INSTITUTE FOR DEFENSE ANALYSES

The Missing Compliance Framework in the 2015 U.S.-China Cybersecurity Agreement

B. David A. Mussington

November 18, 2015

Approved for public release; distribution is unlimited.

IDA Non Standard
NS D-5648
Log: H 5-001115
Copy

INSTITUTE FOR DEFENSE ANALYSES
4850 Mark Center Drive
Alexandria, Virginia 22311-1882

The Institute for Defense Analyses is a non-profit corporation that operates three federally funded research and development centers to provide objective analyses of national security issues, particularly those requiring scientific and technical expertise, and conduct related research on other national challenges.

About This Publication

This work was conducted as an independent paper by the Institute for Defense Analyses (IDA). The views, opinions, and findings should not be construed as representing the official position of either the Department of Defense or the sponsoring organization.

Acknowledgments

Priscilla E. Guthrie, Margaret E. Myers

Copyright Notice

© 2015 Institute for Defense Analyses
4850 Mark Center Drive, Alexandria, Virginia 22311-1882 • (703) 845-2000.

This material may be reproduced by or for the U.S. Government pursuant to the copyright license under the clause at DFARS 252.227-7013 (a)(16) [Jun 2013].

The Missing Compliance Framework in the 2015 U.S.–China Cybersecurity Agreement

B. David A. Mussington

Summary

In September 2015 the United States and the Peoples' Republic of China reached an agreement designed to advance progress toward norms of acceptable cyber behavior. Condemning the cyber theft of commercial intellectual property (IP) – both as a matter of national policy *or when undertaken indirectly through proxies* – the two countries seemed poised to at last make progress on a difficult issue. Public comments by "informed" officials in the United States seemed to suggest that the threat of sanctions and a perceptibly hardening of the U.S. position (especially after the Office of Personnel Management (OPM) cyber intrusions) were causal in the emergence of agreement condemning commercial cyber theft. More recently, revelations on the continuation of targeted attacks against U.S. and Western firms by groups ostensibly operating from locations in China has highlighted the lack of clear compliance metrics or a framework for defining new rules of the road.

A bilateral understanding that limits "some" cyber activities was achieved, but what is the character of an agreement in which neither side seeks to verify its tenets? Is the agreement meaningful because it reveals that neither side is ready to initiate a fundamental conflict because the perceived losses from deteriorating relations are too high? And what about definitions? Is operational data in a critical infrastructure, for example, protected by such an agreement, or is such information a legitimate object for foreign intelligence? What are the threshold cases? And where are the bright lines differentiating "what is in" from "what is out?"

Background: Agreeing to Disagree?

President Obama's September comments on the unacceptability of China's cyber behavior garnered attention. Seeing a U.S. position evolving toward one of confrontation, perhaps China's leaders chose a position balancing denials of culpability with limited cooperation in the name of norms to which it was already committed under World Trade Organization rules and ordinary commercial practice. That some of China's own State-Owned-Enterprises (SOE) could fall victim to commercial IP theft and predation was seen as an emerging incentive that would shape its national policies. Lastly, China's President Xi may, it was thought, simply have concluded that China no longer needed practices that

may have been key to its technological and industrial rise – risking accusations with the potential to sully his country's international reputation. Or perhaps a combination of these factors helped foster a change in official views (and actions).

The pronounced ambiguity may persist for an extended period, leaving little possibility for anything more than tactical handling of particular cyber disputes. Situational awareness requirements for even such limited agreements may accumulate, however, suggesting that as increasingly complex cyber behavior is seen as threatening economic, political, and, conceivably, military interests, a compliance framework of some kind may be a requirement to preserve strategic stability. Diplomatic interchange is clearly the primary and most developed channel for this purpose. Arms control – or technical risk management activities and protocols – will likely have an essential role. But what might a compliance framework in the cyber aspects of commercial IP theft be able to achieve?

Compliance and Detection in the U.S.–China Cyber Agreement

If an aversion to costly impacts on economic and political conditions from disruptive cyber activities is a shared concern, a compliance framework that detects and documents defection from even limited agreements may still have value. Clarity needs to be achieved, however, on the potential for such an agreement – and on its limited temporal and issue-linkage boundaries.

A compliance framework that detects and documents defection behaviors may:

- Clarify the nature, magnitude and objectives justifying threat actor behavior;
- Assist in prioritizing vulnerabilities for mitigation;
- Aid in identifying the composition of and magnitude of accumulated losses suffered by IP rights holders, perhaps providing a basis for redress of claims in an appropriate forum or jurisdiction.

Two key detection challenges would characterize any such framework:

- Detecting changes in cyber threat actor behavior following an agreement;
- Detecting changes in cyber actor attack platforms that suggest alteration in preparation and operation of any covert infrastructure for such activity.

What are some benefits of an explicit compliance framework?

Initially it was thought that such a framework might exist, but be largely implicit – avoiding public discussions of sensitive areas (and concrete cases) that might serve to exacerbate, rather than lessen, the intensity of cyber controversy. There is little reason to think that such an implicit agreed framework has been reached, however. And any such arrangement would need to have at least *some* real-world instantiation in order to track policy progress.

A concrete compliance framework would be a significant diplomatic and political breakthrough – indicating that both sides had considered the costs of continuing the status quo – selecting instead an alternate course with agreed facts, definitions, and dispute discussion (if not resolution) procedures. Further, such a bilateral framework might partially insulate the relationship from *temporary* hiccups – caused by the discovery of ongoing activities (legacy) that had yet to be reined in consistent with the new rules of the game. CERT[1]-to-CERT-type contacts would further deepen the linkage between bilateral agreements to refrain from proscribed actions in cyber and operational exchanges on data that support non-controversial investigations of cyber-crime. Lastly, such a framework could provide a mechanism for discussion of IP rights holder injury and remediation options. In this way the compliance framework would provide added support to law enforcement cooperation on cyber-crime already established, as well as aligning well with norms emerging from the United Nations Group of Governmental Experts (GGE) process.

Summing Up – Compliance as a Metaphor for Muddling Through

In recent days the United Kingdom (UK) reached an agreement with China on cyber norms closely paralleling that reached by the United States. In this case the UK Government seems to be seeking a deeper relationship with China for economic purposes, and as a political engagement driven by the practicalities of global politics – emphasizing pragmatism. Narrow compliance judgments or mechanisms for minimizing cyber-enabled IP theft are absent from public pronouncements. The economic stakes in play are significant and suggest a hedging strategy where – unsure that the United States will persist in a disciplined and nuanced approach to cyber differences – the UK may be seeking its own way with a rising power – achieving concrete benefits in the near term, taking advantage of the aversion to escalated cyber conflict that China and the United States ostensibly share. UK success in this approach might make this route attractive to other Western nations, further diminishing the likelihood of collective action against what some perceive as a long-standing strategic technology and scientific data exfiltration campaign supporting China's macroeconomic development.

Absent a specific compliance management approach, cyber risk mitigation actions in national policy may appear to be de-linked from actual threat actor behavior proscribed in the agreement. This weakens potential deterrence, reducing incentives to avoid restricted activities due to the continuing small likelihood of successful and "objective" attacker attribution. In turn, basic data on risks, losses, and attacker identity will be less available (from government sources) and arguably of lower quality. Private Cyber threat information providers may, however, be able to document a baseline on risks, costs, and behavior. Note that definitions of "attack," "vulnerability," and cyber norms remain uncertain in this situation – again preventing clearer understanding of whether violations of nascent norms

[1] Computer Emergency Response Team

are actually occurring. Also clear in such a situation is a growing dissonance between public reporting of cyber intrusions and risk activity and the risks posed by state or state-sponsored cyber-attacks on critical infrastructures and sensitive data. Accurate data on attacker behavior, cyber campaign plans, and targeting of vital services and critical infrastructures should enable better cyber risk decisions and investments. Absent a compliance framework such data will be less rich, less easily shareable, and less useful for shaping cyber protections and resilience responses.

Cyber risk disputes between the United States and China will continue. An explicit compliance framework offers benefits in terms of transparency, data availability and improved attacker attribution. This information might assist in bilateral risk management between the two countries. More generally, enhanced information availability will enable improved alignment of incentives for commercial IP owners to invest in protections capable of matching changes in cyber risk conditions. Better information quality might lead to more effective asset, critical infrastructure, and sensitive data cyber protection options in the market place. A compliance framework might produce a novel and useful extra benefit: a bootstrap for improved cyber risk data availability and quality – leading to more accurate calculation of cyber risk exposures and mitigation effectiveness. In turn, such a development might accelerate broader and deeper improvements in planning – facilitating better management of legacy and emerging cyber risks.

Elaborating on a cyber-risk compliance framework in the U.S.–China bilateral agreement may seem like expecting too much. Far from it. China is a leading source of cyber intrusion activity targeting U.S. Government and private sector institutions. Narrowing differences through discussion and diplomatic interchange can facilitate risk management and transparency. By leaving compliance unaddressed, the agreement fails to clarify not only the risks posed to U.S. interests by China-directed or -sponsored cyber activity, but it also misses an opportunity to enrich the data upon which cross-infrastructure cyber risk management decisions might be made.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
18-11-15	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Missing Compliance Framework in the 2015 U.S.-China Cybersecurity Agreement	N/A
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
B. David A. Mussington	Independent Paper
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESSES	8. PERFORMING ORGANIZATION REPORT NUMBER
Institute for Defense Analyses 4850 Mark Center Drive Alexandria, VA 22311-1882	NS D-5648 H 15-001115

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
N/A – Independent paper	N/A
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: B. David A. Mussington

14. ABSTRACT

The 2015 US-PRC cyber agreement created expectations regarding changes in China's cyber behavior in relation to the theft of commercial IP. Such changes need to be measurable, but the agreement itself lacks a verification mechanism. This paper outlines some requirements for such a mechanism, and offers an approach to evaluating one.

15. SUBJECT TERMS

Cybersecurity, Critical Infrastructure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include Area Code)
Unclassified	Unclassified	Unclassified	Unlimited	4	