined employee monitoring system that is capable of detecting unusual employee activities such as accessing data not needed for their normal job functions, or accessing functions for some purpose that is outside of one's job scope. Another example would be government agencies with special security functions having an approach to detect unusual member activities such as accessing data or system functions that are not needed for a job.

CN-US 13-117	Policy that Controls Internal Risk of Unauthorized Access
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should establish an internal policy that emphatically pronounces as unacceptable: any members' unauthorized use of the organizations' capabilities in cyberspace for (i) access of private data, (ii) control of the operation of an asset, or (iii) any activity that may cause unintended consequences, in order to prevent these resources from being used in harmful hacking.

CN-US 13-118	Control Inner Risk of Unauthorized Access Policy Deployment
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should develop and implement a plan to realize the organization's Unauthorized Use Policy, in order to prevent these resources from being used in harmful hacking.

CN-US 13-119	Performance Measurement of Unauthorized Access Policy
 1 2 3 4 5 6 7	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans for unauthorized use by members of its assets in cyberspace, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-120	Corrective Action on Unauthorized Access Policy
 1 2 3 4 5 6 7	Organizations should make use of performance feedback to make corrective actions to unauthorized use policies and deployment plans, in order to improve the effectiveness of both.

Harmful Hacktivism

A specific example would be companies that stand together to refuse to offer services to organizations that have a practice of conducting harmful hacktivism.

CN-US 13-121	Policies that Address Harmful Hacktivism
1 2 3 4 5 6	Organizations should consider establishing policies to address the motivation of hackers to use skills to advance ideological interests, in order to discourage hacktivists from causing harm to applications, systems or organizations.

CN-US 13-122	Policy Deployment that Addresses Harmful Hacktivism
1 2 3 4 5 6	Organizations should implement comprehensive plans, including international cooperation aspects where appropriate that discredit ideological movements that use hacktivism with harmful effects, in order to discourage hacktivists from using their skills to cause harm.

CN-US 13-123	Performance Measurement of Addressing Harmful Hacktivism
1 2 3 4 5 6	Organizations should continuously review and measure the performance of stated policies and related policy deployment plans for addressing harmful hacktivism, including international cooperation aspects, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-124	Corrective Action on Harmful Hacktivism Policy and Deployment
1 2 3 4 5 6	Organizations should make use of performance feedback to make corrective actions to harmful hacktivism policies and deployment plans, in order to improve the effectiveness of both.

Conflict Screening

A specific example would be government agencies and companies carefully selecting members; e.g., a candidate that had a record of committing hacking crimes would be flagged as being high risk for the organization.

CN-US 13-125	Screening for Conflicts of Interest Policy
1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should establish a policy, consistent with relevant laws, that screens candidates that are at high risk for using the organizations' capabilities for hacking, in order to reduce the risk of the organization's resources being used for harmful hacking.

CN-US 13-126	Screening for Conflicts of Interest Policy Deployment
1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace, should develop and put into effect a plan, which is consistent with applicable laws, for ensuring candidates that are at a high risk for misusing organization resources are screened, in order to reduce the risk of the organization's resources being used for harmful hacking.

CN-US 13-127	Performance Measurement for Screening for Conflicts of Interest
1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should continuously review and measure the performance of stated policies and related policy deployment plans for ensuring candidates that are at a high risk for misusing organization resources are screened, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-128	Corrective Measures for Screening for Conflicts of Interest
1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should make use of performance feedback to make corrective actions to policies and policy deployment plans for screening for candidates that are at high risk for misusing organization resources are screened, in order to improve the effectiveness of both.

Purely Humanitarian Interests

A specific example would be a hospital declaring its purely humanitarian interests and practices.

CN-US 13-129	Purely Humanitarian Entity Policy
 1	Organizations with enhanced access to assets in cyberspace whose mission and operations are purely humanitarian should provide a public statement that articulates their policy regarding no unauthorized use of its enhanced capabilities by any of its members, including for commercial or national security interests, in order to avoid selection as a target by hackers.

CN-US 13-130	Purely Humanitarian Entity Policy Deployment
 1	Organizations with enhanced access to assets in cyberspace whose mission and operations are purely humanitarian should develop and implement a plan to prevent unauthorized use of its enhanced capabilities by any of its members, including for commercial or national security interests, in order to avoid selection as a target by hackers.

CN-US 13-131	Corrective Action for Purely Humanitarian Entity Policy
 1	Organizations whose mission and operations are purely humanitarian should continuously review and measure the performance of stated policies and related policy deployment plans for unauthorized use by organization members of its assets in cyberspace, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-132	Performance Measurement of Purely Humanitarian Entity Policy
 1	Organizations whose mission and operations are purely humanitarian should make use of performance feedback to make corrective actions to unauthorized use policies and deployment plans, in order to improve the effectiveness of both.

Declare Commercial Interests

A specific example would be a public communications network operator making it clear that it uses its assets only for commercial reasons, with any exceptions explained with sufficient clarity.

CN-US 13-133	Commercial Entity Policy
3	Organizations with enhanced access to assets in cyberspace whose mission and operations are commercial should provide a public statement that articulates their policy regarding no unauthorized use of its enhanced capabilities by any of its members, including for national security interests, in order to avoid selection as a target by hackers.

CN-US 13-134	Commercial Entity Policy Deployment
3	Organizations with enhanced access to assets in cyberspace whose mission and operations are commercial should develop and implement a plan to prevent unauthorized use of its enhanced capabilities by any of its members, including for national security interests, in order to avoid selection as a target by hackers.

CN-US 13-135	Corrective Action for Commercial Entity Policy
3	Organizations whose mission and operations are commercial should continuously review and measure the performance of stated policies and related policy deployment plans for unauthorized use by organization members of its assets in cyberspace, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-136	Performance Measurement of Commercial Entity Policy
3	Organizations whose mission and operations are commercial should make use of performance feedback to make corrective actions to unauthorized use policies and deployment plans, in order to improve the effectiveness of both.

Normalize Collaboration with Government

A specific example would be a social media company cooperating with law enforcement in ways beyond that which is required in order to track down child predators.

CN-US 13-137	Collaborating and Cooperating Policy for Humanitarian and Commercial Entities
 1 2 3 4 5 6	Organizations with enhanced access to assets in cyberspace, whose mission is not security-related, but who cooperate, whether proactively or by government requirement, with government initiated activities, should provide a public statement that articulates their policy regarding unauthorized use of its enhanced capabilities by its members, with a further clarifying statement that the organization cooperates with the government for national security activities (i) proactively, (ii) when required by the government, or (iii) both, as appropriate, in order to avoid possible selection as a target by foreign belligerents.

CN-US 13-138	Collaborating and Cooperating Policy Deployment for Humanitarian and Commercial Entities
 1 2 3 4 5 6	Organizations with enhanced access to assets in cyberspace, whose mission is not security-related, but who cooperate, whether proactively or by government requirement, with government initiated activities, should develop and implement a plan to ensure its policy regarding unauthorized use of its enhanced capabilities by any of its members is enforced, in order to avoid possible selection as a target by foreign belligerents.

CN-US 13-139	Performance Measurement of Collaborating and Cooperating Policy for Humanitarian and Commercial Entities
 1 2 3 4 5 6	Organizations with enhanced access to assets in cyberspace, whose mission is not security-related, but who cooperate, whether proactively or by government requirement, with government initiated activities, should continuously review and measure the performance of stated policies and related policy deployment plans for collaboration and cooperation with the government, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-140	Corrective Action for Collaborating and Cooperating Policy for Humanitarian and Commercial Entities
 1 2 3 4 5 6	Organizations with enhanced access to assets in cyberspace, whose mission is not security-related, but who cooperate, whether proactively or by government requirement, with government initiated activities, should make use of performance feedback to make corrective actions to policies and deployment plans for collaboration and cooperation with the government, in order to improve the effectiveness of both.

Security Team

A specific example would be a company establishing an internal CSIRT/CERT that is responsible for safeguarding its ICT systems, recruiting qualified individuals to staff the team.

CN-US 13-141	Establish Security Team Policy
 1 2 3 4 5 6 7	Organizations should have a policy regarding establishing an internal security incident response capability, in order to protect their ICT systems.

CN-US 13-142	Establish Security Team Policy Deployment
 1 2 3 4 5 6 7	Organizations should develop and implement a plan for their security team policy, considering the appropriateness of standing up a CERT, in order to protect their ICT systems.

CN-US 13-143	Performance Measurement of Security Team Establishment
 1 2 3 4 5 6 7	Organizations should continually review the deployment of their security team policy, and measure the performance of the team, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-144	Corrective Action for Security Team Establishment
 1 2 3 4 5 6 7	Organizations whose have no policy to establish a security team, or whose security team has not performed well, or cannot complete their mission, should take corrective action, in order to improve the protection of ICT assets.

Security System

A specific example would be a company deploying Internetwork Packet Exchange (IPX) systems at their Internet gateway.

CN-US 13-145	Security System Policy
 1 2 3 4 5 6 7	Organizations should establish a policy for a comprehensive security system, in order to safeguard their ICT systems and online assets.

CN-US 13-146	Security System Policy Deployment
 1 2 3 4 5 6 7	Organizations should develop and implement a plan for the deployment of their policy regarding a comprehensive security system, in order to safeguard their ICT systems and online assets.

CN-US 13-147	Performance Measurement of Security System
 1 2 3 4 5 6 7	Organizations should continually review the deployment of their comprehensive security system, and measure the performance of the system, in order to determine the effectiveness of the policies and deployment.

CN-US 13-148	Corrective Action for Security System
 1 2 3 4 5 6 7	Organizations whose have no policy to establish a security system, or whose security system does not perform well, should take corrective action, in order to provide necessary protection for ICT assets.

Vulnerability Fixes

A specific example would be a company having its web site and email server monitored for vulnerabilities on a periodic basis, and fixing vulnerabilities discovered as soon as possible.

CN-US 13-149	Policy for Vulnerability Fixes
 3	Network operators, service providers and software suppliers should consider having a policy to scan and examine the vulnerabilities of their own systems or applications, in order to decrease the risk of being hacked.

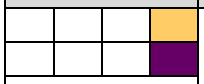
CN-US 13-150	Policy Deployment for Vulnerability Fixes
 3	Network operators, service providers and software suppliers should consider developing and implementing a plan to scan and examine the vulnerabilities of their own systems or applications, in order to decrease the risk of being hacked.

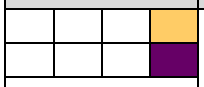
CN-US 13-151	Performance Monitoring for Vulnerability Fixes
 3	Network operators, service providers and software suppliers should continuously monitor the performance of their policy and policy deployment plans for fixing vulnerabilities, in order to determine the effectiveness of both.

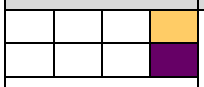
CN-US 13-152	Corrective Action for Vulnerability Fixes
 3	Network operators, service providers and software suppliers should make use of performance feedback to make corrective actions to policies and policy deployment plans for fixing vulnerabilities, in order to improve the effectiveness of both.

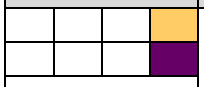
Incident Response Planning

A specific example would be an online game company just carrying out a practice drill for a DDoS attack in which the incident is to be handled according to its plan.

CN-US 13-153	Policy for Incident Response Planning
 1 2 3 4 5 6 7	Organizations should consider establishing a policy for operational readiness for handling a hacking incident, including for international incidents, in order to reduce the impact of such events.

CN-US 13-154	Policy Deployment for Incident Response Planning
 1 2 3 4 5 6 7	Organizations should develop and implement a plan for their incident response capabilities, in order to reduce the impact of a hacking event.

CN-US 13-155	Performance Monitoring for Incident Response Planning
 1 2 3 4 5 6 7	Organizations should monitor the performance of their incident response capabilities to determine failures of their policy or policy deployment with regard to readiness, in order to determine the effectiveness of both.

CN-US 13-156	Corrective Action for Incident Response Planning
 1 2 3 4 5 6 7	Organizations should make use of performance feedback to make corrective actions to policies and policy deployment plans for their incident response capabilities, in order to improve the effectiveness of both.

5.2 Best Practices for the Implementation Phase of Hacking and the Response Phase of Defense

These voluntary Best Practices are developed to address the *Implementation Phase and the Response Phase* of the hacking lifecycle (Figure 10). The highest priority of these Best Practices is to discourage hackers from causing harm to the organizations.

Abnormal Traffic

A specific example would be an ISP defining the baseline ICMP flows so as to detect a DDoS attack that was launched with ICMP packets.

CN-US 13-157	Policy for Detection of Abnormal International Payload
 3 4 5	Network Operators and Service Providers should consider establishing a policy to detect abnormal international traffic, in order to identify potential malicious traffic that may be harmful.

CN-US 13-158	Policy Deployment for Detection of Abnormal International Payload
 3 4 5	Network Operators and Service Providers should develop and implement a plan to use their operational knowledge of typical network activity, especially that of internationally originating payload, as well as information provided by their industry peers or respective CERTs, in order to identify potential malicious traffic that may be harmful.

CN-US 13-159	Performance Monitoring for Detection of Abnormal International Payload
 3 4 5	Network Operators and Service Providers should continuously review and measure the performance of stated policies and related policy deployment plans to detect abnormal international network traffic, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-160	Corrective Action for Detection of Abnormal International Payload
 3 4 5	Network Operators and Service Providers should make use of performance feedback to make corrective actions to policies and deployment plans for detecting abnormal international network traffic, in order to improve the effectiveness of both.

Timely Warning

A specific example would be an anti-virus company publishing a warning message about a new emerging computer virus on their website.

CN-US 13-161	Policy for Timely Warning
2 3 4	Software application companies should have a policy to provide alerts to users when a new and dangerous threat emerges, in order to raise the security awareness of the public and give technical advice for dealing with it.

CN-US 13-162	Policy Deployment for Timely Warning
2 3 4	Software application companies should develop and implement a plan to provide alerts to users when a new and dangerous threat emerges, in order to raise the security awareness of the public and give technical advice to deal with it

CN-US 13-162	Performance Monitoring for Timely Warning
2 3 4	Software application companies should continuously monitor the performance of their policy and policy deployment plans for timely warning, in order to determine the effectiveness of both.

CN-US 13-164	Corrective Action for Timely Warning
2 3 4	Software application companies should make use of performance feedback to make corrective actions to policies and policy deployment plans for timely warning, in order to improve the effectiveness of both.

Attack Blocking

A specific example would be a government agency immediately identifying the means used by an inside hacker and removing those means from the work environment.

CN-US 13-165	Policy for Cutting off Attacks
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should establish policy for blocking attacks, including for international incidents, in order to prevent the further damage an ongoing attack.

CN-US 13-166	Policy Deployment for Cutting off Attacks
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should develop and implement a plan for cutting out attacks, including removal of (i) malware source, (ii) block access of abuse, in order to prevent the further damage an ongoing attack.

CN-US 13-167	Performance Monitoring for Cutting off Attacks
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should continuously monitor the performance of their policy for cutting off an attack, in order to determine the effectiveness of both.

CN-US 13-168	Corrective Action for Cutting off Attacks
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should make use of performance feedback to make corrective actions to policies and policy deployment plans for cutting off attacks, in order to improve the effectiveness of both.

Trace Source

A specific example is an ISP identifying the apparent source(s) of a DDoS from examination of the network maintenance tools.

CN-US 13-169	Policy for Tracing the Source
3	ISPs should establish policy for tracing the source of a hacking incident, including seeking international cooperation, in order to stop the attack from the starting point.

CN-US 13-170	Policy Deployment for Tracing the Source
3	ISPs should develop and implement a plan for tracing the source of hacking, including seeking international cooperation, in order to stop the attack from the starting point.

CN-US 13-171	Performance Monitoring for Tracing the Source
3	ISPs should continuously monitor the performance of their policy for tracing the source, in order to determine the effectiveness of both.

CN-US 13-172	Corrective Action for Tracing the Source
3	ISPs should make use of performance feedback to make corrective actions to policies and policy deployment plans for tracing the source, in order to improve the effectiveness of both.

Clean-up Online Environment

A specific example is a domain registrar company that suspends domain names being used for phishing, or an anti-virus company patching their product to remove malware on users' computers.

CN-US 13-173	Policy for Cleaning-up Online Environment
 1 2 3 4	Domain registrars, ISPs and anti-virus suppliers should establish a policy for cleaning-up the online environment, in order to decrease the risk of serious cyber attacks.

CN-US 13-174	Policy Deployment for Cleaning-up Online Environment
 1 2 3 4 5 6 7	Domain registrars, ISPs and anti-virus suppliers should develop and implement a plan for cleaning-up the online environment, in order to decrease the risk of serious cyber attacks.

CN-US 13-175	Performance Monitoring for Cleaning-up Online Environment
 1 2 3 4 5 6 7	Domain registrars, ISPs and anti-virus suppliers should continuously monitor the performance of their policy for cleaning-up the online environment, in order to determine the effectiveness of both.

CN-US 13-176	Corrective Action for Cleaning-up Online Environment
 1 2 3 4 5 6 7	Domain registrars, ISPs and anti-virus suppliers should make use of performance feedback to make corrective actions to policies and policy deployment plans for cleaning-up the online environment, in order to improve the effectiveness of both.

Block Fake IP Addresses

A specific example is an ISP using the ingress filtering or ACL function to block traffic with fake source IP addresses, which are usually used for DDoS attack.

CN-US 13-177	Policy for Blocking Fake IP
 3	ISPs should establish policy for blocking traffic with a fake source IP, in order to stop DDoS attacks.

CN-US 13-178	Policy Deployment for Blocking Fake IP
 3	ISPs should develop and implement a plan for blocking traffic with a fake source IP, in order to stop DDoS attacks.

CN-US 13-179	Performance Monitoring for Blocking Fake IP
 3	ISPs should continuously monitor the performance of their policy for blocking traffic with a fake source IP, in order to determine the effectiveness of both.

CN-US 13-180	Corrective Action for Blocking Fake IP
 3	ISPs should make use of performance feedback to make corrective actions to policies and policy deployment plans for blocking traffic with fake source IP, in order to improve the effectiveness of both.

Joint Analysis of Experts

A specific example is when a serious cyber attack happens; experts from different entities with their own perception and evidence carry out a joint incident analysis of the problem.

CN-US 13-181	Policy for Joint Analysis of Experts
 1 2 3	Organizations and industry associations should establish policy of joint analysis by experts on serious cyber attacks, including for international incidents, in order to find out the problems and solutions quickly and effectively.

CN-US 13-182	Policy Deployment for Joint Analysis of Experts
 1 2 3	Organizations and industry associations should develop and implement a plan of joint analysis by experts on serious cyber attacks, in order to find out the problems and solutions quickly and effectively.

CN-US 13-183	Performance Monitoring for Joint Analysis of Experts
 1 2 3	Organizations, industry associations should continuously monitor the performance of their policy of joint analysis by experts on serious cyber attacks, in order to determine the effectiveness of both.

CN-US 13-184	Corrective Action for Joint Analysis of Experts
 1 2 3	Organizations, industry associations should make use of performance feedback to make corrective actions to policy of joint analysis by experts on serious cyber attacks, in order to improve the effectiveness of both.

5.3 Best Practices for Escape Phase of Hacking and the Follow-up Phase of Defense

The next set of Best Practices are *the Escape phase and the Follow-up phase* that are characterized by attempts to cover the hacker's tracks and avoid punishment. Best Practices for this phase focus on keeping necessary logs for a certain time so that the investigation can be carried out with sufficient data that may include the path of the hacker.

Recover Business First

A specific example would be an online bank building warm back up systems that attacks to the main server do not influence, in order to have continuity of bank operations.

CN-US 13-185	Policy to Recover Business First
 3	Major Internet service companies should establish a policy regarding the recovery of business when their primary service is impaired, in order to protect the interests of their users.

CN-US 13-186	Policy Deployment to Recover Business First
 3	Major Internet service companies should develop and implement a plan for business continuity when attacks impair primary services, in order to protect the interests of their users.

CN-US 13-187	Performance Evaluation Recover Business First
 3	Major Internet service companies should continuously review and measure the performance of stated policies and related policy deployment plans for business continuity when attacks impair primary services, in order to determine the effectiveness of both.

CN-US 13-188	Corrective Action to Recover Business First
 3	Major Internet service companies should make use of performance feedback to make corrective actions to policies and policy deployment plans for business continuity when attacks impair primary services, in order to improve the effectiveness of both.

Thorough Investigation

A specific example would be after a serious attack, a company establishes a task group that spends a month to carry out a precise investigation and confirms the exact method and source of an attack.

CN-US 13-189	Policy for Precise Investigation
 1 2 3 4 5 6 7	Organizations and companies should establish a policy to conduct a thorough investigation after being attacked, in order to find out the problems and prevent them in the future.

CN-US 13-190	Policy Deployment for Precise Investigation
 1 2 3 4 5 6 7	Organizations and companies should develop and implement a plan to deploy the policy to conduct a thorough investigation after be attacked, in order to find out the problems and prevent them in the future.

CN-US 13-191	Performance Evaluation for Precise Investigation
 1 2 3 4 5 6 7	Organizations and companies should continuously review and measure the performance of stated policies and related policy deployment plans for carrying out a thorough investigation after being attacked, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-192	Corrective Action for Precise Investigation
 1 2 3 4 5 6 7	Organizations and companies should make use of performance feedback to make corrective actions conducting thorough investigations, in order to determine the effectiveness of the policies and deployment plans.

Incident Summary

A specific example would be organizations conducting an analysis that is able to confirm that an incident was unintended, training that and other members of the ways to prevent future similar accidents, and modifying systems to prevent similar future incidents.

CN-US 13-193	Policy for Incident Summary
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should establish a policy for documenting hacking incident analyses, in order to prevent and ameliorate future events.

CN-US 13-194	Policy Deployment for Incident Summary
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should develop and put into effect a plan for summarizing hacking incident analyses conclusions, in order to prevent and ameliorate future events

CN-US 13-195	Performance Measurement for Incident Summary
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should continuously review and measure the performance of summary policies and related policy deployment plans for hacking incident analysis documentation, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-196	Corrective Action for Incident Summary
 1 2 3 4 5 6 7	Organizations with enhanced access to assets in cyberspace should make use of performance feedback to make corrective actions to policies and policy deployment plans for documenting hacking incident analysis conclusions, in order to improve the effectiveness of both.

Punish the Hacker by Law Enforcement

A specific example would a hacker who launches a DDoS attack to another online game being prosecuted by the legal system.

CN-US 13-197	Policy for Improving Laws
1 2 3 4 5 6 7	Government law making bodies should create and improve policies and laws that punish harmful hacking, including those needed for international incidents, in order to protect the interests of society.

CN-US 13-198	Policy Deployment - Improving Laws
1 2 3 4 5 6 7	Government law making bodies should develop and implement a plan to keep improve the laws so that harmful hacking will be punished, including those needed for international incidents, in order to protect the interests of society.

CN-US 13-199	Performance Evaluation – Improving Laws
1 2 3 4 5 6 7	Government law making bodies should continuously review and measure the performance of stated policies that to improve laws to punish harmful hackers, in order to determine the effectiveness of the policies and deployment plans.

CN-US 13-200	Corrective Action - Improving Laws
1 2 3 4 5 6 7	Government law making bodies should make use of performance feedback to improve laws, in order to determine the effectiveness of the policies and deployment plans.

Observe good faith and justice toward all nations.

Cultivate peace and harmony with all.

- George Washington

A journey of a thousand miles begins with a single step.

- Laozi

6. Conclusion

This *Frank Communication and Sensible Cooperation to Stem Harmful Hacking* Report acknowledges that the hacking issue is a *sanity test* for the future friendship of China and the United States. However this China-U.S. bilateral guidance does *not* force a naïve view of trust where trust does not belong. Rather, its pages provide practical, "down to earth" directions to make the relationship succeed in this test.

This report was produced with a joint team of subject matter experts and stakeholders with over two thousand years of combined experience. The study employed a number of methodologies that included many private consultations with experts and stakeholders from a wide range of backgrounds, analyses based on rigorous scientific fundamentals and engineering principles, exploration of the lifecycle of a hack and an openness to discuss any issues candidly.

From these and other analyses, 80 Key Observations were selected from among thousands. These observations were oriented around the three critical realities of *the current situation*, *understanding the problem* and *the solution space* (Section 3).

These Key Observations are then used to provide critical insights that were used to fashion the report's eight Recommendations (Section 4). These immediately actionable Recommendations, if implemented, will establish practical conversations and relationships that can slow the rate of destabilization around this subject and then reverse the trend's direction. In these Recommendations the interests of all sorts of organizations are protected, whether they are humanitarian, commercial, or national security. For each of these Recommendations there are suggested next steps that form an action plan to create and maintain momentum in their implementation. For each Recommendation there are also measures of success by which an evaluation can be made about progress.

The Recommendations are next complimented with 100 voluntary Best Practices that were informed by the limits and enablement of the underlying hard science, the lifecycle of a hack and practical experience (Section 5). As these Best Practices are applied, confidence will develop among and between various levels, from those responsible for technical implementation, through middle management to senior decision-makers; confidence will also develop across the Pacific Ocean. Risk will be better managed and numerous chains of trust assembled. Numerous formal ties will ensue, not for meeting sake, but rather as the natural course of doing what makes sense to solve problems. Many of the subject matter experts who contributed to the development of this report are excited about moving forward with the next steps of implementation.

The first four recommendations are part of a Total Trust Management "air-tight" system of assurance, able to detect variations in policy and policy deployment and reality in the field. Early circulation of the total trust management model elicited two notable responses: On one hand, some engineers felt that it was *too simple*. On the other hand, some career politicians found the same model *too complicated*. For the former it was hard to imagine that an organized group of people in this day and age would not already be operating with such basic principles of management toward objectives and accountability. For the latter it was hard to embrace the (even minimal) transparency and accountability, making it seem very challenging from the start. The result of factoring in these two reactions was even more confidence that the Recommendations are in line with exactly what is needed. The truth is that the guidance is simple, but that in the current situation there are many breakdowns. These Recommendations and voluntary Best Practices provide the intelligence and energy to reverse the entropy that has had its way for too long on this issue.

This brings us to some parting questions . . .

> *Can the relationship survive intact with the hacking issue unresolved?*
> Maybe. But it is more likely that it will continue to suffer if unresolved.
>
> *Would resolution offer significant benefit?*
> Most certainly; and not only for China and the U.S., but also for the rest of the world.
>
> *Will the hump be too hard to get over?*
> When it was *one big* hump, recent history says 'yes.'
> But now, with the Recommendations offered herein, there is no longer one big hump, as the difficulty has been divided into many manageable, little humps that are "down to earth" and can be stepped over.

The experts and stakeholders have thought and worked very hard on how to make cyberspace safer, more stable and secure. We are enthusiastic about how this report has the potential for having a broad and far-reaching effect for China, the United States and the rest of the world.

Around the world, the hacker and cybersecurity communities have developed cultures that are evolving over time. We expect they will continue to have cultures that interface in important ways with the rest of society. As ICT advances, so will these cultures. Many people have had to learn to think differently as they use technology. We hope that the hacker and cybersecurity communities will also begin to think differently, with an end result of having more caution and respect for the danger of harmful hacking, having a greater commitment to frank interactions and sensible cooperation and an unquenchable desire to make the world a safer place for all of us.

In conclusion, this report is *not* a typical policy paper, but a document that includes what it takes to solve the problem. The guidance within is sound and its requests of stakeholders are reasonable. These Recommendations are the alternative to brinkmanship.

About the Authors

KARL FREDERICK RAUSCHER

Karl Rauscher saw a need for engineers to help failing international policy for high consequence issues in cyberspace and envisioned how science diplomacy could make the critical difference for success. In recent years he has led studies and authored bilateral reports among the cyber superpowers: China, the EU, India, Russia, and the U.S. He has brought hundreds of engineers, business leaders and other stakeholders together in designing and implementing 'future-proof' policy solutions.

Karl is a Bell Labs Fellow, and served as CTO and a Distinguished Fellow at the EastWest Institute. He previously served as the Executive Director of the Bell Labs Network Reliability & Security Office. He has been an advisor on five continents, including as vice chair of the U.S. President's National Security Telecommunications Advisory Committee (NSTAC) industry executive committee and as leader of the European Commission study on the Availability and Robustness of Electronic Communications Infrastructures (ARECI). He is active in the IEEE, serving as chair-emeritus of the IEEE Communications Quality & Reliability (CQR) advisory board, authoring the IEEE Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report and the IEEE Wireless Engineering Book of Knowledge (policy chapter).

He has over 50 patents/pending in fields that span artificial intelligence, critical infrastructure protection, emergency communications, and telemedicine. He discovered over 1,000 software bugs in live networks. Mr. Rauscher is a high distinction and high honors graduate with a M.S. E.E. from Rutgers University, a B.S. E.E. from Pennsylvania State University, and a M.A. degree in Biblical Studies from Dallas Theological Studies. His business training includes the MIT Sloan School executive development program.

ZHOU YONGLIN

ZHOU Yonglin is the Secretary General, Information & Network Security Committee, Internet Society of China and the Director, Department of Science & Technology, CNCERT

ZHOU Yonglin graduated from Harbin Institute of Technology (HIT) of China in 1999 with a master degree of computer science. Now he has been working on network security for 14 years. He has led or joined tens of projects on network security monitoring, vulnerability handling and malware analysis. Leading his team, he works closely with government, ISPs, ICPs, domain name registrars, security service providers and product vendors on cyber security threat and incident watching and response, especially makes great efforts on stopping spam, botnet and DDoS attacks. He helped initiative industry collaboration, including the Anti-Network-Virus Association (ANVA) and China National Vulnerability Database (CNVD), from which the quickly growing Internet industry and users in China could get timely, trusted and professional assistance. Mr. Zhou has been invited to work as technical consultant and part-time professor by government and universities.

In 2008, he was invited as an Information Network Security Advisor of Beijing Olympic Games Organizing Committee. He has published tens of papers around his research area. He has actively joined international cooperation on network security and gave presentations in many conferences.

Due to the remarkable research outputs, he has won the National Science and Technology Progress Award (First Class) twice and some other ministerial/provincial awards on science and technology for five times.

Acronymns

3G	Third Generation Wireless
4G	Fourth Generation Wireless
5G	Fifth Generation Wireless
8i Framework	Eight Ingredient Framework
ACL	Access Control List
APT	Advanced Persistent Threat
ARECI	Availability and Robustness of Electronic Communications Infrastructures
ARIN	American Registry for Internet Numbers
ASPR	Agreements, Standards, Policies and Regulations
ATIS	Alliance for Telecommunications Industry Solutions
ATM	Asynchronous Transfer Mode
AVG	American Volunteer Group
BAN	Body Area Network
BWA	Broadband Wireless Access
C7	Signalling System 7
CAN	Campus Area Network
CC	Coordination Center of China
CDMA	Code Division Bluetooth, Multiple Access
CEO	Chief Executive Officer
CERT	Computer Emergency Readiness (or Response) Team
CIA	Central Intelligence Agency (U.S.)
CIRT	Computer Incident Response Team
CN	China
CNCERT	National Computer Network Emergency Response Technical Team
CN-US	China-United States (Best Practice designation)
COE	Council of Europe
CPC	Communist Party of China
CQR	Technical Committee on Communications Quality & Reliability (IEEE)
CWG	Cyber Working Group
DHS	Department of Homeland Security (U.S.)
DOCSIS	Data Over Cable Service Interface Specification
DoD	Department of Defense (U.S.)
DoS	Department of State (U.S.)
DoS	Denial of Service
DDoS	Distributed Denial of Service
DNI	Director of National Intelligence (U.S.)
DTOT	Decision Tree Optimized for Trust-Building
E6	Ethernet Globalization Protocols
EC	European Commission
EU	European Union
EWI	EastWest Institute
FBI	Federal Bureau of Investigation (U.S.)
FCC	Federal Communications Commission (U.S.)
FDI	Foreign Direct Investment
FISA	Foreign Intelligence Surveillance Act (U.S.)
FTP	File Transfer Protocol

GSM	Global System for Mobile communication
GUCCI	Global Undersea Communications Cable Infrastructure
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IAN	Internet Area Network
ICMP	Internet Control Message Protocol
ICPC	International Cable Protection Committee
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IHL	International Humanitarian Law
IMS	IP Multimedia Subsystem
IN	Intelligent Network
IP	Internet Protocol
IP	Intellectual Property
IPR	Intellectual Property Rights
IPX	Internet Packet Exchange
ISC	Internet Society of China
ITU	International Telecommunication Union
IWM	Information Warfare Monitor
JLG	Joint Liaison Group (on Law Enforcement Cooperation)
KCC	Korea Communications Commission
KLIC	Karl's Landscape of Interests in Cyberspace
LAN	Local Area Network
LTE	Long Term Evolution
MAN	Metropolitan Area Network
M^3AAWG	The Messaging, Malware and Mobile Anti-Abuse Working Group
MII	Ministry of Information Industry (China)
MIIT	Ministry of Industry and Information Technology (China)
MOST	Ministry of Science and Technology (China)
NAN	Near-me Area Network
NFC	Near Field Communication
NGN	Next Generation Networks
NPC	National People's Congress (China)
NSA	National Security Agency (U.S.)
NTP	Network Time Protocol
NYSE	New York Stock Exchange
PAN	Personal Area Network
POP	Post Office Protocol
POTS	Plain Old Telephone System
PRC	People's Republic of China
ROGUCCI	Reliability of Global Undersea Communications Cable Infrastructure
SARS	Severe Acute Respiratory Syndrome
SCIO	State Council Information Office (SCIO)
SDH	Synchronized Digital Hierarchy
SDO	Standards Development Organization
SFTP	Secure File Transfer Protocol
SIP	Session Initiation Protocol
SIIS	Systems and Internet Infrastructure Security Laboratory
SMTP	Simple Mail Transfer Protocol
SONET	Synchronized Optical Networking

SSD	Strategic Security Dialogue
SS7	Signalling System 7
SSH	Secure Shell
SSL	Secure Socket Layer
STEM	Science, Technology, Engineering and Mathematics
TCA	Taking Corrective Action
TTM	Total Trust Management
TTMM	Total Trust Management Model
TTN	Telnet Telephone Network
TDM	Time-Division Multiplexing
TLS	Transport Layer Security
UN	United Nations
U.S.	United States (of America)
VIDT	Verdict-Initiated Decision Tree
WERT	Wireless Emergency Response Team
WIFI	Wireless, Fidelity IEEE 802.11
WIPO	World Intellectual Property Organization
WLAN	Wireless Local Area Network
WIMAX	Worldwide Interoperability for Microwave Access IEEE 802.16
UMTS	Universal Mobile Telecommunications Service
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team

References

2007 National People's Congress, 5th Plenary Session of the 10th National People's Congress, March 5 to March 15, 2007.

Adam, A.E., *Hacking into Hacking: Gender and the Hacker Phenomenon*, Information Systems Research Centre, University of Salford, Volume 33 Issue 4, December 2003.

Agreement Between the Government of the United States of America and the Government of the People's Republic of China on Mutual Legal Assistance in Criminal Matters, Beijing, 19 June 2000.

Annual Report - National Computer network Emergency Response Technical Team /Coordination Center of China – People's Republic of China, 2012.

APT1: Exposing One of China's Cyber Espionage Units, Mandiant, February 2013.

Avalon Project, Yale University, avalon.yale.edu.

ATIS Network Reliability Steering Committee (NRSC) 2002 Annual Report, www.atis.org/nrsc .

ATIS Telecom Glossary, http://www.atis.org/glossary, 2013.

Blair, Dennis, C., Huntsman, Jon, M. Jr., *The IP Commission Report – The Report of the Commission on the Theft of Intellectual Property*, The National Bureau of Asian Research, May 2013.

Blankenship, Llyod ("The Mentor"), *Conscience of a Hacker, The* (also known as *The Hacker Manifesto*), 8 January 1986.

Brown, G. and Tullos, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 11 December 2012.

Bus, Jacques, *Societal Dependencies and Trust: Modern Societies' Dependency on ICTs and the Internet*, Section 3.1 of *The Quest for Cyber Peace,* International Telecommunications Union, January 2011.

Chapman, Glenn, *Yahoo CEO Fears Defying NSA Could Mean Prison*, Yahoo News, 12 September 2013.

Charter of the United Nations, The, 1973.

Clinton Administration's Policy on Critical Infrastructure Protection, The, Presidential Decision Directive No. 63, White Paper, 22 May 1998.

Charney, Scott, Remarks in Speech at EWI's Second Worldwide Cybersecurity Summit, London, June 2011.

China Science and Technology Newsletter No. 5, 2012.

Chinese Police Chief Vows International Cooperation in Fighting Internet Crimes, People's Daily, 31 August 2011.

Chinese Proverbs from Olden Times, Peter Pauper Press, Mt. Vernon, N.Y., 1956.

Clapper, James, R., *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, 6 June 2013.

Copyright Law of the People's Republic of China, 15th Meeting of the Standing Committee of the Seventh National People's Congress on 7 September 1990; amended according to the Decision on Amending the Copyright Law of the People's Republic of China, 24th Meeting of the Standing Committee of the Ninth National People's Congress, 27 October 2001.

Council of Europe, *Convention on Cybercrime*, Budapest, 2001.

Critical Infrastructure Protection, Executive Order 13010, Executive Order 13010, Federal Register, 17 July 1996. Vol. 61, No. 138.

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, White House, 2009.

Custer, C., *Chinese Media: Snowden Says Cisco Helped the US Spy on China*, Tech in Asia, 19 June 2013.

Custer, C., *Report Says Cisco, Other US Companies Pose Threat to Chinese Information Security*, Tech in Asia, 28 November 2012.

Daniels, Victor, *China Proverbs*, 2005. (www.sonoma.edu/users/d/daniels/chinaproverbs.html).

Davidow, William H., *OVERconnected – the Promise and Threat of the Internet*, Delphinium Books, 2011.

Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security, The, 19th Meeting of the Ninth Standing Committee of the National People's Congress, 28 December 2000.

Definition of Aggression, UN General Assembly Resolution 3314 (XXIX), 1974.

DigitalAttackMap.com .

Dion, Maeve, *When Cyber Incidents Threaten National or International Security: What is the Law?*, The CIP Report, Legal Insights, Volume 9 Number 7, January 2011.

Donovan, Fred, *China-based Hidden Lynx Responsible for High-Profile Cyberattacks, Says Symantec Group Blamed for Bit9 Breach, Operation Aurora, Fierce IT Security*, 19 September 2013.

Dourado, Eli, *Let's Build a More Secure Internet*, The New York Times, 8 October 2013.

Establishing the Office of Homeland Security and the Homeland Security Council, Executive Order 13228, Federal Register, Volume 66, No. 196, 8 October 2001.

Fei, Gao, *China's Cybersecurity Challenges and Foreign Policy*, Georgetown Journal of International Affairs, International Engagement on Cyber – Establishing Norms and Improving Security, 2011.

Fitz-Morris, James, *Why Would Canada Spy on Brazil Mining and Energy Officials? Department of Mining and Energy Is Tasked with Auctioning Rights to Develop Libra Oil Field*, CBC News, 9 October 2013.

Gady, Franz-Stefan, *Strategic Stability in Cyberspace*, ChinaUSFOcus.com, 4 June 2013.

Gallagher, Billy, *Zuckerberg Says The "Government Blew It" On The NSA Scandal*, TechCrunch, 11 September 2013.

Gellman, Barton, Soltani, Ashkan, NSA Secretly Taps Yahoo, Google Links Between Data Centers Infiltrated, Files Show, Washington Post, 30 October 2013.

General Principles of the Civil Law of the People's Republic of China, 4th Session of the Sixth National People's Congress, 12 April 1986.

Gerstein, Josh, *Obama and Xi Talk Cyber to Press, Not So Much Each Other*, Politico, 8 June 2013.

Geneva Convention, The, The Geneva Conventions of 1949 and their Additional Protocols, Geneva.

Geneva Protocol, The; Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, Geneva, 1925.

Geron, Tomio, *Mark Zuckerberg: U.S. Government 'Blew It' On NSA Issue*, Forbes, 11 September 2013.

Gertz, Bill, *China's Military Preparing for 'People's War' in Cyberspace, Space Translated Report Reveals High-Tech Plans for Cyber Attacks, Anti-Satellite Strikes*, 30 July 2013.

Graham, Paul, *A Plan for Spam*, paulgraham.com, August 2002.

Greenwald, Glenn, *The NSA's Mass and Indiscriminate Spying on Brazilians As It Does in Many Non-Adversarial Countries, the Surveillance Agency Is Bulk Collecting the Communications of Millions of Citizens of Brazil*, The Guardian, 6 July 2013.

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations A/68/98*, Sixty-eighth Session, 24 June 2013.

Gurmeet, Kanwal, *China's Emerging Cyber War Doctrine, Journal of Defense Studies*, New Delhi, Vol. 3 No. 3, July 2009.

Hague Convention, The Hague Convention of 1899 and 1907 The Hague.

Hou Qiang, *Pentagon's Cyber Attack Accusations Irresponsible: Expert*, Xinhua, 7 May 2013.

Kahn, Robert E., *America's Cyber Future - Security and Prosperity in the Information Age - The Role of Architecture in Internet Defense,* 2011.

Kramer, Franklin, D., Starr, Stuart, H., Wentz, Larry K., *Cyberpower and National Security*, NDU Press, 2009.

Hathaway, Melissa E. and Savage, John E., Stewardship of Cyberspace – Duties for Internet Service Providers, CyberDialogue, 2012.

Healy, Jason, *Time to Split the Cyber 'Deep State' of NSA and Cyber Command*, Huffington Post, 2 October 2013.

Hille, Kathrin, *Chinese Media Hit at 'White House's Google'*, Financial Times, 20 January 2013.

Chunying, Hua, *Foreign Ministry Spokesperson Regular Press Conference,* 24 April 2013.

IEEE Spectrum, *Two Face of Hacking, The*, July 2011.

International Cable Protection Committee (ICPC), www.iscpc.org .

Internet in China, The, Information Office of the State Council of the People's Republic of China, Beijing, June 2010.

Jones, Andrew, *Chinese Newspaper Compares Eight US Companies to Occupying Foreign Powers Chinese Newspaper Compares Google, Apple, Microsoft and Others of Being Even More Dangerous than a 1900 Alliance of Foreign Powers that Occupied Beijing*, GBTimes, 6 June 2013.

Joye, Christopher, *Transcript: Interview with former CIA, NSA chief Michael Hayden,* Australian Financial Review, The, 19 July 2013.

Lam, Lana and Chen, Stephen, *EXCLUSIVE: US Spies on Chinese Mobile Phone Companies, Steals SMS Data: Edward Snowden - The US Government Is Stealing Millions of Text Messages in Their Hacking Attacks on Major Chinese Mobile Phone Companies*, *Edward Snowden Has Told the Post*, South China Morning Post, 23 June 2013.

Law of the People's Republic of China on Electronic Signatures, The, 11th Conference of the Standing Committee of the 10th State Council of the People's Republic of China, 28 August 2004.

Law of the People's Republic of China on the Protection of Minors, 21st Meeting of the Standing Committee of the Seventh National People's Congress, 4 September 1991.

Law of the People's Republic of China on Punishments in Public Order and Security Administration, 17th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, 28 August 2005.

Lee, Cyrus, *Huawei Fed Up, Tells US Critics 'Shut Up'*, ZDNet, 19 July 2013.

Lewis, James and Baker, Stewart, *Economic Impact of Cybercrime and Cyber Espionage, The,* Center for Strategic Studies, July 2013.

Lotrionte, Catherine, *Strengthening the Norms of State Responsibility*, Georgetown Journal of International Affairs, International Engagement on Cyber – Establishing Norms and Improving Security, 2011.

MacArthur, Douglas, *Message on Formosa*, 17 August 1950.

Malkin, G., *Internet Users' Glossary*, Internet Engineering Task Force (IETF) Network Working Group RFC 1392, January 1993.

McMillan, Robert, *As Hacking Hits Home, China Strengthens Cyber Laws*, PCWorld, May 2009.

Meacham, T. Chase, *PRISM: The 8 Tech Companies Who Gave Your Data to the Government Have This to Say About the Scandal*, PolicyMic, July 2013.

Measures on the Administration of Internet Information Services, 31st Regular Meeting of the State Council, 20 September 2000.

Measures on the Administration of Security Protection of the International Networking of Computer Information Networks, Decree No. 33 of the State Council, 11 December 1997.

Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), The, www.maawg.org .

Meyer, David, *Don't Trust Huawei and ZTE, US Congressional Committee Warns*, ZDNet, 8 October 2012.

Military and Security Developments Involving the People's Republic of China 2013, U.S. Department of Defense to Congress, 6 May 2013.

National Military Strategy of the United States of America, The, Office of the Chairman of the Joint Chiefs of Staff, Washington, DC. 2004.

National Strategy for Homeland Security, The, U.S. Office of Homeland Security, 16 July 2002.

National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, The, Office of the President, February 2003.

Negroponte, John D. and Palmisano, Samuel J., *Defending a Open, Global, Secure and Resilient Internet*, Council on Foreign Relations - Independent Task Force Report No. 70.

Network Reliability Steering Committee (NRSC), www.atis.org .

Next Generation Networks Task Force Report, NSTAC, March 28, 2006.

Office of the President of the United States of America*, International Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World,* The White House, May 2011.

Preventing a U.S.-China Cyberwar, The Editorial Board, The Wall Street Journal, 25 May 2013.

Project on Cybercrime, Council of Europe.

Property Law of the People's Republic of China, National People's Congress, 2007.

Protalinski, Emil, *15-Year-Old Arrested for Hacking 259 Companies*, ZDNet, 17 April 2012.

Provisions on the Administration of Electronic Bulletin Services via the Internet, 4th Ministerial Meeting of the Ministry of Information Industry, 8 October 2000.

Provisions on the Administration of Foreign-funded Telecommunications Enterprises, Decree No. 333 of the 49th Executive Meeting of the State Council, 5 December 2001.

Provisions on the Administration of Internet News Information Services, Information Office of the State Council and Ministry of Information Industry, 25 September 2005.

Public Data Network Reliability Focus Group Final Report, Issue 3, NRIC VII, October 2005.

Qingmin, Zhang, *China's Diplomacy*, China Intercontinental Press, 2010.

Rauscher, Karl F., *Protecting Communications Infrastructure*, Bell Labs Technical Journal – Special Issue: Homeland Security, Volume 9, Issue 2, 2004.

Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight ingredients of communications infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security*, Bell Labs Technical Journal, Volume 11, Issue 3, 2006.

Rauscher, Karl F., European Commission-Sponsored, *Availability And Robustness Of Electronic Communications Infrastructures (ARECI) Report*, March 2007.

Fresh Rauscher, Karl Frederick, *Fresh Tracks for Cybersecurity Policy Laterals Updating the Track 1 -Track 2 Paradigm to Tracks κ, ε and φ*, IEEE Proceedings of the Third Worldwide Cybersecurity Summit, New Delhi, 2012.

Rauscher, Karl Frederick, *Reliability of Global Undersea Communications Cable Infrastructure (ROGUCCI) Report, The*, IEEE: 2010.

Rauscher, Karl Frederick, Korotkov, Andrey, *Russia-U.S. Bilateral on Critical Infrastructure Protection - Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace,* EastWest Institute, February 2011.

Rauscher, Karl Frederick, Zhou, Yonglin, *China-U.S. Bilateral on Cybersecurity: Fighting spam to Build Trust*, EastWest Institute and Internet Society of China, 2011.

Rauscher, Konrad M., *The Digital Shrink Wrap Dilemma - When We Don't Necessarily Agree with Agreements, But Agree to Them Anyway*, Proceedings of the IEEE-EWI Third Worldwide Cybersecurity Summit, New Delhi, 2012.

Regulations on the Protection of Computer Information System Security of the People's Republic of China, Decree No.147, State Council of the People's Republic of China, 18 February 1994.

Regulations on Telecommunications of the People's Republic of China, 31st Regular Meeting of the State Council, 20 September 2000.

Regulations on the Protection of the Right to Online Dissemination of Information, Order No. 468 of the State Council, 135th Executive Session of the State Council, 10 May 2006.

Remarks by President Obama and President Xi Jinping of the People's Republic of China After Bilateral Meeting, Sunnylands Retreat, Rancho Mirage, California, 8 June 2013.

Sanger, David, *U.S. Blames China's Military Directly for Cyberattacks*, New York Times, 6 May 2013.

Schmitt, Michael, N., *Tallinn Manual on the International Law Application to Cyber Warfare*, Cambridge University Press, 2013.

Shanghai Cooperation Organization, The, www.sectsco.org/EN/ .

Laura Smith-Spark, Laura, *Germany's Angela Merkel: Relations with U.S. 'Severely Shaken' Over Spying Claims*, CNN, 24 October 2013.

Sun Tzu, *Art of War, The*, circa 5th Century B.C.; Translation: 1910; Barnes and Noble Classics, 2003.

Tencent Cyberlaw Research Center .

Thomas, Timothy L., *Dragon Bites*, Chinese Information War, 2003 .

Timberg, Craig and Nakashima, Ellen, *Amid NSA Spying Revelations, Tech Leaders Call for New Restraints on Agency,* The Washington Post, 1 November 2013.

Toure, Hamadoun I., *Quest for Cyber Peace, The*, International Telecommunication Union, January 2011.

Troianovski, Anton; Gryta, Thomas and Schechnernsa, Sam, *Fallout Thwarts AT&T as Carrier Considers Vodafone, Wider Distrust of U.S. Spying May Upend Its Takeover Ambitions, Wall Street Journal, 30 October 2013.*

Yang, Jia Lynn, *Snowden: U.S. Massively Hacking China's Networks,* Washington Post, 14 June 2013.

U.S. Army Cyber Operations and Cyber Terrorism Handbook, 1.02, US Army Training and Doctrine Command, Fort Leavenworth, Kansas, 2005.

U.S. Cyber Command Fact Sheet, U.S. Department of Defense, May 2010.

Verton, Dan, *Black Hat Highlights Real Danger of Script Kiddies*
Reckless probing by amateurs could actually be helping cybercriminals, ComputerWorld, 23 July 2011.

The Real U.S.-Chinese Cyber Problem .

VornDick, Wilson, *The Real U.S.-China Cyber Problem*, The National Interest, 30 July 2013.

Wang Peiran, *China's Perceptions of Cybersecurity*, Georgetown Journal of International Affairs, International Engagement on Cyber 2012 – Establishing Norms and Improving Security, 2012.

Watkins, Tom, *Is the Cyber Sky Falling on China?* ChinaUSFocus.com, 15 March 2013.

World Intellectual Property Organization (WIPO), www.wipo.int .

World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks, 2013.

Yingkui, Tian, *China's Path – the Scientific Outlook on Development*, Foreign Languages Press, 2008.

Zhongqing, Yin, *China's Political System*, China Intercontinental Press, 2010.

Zhong Shen, *Defaming China Cannot Cover US Evil Acts*, People's Daily, 9 May 2013.

Zuckerberg, Mark, Letter to Investors: *The Hacker Way*, 1 February 2012.

APPENDIX A: Laws Related to Cyber Crime

This appendix includes information regarding laws that may relate to cyber crime that is referred to during the study and throughout the report. It consists of summary information.

China's Laws that Apply to the Internet Administration and Security

China's government references numerous laws as applicable to "Basic Principles and Practices of Internet Administration," namely:[234]

- Decision of the National People's Congress Standing Committee on Guarding Internet Security[235]
- Law of the People's Republic of China on Electronic Signatures[236]
- Regulations on Telecommunications of the People's Republic of China[237]
- Measures on the Administration of Internet Information Services[238]
- Regulations on the Protection of Computer Information System Security of the People's Republic of China[239]
- Regulations on the Protection of the Right to Online Dissemination of Information[240]
- Provisions on the Administration of Foreign-funded Telecommunications Enterprises[241]
- Measures on the Administration of Security Protection of the International Networking of Computer Information Networks[242]
- Provisions on the Administration of Internet News Information Services[243]
- Provisions on the Administration of Electronic Bulletin Services via the Internet[244]

In addition, the Chinese government has identified relevant provisions of the Criminal Law of the People's Republic of China, namely:

- General Principles of the Civil Law of the People's Republic of China[245]
- Copyright Law of the People's Republic of China[246]
- Law of the People's Republic of China on the Protection of Minors[247]
- Law of the People's Republic of China on Punishments in Public Order and Security Administration[248]

Cyber Crime Laws – Substantive Criminal Law

[234] *Internet in China, The*, Information Office of the State Council of the People's Republic of China, Beijing, June 2010. pp. 17-23.
[235] *Decision of the Standing Committee of the National People's Congress on Maintaining Internet Security, The*, 19th Meeting of the Ninth Standing Committee of the National People's Congress, 28 December 2000.
[236] *Law of the People's Republic of China on Electronic Signatures, The*, 11th Conference of the Standing Committee of the 10th State Council of the People's Republic of China, 28 August 2004.
[237] *Regulations on Telecommunications of the People's Republic of China*, 31st Regular Meeting of the State Council, 20 September 2000.
[238] *Measures on the Administration of Internet Information Services*, 31st Regular Meeting of the State Council, 20 September 2000.
[239] *Regulations on the Protection of Computer Information System Security of the People's Republic of China*, Decree No. 147, State Council of the People's Republic of China, 18 February 1994.
[240] *Regulations on the Protection of the Right to Online Dissemination of Information*, Order No. 468 of the State Council, 135th Executive Session of the State Council, 10 May 2006.
[241] *Provisions on the Administration of Foreign-funded Telecommunications Enterprises*, Decree No. 333 of the 49th Executive Meeting of the State Council, 5 December 2001.
[242] *Measures on the Administration of Security Protection of the International Networking of Computer Information Networks*, Decree No. 33 of the State Council, 11 December 1997.
[243] *Provisions on the Administration of Internet News Information Services*, Information Office of the State Council (SCIO) and Ministry of Information Industry (MII), 25 September 2005.
[244] *Provisions on the Administration of Electronic Bulletin Services via the Internet*, 4th Ministerial Meeting of the MII, 8 October 2000.
[245] *General Principles of the Civil Law of the People's Republic of China*, 4th Session of the Sixth National People's Congress, 12 April 1986.
[246] *Copyright Law of the People's Republic of China*, 15th Meeting of the Standing Committee of the Seventh National People's Congress on September 7, 1990; amended according to the Decision on Amending the Copyright Law of the People's Republic of China, 24th Meeting of the Standing Committee of the Ninth National People's Congress, 27 October 2001.
[247] *Law of the People's Republic of China on the Protection of Minors*, 21st Meeting of the Standing Committee of the Seventh National People's Congress, 4 September 1991.
[248] *Law of the People's Republic of China on Punishments in Public Order and Security Administration*, 17th Meeting of the Standing Committee of the Tenth National People's Congress of the People's Republic of China, 28 August 2005.

Both the United States and China are developing laws and regulations to deal with cyber crimes. Table 24 provides a summary of the substantive criminal law using a comparison of the Council of Europe Convention for structure. The one notable difference in this area is Article 6, 'Misuse of Devices', where China does not yet have a law according to this analysis.

Table 23. Legal Coverage Comparison – Substantive Criminal Law

China[249]	Article	Council of Europe Framework	United States
Chapter II - Measures to be taken at the national level *Section 1 – Substantive criminal law*			
Art. 285 of Criminal Law of the People's Republic of China	2	**Illegal access**	18 U.S.C. § 1030 (2) (1) – (5)[250]
Art. 252 of Criminal Law of the People's Republic of China	3	**Illegal interception**	18 U.S.C. § 1030; 18 U.S.C. § 2511
Art. 286 of Criminal Law of the People's Republic of China	4	**Data interference**	18 U.S.C. § 1030 (a) (5)
Art. 286 of Criminal Law of the People's Republic of China	5	**System interference**	18 U.S.C. § 1030 (a) (5)
There is no provision related in China legislation	6	**Misuse of devices**	18 U.S.C. § 1029; 18 U.S.C. § 1030; 18 U.S.C. §2512[251]
Art. 287 "or other crimes" of Criminal Law of the People's Republic of China	7	**Computer-related forgery**	18 U.S.C. § 1029[252]
Art. 287 "or other crimes" of Criminal Law of the People's Republic of China	8	**Computer-related fraud**	18 U.S.C. § 1030 (a) (4); 18 U.S.C. § 1343
Arts. 363, 364, 367 of Criminal Law of the People's Republic of China	9	**Offences related to child pornography**	18 U.S.C. §2251; 18 U.S.C. §2252; 18 U.S.C. §2252A

[249] Hong Kong has a few exceptions in its regional legislation. Those exceptions were not reflected in this table.
[250] The United States of America declares, pursuant to Articles 2 and 40, that under United States law, the offenses set forth in Article 2 ("Illegal access") includes an additional requirement of intent to obtain computer data.
[251] The United States of America declares, pursuant to Articles 6 and 40, that under United States law, the offense set forth in paragraph (1) (b) of Article 6 ("misuse of devices") includes a requirement that a minimum number of items be possessed. The minimum number shall be the same as that provide for by applicable United States federal law.
[252] The United States of America declares, pursuant to Articles 7 and 40, that under United States law, the offenses set forth in Article 7 ("Computer-related forgery") includes a requirement of intent to defraud.

Cyber Crime Laws – Copyright and Related Rights

Both the United States and China have laws and regulations to deal with cyber crimes, including offenses related to infringements of copyright and related rights. Table 25 provides a summary of these laws using a comparison of the Council of Europe Convention for structure. Both and China and the U.S. have some laws for each of the four articles of the COE framework.

Table 24. Legal Coverage Comparison – Copyright and Related Rights

China[253]	Article	Council of Europe Framework	United States
Title 4 – Offences related to infringements of copyright and related rights			
Arts. 217, 218, 220 of Criminal Law of the People's Republic of China. Art. 1 "protecting the copyright of authors in their literary, artistic and scientific works and the copyright-related rights and interests" of Copyright Law of the People's Republic of China. See also Art. 3, Art. 9, Art. 10 (5), "by any other means," (6) "the right of distribution" of Copyright Law of the People's Republic of China. For Art. 10 (2) – Arts. 10 (11-12), (15); Art. 12 "adaptation, translation" of Copyright Law of the People's Republic of China. Also Art. 11 "the copyright in a work shall belong to its author" and Art. 20; Art. 24(2) of Copyright Law of the People's Republic of China.	10	**Offences related to infringements of copyright and related rights**	18 U.S.C. §2319; 17 U.S.C. §506
Arts. 22, 23, 24, 27, 29 of Copyright Law of the People's Republic of China	11	**Attempt and aiding or abetting**	Aiding and Abbeting: 18 U.S.C. §2 Attempt: 18 U.S.C. §1030 (c); 18 U.S.C. §1029 (b); 18 U.S.C. §2251 (d); 18 U.S.C. §2252 (b); 18 U.S.C. §2252A (b)
Arts. 30, 31 of Copyright Law of the People's Republic of China	12	**Corporate liability**	Common law recognizes corporate criminal as well as civil liability. See for example: 18 U.S.C. §1030 (e);
Arts 32, 33, 34 of Copyright Law of the People's Republic of China	13	**Sanctions and measures**	See for example: 18 U.S.C. §1030 of the U.S. Code

[253] Hong Kong has a few exceptions in its regional legislation. Those exceptions were not reflected in this table.

Cyber Crime Laws – Procedural Law

Both the United States and China are developing laws and regulations to deal with procedural law as it relates to cyber crimes. Table 26 provides a summary of these laws using a comparison of the Council of Europe Convention for structure. Of note, China does not yet have laws for conditions and safeguards (Article 15), expedited preservation of stored computer data (Article 16), and production order (Article 18). The United States has some unique laws around conditions and safeguards.

Table 25. Legal Coverage Comparison – Procedural Law

China[254]	Article	Council of Europe Framework	United States
Section 2 – Procedural Law			
There is no provision related in China legislation	14	**Scope of procedural provisions**	
There is no provision related in China legislation	15	**Conditions and safeguards**	Common law has a complex system of safeguards that meet the requirements of the Convention on Cybercrime
There is no provision related in China legislation	16	**Expedited preservation of stored computer data**	18 U.S.C. §2703 (f)
Art. 14 of Regulation on internet Information Service of the People's republic of China, Art. 19 of Working rules of Interim Regulation of International networking of Computer Information network, Art. 10 of Regulations on Internet Surfer Service Sites, Arts. 14, 15 of Provisions for the Administration of Internet Electronic Bulletin	17	**Expedited preservation and partial disclosure of traffic data**	18 U.S.C. §2703 (f)
There is no provision related in China legislation	18	**Production order**	18 U.S.C. §2703
Art. 116 of Criminal Procedure Law of the People's Republic of China, Art. 188, 192 of People's Procuratorate Rules of Criminal Procedure, Arts. 57, 58 of Procedural Rules for Criminal Cases by Public Security Organs	19	**Search and seizure of stored computer data**	18 U.S.C. §2513
Art. 10 of State Security Law of the People's Republic of China, Art. 16 of People's police Law of the People's Republic of China	20	**Real-time collection of traffic data**	18 U.S.C. §2704; 18 U.S.C. §3121-3127
Art. 10 of State Security Law of the People's Republic of China, Art. 16 of People's police Law of the People's Republic of China	21	**Interception of content data**	18 U.S.C. §2511

[254] Idem.

Cyber Crime Laws – Jurisdiction

Both the United States and China have laws and regulations to deal with jurisdiction as it relates to cyber crimes. Table 27 provides a summary of these laws using a comparison of the Council of Europe Convention for structure. The United States has some distinctions of note.

Table 26. Legal Coverage Comparison - Jurisdiction

China[255]	Article	Council of Europe Framework	United States
Section 3 - Jurisdiction			
Arts. 6, 7, 8, 9, 10, 11, 12 of Copyright Law of the People's Republic of China	22	**Jurisdiction**	No single clause implementation. In general federal criminal jurisdiction is conferred by an element of interstate or foreign commerce or communication. Even by making use of the possibility to restrict the jurisdiction the federal jurisdiction will not be fully correspond with the requirements of Art. 22 CoC

[255] Idem.

Cyber Crime Laws – International Cooperation

China has laws and regulations to deal with international cooperation as it relates to cyber crimes. Table 28 provides a summary of these laws using a comparison of the Council of Europe Convention for structure. In this comparison, the United States has numerous distinctions of note. The U.S. tends to cooperate with other countries on a bilateral basis.

Table 27. Legal Coverage Comparison – International Cooperation

China[256]	Article	Council of Europe Framework	United States
Chapter III – International cooperation			
Arts. 3, 4, 5, 7, 8, 9 of Extradition Law of the People's Republic of China	24	**Extradition**	
There is no provision related in China legislation	25	**General principles relating to mutual assistance**	
There is no provision related in China legislation	26	**Spontaneous information**	
There is no provision related in China legislation	27	**Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**	See note[257]
There is no provision related in China legislation	28	**Confidentiality and limitation on use**	
There is no provision related in China legislation	29	**Expedited preservation of stored computer data**	
There is no provision related in China legislation	30	**Expedited disclosure of preserved traffic data**	
There is no provision related in China legislation	31	**Mutual assistance regarding accessing of stored computer data**	
There is no provision related in China legislation	32	**Trans-border access to stored com data with consent of where publicly available**	
There is no provision related in China legislation	33	**Mutual assistance in the real-time collection of traffic data**	
There is no provision related in China legislation	34	**Mutual assistance regarding the interception of content data**	
There is no provision related in China legislation	35	**24/7 Network**	See note[258]

Notes:

The U.S. and China do not have an extradition treaty thus the blank for the U.S. with regard to Art. 24. Some of the blanks for the U.S. and assertions that there is no Chinese law on articles relating to legal assistance do not take account of the U.S.-China MLAT, which is available here: http://www.state.gov/documents/organization/126977.pdf. The use of bi-lateral treaties to address legal assistance is standard in international law, and the U.S. has MLATs with most countries. The blank for Art. 35 (24/7 point of contact) is questionable. One of the U.S. Declarations upon ratifying the

[256] Idem.
[257] The United States of America declares, pursuant to Articles 27 and 40, that requests made to the United States under paragraph 9(e) of Article 27 ("Procedures pertaining to mutual assistance requests in the absence of applicable international agreements") are to be addressed to its central authority for mutual assistance.
[258] Pursuant to Article 35, paragraph 1, of the Convention, the Computer Crime and Intellectual Property Section, United States Department of Justice, Criminal Division, Washington, D.C., 20530, is designated as the point of contact available on a twenty-four hour, seven-day-a-week basis to ensure the provision of immediate assistance under the Convention.

treaty designates the point of contact: Computer Crime and Intellectual Property Section, United States Department of Justice, Criminal Division, Washington, D.C., 20530.[259]

Cyber Crime Laws – Additional Notes

Within the United States there is cooperation among federal, state and local levels of law enforcement to both investigate and prosecute cyber crimes. The Chinese experts were quite aware of the laws in China that prohibit the misuse of social media, such as Weibo, and hacking critical infrastructure.[260] China is making progress revising its legal system and cooperation between central and local governments.

> Such theft of intellectual property rights (I.P.R.) is contrary to China's domestic law and international treaty commitments in place for more than a decade. Recent efforts by China to honor its commitments have been substantial considering that it had no such laws for most of its history. But there is a joke in China that its courts are where American corporations go to lose I.P.R. cases.[261]

China's Laws Prohibit Theft of Trade Secrets

China has detailed laws on the books against individuals or organizations that infringe upon business secrets:

> Article 219
> Whoever commits any of the following acts of infringing on business secrets and thus causes heavy losses to the obligee shall be sentenced to fixed-term imprisonment of not more than three years or criminal detention and shall also, or shall only, be fined; if the consequences are especially serious, he shall be sentenced to fixed-term imprisonment of not less than three years but not more than seven years and shall also be fined :
>
> (1) obtaining an obligee's business secrets by stealing, luring , coercion or any other illegitimate means;
> (2) disclosing, using or allowing another to use the business secrets obtained from the obligee by the means mentioned in the preceding paragraph; or
> (3) in violation of the agreement on or against the obligee's demand for keeping business secrets, disclosing, using or allowing another person to use the business secrets he has.
>
> Whoever obtains, uses or discloses another's business secrets, which he clearly knows or ought to know falls under the categories of the acts listed in the preceding paragraph, shall be deemed an offender who infringes on business secrets.
>
> "Business secrets" as mentioned in this Article refers to technology information or business information which is unknown to the public, can bring about economic benefits to the obligee, is of practical use and with regard to which the obligee has adopted secret-keeping measures.
>
> "Obligee" as mentioned in this Article refers to the owner of business secrets and the person who is permitted by the owner to use the business secrets.
>
> Article 220
> Where a unit commits any of the crimes mentioned in the Articles from 213 through 219 of this Section, it shall be fined, and the persons who are directly in charge and the other persons who are directly responsible for the crime shall be punished in accordance with the provisions of the Articles respectively.[262]

There is no special cyber law or regulations for the military, and the applicable articles of the Criminal Law Code should apply.[263]

---

[259] Notes from David Fagan.
[260] Wiebo is a Twitter-like micro-blogging application. E.g., On August 25, 2013, the CNCERT detected that the source of a DDoS attack was a hacker in Qingdao City. Nan Zhang, *Attack .CN Domain Hacker Arrested in Qingdao*, Read Daily News, 23 September 2013.
[261] Austin, Greg, *China Won't Cut Its Cyberspying*, The New York Times, 19 February 2013.
[262] *Criminal Law of the People's Republic of China*, 2nd Session of the Fifth National People's Congress (1979); revised at the 5th Session of the Eighth National People's Congress on 14 March 1997.

APPENDIX B: Experts Survey

*As part of the study, a survey was used to collect the perspectives of the contributors. This survey was **not** designed to be a scientific study, but rather an efficient means of collecting a large amount of information in a consistent way. Because of the critical mass of expertise represented by this group, some of these responses are cited in support of some key observations (Section 3).*

China-US Cyber Security Dialogue
Cyber Security Cooperation Survey Report
（October 2013）

Hosted by:

中国互联网协会
Internet Society of China

Organizer:
Network and Information Security Committee, Internet Society of China

Preface

Since 2009, the Internet Society of China (ISC) and the think-and-do tank EastWest Institute (EWI) began to cooperate on the project of China-U.S. bilateral dialog on Cyber Security at a non-government level. The project plans to carry out four main subjects, namely, fighting spam, anti-hacking, youth protection and intellectual property protection. During nearly 12 months from 2010 to 2011, ISC and EWI have successfully cooperated on fighting spam. After published, the final report Fighting Spam to Build Trust is broadcasted and presented in many international conferences such as the World Cybersecurity Summit hosted by EWI and conferences hosted by the Messaging, Malware and Mobile Anti-Abuse Working Group (MAAWG). And major media, such as The New York Times, have given high profile coverage and positive reviews.

In 2013, the China-U.S. Dialogue on Cyber Security project launched the second subject with the theme anti-hacking. As the cyber security situation is grim and both China and the U.S. are paying great attentions on this topic, the Chinese experts team and the U.S. experts team were established with a big number of carefully chosen people who have great experience or insights on cybersecurity . In order to enhance the cooperation between China and the U.S. in cyberspace security, two teams from each sides held nearly ten talks, including conference calls, Web conferencing and face-to-face meetings, with topics of the definition of hacking, the understanding to current cyber security situation and threats and the understanding of cooperation between China and the U.S. At present, both sides are drafting the final report, of which the core insights and part of the achievements is planning to be presented on the World Cyberspace cooperation Summit IV held at the beginning of November in Silicon Valley in America.

In order to know better about the Internet industry in China and the U.S., especially the insights of experts on the current cyber security situation and the relationship on cyber security between both sides, the joint China-U.S. working team developed a survey, which aims to study the advises that enhance the bilateral cooperation on Internet Industry and build trust. There are 74 Chinese experts and 12 U.S. experts taking part in the survey. Here we would like to extend sincerest thanks to them!

Network and Information Security Committee
Internet Society of China

[263] Consultation with Professor Liu Deliang, Director of Asia-Pacific Institute for Cyber-law Studies, Professor of Law at the Law School, Beijing Normal University, October 2013.

Table of Contents

Abstract

1. Background of the participants

- Most of the participants are professionals in cyber security the area.

2. Knowledge on cyber security situation

- Both China and the U.S. held negative attitudes toward the cyber security situation.
- The most serious technical problem of cyber security is the vulnerability of information system.
- The two main sources of cyber threat are the cyber attacks launched by hacking underground economy and the attacks by nations.
- Every country will develop cyber warfare capabilities either openly or secretly. The cyber war is inevitable unless necessary measures are taken.
- The U.S. has the strongest cyber war capability. China thinks that the most possible country to launch a cyber war is the U.S., and the U.S. thinks it's North Korea who is the most possible nation to launch a cyber war.

3. Perceptions on cyber security cooperation between China and the U.S.

- The current situation of cooperation between two sides is fair, but there are few tangible examples of cooperation.
- China thinks that the threats from the U.S. to China is bigger than the threats from China to the U.S.

4. Suggestions on enhancing cyber security cooperation between China and the U.S.

- Establish a mutual trust mechanism, strengthen communication and cooperate at multiple levels.
- Improve laws and regulations, and cooperate in handling cross-border cyber crime at government regulation level.
- Pay more efforts to the cooperation on a technical level. Realize the win-win relationship.

Chapter 1 Introduction to the Survey

1. Scope

This survey was organized by the Internet Society of China and the EastWest Institute, as a part of the ongoing joint China-U.S. cyber security dialogue. The goal of this survey is to consult the professionals from both sides and understand their insights of the current Internet security situation and relationship between China and the U.S. in cyber security, and moreover, ask for their advice to improve. The survey focuses on the following aspects:

- Macroscopic knowledge and technical analysis to global Internet circumstances by both sides
- Understanding of Internet cooperation and the relationship between China and the U.S. in the cyber area
- Suggestions on advancing cyber security cooperation and building mutual trust between China and the U.S.

2. Approaches

This survey has multiple choice questions, logical order questions and essays. In order to reflect the real and subjective opinion of the participants, this survey is carrying out anonymously. There are

online questionnaire part and off-line part.

1. Offline: the members of cyber security dialogue team receive the questionnaire and the committee secretary collected the survey results.
2. Online: the survey is released on web platform, and we invite experts from both sides and the people who care about the cyber security in the industry.

Chapter 2 Knowledge Background of participants

1. Working background of participants

The participants who are mainly engaged in cyber-security technology research and operations is 81.08 percent of the total. Most of the participants have a professional cyber security field background, so the result of the survey in a way represent the opinion of those who work in cyber security area from both China and the U.S.

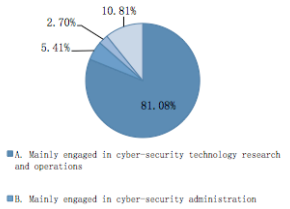


Figure-1 Status that the participants are engaged in cyber-security

2. The channel to get knowledge and information of cyber security

Most of the participants get knowledge and information of cyber security from their own research and the results of their own work or their peers'.

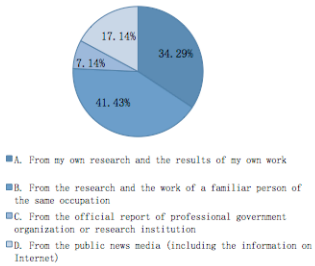


Figure-2 Channel to get knowledge and information of cyber security

Chapter 3 Current situation of cyber security

1. Understanding to current global network security

Both China and the U.S. think the current situation of global network security is not positive, none of them think that the current network is completely safe. More than 90 percent of the participants think that there are problems in cyber security, most of which think that the overall situation is worrying, and there are a lot of serious problems. In a word, the situation of network security is very grim.

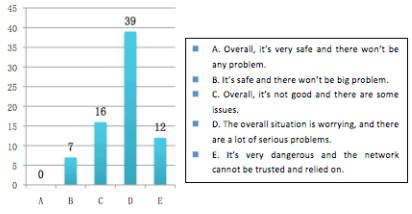


Figure-3 Current situation of cyber security

2. Rank of the problems that the Internet faces now

Both sides think the most serious problem that the Internet faces now is the vulnerabilities of Information system. For the second

serious one, the Chinese experts think malicious code flood (including Botnet and Trojan) and serious APT attack are next to the vulnerabilities, while the American experts think the flaws of the architecture and protocols of IP routing system, DNS and serious DDoS attack are next to the top.

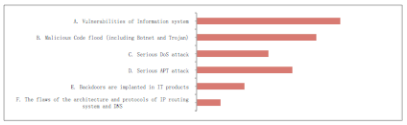


Figure-4-a Security problem ranking by Chinese participants

Figure-4-b Security problem ranking by American participants

3. Source of the Internet security threats

Both sides think that the state-sponsored cyber attacks and hacker underground economy-sponsored cyber attacks are the main source of threats to Internet security.

Figure-5-a Rank of the source of threats by Chinese experts

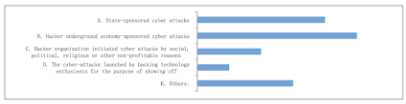


Figure-5-b Rank of the source of threats by American experts

4. Cyber war

When thinking about the potential for the cyber war in the future, both sides think that each country will develop cyber warfare capabilities either aboveboard or secretly. The cyber war is inevitable unless necessary measures are carried out. 24.32 percent of the Chinese participants and half of the American participants think that the cyber war between nations can be avoided and there are approaches to address it peacefully.

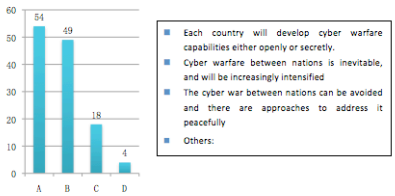


Figure-6 Survey on Cyber war

5. Capability of cyber war of each country and their possibilities to launch cyber war

Both sides think that the U.S. is the country who has the strongest capability in cyber war. However, Chinese experts think it is the U.S. who is most possible to launch a cyber war, while the U.S. experts think it is North Korea who is most possible to do this.

✧ Ranking of cyber war capability for each country

Ranking by Chinese participants

U.S.> Russia>North Korea>Israel>China>Iran>South Korea>France>U.K.>India>Japan>Germany>Australia

Ranking by American participants

U.S.>China>North Korea>Russia>Israel>Australia>Japan>France>U.K.>Iran>South Korea>India>Germany

✧ **Ranking of possibility of each country to launch cyber war**

Ranking by Chinese participants

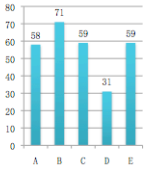
U.S.>Israel>North Korea>China>Russia>Iran>UK>Japan>Australia>France>India>South Korea>Germany

Ranking by American participants

North Korea>Iran>China>Israel>UK>Austrilia>Japan>France>India>U.S.>South Korea>Germany

6. The purpose of countries to launch cyber war

For the actions that launch a cyber war to another country, both sides think the purpose is aiming at government and military information. The survey result of American experts shows that meanwhile they want to steal data and information from others' companies, research institutions, and social organizations. Whereas the Chinese experts think their purposes next to the top is that they not only want to steal data and information from others' companies, research institutions, and social organizations, but also want to sabotage others' Internet infrastructure, power, finance and other important information systems.



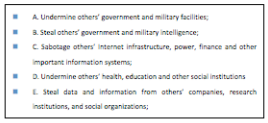


Figure-7 Purpose of cyber war

7. Main factors leading to the growth of underground economy of hacking

Chinese and the U.S. experts hold different opinions of the main factors which lead to the growth of underground hacking industry. The Chinese experts think the main reason is that the level of protection to information system is poor and the security awareness of user is weak, while the U.S. experts think that the main reason is that it's easy for hackers to get the technology and tools to launch cyber attack.

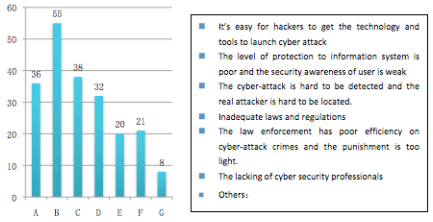


Figure-8 Reason of the growth of underground hacking industry

Chapter 4 Relationship between China and the U.S. on cyber security

1. Current situation of cooperation between two sides.

Both China and the U.S. think the cooperation between the two sides is fair and there are few tangible examples of cooperation. There are many divergences in communication and dialogue. 44.59 percent of the Chinese experts think that the two countries are able to communicate with each other and have some cooperation, while half of the U.S. experts think there is a lot of divergence between the two sides.

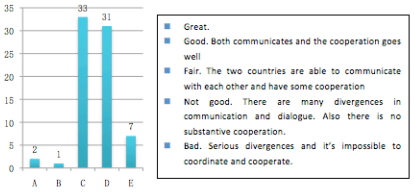


Figure-9 Current situation of China-U.S. cooperation

2. Mutual influence from China and the U.S. to each other

The two sides hold different views on this topic. 85.13 percent of Chinese participants think the threats from the U.S. to China are greater than the threats from China to the U.S., but none of the U.S. participants hold the same idea. 33.33 percent of the American participants think the threats from China to the U.S. are greater than the threats from the U.S. to China, whereas only 1.35 percent of the Chinese participants hold the same idea as the American participants. Half of U.S. participants think the influences from China and the U.S. are the same to each other.

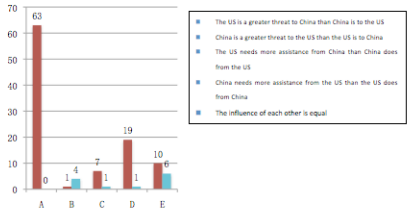


Figure-10 Mutual influence

3. Problems and obstacles on China-U.S. cyber security cooperation

The main obstacle on the front of the cooperation between the two sides at the cyber security level is the serious lack of trust in politics and deviation in knowledge as well as understanding between each other.

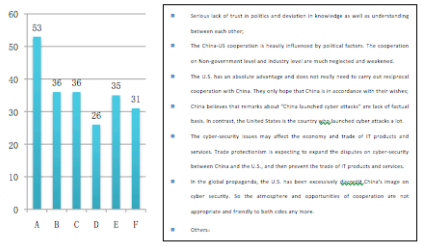


Figure-11 Problems and obstacles of cooperation

4. Breakthrough points of cooperation

Both China and the U.S. think two sides should strengthen the communication and talks at high government level. The Chinese experts think we should attach importance to encourage and pay more attention on the non-government level and industry level cooperation, while the American experts think the cooperation should seek opportunities to work together on laws and regulations.

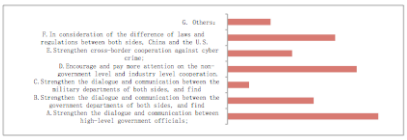


Figure-12-a Ranking of breakthrough points by Chinese experts

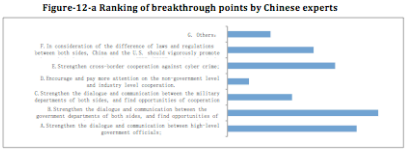


Figure-12-b Ranking of breakthrough points by the U.S. experts

(Options:

A. Strengthen the dialogue and communication between high-level government officials;

B. Strengthen the dialogue and communication between the government departments of both sides, and find opportunities of cooperation in the laws, regulations and regulatory mechanisms;

C. Strengthen the dialogue and communication between the military departments of both sides, and find opportunities of cooperation on cyber war control;

D. Encourage and pay more attention on the non-government level and industry level cooperation;

E. Strengthen cross-border cooperation against cyber crime;

F. In consideration of the difference of laws and regulations between both sides;China and the U.S. should vigorously promote the technical cooperation between CERTs/CSIRTs to jointly deal with cyber attacks.

Chapter 5 Suggestions on China-U.S. cyber security cooperation

1. Importance of cooperation

1.1 Precondition

From the perspective of the survey results, China and the U.S. have very little tangible cooperation in the cyber security area and have a lot of divergence because of the lack of trust in politics. Chinese and American experts suggest that the two sides build trust at the government level, establish regular communication channels, exchange frequent ideological thoughts with each other and have meetings and forums at high government levels. Mutual trust is one of the necessary preconditions for cooperation and strengthening communication, which is the most effective way to build mutual trust, eliminating potential instability of the ongoing cooperation as well as in the future. This lays a good foundation for cooperation.

1.2 Breakthrough points

In order to break the wall, experts from both sides suggest that China and the U.S. begin to cooperate in fields that both sides could benefit from. It is very important to cooperate in the area with the same thoughts, however, at the same time allow the existence of divergence. On this basis, China and the U.S. could extend cooperation to more fields. Thus, two sides should be explicit in their respective interests. For example, China and the U.S. could cooperate on handling cyber crime, terrorism and technology on the field of cyber security.

2. Different levels of cooperation

2.1 Laws and regulations

Participants suggest cooperating on the laws, regulations and supervision mechanism, and establishing legislation research team.

2.2 Government level

Cross-border cyber crimes are increasingly furious. The Chinese experts hope that the governments of both sides could strengthen cooperation on handling cross-border cyber crimes. Both China and the U.S. participants suggest establishing a joint emergency coordination center. The Chinese suggest building standard response process for security incidents in industry and establish regular notification mechanism to notify and exchange the information of security incidents of both sides.

Moreover, the Chinese suggest that the governments of both sides take measures to lower the influence from the trade protectionism on the cyber security cooperation. It is a good method to set up certification mechanisms to identify and assess companies according to a standard process when they are entering the market without the influence of politics.

The Chinese experts also suggest bringing in persons with expertise in the community. Community experts may hold different views to the same problem, which make the solution more comprehensive and protect information security more completely.

2.3 Technical cooperation

The two sides suggest strengthening technical communication and sharing, cooperating in areas which both could benefit from such as spam, phishing and DDoS attacks. The Chinese suggest the two sides open more software product source code and intellectual property. They suggest for the U.S. to open more Internet resources such as IP addresses and the domain name system.

Chapter 6 Conclusion

1. Understanding from both sides to cyber security situation

Both Chinese and American experts think the current network situation is overall worrying and there are a lot of serious problems. Moreover, they think each country will develop cyber war capability and the cyber war is inevitable unless we take relative measures. Meanwhile, the main sources of threats is the hacking attacks launched by nation actions and hacking industry, which both sides think the latter is on the top.

2. Understandings from both sides to cyber security relationship

Both China and the U.S. think the cooperation between them is fair. They could seldom carry out tangible cooperation because of the divergences and lack of communication. They also think the political factor has great impact on the China-U.S. cooperation on Internet security. The lack of trust in politics results in few achievements of the cyber security cooperation. At the same time, the experts from both sides think that China and the U.S. should build communication and carry out cooperation as soon as possible.

3. Advice from both sides

On one hand, both sides suggest strengthening communication and begin cooperation at the government level, especially relevant departments. On the other hand, they suggest carrying out tangible, specific cyber security protection and incident handling oriented in technical cooperation at the Internet industry level as well as at the emergency response level. It could not only circumvent political contradiction, but also make a contribute to the Internet security protection of both countries. Furthermore, the achievements of the cooperation at this level could drive the cooperation at government level in turn.

APPENDIX C: Example Templates for Policy Statements

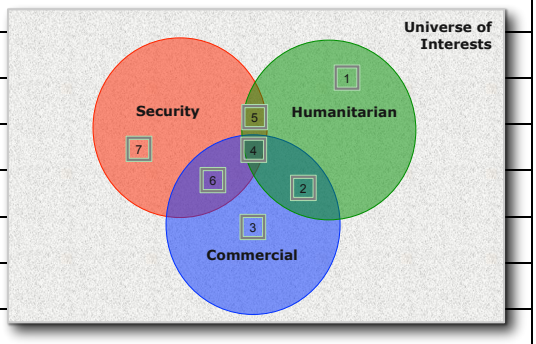
Recommendation No. 1, *Stated Policy*, These example checklists are intended to supplement the introduction provided in Section 4.1, *Stated Policy*. They are intended to serve as starting points for internal discussions around developing a policy statement of sufficient completeness and clarity. They are not complete in terms of being able to suggest all issues to consider. Thus, stakeholders should be consulted to identify additional components that should be considered.

The following examples are provided here in this appendix:

- Example Policy Checklist A – Disaster Relief Organization
- Example Policy Checklist B – For-Profit Hospital
- Example Policy Checklist C – Public Communications Network Operator
- Example Policy Checklist D – Internet Search Engine
- Example Policy Checklist E – An Airport
- Example Policy Checklist F – International Relations Think Tank
- Example Policy Checklist G – Defense Contractor
- Example Policy Checklist H – Defense Department

Table 28. Example Policy Statement A – Disaster Relief Organization

The Interests of the Organization (select one)
☒ 1. Humanitarian
☐ 2. Humanitarian + Commercial
☐ 3. Commercial
☐ 4. Humanitarian + Commercial + Security
☐ 5. Humanitarian + Security
☐ 6. Commercial + Security
☐ 7. Security
☐ 8. Other

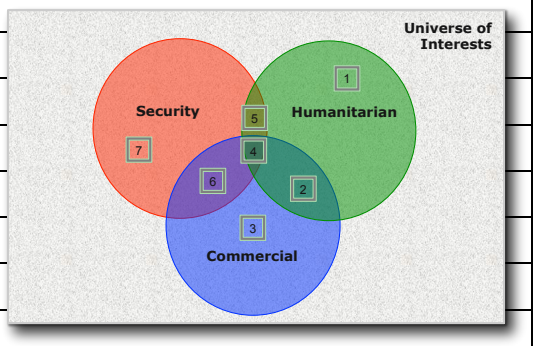


The Organization's Normal Use of Assets in Cyberspace (select one)
☒ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐ 3. Generate a profit for owners
☐ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☐ 7. Engage in belligerent activities
☐ 8. Other (describe)

Explicit Conditions for Exceptions (select all that apply)
☐ A. None
☐ B. In response to lawful government directive in home country
☐ C. In response to lawful government directive in foreign country where operating
☐ D. In response to lawful government directive in foreign country where *not* operating
☐ E. In response to government request in home country
☐ F. In response to government request in foreign country where operating
☐ G. In response to government request in foreign country where *not* operating
☒ H. Voluntary assistance in cases where life or human safety are threatened
☐ I. Voluntary assistance in cases of a state of national emergency
☐ J. "Hacking-back" at sources of malicious activity
☐ K. Academic research
☐ L. Other (describe)

Table 29. Example Policy Statement B – For-Profit Hospital

The Interests of the Organization (select one)	
☐	1. Humanitarian
☒	2. Humanitarian + Commercial
☐	3. Commercial
☐	4. Humanitarian + Commercial + Security
☐	5. Humanitarian + Security
☐	6. Commercial + Security
☐	7. Security
☐	8. Other



The Organization's Normal Use of Assets in Cyberspace (select one)	
☐	1. Serve medical, cultural or spiritual needs
☒	2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐	3. Generate a profit for owners
☐	4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐	5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐	6. Generate a profit for owners and engage in belligerent activities
☐	7. Engage in belligerent activities
☐	8. Other (describe)

Explicit Conditions for Exceptions (select all that apply)	
☐	A. None
☒	B. In response to lawful government directive in home country
☐	C. In response to lawful government directive in foreign country where operating
☐	D. In response to lawful government directive in foreign country where *not* operating
☐	E. In response to government request in home country
☐	F. In response to government request in foreign country where operating
☐	G. In response to government request in foreign country where *not* operating
☐	H. Voluntary assistance in cases where life or human safety are threatened
☐	I. Voluntary assistance in cases of a state of national emergency
☐	J. "Hacking-back" at sources of malicious activity
☐	K. Academic research
☐	L. Other (describe)

Table 30. Example Policy Statement C – Public Communications Network Operator

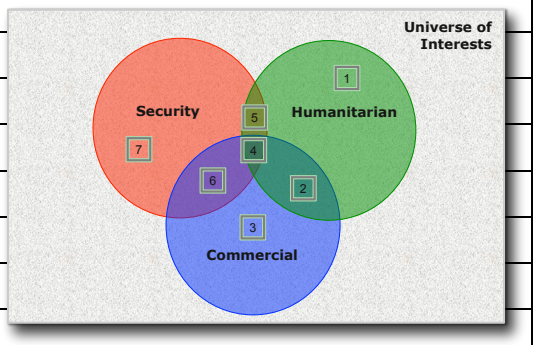
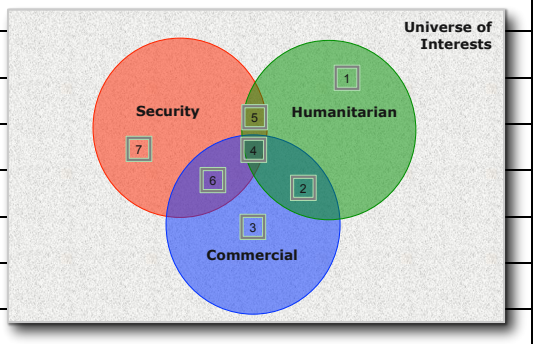
The Interests of the Organization (select one)	
☐	1. Humanitarian
☐	2. Humanitarian + Commercial
☒	3. Commercial
☐	4. Humanitarian + Commercial + Security
☐	5. Humanitarian + Security
☐	6. Commercial + Security
☐	7. Security
☐	8. Other
	
The Organization Normal Use of Assets in Cyberspace (select one)	
☐	1. Serve medical, cultural or spiritual needs
☐	2. Serve medical, cultural or spiritual needs and generate a profit for owners
☒	3. Generate a profit for owners
☐	4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐	5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐	6. Generate a profit for owners and engage in belligerent activities
☐	7. Engage in belligerent activities
☐	8. Other (describe)
Explicit Conditions for Exceptions (select all that apply)	
☐	A. None
☒	B. In response to lawful government directive in home country
☒	C. In response to lawful government directive in foreign country where operating
☐	D. In response to lawful government directive in foreign country where *not* operating
☐	E. In response to government request in home country
☐	F. In response to government request in foreign country where operating
☐	G. In response to government request in foreign country where *not* operating
☒	H. Voluntary assistance in cases where life or human safety are threatened
☒	I. Voluntary assistance in cases of a state of national emergency
☐	J. "Hacking-back" at sources of malicious activity
☐	K. Academic research
☐	L. Other (describe) – products can have dual use and be used for humanitarian purposes (i.e. in a disaster)

Table 31. Example Policy Statement D – Internet Search Engine

The Interests of the Organization (select one)
☐ 1. Humanitarian
☐ 2. Humanitarian + Commercial
☒ 3. Commercial
☐ 4. Humanitarian + Commercial + Security
☐ 5. Humanitarian + Security
☐ 6. Commercial + Security
☐ 7. Security
☐ 8. Other

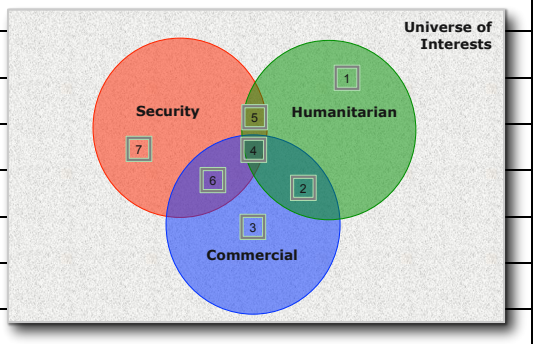


The Organzition's Normal Use of Assets in Cyberspace (select one)
☐ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☒ 3. Generate a profit for owners
☐ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☐ 7. Engage in belligerent activities
☐ 8. Other (describe)

Explicit Conditions for Exceptions (select all that apply)
☐ A. None
☐ B. In response to lawful government directive in home country
☒ C. In response to lawful government directive in foreign country where operating
☐ D. In response to lawful government directive in foreign country where *not* operating
☐ E. In response to government request in home country
☐ F. In response to government request in foreign country where operating
☐ G. In response to government request in foreign country where *not* operating
☐ H. Voluntary assistance in cases where life or human safety are threatened
☐ I. Voluntary assistance in cases of a state of national emergency
☒ J. "Hacking-back" at sources of malicious activity
☐ K. Academic research
☐ L. Other (describe)

Table 32. Example Policy Statement E – An Airport

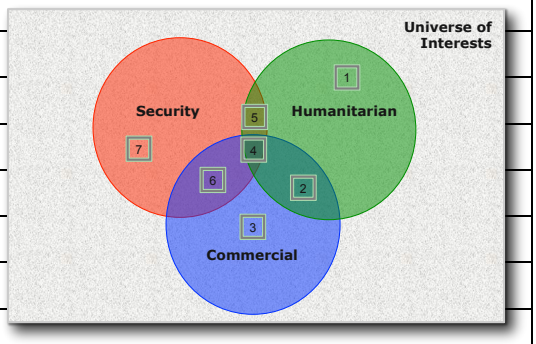
The Interests of the Organization (select one)
☐ 1. Humanitarian
☐ 2. Humanitarian + Commercial
☐ 3. Commercial
☒ 4. Humanitarian + Commercial + Security
☐ 5. Humanitarian + Security
☐ 6. Commercial + Security
☐ 7. Security
☐ 8. Other



The Organization's Normal Use of Assets in Cyberspace (select one)
☐ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐ 3. Generate a profit for owners
☒ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☐ 7. Engage in belligerent activities
☐ 8. Other (describe)

Explicit Conditions for Exceptions (select all that apply)
☐ A. None
☐ B. In response to lawful government directive in home country
☐ C. In response to lawful government directive in foreign country where operating
☐ D. In response to lawful government directive in foreign country where *not* operating
☐ E. In response to government request in home country
☐ F. In response to government request in foreign country where operating
☐ G. In response to government request in foreign country where *not* operating
☐ H. Voluntary assistance in cases where life or human safety are threatened
☐ I. Voluntary assistance in cases of a state of national emergency
☐ J. "Hacking-back" at sources of malicious activity
☐ K. Academic research
☐ L. Other (describe)

Table 33. Example Policy Statement F – International Relations Think Tank

The Interests of the Organization (select one)	
☐ 1. Humanitarian	
☐ 2. Humanitarian + Commercial	
☐ 3. Commercial	
☐ 4. Humanitarian + Commercial + Security	
☒ 5. Humanitarian + Security	
☐ 6. Commercial + Security	
☐ 7. Security	
☐ 8. Other	

The Organization's Normal Use of Assets in Cyberspace (select one)
☐ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐ 3. Generate a profit for owners
☐ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☒ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☐ 7. Engage in belligerent activities
☒ 8. Other (describe) *other humanitarian interests, i.e. security of societies

Explicit Conditions for Exceptions (select all that apply)
☐ A. None
☒ B. In response to lawful government directive in home country
☒ C. In response to lawful government directive in foreign country where operating
☒ D. In response to lawful government directive in foreign country where *not* operating
☐ E. In response to government request in home country
☐ F. In response to government request in foreign country where operating
☐ G. In response to government request in foreign country where *not* operating
☐ H. Voluntary assistance in cases where life or human safety are threatened
☐ I. Voluntary assistance in cases of a state of national emergency
☐ J. "Hacking-back" at sources of malicious activity
☐ K. Academic research
☐ L. Other (describe)

Table 34. Example Policy Statement G – Defense Contractor

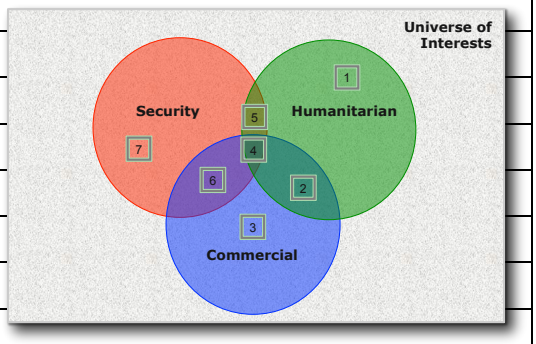
The Interests of the Organization (select one)	
☐	1. Humanitarian
☐	2. Humanitarian + Commercial
☐	3. Commercial
☐	4. Humanitarian + Commercial + Security
☐	5. Humanitarian + Security
☒	6. Commercial + Security
☐	7. Security
☐	8. Other
	
The Organization's Normal Use of Assets in Cyberspace (select one)	
☐	1. Serve medical, cultural or spiritual needs
☐	2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐	3. Generate a profit for owners
☐	4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐	5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☒	6. Generate a profit for owners and engage in belligerent activities
☐	7. Engage in belligerent activities
☒	8. Other (describe) *products used for cyber conflict
Explicit Conditions for Exceptions (select all that apply)	
☒	A. None
☐	B. In response to lawful government directive in home country
☐	C. In response to lawful government directive in foreign country where operating
☐	D. In response to lawful government directive in foreign country where *not* operating
☐	E. In response to government request in home country
☐	F. In response to government request in foreign country where operating
☐	G. In response to government request in foreign country where *not* operating
☐	H. Voluntary assistance in cases where life or human safety are threatened
☐	I. Voluntary assistance in cases of a state of national emergency
☐	J. "Hacking-back" at sources of malicious activity
☐	K. Academic research
☐	L. Other (describe)

Table 35. Example Policy Statement H – Defense Department

The Interests of the Organization (select one)
☐ 1. Humanitarian
☐ 2. Humanitarian + Commercial
☐ 3. Commercial
☐ 4. Humanitarian + Commercial + Security
☐ 5. Humanitarian + Security
☐ 6. Commercial + Security
☒ 7. Security
☐ 8. Other
The Organization's Normal Use of Assets in Cyberspace (select one)
☐ 1. Serve medical, cultural or spiritual needs
☐ 2. Serve medical, cultural or spiritual needs and generate a profit for owners
☐ 3. Generate a profit for owners
☐ 4. Serve medical, cultural or spiritual needs; generate a profit for owners and engaged in belligerent activities
☐ 5. Serve medical, cultural or spiritual needs and engage in belligerent activities
☐ 6. Generate a profit for owners and engage in belligerent activities
☒ 7. Engage in belligerent activities
☐ 8. Other (describe) *products used for cyber conflict
Explicit Conditions for Exceptions (select all that apply)
☒ A. None
☐ B. In response to lawful government directive in home country
☐ C. In response to lawful government directive in foreign country where operating
☐ D. In response to lawful government directive in foreign country where *not* operating
☐ E. In response to government request in home country
☐ F. In response to government request in foreign country where operating
☐ G. In response to government request in foreign country where *not* operating
☐ H. Voluntary assistance in cases where life or human safety are threatened
☐ I. Voluntary assistance in cases of a state of national emergency
☐ J. "Hacking-back" at sources of malicious activity
☐ K. Academic research
☐ L. Other (describe)

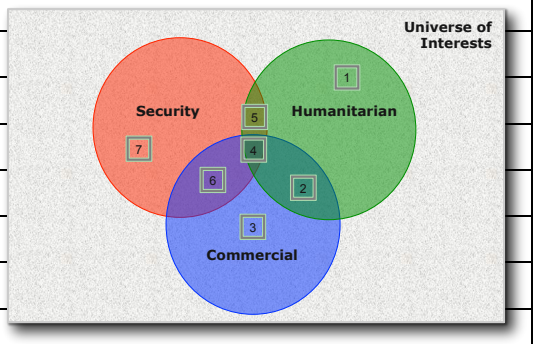


Table 36. Example Policy Checklist - Additional Considerations for Commercial *Businesses with Humanitarian Scope*

Businesses
☐ Storage of statistical data from netizen use
☐ Storage of content data from netizen use
☐ Harvesting of commercial intelligence from netizen use statistics
☐ Harvesting of commercial intelligence from netizen content
☐ Provision of netizen statistical data to third parties
☐ Provision of netizen content data to third parties
☐ Dual use of functionality for belligerent purposes
☐ Other (describe)

Table 37. Checklist Template for Organization Policy Statements – Additional Considerations for *Governments*

Governments
☐ Acceptability for its citizens to take advantage of vulnerabilities in others' assets in cyberspace
☐ Acceptability for its citizens to steal intellectual property from others in cyberspace
☐ Explicit conditions for interfering in the affairs of vetted and confirmed humanitarian organizations
☐ Use of commercial organizations within its jurisdiction for belligerent missions
☐ Acceptability for its companies to "hack-back" against presumed sources of malicious activity
☐ Prohibition for organization members to misuse assets in cyberspace
☐ Other (describe)

Table 38. Checklist Template for Organization Policy Statements – Additional Considerations for *Businesses*

Businesses
☐ Storage of statistical data from netizen use
☐ Storage of content data from netizen use
☐ Harvesting of commercial intelligence from netizen use statistics
☐ Harvesting of commercial intelligence from netizen content
☐ Provision of netizen statistical data to third parties
☐ Provision of netizen content data to third parties
☐ Dual use of functionality for belligerent purposes
☐ Prohibition for organization members to misuse assets in cyberspace
☐ Other (describe)

APPENDIX D: Discussion on the Meaning of the Term "Hacking"

These additional notes supplement the discussion of the definition of term "Hacking" provided in Section 2.4.2.

The most significant of all scoping issues was defining 'hacking', which was the initial label used to describe the subject matter for this initiative. Very soon after commencing the study, there was a realization that 'hacking' is an imperfect term. Indeed, the word 'hacking' was sufficiently ambiguous to render it unsuitable for effective discussion at the deeper level undertaken here in this study.

This discussion provides a more detailed analysis of this discussion. This section summarizes the analysis of the terms used in the media, options available in both languages and, most importantly, alignment with the essential concerns that motivate this study (Section 2.1).

Evidence of the ambiguity of the term 'hacking' in the context of cyberspace is apparent when one seeks clarification around simple questions like:

1) *Is 'hacking' inherently wrong?*
2) *Does 'hacking' include only passive access, or also active control?* and,
3) *Is it hacking if it is war?* or, *is it war if there is hacking?*

This first question brings us to two very different value orientations of the term. On the one hand, the common practice among political leaders, journalists, and the public at large, has a clearly negative connotation, where *a moral offense* has been committed. High profile examples of this practice include [emphasis added]:

- *"[China is] stealing our intellectual property, our patents, our designs, our technology, **hacking** into our computers, counterfeiting our goods. They have to understand, we want to trade with them, we want a world that's stable, we like free enterprise, but you got to play by the rules."*
  - U.S. presidential candidate Mitt Romney[264]

- US **Hacking** China for Years: Report
  *"US whistleblower Edward Snowden said the US government had been **hacking** into computers in Hong Kong and on the Chinese mainland for years."*
  – China Daily[265]

- *"America must also face the rapidly growing threat from cyber-attacks. Now, we know **hackers** steal people's identities and infiltrate private emails. We know foreign countries and companies swipe our corporate secrets. Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems. We cannot look back years from now and wonder why we did nothing in the face of real threats to our security and our economy."*
  – U.S. President Barack Obama[266]

- **Hacking** Becomes Sticking Point after Obama-Xi Summit
  *Cybersecurity and the threat posed by Chinese **hackers** provided the main source of discord in the otherwise amicable meeting in the California desert over the weekend between President Obama and new Chinese leader Xi Jinping . . .*
  - Washington Times[267]

- **Cyberhacking** Accusation rebutted
  "China is a victim of cyberattacks and we hope that earnest measures can be taken to resolve this matter," he told reporters, with Mr. Obama at his side. Mr. Xi said he wanted to dispel America's 'misgivings' about China's alleged role in cyberhacking."

[264] Remarks during debate with U.S. President Barack Obama, 23 October 2012.
[265] ChinaDaily.com, 13 June 2013.
[266] State of the Union Address to Congress, 12 February 2013.
[267] 9 June 2013.

Not all uses of the term by politicians and the media are with the pejorative moral connotation. Examples of exceptions include:

- National Day of Civic **Hacking**[268]
  ". . . an event during which citizens from around the country will work together with local, state and federal governments as well as private sector organizations with the common goal of improving their community."

  - Hack for Change

  At the White House, *". . . participants will focus on producing full, production ready apps and visualization tools that will be featured on the We the People website and made available under an open source license."*

  - The White House[269]

- PBS Shows How **Hacking** Is Reclaiming Its Good Name After a Bad Rap
  *"**Hacking** is still a loaded concept for many, often conjuring negative images of corporate espionage, fraudsters and prank-minded script kiddies. PBS' Off Book wants to remind us that **hacking** wasn't always seen this way -- and, thanks to modern developments, is mending its reputation. Its latest episode shows that hacking began simply as a desire to advance devices and software beyond their original roles, but was co-opted by a sometimes misunderstanding press that associated the word only with malicious intrusions. Today, **hacking** has regained more of its original meaning: **hackathons**, a resurgence of DIY* [do-it-yourself] *culture and digital protests prove that **hacks** can improve our gadgets, our security and even our political landscape."*

  - engadget[270]

On the other hand, the technical community, which certainly can't be ignored as cyberspace is their turf after all, has a practice of focusing on the *skill* associated with hacking as one of value and, moreover, is generally indifferent toward the moral nature of its use. Examples of this mindset that cannot be ignored include:

- Facebook enshrining the term in landscape architecture and street and building names.

Figure 26. Facebook Headquarters, Menlo Park, California:
(a) Ariel View of 'Hack Courtyard', (b) The Hacker Company Sign, and (c) Hacker Way Road Sign.

Yahoo! Has held an annual Hack Day event for over a decade.

Figure 27. Yahoo! Hack Day Events.

[268] www.hackforchange.org .
[269] www.whitehouse.gov .
[270] Fingas, Jon, www.engagnet.com, 31 March 2013.

- Industry conferences for the hacker community

  - HOPE (**Hackers** on Planet Earth) Conference
  This event is sponsored by *2600: The **Hacker** Quarterly*[271]

  - Def Con **Hacker** Conference[272]
  In its Frequently Asked Questions (FAQ) answers the query: *"Do criminals go to DEF CON?"*

  > *"Yes. They also go to high school, college, work in your workplace, and the government. There are also lawyers, law enforcement agents, civil libertarians, cryptographers, and **hackers** in attendance. Ssshhh. Don't tell anyone."*[273]

  - ToorCon
  This community describes itself as ". . . originally established in 1999 in San Diego, California, is the best collection of **Hacker** Events that brings together the top **Hackers**, Makers, Breakers, and Shakers."[274]

  - The **Hackers** Conference
  The Hackers Conference is an unique event, where the best of minds in the hacking world, leaders in the information security industry and the cyber community along with policymakers and government representatives on cyber security meet face-to-face to join their efforts to co-operate in addressing the most topical issues of the Internet Security space.[275]

In Statements:

> *"In reality, **hacking** just means building something quickly or testing the boundaries of what can be done. Like most things, it can be used for good or bad, but the vast majority of **hackers** I've met tend to be idealistic people who want to have a positive impact on the world.*
>
> *The **Hacker** Way is an approach to building that involves continuous improvement and iteration. **Hackers** believe that something can always be better, and that nothing is ever complete. They just have to go fix it — often in the face of people who say it's impossible or are content with the status quo."*
>
> - Mark Zuckerberg[276]

Early definitions:

> hacker: a person who delights in having an intimate understanding of the internal workings of a system, computers and computer networks in particular. The term is often misused in a pejorative context, where "cracker" would be the correct term.[277]

From a solely moral outlook, the two practices of use for the word 'hacking' reviewed above seem diametrically opposed. And because the chief distinguishing elements (i.e. moral offense and valued skill) is such a potent aspect for both communities, but most particularly for the former, it at first appears that a consensus agreement may be unreachable. However fortunately, a semantic decomposition of the essential elements of both usages yielded a tight articulation of meaning that serves both communities.

Note that these definitions accommodate both the behaviors that are widely judged as morally wrong, such as hacking another person's computer and extracting personal financial data, and behaviors that are esteemed for their creativity in the technical community, such as bypassing a constraint in a software program to provide or enhance functionality.

Associated Terms Used in the Media

[271] www.2600.com .
[272] www.defcon.org .
[273] Ibid.
[274] www.toorcon.net .
[275] www.thehackersconference.com .
[276] Mark Zuckerberg's Letter to Investors: *The Hacker Way*, 1 February 2012.
[277] Malkin, G., *Internet Users' Glossary*, Internet Engineering Task Force (IETF) Network Working Group RFC 1392, January 1993.

The term 'hacking' is often used as a catch-all word for referring to a wide range of behaviors. This can be confusing as such usage can also imply interchangeability with other specific terms (Table 40).

Table 39. Major Media Proximity Language for Hacking.

Headline in Media	Hacking or Variant	Proximity Term
Syrian **Hackers** Claim Responsibility for **Disrupting** Twitter, New York Times Web Site[278]	Hackers (noun)	Disrupting (verb)
Hackers Vow New 'Anonymous' **Attacks** on Kremlin Groups[279]	Hackers (noun)	Attacks (noun)
Hacking Assaults on Media Sites Intensify[280]	Hacking (adjective)	Assaults (noun)
U.S. Indicts **Hackers** in Biggest Cyber **Fraud** Case in History[281]	Hackers (noun)	Fraud (adjective)
Eight Charged in **Hacking Theft** From Dozen Financial Firms[282]	Hacking (adjective)	Theft (noun)
FBI Taps **Hacker** Tactics to **Spy** on Suspects[283]	Hacker (adjective)	Spy (verb)
The **Hacked** Tweet That **Took Down** Wall Street[284]	Hacked (adjective)	Took Down (verb)
Snowden Spy Row Grows As US Is **Accused** of **Hacking** China[285]	Hacking (verb)	Accused (verb)
How Bad Is **Hacking** and Corporate **Espionage**?[286]	Hacking (noun)	Espionage (noun)
NSA **Targeted** China's Tsinghua University in Extensive **Hacking Attacks**, Says Snowden[287]	Hacking (verb)	Attacks (noun)
Corporate **Victims** of Chinese **Hackers** Speak Out[288]	Hackers (noun)	Targeted (verb), Victims (noun)
China Is **Victim** of **Hacking Attacks**[289]	Hacking (adjective)	Victim (noun, Attacks (noun)
Chinese **Hackers Infiltrated** *The New York Times's* Computer Systems, Getting Passwords for Its Reporters and Others.[290]	Hackers (noun)	Infiltrated (verb)
New York Times, *Wall Street Journal* Say Chinese **Hackers Broke into** Computers[291]	Hackers (noun)	Broke into (verb)

[278] Tsukayama, Hayley and Farhi, Paul, The Washington Post, 27 August 2013.
[279] BBC News Europe, 9 February 2012, www.bbc.co.uk .
[280] Acohido, Byron and Yu, Roger, USA Today, 15 August 2013.
[281] Jones, David and Finkle, Jim, Reuters, 25 July 2013.
[282] Voreacos, David, Bloomberg, 12 June 2013.
[283] Valentino-Devries, Jennifer, and Yadron, Danny, Wall Street Journal, 3 August 2013.
[284] Charette, Robert, N., IEEE Spectrum, 24 April 2013.
[285] Helm, Toby, Boffey, Daniel, and Hopkins, Nick, The Guardian – The Observer, 22 June 2013.
[286] Edson, Rich, Fox Business News, 9 July 2013.
[287] Lam, Lana, South China Morning Post, 13 August 2013.
[288] Schecter, Anna, NBC News Rock Center, 22 February 2013.
[289] Xiaokun, Li, China Daily, 5 June 2013.
[290] Perlroth, Nicole, The New York Times, 30 January 2013.
[291] Mullen, Jethro, CNN, 31 January 2013.

Early History of the Culture: "A Hacker's Manifesto"

```
File: archives/7/p7_0x03_Hacker's Manifesto_by_The Mentor.txt
                              ==Phrack Inc.==

                    Volume One, Issue 7, Phile 3 of 10

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
The following was written shortly after my arrest...

                       \/\The Conscience of a Hacker/\/

                                      by

                               +++The Mentor+++

                          Written on January 8, 1986
=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

        Another one got caught today, it's all over the papers.  "Teenager
Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
        Damn kids.  They're all alike.

        But did you, in your three-piece psychology and 1950's technobrain,
ever take a look behind the eyes of the hacker?  Did you ever wonder what
made him tick, what forces shaped him, what may have molded him?
        I am a hacker, enter my world...
        Mine is a world that begins with school... I'm smarter than most of
the other kids, this crap they teach us bores me...
        Damn underachiever.  They're all alike.

        I'm in junior high or high school.  I've listened to teachers explain
for the fifteenth time how to reduce a fraction.  I understand it.  "No, Ms.
Smith, I didn't show my work.  I did it in my head..."
        Damn kid.  Probably copied it.  They're all alike.

        I made a discovery today.  I found a computer.  Wait a second, this is
cool.  It does what I want it to.  If it makes a mistake, it's because I
screwed it up.  Not because it doesn't like me...
                Or feels threatened by me...
                Or thinks I'm a smart ass...
                Or doesn't like teaching and shouldn't be here...
        Damn kid.  All he does is play games.  They're all alike.

        And then it happened... a door opened to a world... rushing through
the phone line like heroin through an addict's veins, an electronic pulse is
sent out, a refuge from the day-to-day incompetencies is sought... a board is
found.
        "This is it... this is where I belong..."
        I know everyone here... even if I've never met them, never talked to
them, may never hear from them again... I know you all...
        Damn kid.  Tying up the phone line again.  They're all alike...

        You bet your ass we're all alike... we've been spoon-fed baby food at
school when we hungered for steak... the bits of meat that you did let slip
through were pre-chewed and tasteless.  We've been dominated by sadists, or
ignored by the apathetic.  The few that had something to teach found us will-
ing pupils, but those few are like drops of water in the desert.

        This is our world now... the world of the electron and the switch, the
beauty of the baud.  We make use of a service already existing without paying
for what could be dirt-cheap if it wasn't run by profiteering gluttons, and
you call us criminals.  We explore... and you call us criminals.  We seek
after knowledge... and you call us criminals.  We exist without skin color,
without nationality, without religious bias... and you call us criminals.
You build atomic bombs, you wage wars, you murder, cheat, and lie to us
and try to make us believe it's for our own good, yet we're the criminals.

        Yes, I am a criminal.  My crime is that of curiosity.  My crime is
that of judging people by what they say and think, not what they look like.
My crime is that of outsmarting you, something that you will never forgive me
for.

        I am a hacker, and this is my manifesto.  You may stop this individual,
but you can't stop us all... after all, we're all alike.

                               +++The Mentor+++
```