INSTITUTE FOR DEFENSE ANALYSES

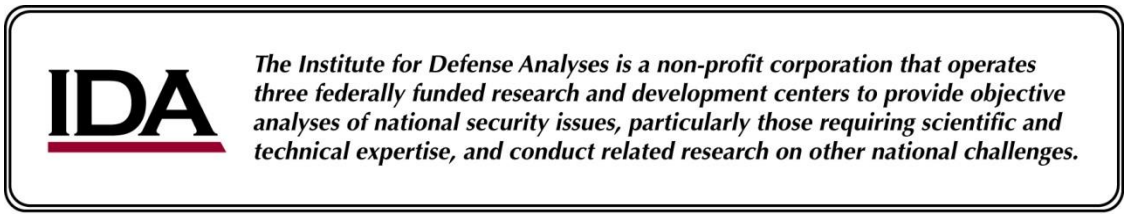
Defending Our Economic Future Against Cyber Threats to Innovation

John C. Mallery
Brian David A. Mussington
Jonathan P. Gill

July 1, 2016

IDA
NS D-8061
Log: H 2016-000804 Rev.
Copy

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



Defending Our Economic Future
Against Cyber Threats to Innovation

July 14, 2016

John C. Mallery
Research Scientist, Computer Science & Artificial Intelligence Laboratory, Massachusetts Institute of Technology

David Mussington
Assistant Director for Information Technology and Systems, Institute for Defense Analyses

Jonathan P. Gill
Former White House Staff - New Media Initiatives

To protect against theft of United States intellectual property (IP) and trade secrets, we must defend the innovation processes underpinning our knowledge-based economy with a systematic strategy for economic deterrence and cyber security.

During his tenure as the National Intelligence Officer for Cyber Issues, Sean Kanuck observed in public remarks that "in agricultural economies, countries defended their fields from foreign militaries, and later, during the industrial age they defended their factories." Now, if we cannot defend our knowledge and secure our fundamental intellectual and human capital, how can we compete successfully in the 21st century global knowledge economy?

Large-scale theft of intellectual property and trade secrets from U.S. businesses undermines our international competitiveness and erodes high-skill jobs for U.S. workers. The 2013 Intellectual Property (IP) Commission, led by Admiral (ret) Blair and Jon Huntsman, estimated our losses at $300 billion annually. Over the 20 years since the Internet revolution of the 1990s, annual global sales in information and communications technologies (ICT) products and services have reached $4 trillion. Markets for ICT are rapidly becoming a top component of our digital economy, and a major segment of international trade. If the United States cannot protect our IP across the research and development (R&D) pipeline from universities, to startups, to industry, our technology leadership will be eclipsed, our economic potential eroded, and our future growth stolen.

In his annual Congressional testimony on the Worldwide Threat Assessment, Director of National Intelligence James Clapper listed "cyber and technology" threats as the top risks to U.S. national security for the past three years. A 2014 Department of Justice indictment of five People's Liberation Army (PLA) hackers illustrated how state-sponsored, cyber-enabled theft of confidential IP and trade secrets caused specific harm to U.S. businesses and cumulative economic damage as China sought to raise its technology level. PLA hackers stole IP and business secrets from a solar power company and a nuclear power equipment manufacturer so that Chinese state-owned companies could unfairly gain market share, save on R&D costs, and fight legal responses by the victims. Emerging technologies like additive manufacturing, or "3D printing," foreshadow a future digital economy in which businesses and national economies will not be viable unless they can protect their designs, automated production processes, and trade secrets from theft.

As our society becomes ever more deeply dependent on ICT, our ability to protect vital information and digital systems is not improving fast enough. Indeed, after 18 years of incremental Federal Government effort, accelerating threats continue to outpace defenses—as demonstrated by recent serious cyber intrusions at the Office of Personnel Management (OPM), the White House, the State Department, and the Joint Chiefs of Staff, not to mention large cyber thefts via the SWIFT international financial transfer system.

The economic benefits of the continuing adoption of ICT are offset by exponential expansion of vulnerabilities and attack surfaces of technical and societal systems. In the current "unsecurable" and "indefensible" technological terrain, risk is transferred downstream to enterprises and consumers, which are unable to cope. Unregulated markets for ICT currently fail to allocate risk to entities that have the technical capacity to mitigate it, which are often the liability-free producers of ICT capital goods.

To defend against these risks, U.S. businesses and consumers need higher-assurance products and services whose effectiveness can be meaningfully measured. At this point, the dangers to national and economic security have become so grave that the United States must now systematically marshal the resources of the nation to reverse the losses accruing from pervasive cyber vulnerability. Such a cyber defense initiative will build renewed trust in U.S. ICT products, generate new jobs to protect the digital economy, and create the next generation of secure and smart ICT.

Federal efforts to enhance the technical capacity of businesses to defend themselves, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the broader Cybersecurity National Action Plan (CNAP), have not explicitly tackled either market failures or the inadequate supply of secure technology, despite significant Federal R&D funding for impressive point solutions.

In 2013, the Snowden revelations set back an initiative to deter IP theft by National Security Advisor Tom Donilon at the Sunnyvale Obama–Xi Summit. But, with recognition of the economic motivation for IP theft and the subsequent formation of an interagency task force on trade enforcement, the U.S. Government began to treat IP theft as a trade issue rather than merely a cybersecurity problem. In 2015, an informal G7 dialogue in Paris on IP theft helped catalyze an economic deterrence approach. This elicited a change in Chinese declaratory policy by the September 2015 summit when Chairman Xi Jinping reaffirmed World Trade Organization (WTO) rules against theft of IP or business secrets for commercial gain from the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). Recent confirmed reports of significant reductions in Chinese cyber intrusions against U.S. business may reflect either follow-through on Xi's commitment, a tactical pause, or more precise targeting and more professionalized cyber operations requiring better detection techniques. In any case, the United States must remain vigilant because faith in cyber norms alone is not a strategy to secure American innovation.

To protect the economic gains from ICT, the United States needs an effective strategy for defending IP (including trade secrets) that incorporates deterrence based on economics and technology. Economic deterrence can be strengthened by using the WTO Dispute Resolution Processes to clarify TRIPS by winning cases against states; by forging new trade agreements like the Trans Pacific Partnership (TPP) to strengthen treaty trade protections of IP and enforcement; by threatening unilateral sanctions for serious cyber operations against the U.S (like Presidential Executive Order 13694 in April 2015); and by harmonizing national law to facilitate trade or civil actions by victims against IP infringers across jurisdictions of the Organization for Economic Cooperation and Development (OECD) (like the European Union Directive to protect business secrets on June 8, 2016). Technological deterrence requires deploying affordable yet high-security systems for enterprises to protect critical IP and trade secrets, detect intrusions, and acquire legally-actionable evidence across the lifecycle of innovation—from university research, to startups, to industry—based on stratified business processes, phased enhancements to commercial ICT technologies, and introduction of next-generation ICT designed to resist modern threats.

The strategy must focus on measurable impact and drive implementation based on systematic planning supported by effective organization. Engineering technical and policy moves that produce multiplicative impacts on the capacity of threat actors to pursue their malicious business models can offset exponential disadvantages of defense. A key disruption stratagem is to innovate aggressively and adaptively to get inside the innovation loop of the hackers to make their tools and techniques obsolete faster than their capacity to develop new ones. The next Deputy National Security Advisor for International Economics should coordinate this interagency strategy for protection of innovation across trade, legal, intelligence, and technology dimensions.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE (DD-MM-YY)	2. REPORT TYPE	3. DATES COVERED (From – To)
28-06-16	Non-Standard	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Defending Our Economic Future Against Cyber Threats to Innovation	HQ0034-14-D-0001
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBERS

6. AUTHOR(S)	5d. PROJECT NUMBER
John C. Mallery, Brian David A. Mussington, Jonathan P. Gill	ITSDPB
	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-8061 H 2016-000804 Rev

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR'S / MONITOR'S ACRONYM
ITSD Special Projects	
	11. SPONSOR'S / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Project Leader: Brian David A Mussington

14. ABSTRACT

This paper argues for the priority of IP protection and trade secret protection as priorities in U.S. foreign economic policy.

15. SUBJECT TERMS

Intellectual property, trade secrets, cybersecurity, ICT

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	Unlimited	2	