AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

CYBER ATTACKS: AN UNPRECEDENTED THREAT TO U.S. NATIONAL SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON EUROPE, EURASIA, AND EMERGING THREATS

OF THE

COMMITTEE ON FOREIGN AFFAIRS
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

MARCH 21, 2013

Serial No. 113–8

Printed for the use of the Committee on Foreign Affairs

Available via the World Wide Web: http://www.foreignaffairs.house.gov/ or http://www.gpo.gov/fdsys/

U.S. GOVERNMENT PRINTING OFFICE

80–123PDF WASHINGTON : 2013

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON FOREIGN AFFAIRS

EDWARD R. ROYCE, California, *Chairman*

CHRISTOPHER H. SMITH, New Jersey
ILEANA ROS-LEHTINEN, Florida
DANA ROHRABACHER, California
STEVE CHABOT, Ohio
JOE WILSON, South Carolina
MICHAEL T. McCAUL, Texas
TED POE, Texas
MATT SALMON, Arizona
TOM MARINO, Pennsylvania
JEFF DUNCAN, South Carolina
ADAM KINZINGER, Illinois
MO BROOKS, Alabama
TOM COTTON, Arkansas
PAUL COOK, California
GEORGE HOLDING, North Carolina
RANDY K. WEBER SR., Texas
SCOTT PERRY, Pennsylvania
STEVE STOCKMAN, Texas
RON DeSANTIS, Florida
TREY RADEL, Florida
DOUG COLLINS, Georgia
MARK MEADOWS, North Carolina
TED S. YOHO, Florida
LUKE MESSER, Indiana

ELIOT L. ENGEL, New York
ENI F.H. FALEOMAVAEGA, American Samoa
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
ALBIO SIRES, New Jersey
GERALD E. CONNOLLY, Virginia
THEODORE E. DEUTCH, Florida
BRIAN HIGGINS, New York
KAREN BASS, California
WILLIAM KEATING, Massachusetts
DAVID CICILLINE, Rhode Island
ALAN GRAYSON, Florida
JUAN VARGAS, California
BRADLEY S. SCHNEIDER, Illinois
JOSEPH P. KENNEDY III, Massachusetts
AMI BERA, California
ALAN S. LOWENTHAL, California
GRACE MENG, New York
LOIS FRANKEL, Florida
TULSI GABBARD, Hawaii
JOAQUIN CASTRO, Texas

AMY PORTER, *Chief of Staff* THOMAS SHEEHY, *Staff Director*
JASON STEINBAUM, *Democratic Staff Director*

SUBCOMMITTEE ON EUROPE, EURASIA, AND EMERGING THREATS

DANA ROHRABACHER, California, *Chairman*

TED POE, Texas
TOM MARINO, Pennsylvania
JEFF DUNCAN, South Carolina
PAUL COOK, California
GEORGE HOLDING, North Carolina
STEVE STOCKMAN, Texas

WILLIAM KEATING, Massachusetts
GREGORY W. MEEKS, New York
ALBIO SIRES, New Jersey
BRIAN HIGGINS, New York
ALAN S. LOWENTHAL, California

CONTENTS

Page

WITNESSES

Mr. Christopher Painter, Coordinator, Office of the Coordinator for Cyber Issues, U.S. Department of State 7
Mr. Richard Bejtlich, chief security officer and security services architect, Mandiant Corporation 26
Mr. Greg Autry, senior economist, Coalition for a Prosperous America 36
Mr. Michael Mazza, research fellow, American Enterprise Institute 46
Martin C. Libicki, Ph.D., senior management scientist, RAND Corporation 55

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

The Honorable Dana Rohrabacher, a Representative in Congress from the State of California, and chairman, Subcommittee on Europe, Eurasia, and Emerging Threats: Prepared statement 3
Mr. Christopher Painter: Prepared statement 9
Mr. Richard Bejtlich: Prepared statement 29
Mr. Greg Autry: Prepared statement 38
Mr. Michael Mazza: Prepared statement 48
Martin C. Libicki, Ph.D.: Prepared statement 57

APPENDIX

Hearing notice 70
Hearing minutes 71

CYBER ATTACKS: AN UNPRECEDENTED THREAT TO U.S. NATIONAL SECURITY

THURSDAY, MARCH 21, 2013

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON EUROPE, EURASIA, AND EMERGING THREATS,
COMMITTEE ON FOREIGN AFFAIRS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9 o'clock a.m., in room 2172 Rayburn House Office Building, Hon. Dana Rohrabacher (chairman of the subcommittee) presiding.

Mr. ROHRABACHER. There it is. It is called to order and the mic is on. And let me just note that when you are speaking through a microphone, you are utilizing the energy that is produced some way by someone at some cost. So I call this meeting to order. And today's topic is Cyber Attacks: An Unprecedented Threat to National Security.

After the ranking member and I each take 5 minutes to make opening remarks, each member present will have 1 minute to make their opening remarks, alternating between the majority and minority. And without objection, all members may have 5 days to submit statements, questions, and extraneous material for the record, and hearing no objections, so ordered.

There have been several congressional hearings on cyber warfare, but most have concentrated on the technology involved and how we can devise defenses to block hackers from breaking into our Government and business computers. The greatest danger to our nation, the greatest dangers, however, are not really about technology. It is about international relations, foreign governments that employ cyber warriors to attack other countries, or which allow hackers to attack other countries in their behalf.

And what is it we are we talking about? We are talking about something that should be considered as a hostile government action against another act. It is as if the government was supporting terrorism if they support the same type of aggression, cyber aggression. These acts, which put our country in severe jeopardy, must be met with the same national security and diplomatic measures that we use to meet other external threats.

The type of targets hackers assault are often placed in two categories. Strategic targets are those which would be attacked by military means in a war. For example, transportation systems, power grids, defense industries, communications, and government centers. And China, Iran, North Korea, and Russia have all used

cyber attacks aimed at strategic infrastructure targets. Targets that would be attacked in another way if there was a war.

In January, Iran conducted probing attacks on U.S. banks. Such potential damaging and brazen attacks on the United States should provoke a much more aggressive and powerful response than we are currently exercising. We should deter, not just to try to block, but we should deter cyber attacks and perhaps counterattack. More insidious, however, is the ongoing attacks on our economy by the Chinese, among others. This second form of attack is in the form of commercial warfare. The scale upon which it is being conducted is beyond anything we have experienced and far exceeds traditional espionage.

The Mandiant report which came out last month identified a unit of the Chinese People's Liberation Army that has been conducting commercial warfare since 2006. A military unit hacking business and industry targets, and then we have a situation where these targets play a central role in the economy of one nation and has a lot to do with the balance of power between the nations. So you have a Chinese People's Liberation Army involved in an attack that has a lot to do with the power between our countries, and is a cyber attack.

The commander of U.S. Cyber Command, Keith Alexander, estimated last year that computer hacking from overseas costs the American economy $250 billion a year. He called it the greatest transfer of wealth in history. The Mandiant study found that the targets "match industries that China has identified as strategic for their growth, including four of the seven strategic emerging industries that China has identified as part of its 12th 5-year plan."

The Chinese firms that compete in these industries are dominated by state-owned enterprise which ties Communist Party officials and their families to this crime against the United States and others throughout the world. It is a matrix that not only serves to grow the wealth and power of China but also the personal fortunes of its leaders. Yet, even this is only the tip of the iceberg. The transfer of wealth by the theft of technology and other information vital to the development of industry is then used to gain a competitive advantage in world trade, which brings even more wealth to China.

Over the last 10 years, that is 2003 to 2012, the United States trade deficit in goods with China totaled over $2.4 trillion. Entire industries have been moved across the Pacific to create what we see as the rise of China. Well, we cannot just rely on technology to defend against these type of attacks. We must use diplomacy to deter them by telling Beijing and others in clear terms that we will not allow their hacking to continue without retaliation. We should sanction states that support hacking just as we sanction states that support terrorism or engage in other hostile actions. This war will not just be waged in cyberspace, but across every front and using every lever of American power to defeat an aggressor and to take the profit out of attacking our businesses, our defenses, and yes, our country.

[The prepared statement of Mr. Rohrabacher follows:]

Subcommittee on Europe, Eurasia, and Emerging Threats
Committee on Foreign Affairs
Dana Rohrabacher (R-CA), Chairman

March 21, 2013

Opening Statement

Cyber Attacks: An Unprecedented Threat to U.S. National Security

I call to order this hearing of the Foreign Affairs Subcommittee on Europe, Eurasia, and Emerging Threats. Today's topic is "Cyber Attacks: An Unprecedented Threat to National Security."

After the Ranking Member and I each take 5 minutes to make opening remarks, each Member present will have one minute to make their opening remarks, alternating between Majority and Minority Members. And without objection, all Members may have five days to submit statements, questions, and extraneous materials for the record. Hearing no objection, so ordered.

There have been several Congressional hearings on cyber warfare, but most have concentrated on the technology involved and how we can devise defenses to block hackers from breaking into our government and business computer networks.

The greatest dangers to our nation are not, however, really about technology. It is about international relations. Foreign governments that employ cyber warriors to attack other countries, or which "allow" hackers to attack other countries should be considered as hostile as governments which support terrorism. These are acts which put our country in severe jeopardy and must be met with the same national security and diplomatic measures that we use to meet any other external threat.

The types of targets hackers assault are often placed in two categories. Strategic targets are those which would be attacked by military means in a war: transportation systems, the power grid, defense industries, communications, and government centers. China, Iran, North Korea and Russia have all used cyber attacks aimed at strategic infrastructure targets.

In January, Iran conducted probing attacks on U.S. banks. Such potentially damaging and brazen attacks on the United States should provoke a much more aggressive and powerful response than we are currently exercising.

We should deter, not just try to block, cyber attacks.

More insidious, however, is the ongoing attacks on our economy by the Chinese, among others. This second form of attack is a form of commercial warfare. The scale upon which it is being conducted is beyond anything we have ever experienced and far exceeds traditional espionage.

The Mandiant report, which came out last month, identified a unit of the Chinese People's Liberation Army that has been conducting commercial warfare since 2006. A military unit hacking business and industry targets highlights the central role that economics plays in the balance of power between nations.

The commander of US Cyber Command, General Keith Alexander, estimated last year that computer hacking from overseas cost the US economy $250 billion a year. He called it "the greatest transfer of wealth in history."

The Mandiant study found that the targets "match industries that China has identified as strategic for their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan."

The Chinese firms that compete in these industries are dominated by state-owned enterprises with ties to Communist Party officials and their families. It is a matrix that not only serves to grow the wealth and power of China, but also the personal fortunes of its leaders.

Yet, even this is only the tip of the iceberg. The transfer of wealth by the theft of technology and other information vital to the development of industry is then used to gain a competitive advantage in world trade which brings even more wealth to China. Over the last ten years (2003-212), the U.S. trade deficit in goods with China totaled over $2.4 trillion.

Entire industries have been moved across the Pacific to create the "rise" of China

We cannot just rely on technology to defend against these attacks. We must use diplomacy to deter them by telling Beijing and others in clear terms that we will not allow their hacking to continue without retaliation.

We should sanction states that support hacking just as we sanction states that support terrorism or engage in other hostile actions.

This war will not just be waged in cyber space, but across all fronts using every lever of American power to defeat aggressors and take the profit out of attacking our businesses, our defenses, and our country.

Mr. ROHRABACHER. With that I would turn to Mr. Keating for his opening remarks.

Mr. KEATING. Well, thank you, Mr. Chairman, and thank you for holding today's hearing.

During the highly publicized Benghazi hearing earlier this year, Secretary Clinton warned this committee that cyber threats would be at the top of our agenda in the coming months and she certainly was correct in that prediction. With the number of cyber threats escalating worldwide, the need for comprehensive security analysis, assessment, and actions has never been greater.

Although cyber attacks and instances of cyber espionage are receiving a great degree of media attention and are undoubtedly increasing and really evolving at a highly rapid rate, cyber threats are not a new phenomenon. The GAO designated Federal information security as a high-risk area in 1997, and in 2003 expanded this area to include protecting our nation's critical infrastructure.

Ten years later, just this February, it was President Obama that signed an executive order to facilitate information sharing about emerging threats and solicit new, voluntary cybersecurity standards for the nation's power grid, financial sector, and other key institutions, yet the price of cybersecurity is certainly not cheap. Government agencies would need to boost cybersecurity spending more than seven times to block 95 percent of hacker attacks according to Bloomberg Government study.

This translates into an annual average spending of $190.3 million per agency, up from the current $26 million, according to the study, based on interviews with officials of 48 Federal, State, and municipal agencies. The current combined financial impact on public and private sector cyber attacks is unknown but estimates are in the billions.

As we add up the dollars and weigh the risks, we must not forget that the greatest attack of all will be on the confidence of the American people if even one large-scale cyber attack scenario were to materialize. As a former district attorney, I believe that our country's efforts toward deterence and response to a known cyber attack do matter, even if we are not always sure who the aggressor is, their motive is, or where they might be. While the issuance of the executive order is a welcome development, it will take responsible, legislative action to fully address cyber threats and vulnerabilities to critical infrastructure, and time is of the essence.

Further, the Internet is an open, international domain, and cyber crimes clearly go beyond traditional law enforcement models. For this reason, national policies are incomplete without firm international cybersecurity standards and norms between like-minded allies.

The U.S. recently played an incredibly constructive role during the World Conference on International Telecommunications, and beat back proposals by Russia, China, Saudi Arabia, and others that sought to explicitly extend International Telecommunications Regulations jurisdiction over the Internet. Unfortunately, the U.S. also does not participate in many of the concrete initiatives put forth by the International Telecommunications Union, the ITU, and other international organizations. However, these efforts further the connectivity and the interoperability of the world's tele-

communication networks which, in turn, enhance America's defense and intelligence communication capabilities.

Also just this week, NATO Secretary General Rasmussen was in Estonia. As most of us here know, Estonia has experienced devastating cyber attacks directed from Russia at its Parliament, ministries, banking systems, newspapers, and broadcasters, in 2007. This week's NATO meeting alluded to these attacks. It highlighted the importance of moving on to an interoperability paradigm between like-minded allies. It is interesting with Estonia as well, I was informed this week that they are going to have the model that the EU is adopting. And even in Estonia it is interesting to note as well, they are teaching cybersecurity in the first grade.

I am thankful for the participation of our witnesses here today, and look forward to hearing their thoughts on our current cyber state of affairs as well as ongoing cyber espionage efforts and attacks stemming from China, Russia, Iran, and others. And before I close, I would like to note that this hearing is taking place at a time when the effects of across-the-board spending cuts are just beginning to be realized. And I look forward to hearing from you, Mr. Painter, about how the sequester and the perpetual uncertainty around budgeting impacts might affect our nation's cybersecurity efforts. With that I go back to my chairman and yield back time, all 5 seconds.

Mr. ROHRABACHER. Thank you very much. You were noting what was going on in Estonia, and yesterday, several banks and broadcast outlets in South Korea were attacked, and apparently the assumption was that the cyber attacks were from North Korea. However, the news this morning is that South Korea is claiming that these attacks were located, the attacker was located in China. And the story is still developing, but it raises questions as to whether China and North Korea are cooperating in cyber warfare against people that they think are their enemies.

But with that Mr. Duncan has an opening statement, I understand.

Mr. DUNCAN OF SOUTH CAROLINA. Thank you, Mr. Chairman. I think that the hearing today is very, very timely, especially in light of the director of National Intelligence on 12 March, James Clapper, said this, "We judge that there is a remote chance of a major cyber attack against U.S. critical infrastructure systems during the next 2 years that will result in a long-term, wide-scale disruption of services such as regional power outage."

So I appreciate you having this hearing. As a member of the House Committee on Homeland Security, we are taking cyber threats very, very seriously. I know Chairman McCaul is very interested in the cyber threats of this country in his role as chairman of the House Homeland Security Committee. So I appreciate the committee hearing, and I look forward to the testimony of the witnesses. Thank you, I yield back.

Mr. ROHRABACHER. Thank you very much. And if the microphones go off and the lights go off, we will know someone is watching. We are under attack. All right, Mr. Stockman, I understand, has an opening statement as well.

Mr. STOCKMAN. Yes, I was just going to comment that this morning—you stole my thunder a little bit. I was going to discuss the

South Koreans. In fact, the IP address was that of China, and now there is some discussion over that. But I think it is a critical time that you do this hearing and I appreciate it. But also I know our Chinese friends are probably watching. I don't think that we should engage in this warfare, but if it is started I am sure that the chairman would lead us through a victorious end, because this is really alarming to many of us in this country. Thank you.

Mr. ROHRABACHER. Thank you very much. Our first panel is a single witness. Christopher Painter is Coordinator for Cyber Issues at the U.S. Department of State. Mr. Painter has served in the White House as senior director for Cybersecurity Policy in National Security Staff, and this is on the National Security Council, is that correct? Okay. During his 2 years in the White House, Mr. Painter conducted the President's Cyber Policy Review, and subsequently served as acting cybersecurity coordinator.

Mr. Painter began his Federal career as Assistant U.S. Attorney in Los Angeles where he led some of the most high profile and significant cyber crime prosecutions that took place in our country, then moved onto Computer Crime and Intellectual Property Section of the U.S. Department of Justice and served there for a short time as deputy assistant director of the FBI Cyber Division. He has worked with dozens of foreign governments on these issues, and he is a graduate of Stanford Law School and Cornell University.

Mr. Painter, you may proceed.

STATEMENT OF MR. CHRISTOPHER PAINTER, COORDINATOR, OFFICE OF THE COORDINATOR FOR CYBER ISSUES, U.S. DEPARTMENT OF STATE

Mr. PAINTER. Chairman Rohrabacher and Ranking Member Keating and members of the subcommittee, thank you for the opportunity to testify on the State Department's role in countering cyber threats. I commend the subcommittee for focusing on this foreign policy imperative, and for your support promoting diplomacy as a tool for improving our nation's cybersecurity, and by extension, our national security and economic interests.

The State Department plays a leading role in diplomatic efforts to stabilize cyberspace and to advance the vision of an open, interoperable, secure and reliable Internet articulated in the President's 2011 International Strategy for Cyberspace. We currently face several kinds of threats in cyberspace. First, there are the operational threats, which you just described, to our cyber networks that can potentially harm both our security and our economic interests, like the recent Distributed Denial of Service attacks against our financial sector.

The State Department has worked closely in that instance with our Department of Homeland Security and other agencies to help share technical data that can then help mitigate the threat, and the sharing has been with both our international partners in countries and with industry. This kind of information sharing not only helps counter the immediate threat, but promotes a practice of international cooperation that will help prevent future attacks. It creates a norm of cooperation, if you will.

Another kind of threat that has been making the news lately is obviously the large-scale wholesale theft, cyber theft of intellectual

property and trade secrets from the private sector. The State Department has consistently raised our concerns about these cyber intrusions with senior Chinese officials, and we will continue to do so. I welcome recent Chinese official statements that suggest a willingness to engage in a more sustained dialogue and discussion on this important issue.

It is critical that we continue to emphasize cyber issues in all of our international engagements to promote global cooperation, to ensure that states take threats seriously, to build consensus on norms of responsible conduct in cyberspace that enhance international cybersecurity, and to address the kinds of malicious activity that have recently received such extensive media coverage. Cyber policy issues are on the agenda in every major international forum, and in those forums some states seem to view the dynamism and innovation of the Internet as a threat to the stability of their regimes. They reject the successful multi-stakeholder model of Internet governance that includes a role for states, for civil society, and for industry in favor of top-down intergovernmental control that enables both state control and regulation of content.

The U.S. strongly promotes an alternative vision. We believe that a cyberspace that rewards innovation, empowers individuals, develops communities, safeguards human rights, and enhances personal privacy will build better governments and strengthen national and international security. We promote this vision by working not only with our closest partners and allies, but also with states that are emerging as global leaders in this area, and with developing nations looking for ways to play a role in the cyber world and even with states with whom we do not always see eye-to-eye. The U.S. engages on cyber issues with a multitude of states bilaterally, regional groups such as the European Union, and NATO.

In the last year alone we, my office, has launched dedicated cyber, whole of government, meaning not just my office but all the different agencies in our Government and the counterpart governments, senior policy dialogues with India, Brazil, South Africa, South Korea, Japan, and Germany in order to share perspectives and build a consensus view of the future of cyberspace. We continue to seek deeper engagement with countries like Russia and China who clearly have a different world view and with whom we have challenges but we need to find ways to develop a stronger relationship.

The State Department will continue to focus on both the kinds of operational threats that you have identified here today, and on the long-term policy efforts that will help mitigate them in the long run. In his confirmation hearing, Secretary Kerry, then Senator Kerry, cited the importance of "cyber diplomacy and cyber negotiations," stressing the need to affirm "'rules of the road' that help us be able to cope with challenges in cyberspace." State is doing just that. We are working with other nations on efforts that will not only contribute to greater security and stability in cyberspace, but will protect freedom of expression, ensure opportunities to innovate, and promote economic growth around the world.

Thank you, Mr. Chairman and Ranking Member Keating, and I look forward to your questions.

[The prepared statement of Mr. Painter follows:]

STATEMENT FOR THE RECORD

CHRISTOPHER PAINTER

Coordinator for Cyber Issues

Before the

House Foreign Affairs Committee

Subcommittee on Europe, Eurasia, and Emerging Threats:

Cyber Attacks: An Unprecedented Threat to U.S. National Security

March 21, 2013

Chairman Rohrabacher, Ranking Member Keating, and members of the Subcommittee, thank you for this opportunity to testify on the State Department's role in countering cyber threats. State is not only a key player in the U.S. response to ongoing cyber threat activity, but the lead agency for cyber diplomacy, promoting international cooperation on cyber issues in order to reduce the cyber threat worldwide. I commend the Subcommittee for focusing on this foreign policy imperative and for your support in promoting diplomacy as a tool for improving our nation's cybersecurity – and, by extension, our national security and economic interests.

The United States is a global leader in promoting the tremendous social and economic benefits inherent to cyberspace. As new technologies expand and progress, peoples of all nations seek to take advantage of emerging forms of connectivity. However, as cyberspace has evolved, so too have the threats to its networks and infrastructure. The United States is also a world leader in facilitating and encouraging cooperation among states to counter these increasingly common threats. The State Department plays a leading role in diplomatic efforts to stabilize cyberspace and to advance the vision of an open, interoperable, secure and reliable Internet articulated in the Obama Administration's 2011 *U.S. International Strategy for Cyberspace*.

We currently face several kinds of threats in cyberspace. First, there are operational threats to our cyber networks that, whether state-sponsored or criminal in nature, can potentially harm our security and do substantial harm to our economic interests. One recent example of this type of threat is the Distributed Denial of Service attacks that have targeted the U.S. financial sector. In these attacks, an attacker harnesses thousands of computers worldwide to use as a 'botnet' in an attempt to disrupt service by overloading systems with requests. To mitigate these kinds of threats, the State Department works closely with the Department of Homeland Security (DHS) and other agencies to share technical data with international partners. The United States has shared information related to the recent attacks with over 100 countries for use in mitigating the impact of similar attacks. Sharing this information not only helps counter the immediate threat, but also promotes international cooperation and transparency that will strengthen international collaboration to help prevent future attacks.

Another kind of threat that has been making news lately is large-scale cyber intrusion for purposes of stealing intellectual property, trade secrets, proprietary technology, and sensitive business information from the private sector. The Administration takes these threats seriously,

and last month, President Obama released the Administration's Strategy on Mitigating the Theft of U.S. Trade Secrets, which identified sustained and coordinated diplomatic engagement regarding trade secret theft and economic espionage as a critical element of the Administration's overall approach to such activities.

National Security Advisor Tom Donilon recently said, "increasingly, U.S. businesses are speaking out about their serious concerns about sophisticated, targeted theft of confidential business information and proprietary technologies through cyber intrusions emanating from China on an unprecedented scale." The State Department has consistently raised our concerns about cyber intrusions with senior Chinese officials, including military officials, and we will continue to do so.

We are seeking meaningful, constructive dialogue with China on these issues. As National Security Advisor Donilon stated, "we need China to engage with us in a constructive direct dialogue." I welcome recent Chinese official statements that suggest a willingness to expand dialogue and discussion, and we have been engaging with China about that type of dialogue. The United States and China must work together to address this problem.

It is crucial that we continue to elevate cyber issues throughout our international engagements to promote global cooperation, to ensure that states take the threats seriously, to build consensus on the norms of responsible conduct in cyberspace that enhance international cyber security, and to address the recent malicious activity that has received extensive media coverage.

We face challenges within the international policy realm as well. Cyber issues are on the agenda in every major international forum and it is imperative that we engage diplomatically in these venues. Some states seem to view the dynamism and innovation of the Internet as a threat to the stability of their regimes. They reject the successful multi-stakeholder model of Internet governance that includes a role for states, civil society, and industry in favor of top-down intergovernmental control that enables state control and regulation of content. The "International Code of Conduct for Information Security" tabled at the UN General Assembly in 2011 by Russia, China, and other countries, is an example of this former approach. This proposal opens the door to greater government control over the Internet, including censorship by states of Internet content. It would limit freedom of expression online in order to promote political stability, a position at odds with existing international human rights instruments. The United States, by contrast, is committed both to a multistakeholder model that gives all appropriate stakeholders in the Internet the ability to participate in its evolution, and to a global consensus in which existing international law forms the basis for responsible behavior, including for protecting human rights online and the conduct of hostilities in cyberspace.

We believe that a cyberspace that rewards innovation, empowers individuals, develops communities, safeguards human rights, and enhances personal privacy will build better governments and strengthen national and international security. The Department of State promotes this vision both by actively working with our closest partners and allies, but also with states that are emerging as global leaders on the cyber stage, developing nations looking for ways to play in the cyber world, and even with states with whom we do not always see eye-to-eye.

The Department of State created my office in 2011 in recognition of the importance of ensuring an organizational focus on cyber policy issues across our international engagements. In my role as Coordinator for Cyber Issues at the Department of State, I coordinate and lead these international engagements. In order to effectively address these challenges, the Administration takes a whole-of-government approach, and the Department of State has worked closely with DHS, Commerce, DOJ, DOD, and other agencies to ensure that our foreign policy positions on cross-cutting cyber issues are fully synchronized. Together, we have sought to achieve the following principles:

1. National Security: Promoting a shared framework of existing norms that are grounded in existing international law.

Many states are developing military cyberspace capabilities—a prospect that has increasing potential to threaten our national security. Key aspects of cyber tools—the challenge of attribution of perpetrators or sponsors of attacks and the dual use nature of the technology—are inherently destabilizing. The State Department has pioneered the promotion of a framework in which States affirm that existing international law, including the law of armed conflict, is the appropriate framework to guide state-on-state behavior in the context of hostilities in cyberspace. We have also proposed transparency and confidence-building measures designed to reduce the risk of miscalculation that could inadvertently lead to conflict. The State Department has taken these concepts to the OSCE, the UN, and the ASEAN Regional Forum. We will continue to work to broaden the group of states who affirm the applicability of existing international law to cyberspace by leveraging our key strategic dialogues and demonstrating to states the benefits of abiding by the norms of conduct based in existing international law.

2. Cybersecurity Due Diligence: Challenge the international community to make cybersecurity a global policy imperative, develop national strategies, and foster transnational cooperation.

Cybersecurity at its core is the idea that each nation must protect its networks and information infrastructure by enhancing its security, reliability, and resiliency. By doing so, global security is enhanced. With our interagency partners, the State Department supports U.S. cybersecurity policy priorities by using our international partnerships; reducing intrusions and disruptions affecting U.S. networks; ensuring robust incident management, resiliency and recovery for information infrastructure; and improving the security of the high-tech supply chain. We also use existing public-private partnerships in support of critical infrastructure protection, international telecommunications, and trade. We complement those partnerships by also collaborating with the private sector on preparation for and participation in global cyber engagement in bilateral, regional, and international fora. A current example is our work with private sector and civil liberties organizations to augment their participation in the October 2013 Seoul Cyber Conference, the follow on to the preceding 2011 London and 2012 Budapest conferences.

The Internet is most rapidly expanding in the developing world, but developing states often lack the capacity to ensure its security. Over the last decade, U.S government international cybersecurity efforts have answered that charge, largely with a focus on helping countries build capacity for domestic cybersecurity. These efforts have been carried out through extensive

bilateral engagements and through concerted, long-term work in the UN, G-8, OAS, OECD. APEC, OSCE and ITU-D. The State Department is now leading the U.S. government in strengthening those efforts, challenging countries to build domestic capacity while simultaneously elevating their view of cybersecurity from a domestic to a global approach, a progression that requires countries to organize effectively and take systematic steps to operate securely in cyberspace, following shared international norms.

My office has supported this transition. We have established interagency capacity building programs to help developing states better protect their cyber and mobile networks, while also emphasizing the importance of protecting fundamental freedoms and promoting affordable access. The first of these programs, in Kenya in July 2011, alerted governments of the East African Community to vulnerabilities and provided tools for securing networks and cooperating internationally. A paired set of programs, in Senegal in September 2012 and Ghana in January 2013, reached fourteen states in West and Central Africa, and launched follow-on engagements to build long-term cyber partnerships in these regions. Programs such as these leverage U.S. government, private sector, and international expertise to help countries take the systematic steps needed to ensure safety and security in cyberspace, which in turn also fosters leaders who can lead and execute compatible capacity building efforts. We understand Ghana intends to craft its own national cyber strategy, and we welcome the continued opportunities to engage with them.

3. Cybercrime: Promote the Budapest Convention and capacity building to help other nations fight cybercrime.

The United States is the clear world leader in combating cybercrime and devotes extensive resources to helping other countries develop their ability to fight it. But unfortunately, cybercrime continues to grow at an exponential rate and most countries are struggling to tackle the challenge. The United States strongly supports the Budapest Cybercrime Convention and uses its structure as a basis for our capacity building efforts. That framework includes three key concepts: (1) ensuring law enforcement agencies have the authorities and tools to fully investigate cybercrime and deal with electronic evidence; (2) enacting substantive cybercrime laws; and (3) creating formal and informal mechanisms like the G-8 24/7 Network to ensure effective and timely international cooperation. We are actively making a renewed push to increase the number of parties to the Budapest Convention, and to increase the membership of the G-8 24/7 Network for law enforcement points of contact. A growing number of states have expressed interest in acceding to the Budapest Convention and we encourage additional cross-border cooperation on combating cybercrime.

4. Internet governance and public policy: Protect and promote inclusive global Internet governance mechanisms and ensure our vision of an open and interoperable Internet.

The Internet is currently managed by multi-stakeholder entities that reflect its dynamic, innovative nature, such as technical and standards bodies like the Internet Engineering Task Force and the Internet Corporation for Assigned names and Numbers. Public policy conferences like the Internet Governance Forum also play a vital role in shaping the Internet in a multi-stakeholder setting. This preferred architecture is under threat from those countries who seek a top-down, state-driven, UN-style mechanism for Internet management. The U.S. remains steadfast in our support for these existing, multi-stakeholder organizations. We also recognize

that their legitimacy is derived both from their efficiency and effectiveness and from a global perception that they are independent, transparent, and non-political institutions. The U.S. must continue to vocally support these institutions, provide constructive contributions as necessary, and encourage our friends and allies to do the same.

5. Internet Freedom: Promote respect for human rights, including freedom of expression online, and more fully integrate Internet freedom policy within broader cyber foreign policy goals.

In the wake of the Arab Spring and in light of increased global access to the Internet, a wider range of countries are pursuing policies that diminish protections for those freedoms of expression, assembly and association that are enshrined in the Universal Declaration of Human Rights. Countries pursue such policies through new domestic laws and regulations, through resolutions and agreements in international and multilateral institutions, and through targeting individual citizens peacefully exercising their rights online. As the State Department continues to respond to the largest Internet Freedom offenders, we have been deeply involved in the creation of the Freedom Online Coalition. The Coalition provides a forum for nineteen like-minded governments from five continents to coordinate efforts to advance Internet freedom. The Coalition works with civil society and the private sector in a multi-stakeholder process to support the ability of individuals to exercise their human rights and fundamental freedoms online. I view the Freedom Online Coalition as a great venue for addressing Internet Freedom and human rights issues with our partners. It can also be a useful venue to consider broader cyber policy concerns that have an Internet Freedom nexus. These fundamental freedoms that form the core of our Internet Freedom policy are also the foundational principles for our cyber policies writ large.

The Department of State works closely with the interagency to further these five principles in an array of international engagements. The U.S. engages on cyber issues with a multitude of states, bilaterally and in regional groups. For example, we are working with our European allies, both with the European Union and in NATO. The European Commission recently launched their cybersecurity strategy, and at last year's Chicago Summit, NATO leaders reaffirmed their commitment to improve the Alliance's cyber defenses. We coordinate very closely with our partners around the world and in the last year alone, we have launched dedicated cyber whole-of-government senior policy dialogues with India, Brazil, South Africa, South Korea, Japan, and Germany to share perspectives and build a consensus view on the future of cyberspace. We continue to seek deeper engagement with countries like Russia and China who may have a different world view but with whom we need to find ways to develop stronger relationships. Through these engagements, we leverage the widespread global public support for an open Internet to champion the multi-stakeholder model with emerging global leaders.

The U.S. government has challenged and persuaded other states to focus on cybersecurity as a critical policy issue. That work goes back many years and includes several UN resolutions on cybersecurity and capacity building. My office was the first of its kind in a foreign affairs agency, and since its creation, many countries have created similar positions and offices in their own foreign ministries as they recognize cyber as a new foreign policy imperative.

The State Department has effectively mainstreamed rapidly-developing cyber policy issues across our regional and functional bureaus, and integrated cyber within our international engagements. We have created internal coordination mechanisms to draw from a range of expertise in the formulation of cohesive and balanced policy. We have also helped our diplomatic posts establish diplomatic cyber points of contact – a corps of cyber attachés if you will – as well as form interagency country teams on cyber issues to communicate globally the U.S. vision of cyberspace and cybersecurity.

The State Department will continue to focus on both the kinds of operational threats you've called us here today to discuss, and on the long-term policy efforts that will help to mitigate them in the long run. In his confirmation hearing, Secretary Kerry cited the importance of "cyber-diplomacy and cyber-negotiations," stressing the need to affirm "rules of the road that help us to be able to cope" with challenges in cyberspace. State is doing just that, working with other nations on efforts that will not only contribute to greater stability and security in cyberspace, but will also protect freedom of expression, ensure opportunity to innovate, and promote economic growth around the world.

Mr. ROHRABACHER. Well, thank you very much. We also have Congressman Lowenthal who has joined us. Thank you very much for joining us this morning. Let us just figure out how serious people are taking this. Have we gotten beyond the let-us-sit-down-and-discuss-it phase with other countries, or do we have an action plan that if we discover cyber attacks going on that there will be some type of retaliation against the criminal element or the government itself that is engaged in this cyber crime?

Mr. PAINTER. So we face a wide range of threats in cyberspace from nation states to transnationally organized criminal groups. And how we respond to those different threats depends on what the threat is. And one of the problems, of course, is that attribution is difficult in this area and you don't know, often, exactly which group is doing what activity. However, speaking first from the cyber crime side, we are promoting around the world what is called the Budapest Convention on Cyber Crime so that every country will have strong laws in this area. They will have the capability to actually prosecute those laws, there will be better international cooperation. We have something——

Mr. ROHRABACHER. How many people have been prosecuted in China for cyber crimes?

Mr. PAINTER. I would have to get back to you about it, sir. I don't know.

[The information referred to follows:]

WRITTEN RESPONSE RECEIVED FROM MR. CHRISTOPHER PAINTER TO QUESTION ASKED DURING THE HEARING BY THE HONORABLE DANA ROHRABACHER

The lack of reliable or transparent statistical information on prosecutions renders it impossible to say exactly how many persons in China have been prosecuted for activities that we would consider to be cybercrimes. When the U.S. discusses cybercrime, we speak in terms of specific conduct criminalized in U.S. criminal laws, such as Title 18 U.S.C. Section 1030, the Computer Fraud and Abuse Act. China, however, takes a very different approach and speaks in terms of "criminal and terrorist activities that use information and communications technologies," as reflected in the Code of Conduct for Information Security that they jointly authored with Russia. The Chinese government considers cybercrime to include online speech that it views as undermining "political, economic and social stability," categories of expression that would in almost all instances be protected in the United States by our Constitution's First Amendment, and that is protected by the right to freedom of expression in international human rights instruments.

Addressing challenges in cyberspace, including combating cybercrime, is a priority for the United States, and we engage routinely with other nations to enhance international cooperation in these areas. Of note, the U.S.-China Cybercrime Working Group, led by the Department of Justice, is working to improve cooperation with China on cybercrime cases.

Mr. ROHRABACHER. Can you tell me any country in the world where we have had the prosecutions and what they have composed of?

Mr. PAINTER. We have had many prosecutions in the United States.

Mr. ROHRABACHER. No, no, not the United States, the other countries of the world.

Mr. PAINTER. There have been prosecutions, and many of our close allies in Australia and England, in Germany and France, there have been prosecutions.

Mr. ROHRABACHER. And what happens to someone in Australia or——

Mr. PAINTER. It depends on their particular legal system. Of course, in the United States we have pretty substantial penalties based on financial harm for cyber crime. Other countries have similar regimes. And what is important about this Budapest Convention, this convention that is really the only existing instrument and the best instrument for cyber crime, is that it creates certain kinds of offenses that didn't exist before.

So you may remember years ago when there was the "I love you" virus, and they thought they found the perpetrator, and the country where they found him didn't have any law that criminalized that issue. So the Budapest Convention allows countries to modernize their laws so there won't be safe havens for this conduct and you can prosecute.

Mr. ROHRABACHER. What would you suggest that we do, for example, if we come to the conclusion that a cyber attack both in terms of a criminal cyber attack and also strategic cyber attacks are actually being blessed, if not perpetuated and actually involved in the government of that country?

Mr. PAINTER. I think we have to look at all the tools that we have at our disposal as a national government. But from my perspective, obviously the tools that we employ are the diplomatic tools. And those tools, I think, are important to make clear to a government that conduct this is a concern.

Mr. ROHRABACHER. And what are those tools, I mean diplomatic tools?

Mr. PAINTER. Those diplomatic tools, I think, are two-fold. One is engaging directly with that government and saying to them that this conduct is something that we find unacceptable.

Mr. ROHRABACHER. Well, I am sure that will upset them a lot.

Mr. PAINTER. Well, but I think you have to look at their overall relationship. With a lot of these countries we have many different types of relationships—economic relationships, other relationships.

Mr. ROHRABACHER. Have we done any of that?

Mr. PAINTER. Yes. In fact, just recently the President has made clear in his call with the new——

Mr. ROHRABACHER. No, what actual sanctions have we put on any country? For example, it is clear that China has been deeply involved in this. Everybody knows it, supposedly. What have we done to say, okay, here is your deadline and this is exactly what is going to happen. You are no longer going to be able to purchase certain things from the United States, or be able to export to the United States, or whatever retaliation we would have.

Mr. PAINTER. Sir, I would speak from my perspective and what we are doing diplomatically. I would say one thing though. I think with any of these threats we would have to be careful of looking at this in terms of retaliation, if it is a retaliation in terms of in-kind retaliation. We want to make sure that we are addressing the problem and addressing it in the larger context of any country we are dealing with. But what I would say is if——

Mr. ROHRABACHER. We have to accuse the right people, right?

Mr. PAINTER. Right. And I do think that if you look at the statements just in the last couple of weeks, and let me go back a ways. We have engaged the Chinese in a strategic security dialogue on sensitive issues. We have only had two meetings of that group, last

year and the year before. We raised cyber at both of those meetings. Secretary Clinton, last year, said that the theft of intellectual property and trade secrets was one of the greatest concerns of the United States, and we have had very frank discussions. And I can't really get into our bilateral private discussions in this setting, but I would be happy to follow up later on.

And then recently, of course, you have heard Tom Donilon, the National Security Advisor, talk about the great concern that this poses for us and say three things. One, we want China to understand the scope and seriousness of this problem of this activity emanating from China. Two, that we want to make sure that it stops. That they actually take some action to investigate and stop this activity. And three, that we need a sustained dialogue with the Chinese. And we have some dialogue, but we don't have a sustained dialogue. And the President said that——

Mr. ROHRABACHER. Well, I am sure threatening to have a sustained dialogue is really going to deter these fellows along with proclamations of great concern. All I know is that I just asked you a specific question about specific actions and all I got was a list of words that had been spoken. And I am sure that words coming out of the mouth of officials of the United States is terribly frightening to the Chinese.

Let me turn to Mr. Keating now.

Mr. KEATING. Thank you, Mr. Chairman. I mentioned in my opening remarks, in 2007 our NATO ally Estonia was subject to a series of cyber attacks directed at their Parliament, their ministries, their banking systems, newspapers, and broadcasters. NATO subsequently established the NATO Cooperative Cyber Defence Centre of Excellence in Estonia to enhance the capability, cooperation, and information sharing among NATO and its partners in cyber defense.

Now does the State Department have any evaluation of the effectiveness of that initiative? And furthermore, some of our NATO allies have looked to the U.S. to lead on cyber initiatives in NATO-member countries. What sort of role has the U.S. had in this initiative going forward, and what kind of role is it willing to play? What implications does this initiative have on information sharing between all of the NATO countries?

Mr. PAINTER. So a couple of things. The NATO Centre of Excellence in Estonia, the U.S. is supporting that effort and actually has personnel stationed there, and I think it is an important effort to look at some of the larger issues involving cyberspace. With respect to NATO, generally, as you know back in the Lisbon Summit, for the first time, and this was a proposal of the U.S., we made cyber a key part of NATO strategic concept. And first and foremost in that concept was making sure that NATO's own networks were secure, and that is something they have been working on in the last couple of years. They have also been promoting information sharing between members of NATO.

Now NATO is not the only way we approach this. We deal obviously with the EU who just released an international—well, they released a strategy document for cyberspace. And it was remarkable because three parts of the EU, the External Action Service, the DG Connect as it is called, and their home ministry got to-

gether and collaborated on this strategy. And the strategy, the international part, is very similar to the U.S. strategy. It is very consistent with our strategy around the world, particularly in terms of promoting norms, and the existence and applicability of international law, existing international law, including the law of armed conflict to cyberspace. Those are critical things.

So we are working with the EU. We are also working with key member states. We are working with the U.K. We are working with Germany. We are working closely with France. We are working closely with the Netherlands, and many others in that context. And we work through other forms, like the G8, for instance, and the OECD, and other forms like that. So there has been a lot of activity that we have been doing. There has also been our Defense Department who works with our allies in making sure that they have better defenses and building those defenses.

And finally, our Homeland Security Department has been working with a number of countries and exchanging information with their computer emergency response teams. One thing, I think, that is a great development not just in Europe but around the world is that countries are developing national strategies for dealing with cyber. We have one here, and many other countries now have them, but in Latin America and other places those are being developed.

The one other thing I would say just to reflect on the last question before yours, I do think it is important that we are raising this issue at a very high level. I think it makes a difference when the President raises this level, when Tom Donilon raises this level. And we are also doing things to protect us at home, like what DHS is doing to share information with the private sector and help harden the targets, make sure our defenses are better.

Mr. KEATING. Yes, I am on the Cybersecurity Subcommittee in Homeland Security as well. But how well are these other countries doing, working with the private sector side? Because governments can work all they want, but if we are not having a dynamic approach dealing with the private side as well we are not going to be successful in this. Are any of the other countries you are familiar with, are they doing a better job getting that kind of cooperation?

Mr. PAINTER. I think we are all trying to make sure that is an effective partnership. I think it is extraordinarily important because the private sector not only owns most of the infrastructure but, frankly, government doesn't have all the answers. We have to engage with the private sector and others to make sure we go forward.

When I started this office, a little less than about 2 years ago now, one of the first things I did was start meeting with various private sector groups. Because they may see opportunities or dangers that perhaps we don't see in government, and it is important to make sure that they communicate with us on that, and they often go to some of these international meetings.

Mr. KEATING. Well, we are trying to balance here whether or not we go through regulations, and government is telling the private sector what they have to do. We are trying to balance off that to a more cooperative way to see if we could do—what are the ap-

proaches in some of these countries? Do we have countries that you are aware of where they are just having their own regulations on the private side and——

Mr. PAINTER. I think there are countries that are more regulatory in nature, just by their nature. What we try to argue when we have our dialogues with other countries is that it is important for them to talk to the private sector. Some countries, frankly, don't have a history or a culture of talking to the private sector the way we do here. I think we made great strides in that here. For instance, even building our National Incident Response plan with the private sector from the ground up, something I don't think we have ever done before, and that was just in the last couple of years.

But one of the things we do is when we do, for instance, capacity building, one of the great efforts of our office not only to help build capacity, but to try to convince the developing world that our way of looking at cyberspace is the correct one and will help them, we bring private sector along with us. We try to tell those governments, dealing with the private sector is critical in actually securing your networks in securing cyberspace.

And I think obviously the executive order is very important, it is just the down payment on what we need. We still need legislation, as you know, and we still need legislation that we have talked about last year and talking about this year, and we hope we get it, that allows that both voluntary but very important connection between the private sector and government.

Mr. KEATING. I yield back, Mr. Chairman.

Mr. ROHRABACHER. Mr. Marino?

Mr. MARINO. Thank you, Chairman. Good morning, Mr. Painter. I am sure that you participate in classified meetings concerning intelligence that we accumulate and share with our allies, and you are between the devil and the deep blue sea here with what you can tell us and what you can't tell us. So I am just going to assume that that is the case. But I am a member of the NATO Parliamentary Assembly, and on a recent trip from a NATO meeting in Belgium it did not appear to me that this subject of cyber warfare was a top priority.

Can you give me a suggestion as to what the administration is doing to make this a top priority, and are our allies behind us or beside in this and will it have an impact on Russia and China?

Mr. PAINTER. Okay. So first, just in terminology, rather than use cyber warfare I just say the cyber threat and how we deal with the cyber threat. And I would say that as I mentioned before the fact that cyber is now part of NATO's operating concept when it never was before is a key consideration. And it is no small task for NATO to actually get its networks to the shape that—this is a foundational thing. If you have your networks, your own networks, NATO networks, and the member states' networks secured, you can build on top of that.

I just met with Ambassador Iklody, yesterday, from NATO, who is their cyber person, and they are doing a lot of activity in this area making sure that they are having better security of their networks, and they are sharing information between member states, and I think that is the most important part.

Mr. MARINO. I understand that. But do you really think we are going to—let us get down in the weeds here. If the NATO members get together and implement severe sanctions, do you really think China and Russia are going to listen to us? I was in China and Russia not too long ago and I brought up the issue with them. They didn't like it. Actually, China acted like it wasn't happening, and Russia simply said so what.

So let me give you a scenario here. Assume we have an attack on Wall Street, the stock exchange, it crashes, and we know from where it came. Have you worked out any scenarios as to what will happen from that point forward on behalf of the United States and some of its allies?

Mr. PAINTER. Yes, to the extent that we have actually, just recently in the National Level Exercise that was conducted last year, for the first time that focused on cyber. So we were looking at very catastrophic events in the context of cyber in that exercise. And that both exercised how we were going to work together, but also we had some of our close allies participating in that exercise.

And as with any other threat, and we lay this out in the international strategy, we use every tool at our disposal whether it be economic, diplomatic, I think we say informational, or even military. Military is a last resort and only after we have exhausted other options in law enforcement of course too. But we have the full suite of tools and we have close allies with whom we are discussing this with all the time, and——

Mr. MARINO. I do not mean to be facetious about this, but do you think that this has been working to any extent at all? I do not see any actual repercussions being implemented or any scenarios that would cause the Chinese or the Russians to stop it or curtail it at least.

Mr. PAINTER. Well, first of all, I would say that we have certainly raised the pressure about how serious this issue is for us recently, as you have seen from the President's statement, from Tom Donilon's statement, et cetera. Other countries, I think, are also looking at this issue and how they are going to deal with this issue. We have made tremendous progress even in the last 2 years in treating this issue as much more, not just a technical issue but an economic issue, a national security issue, and a foreign policy issue. Other governments are doing that too but they are at different stages, and we are dealing with them and talking with them. Again, I really can't talk about our private conversations as you know.

Mr. MARINO. I understand. I have less than 20 seconds now. And I am also involved on the Intellectual Property Subcommittee, and it is a big issue with me, and we are losing billions of dollars and tens of thousands, maybe hundreds of thousands of jobs. But I have, maybe a little tongue-in-cheek sarcasm remedy is since we owe China so much money for our debt, why don't we deduct what they are stealing from us and take it away from the debt? I yield back. Thank you.

Mr. ROHRABACHER. Well, then they might have grave concerns as well if we did something like that.

Mr. Duncan, you may proceed.

Mr. DUNCAN OF SOUTH CAROLINA. Thank you, Mr. Chairman. First off, I will just say America needs to realize that this is a real threat. And we talk about cybersecurity a lot, and it is not just some hacker stealing iTunes downloads or small-scale intellectual property theft. This is on a grand scale. It is not only on grand scale with intellectual property with private corporations, but it is also the theft of military hardware plans such as some of our fighter aircraft.

And so it is not just China. It is Iran. It is the Russians. It is a lot of different groups, organized crime and others that are pinging away at the United States trying to find a chink in our cyber armor. And I think it is important that we also realize that the electrical grid and a lot of the components that keep America operating are also in the sights of the cyber criminals and other entities. So I am concerned about that. And the reason I brought Mr. Clapper's comments up this morning is he also recognizes that this is an imminent threat and concern to the United States.

And so I was reading about a Chinese operative, a scientist who was allowed to work with NASA and Langley through a contract, and was arrested by the FBI as he boarded an airplane carrying hard drives, flashdrives, and computers that most likely contained sensitive data that he downloaded. You can carry a tremendous amount of information on a thumb drive or a computer hard drive. But I think that pales in comparison to what can be downloaded through hacking. And something that is operating behind the scenes 24/7 without an actual person sitting there downloading into a thumb drive, it is going on by behind-the-scenes computers.

And so at what point, in my opinion, does the administration consider that type theft, espionage, and damage to the U.S. computer systems an act of war?

Mr. PAINTER. So again, what an act of war means and what an act of war would trigger, I think, is, as I look at the threats, as DNI Clapper articulated the threats, we have two kinds of conduct. We have the fear of the threat of cyber warfare, which is attacks on infrastructure that could be crippling, which he said as of this point, is remote, but we have to be worried about it, and then we have what we see every day which is the large-scale, unacceptable theft of intellectual property, and that is a real concern. It is a real concern, for me it is a real concern. Throughout our Government we are taking actions to try to both prevent that theft by making sure we have better security. That is why the executive order is there. That is why we are asking for legislation.

We are talking to countries that we believe are involved in this activity. We are talking to our allies about this. We are also considering other actions more generally. But I think it is not that that is cyber warfare, but that is, I think, something that is clearly damaging to the American economy. It is the life's blood of these companies. It is taking away our future innovation. So we are taking it incredibly seriously, and I, certainly, even if I didn't have this job, as a former prosecutor who prosecuted intellectual property cases, I think this is a really important issue and it has gotten a lot of attention, as it should, recently.

And so our part of this is trying to do a couple of things. In the short term, we are working to help mitigate these issues, working

with DHS, working with other interagency partners, and in our diplomatic efforts both bilaterally and multi-laterally with other governments. In the long term, we are trying to make clear that the norm in cyberspace, the norm we are trying to promote is that this kind of theft of intellectual property and trade secrets is simply unacceptable, and countries that are outside of that core will get marginalized much as we did with money laundering back in the '70s. So this is something I think is both a short-term and long-term effort and we are taking actions on both of those——

Mr. DUNCAN OF SOUTH CAROLINA. And I appreciate your willingness to say that because it is not only damaging our economy and our abilities, it is taking our edge away militarily, our advantage. If they are stealing the plans of an F–35 and so we have to send F–35s against a comparable aircraft, that is taking some of that competitive advantage away that we have militarily to protect this country. And it is taking our economic advantage away with cyber crime that is taking intellectual property.

And so at some point in time I would love for this administration to say no more. We are going to hold someone accountable. We are going to hold someone accountable for the theft. We are going to hold the host countries where the operatives are using the cyber attacks, whether it is China or Russia, we need to hold those host countries responsible to some degree for what is going on within their borders. I think we would do that to ourselves. I think the United States ought to be responsible for what is going on within our borders with regard to cyber crime, and I think we are.

And so I think at some point in time we need to make sure that just a very clear line is drawn and a very clear understanding within the international community of what is acceptable and what is not acceptable with regard to cyber crimes, prosecution, and going forward. So Mr. Chairman, I am out of time, so with what I will yield back.

Mr. ROHRABACHER. Yes. What is acceptable and not acceptable and what the consequences are, because they don't care what is acceptable or not acceptable. They have to know what the consequences are, and so far we——

Mr. DUNCAN OF SOUTH CAROLINA. You are saying it a little more eloquently than I did, and I appreciate it.

Mr. ROHRABACHER. No, it has been clear the consequences are statements of great concern and statements of something that will be sustained. And we will give you a chance to answer that one after Mr. Stockman, who is one of our more timid members of the committee, also known as being a ferocious patriot, Mr. Stockman, you have 5 minutes.

Mr. STOCKMAN. I just have a concern. My district encompasses everything from NASA to petrochemical plants. And we were touring some of the plants, and they were stating that they were getting very little cooperation from the government on helping deter some of the cyber attacks. And they were mentioning that it could cripple our nation. Just by turning off a few valves it could blow up a plant. And this is something that is very serious.

This reminds me of 9/11 when we knew about the Philippines. We picked up documents which showed that they wanted to use planes as weapons, yet we ignored all the signs. I feel like we are

ignoring all the signs. And I have on the ground, plant managers telling me their concerns and yet they don't feel we are getting any help from the government. And I am asking you, is there any kind of game plan to help critical infrastructure? Have you identified it and said hey, we are going to talk to you guys? Because one plant alone in my district produces about 600,000 barrels a day. If that were to be taken off the market you would see a quick crisis occur. And if you took off several plants it would shut down the United States.

Mr. PAINTER. So my DHS colleagues deal with this all the time and, in fact, there have been designations of critical infrastructures and ways set up to deal with those industries and talk to those industries about cyber, not just about all the other issues they face and all the other challenges, but about cyber in particular. And certainly it is our goal to make sure that those companies understand both the scope of the problem, which is often a problem. Many companies don't understand, really, what the threat they are facing is, and that has been a problem we have had for the last 10 years, but they understand that the government does care about this and wants to work with them.

And there have been a lot of activities recently in terms of sharing signature information, et cetera, with companies and with ISPs and with other providers to better protect that critical infrastructure. If you look at the executive order and the proposed legislation, that is targeted, again, at critical infrastructure. Narrowly defined but critical, because if something happens to it, as you say, it could really bring us to our knees. And that is extraordinarily important.

And I would say this also, other countries around the world are focusing on critical infrastructure too. Certainly the U.K. and Germany or others are looking at this and say, what is it that we really need? What are the threats we are facing from cyberspace, what can they do to us, and how can we build better defenses? Part of it is building better defenses. Part of any strategy, any deterrence has to be building better defenses, and part of it, and my part of it has to be what we are going to do diplomatically.

But that is only one part. This is a whole-of-government effort that includes DHS, it includes DoD, it includes the Commerce Department and Justice and the FBI in the full range of our activities, but they have to work together. And it is important that we have the foreign policy element, but that is one of the many elements in our tool kit that has to be integrated.

Mr. STOCKMAN. Can I just do a follow-up question there? Can you see from the plant manager's concern if you step in his shoes, and this is recent, the frustration he has that he feels like he is in a vulnerable situation and he is going to be held accountable, but he is not getting any kind of feedback from the administration or, quite frankly, anybody in the governmental body? He is sounding the alarms and then it is falling on deaf ears, so there is a great deal of frustration from his viewpoint.

And I feel like maybe all of us in this committee and maybe in Congress are ignoring his concerns. It is a legitimate concern. As you know there is clips of things that were done remotely that were very devastating, and I will just ask that you somehow follow

through on your plan to work with the critical infrastructure of this nation.

Mr. PAINTER. I would just say that that is something that has been a priority now for a few years in our Department of Homeland Security, and other parts of our Government have been working strongly to do that. Before I came to the State Department in 2009, the cyberspace policy review we wrote talks about this issue exactly, raising awareness and addressing some of these concerns with the critical infrastructure.

And if that plant manager is feeling that way that is certainly unfortunate, but we have to make sure that we are working with him, and I think we are. And the other thing I would say is that compared to even a few years ago the awareness level and the coordination among government agencies and the priority of this issue is higher than it has ever been.

Mr. STOCKMAN. Thank you. And I yield back the balance of my time, Mr. Chairman.

Mr. ROHRABACHER. Thank you very much. I want to thank the witness. And let us just note that we have a huge number of targets in our country that can be attacked via this mechanism, the cyber attack. And we cannot defend. It would be impossible for us to defend all these targets. Thus, the only way that we can defend ourselves is if those who are committing crimes against us face serious consequences and thus will refrain from those attacks.

At this point, from your testimony—and let me just say you are a wonderful person and you take your job seriously. You are a former prosecutor, and I am sure that you put people in jail for committing crimes against other people and crimes against our society, but we can't put in jail the people who threaten us today and could do us great harm.

And people have got to know overseas whether or not there is going to be a serious consequence, not just raising the words at a discussion between heads of state, but a serious consequence if they are found guilty here of being an accomplice to a major crime. A crime of shutting down maybe that oil refinery in order to give them leverage on some oil deals someplace else in the world that they are trying to make, or maybe even putting our air traffic control system out of whack for a day. There is too many targets to defend, and right now those people who could possibly commit these acts don't know what those serious consequences are. And that lack of definition that we have of what you are going to face if you do this, I believe, could cause serious consequences to our people. To our people, rather than the people committing the crime.

So as you move forward in your job we wish you well this year. This committee is here to work with you in trying to—because we are supposed to handle emerging threats, and if there ever was an emerging threat that is what we are talking about. But as a prosecutor, as a tough guy that deals with criminals, let us make sure that we are just as tough dealing with these cyber threats to our well being.

And Mr. Keating, do you have a 1-minute summary would you like to make?

Mr. KEATING. Well, I think there is a lot of activity going. One of the things that we didn't get into that is worth mentioning is,

as some countries move forward on these areas to try and do it under the guise of getting control over cyber threats, we have countries that are going to try and inhibit communication, social media, the kind of communication that is healthy in a democratic country. And so there is a balancing act to be made in that respect, and I think it is worth mentioning that that makes it difficult.

But I would just say this. That I hope that this Congress can come forward with legislation this year. We will be reacting quickly if, indeed, one of our five top financial groups is hacked into for any extended period of time. It is conceivable they could go bankrupt. And if you compare that with what happened with the mortgage crisis, this would have far more devastating impact.

And I do agree, just following up on what the chairman said, internationally with our allies, I think we should have more concrete sanctions and a ratcheting up once we have accountability. Because I think that will indeed help as a deterrence as well so people and countries will know what they are facing as a result. But I thank you for your testimony and your hard work in this area.

Mr. ROHRABACHER. Let us give the witness the courtesy of giving him the last comment, but not more than 1 minute.

Mr. PAINTER. Not long.

Mr. ROHRABACHER. Not more than 1 minute.

Mr. PAINTER. I appreciate that very, very much, Mr. Chairman. I would say that look, I am heartened that this has gotten so much priority and so much interest. Having spent time in this area now for over 20 years, the fact that over the last few years it has now become not just a technical issue but a real foreign policy priority, a real national priority, and a real international priority. It is a huge step, and that is something that we need to build on.

I would also say that taking out of the context of any particular actor, even our international strategy, which by itself—we were the first country to put together an international strategy. We are the first country to create an office like mine, and many other countries have now have followed suit and that is important too. In international strategy we have a deterrent policy there. We say we will use all tools that we have. Diplomatic is one of them. It is just one of them. Diplomatic, economic, law enforcement, military, the full suite of tools in appropriate circumstances given the circumstances that are there.

I think we are making a huge, it is a hugely complex issue. We are dealing with the Internet freedom issues. We are dealing with governance issues and keeping this a multi-stakeholder governments' process. We are dealing with the international security issue, the applicability of international law, building confidence between countries so things don't escalate out of control, so we can actually get some transparency to other governments, and we are working on cyber crime. So all these are important. It is a big lift over the next few years but something, I think, we are really prepared to do. So thank you.

Mr. ROHRABACHER. Well, thank you. Life wasn't so complicated before, was it? Thank you very much.

We have a second panel who will be joining us now. So we have a very distinguished panel for our second panel. And first, what we

will do is I will introduce all of you and then we will proceed with your statements and then we will go into questions after that. And if you gentlemen could make your statements around 5 minutes so that we have a little time for questions. There are votes coming up in the next hour at least, so we will have to adjourn at that point. So we will move forward as soon as we can.

We will start with Mr. Richard Bejtlich is chief security officer at—pronounce that for me.

Mr. LIBICKI. Mandiant.

Mr. ROHRABACHER. Okay, I am blacking out on that pronunciation. He was previously director of Incident Response for General Electric. Prior to GE he operated the TaoSecurity LLC as an independent consultant, where among other things he protected national security interests for Mantech Corporation's Computer Forensic and Intrusive Analysis Division. He began his digital security career as a military intelligence officer working for the Air Force Information Warfare Center and Air Intelligence Agency. He graduated from Harvard University, and the United States Air Force Academy.

We have Michael Mazza, a research fellow at the American Enterprise Institute, and program manager for AEI's annual Executive Program on National Security Policy and Strategy. Michael Mazza has studied and lived in China and writes regularly on U.S. strategy in Asia and on Taiwanese defense strategies. He has a Masters degree in International Relations, Strategic Studies and International Economics from the Paul H. Nitze School of Advanced International Studies at Johns Hopkins University, and a B.A. from Cornell. The second Cornell man we have had today with us.

Greg Autry is a senior economist for the Coalition for a Prosperous America. He is the co-author with Peter Navarro of the book, "Death by China," and I might add it is a great book and a great movie. Considering how many times I was quoted in it that is what makes it even better. And Greg holds a B.A. in History from Cal Poly Pomona, and an M.B.A. from Merage School of Management at UC Irvine.

And finally, Libicki. I am really bad at making these pronunciations. With a name like Rohrabacher you are going to have to—anybody can mispronounce my name, and we will make a deal. A senior management scientist at Rand Corporation, he is the author of Rand's study, "Cyber Deterrence and Cyber War." Prior to joining Rand he spent 12 years at the National Defense University, 3 years on the Navy staff as program sponsor for industrial preparedness, and 3 years as a policy analyst for the General Accounting Office's Energy and Mineral Division. He has received a Ph.D. in Economics from the University of California at Berkeley.

We will start with you.

STATEMENT OF MR. RICHARD BEJTLICH, CHIEF SECURITY OFFICER AND SECURITY SERVICES ARCHITECT, MANDIANT CORPORATION

Mr. BEJTLICH. Thank you, Mr. Chairman. Thank you, Ranking Member Keating, distinguished members of the committee.

My name is Richard Bejtlich and I am the chief security officer at Mandiant. Mandiant is a computer security company that has one mission and that is to detect and respond to advanced intruders. We have been doing that for 9 years. We are unique in that respect that we were founded on the idea that you can't stop determined attackers, and there needs to be someplace for the private sector, or even in some cases, government agencies to call for help. And that is what we do. As I am sitting here today, we have teams out at somewhere between 12 and 15 customers, helping them recover from intrusions. Our software is helping dozens of other companies, hundreds of others, actually, at this point. And that is what we do as a company.

So who is APT 1? Who is this group that we outed in our report? It is important to realize that APT 1—and APT stands for Advanced Persistent Threat. It is a term that was invented by an Air Force colonel in 2006 to tie back to Chinese threat actors. APT 1 is one of two dozen groups that our company tracks. APT 1 is the most prolific of these groups in terms of the number of industries that are affected. We estimate there is about 20 that we have personally witnessed including 141 companies, 115 of which are in the United States.

But there are other groups that we just did not decide to document in our report. APT 1 is actually Unit 61398. This is a unit of the People's Liberation Army. It is the second bureau of the third department. And the third department in the PLA General Staff does signals intelligence. So it makes sense. You take a signals intelligence unit and you turn them into a computer network operations unit. They operate primarily out of a headquarters outside of Shanghai that was built in 2007, 130,000 square feet. And there has been TV coverage recently where reporters from CNN tried to take some footage. They were chased by soldiers and the footage was temporarily confiscated.

Why did we release this report? We released the report because we wanted to move the discussion about this topic forward. As you probably heard, there has been talk of Chinese hackers. You couldn't tell if it was someone in his mother's basement. You couldn't tell if it was an organized crime group or such. We felt that we had been tracking this group for so long, for 7 years, and using a combination of technical indicators and non-technical indicators we were able to trace it back, right to the doorstep of this building, and figure out that this was this military unit.

We wanted to speak for victims. We help hundreds of companies and they are all frustrated. They want something to be done but they don't want to come forward and say something about it. Very infrequently that happens. We have seen that now with the New York Times, Google, RSA, U.S. Chamber of Commerce. Outside of that no one talks about this. We also felt that the time was right. We felt that the time for watching the fireworks had passed, and our sense was that the government wanted to talk about this and we had the evidence to talk about it.

And the report is completely based on our work, completely unclassified, not corroborated with government information. It just shows you what a dedicated group of, in this case our company is former military, former law enforcement, former Intelligence Com-

munity, and then just very motivated, highly skilled computer security people. This is what you can do if you devote yourself to this project. We also felt that if we provided the indicators of compromise, that data that talks about who these guys are, what they do to Western companies, and how they operate that people could defend themselves. And that has been fairly gratifying over the last several weeks since we released the report.

People are finding these groups inside their companies and they are doing something about it. And it gives you an example of what could be done, I think, if the government were more forthcoming in sharing what the government knows about these actors. It is also important to realize, what are you supposed to do with this information? What I would say is, every company in the United States that cares about security needs to be able to take a report like ours, digest the information in it and look for intruders in your company.

If you look at our report—and it is free. We are not charging for it. You download it from the Internet. If you look at this report and you can't do that, you can't figure out how to find intruders in your company, that is probably job one. You need to be able to do that. And secondly, you need to be able to see over time how this affects you. We find too many companies don't treat this as a business process. They treat it as something that engineers and technicians need to deal with. You need to realize that dealing with intruders is a fact of life in the business world and it needs to be a continuous business process that you deal with. I thank you for the opportunity to testify today, and I look forward to your questions.

[The prepared statement of Mr. Bejtlich follows:]

Statement for the Record

Richard Bejtlich
Chief Security Officer
Mandiant Corporation

Before the

U.S. House of Representatives
Committee on Foreign Affairs
Subcommittee on Europe, Eurasia and Emerging Threats.

March 21, 2013

Since 2004, Mandiant has investigated computer security breaches at hundreds of organizations around the world. The majority of these security breaches are attributed to advanced threat actors referred to as the "Advanced Persistent Threat" (APT). We first published details about the APT in our January 2010 M-Trends report. As we stated in the report, our position was that "The Chinese government may authorize this activity, but there's no way to determine the extent of its involvement." Now, three years later, we have the evidence required to change our assessment. The details we have analyzed during hundreds of investigations convince us that the groups conducting these activities are based primarily in China and that the Chinese Government is aware of them.[1]

Mandiant continues to track dozens of APT groups around the world; however, this report is focused on the most prolific of these groups. We refer to this group as "APT1" and it is one of more than 20 APT groups with origins in China. APT1 is a single organization of operators that has conducted a cyber espionage campaign against a broad range of victims since at least 2006. From our observations, it is one of the most prolific cyber espionage groups in terms of the sheer quantity of information stolen. The scale and impact of APT1's operations compelled us to write this report.

The activity we have directly observed likely represents only a small fraction of the cyber espionage that APT1 has conducted. Though our visibility of APT1's activities is incomplete, we have analyzed the group's intrusions against nearly 150 victims over seven years. From our unique vantage point responding to victims, we tracked APT1 back to four large networks in Shanghai, two of which are allocated directly to the Pudong New Area. We uncovered a substantial amount of APT1's attack infrastructure, command and control, and modus operandi (tools, tactics, and procedures). In an effort to underscore there are actual individuals behind the keyboard, Mandiant is revealing three personas we have attributed to APT1. These operators, like soldiers, may merely be following orders given to them by others.

Our analysis has led us to conclude that APT1 is likely government-sponsored and one of the most persistent of China's cyber threat actors. We believe that APT1 is able to wage such a long-running and extensive cyber espionage campaign in large part because it receives direct government support. In seeking to identify the organization behind this activity, our research found that People's Liberation Army (PLA's) Unit 61398 is similar to APT1 in its mission, capabilities, and resources. PLA Unit 61398 is also located in precisely the same area from which APT1 activity appears to originate.

---

[1] Our conclusions are based exclusively on unclassified, open source information derived from Mandiant observations. None of the information in this report involves access to or confirmation by classified intelligence.

Key Findings

APT1 is believed to be the 2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

»» The nature of "Unit 61398's" work is considered by China to be a state secret; however, we believe it engages in harmful "Computer Network Operations."

»» Unit 61398 is partially situated on Datong Road (大同路) in Gaoqiaozhen (高桥镇), which is located in the Pudong New Area (浦东新区) of Shanghai (上海). The central building in this compound is a 130,663 square foot facility that is 12 stories high and was built in early 2007.

»» We estimate that Unit 61398 is staffed by hundreds, and perhaps thousands of people based on the size of Unit 61398's physical infrastructure.

»» China Telecom provided special fiber optic communications infrastructure for the unit in the name of national defense.

»» Unit 61398 requires its personnel to be trained in computer security and computer network operations and also requires its personnel to be proficient in the English language.

»» Mandiant has traced APT1's activity to four large networks in Shanghai, two of which serve the Pudong New Area where Unit 61398 is based.

APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously.[2]

»» Since 2006, Mandiant has observed APT1 compromise 141 companies spanning 20 major industries.

»» APT1 has a well-defined attack methodology, honed over years and designed to steal large volumes of valuable intellectual property.

»» Once APT1 has established access, they periodically revisit the victim's network over several months or years and steal broad categories of intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing

[2] We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has conducted. Therefore, Mandiant is establishing the lower bounds of APT1activities in this report.

documents, partnership agreements, and emails and contact lists from victim organizations' leadership.

»» APT1 uses some tools and techniques that we have not yet observed being used by other groups including two utilities designed to steal email — GETMAIL and MAPIGET.

»» APT1 maintained access to victim networks for an average of 356 days.[3] The longest time period APT1 maintained access to a victim's network was 1,764 days, or four years and ten months.

»» Among other large-scale thefts of intellectual property, we have observed APT1 stealing 6.5 terabytes of compressed data from a single organization over a ten-month time period.

»» In the first month of 2011, APT1 successfully compromised at least 17 new victims operating in 10 different industries.

APT1 focuses on compromising organizations across a broad range of industries in English-speaking countries.
»» Of the 141 APT1 victims, 87% of them are headquartered in countries where English is the native language.

»» The industries APT1 targets match industries that China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan.

APT1 maintains an extensive infrastructure of computer systems around the world.
»» APT1 controls thousands of systems in support of their computer intrusion activities.

»» In the last two years we have observed APT1 establish a minimum of 937 Command and Control (C2) servers hosted on 849 distinct IP addresses in 13 countries. The majority of these 849 unique IP addresses were registered to organizations in China (709), followed by the U.S. (109).

»» In the last three years we have observed APT1 use fully qualified domain names (FQDNs) resolving to 988 unique IP addresses.

---

[3] This is based on 91 of the 141 victim organizations. In the remaining cases, APT1 activity is either ongoing or else we do not have visibility into the last known date of APT1 activity in the network.

»» Over a two-year period (January 2011 to January 2013) we confirmed 1,905 instances of APT1 actors logging into their attack infrastructure from 832 different IP addresses with Remote Desktop, a tool that provides a remote user with an interactive graphical interface to a system.

»» In the last several years we have confirmed 2,551 FQDNs attributed to APT1. In over 97% of the 1,905 times Mandiant observed APT1 intruders connecting to their attack infrastructure, APT1 used IP addresses registered in Shanghai and systems set to use the Simplified Chinese language.

»» In 1,849 of the 1,905 (97%) of the Remote Desktop sessions APT1 conducted under our observation, the APT1 operator's keyboard layout setting was "Chinese (Simplified) — US Keyboard". Microsoft's Remote Desktop client configures this setting automatically based on the selected language on the client system. Therefore, the APT1 attackers likely have their Microsoft® operating system configured to display Simplified Chinese fonts.

»» 817 of the 832 (98%) IP addresses logging into APT1 controlled systems using Remote Desktop resolved back to China.

»» We observed 767 separate instances in which APT1 intruders used the "HUC Packet Transmit Tool" or HTRAN to communicate between 614 distinct routable IP addresses and their victims' systems using their attack infrastructure. Of the 614 distinct IP addresses used for HTRAN communications:

-- 614 of 614 (100%) were registered in China.
-- 613 (99.8%) were registered to one of four Shanghai net blocks.

The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

»» We conservatively estimate that APT1's current attack infrastructure includes over 1,000 servers.

»» Given the volume, duration and type of attack activity we have observed, APT1 operators would need to be directly supported by linguists, open source researchers, malware authors, industry experts who translate task requests from requestors to the operators, and people who then transmit stolen information to the requestors.

»» APT1 would also need a sizable IT staff dedicated to acquiring and maintaining computer equipment, people who handle finances, facility management, and logistics (e.g., shipping).

In an effort to underscore that there are actual individuals behind the keyboard, Mandiant is revealing three personas that are associated with APT1 activity.
»» The first persona, "UglyGorilla", has been active in computer network operations since October 2004. His activities include registering domains attributed to APT1 and authoring malware used in APT1 campaigns. "UglyGorilla" publicly expressed his interest in China's "cyber troops" in January 2004.

»» The second persona, an actor we call "DOTA ", has registered dozens of email accounts used to conduct social engineering and spear phishing attacks in support of APT1 campaigns. "DOTA" used a Shanghai phone number while registering these accounts.

»» We have observed both the "UglyGorilla" persona and the "DOTA " persona using the same shared infrastructure, including FQDNs and IP ranges that we have attributed to APT1.

»» The third persona, who uses the nickname "SuperHard," is the creator or a significant contributor to the AURIGA and BANGAT malware families which we have observed APT1 and other APT groups use. "SuperHard" discloses his location to be the Pudong New Area of Shanghai.

Mandiant is releasing more than 3,000 indicators to bolster defenses against APT1 operations.

»» Specifically, Mandiant is providing the following:

-- Digital delivery of over 3,000 APT1 indicators, such as domain names, IP addresses, and MD5 hashes of malware.
-- Sample Indicators of Compromise (IOCs) and detailed descriptions of over 40 families of malware in APT1's arsenal of digital weapons.
-- Thirteen (13) X.509 encryption certificates used by APT1.
-- A compilation of videos showing actual attacker sessions and their intrusion activities.

»» While existing customers of Mandiant's enterprise-level products, Mandiant Managed Defense and Mandiant Intelligent Response®, have had prior access to these APT1 Indicators, we are also making them available for use with Redline™, our free host-based investigative tool. Redline can be downloaded at www.mandiant.com/resources/download/redline.

The sheer scale and duration of sustained attacks against such a wide set of industries from a singularly identified group based in China leaves little doubt about the organization behind APT1. We believe the totality of the evidence we provide in this document bolsters the claim that APT1 is Unit 61398. However, we admit there is one other unlikely possibility:

> A secret, resourced organization full of mainland Chinese speakers with direct access to Shanghai-based telecommunications infrastructure is engaged in a multi-year, enterprise scale computer espionage campaign right outside of Unit 61398's gates, performing tasks similar to Unit 61398's known mission.

Why We Are Exposing APT1

The decision to publish a significant part of our intelligence about Unit 61398 was a painstaking one. What started as a "what if" discussion about our traditional nondisclosure policy quickly turned into the realization that the positive impact resulting from our decision to expose APT1 outweighed the risk to our ability to collect intelligence on this particular APT group. It is time to acknowledge the threat is originating in China, and we wanted to do our part to arm and prepare security professionals to combat that threat effectively. The issue of attribution has always been a missing link in publicly understanding the landscape of APT cyber espionage. Without establishing a solid connection to China, there will always be room for observers to dismiss APT actions as uncoordinated, solely criminal in nature, or peripheral to larger national security and global economic concerns. We hope that this report will lead to increased understanding and coordinated action in countering APT network breaches.

At the same time, there are downsides to publishing all of this information publicly. Many of the techniques and technologies described in this report are vastly more effective when attackers are not aware of them. Additionally, publishing certain kinds of indicators dramatically shortens their lifespan. When Unit 61398 changes their techniques after reading this report, they will undoubtedly force us to work harder to continue tracking them with such accuracy. It is our sincere hope, however, that this report can temporarily increase the costs of Unit 61398's operations and impede their progress in a meaningful way.

We are acutely aware of the risk this report poses for us. We expect reprisals from China as well as an onslaught of criticism.

Mr. ROHRABACHER. Thank you very much. And let us just note that we do rely on the police to protect us, but also throughout our country we know that there are companies and individuals that seek private protection with security services, and they have guards at their gate and such as that. And so in this case with this particular threat, we of course need to all work together and it will encompass private sector investment as well as government action.

Mr. Autry, you may proceed.

STATEMENT OF MR. GREG AUTRY, SENIOR ECONOMIST, COALITION FOR A PROSPEROUS AMERICA

Mr. AUTRY. Thank you, Chairman Rohrabacher, Mr. Keating, and members. I wanted to particularly thank Mr. Marino for your strong comments with the earlier panelist.

Mandiant Corporation's brilliant report has made obvious to everyone what we have known all along in that there is a giant sucking sound in our economy and it is coming from China. The military origin, the billions of dollars in damages, the infrastructure, and the focus on technology make it clear that this is a 21st century act of war. This is not some petty crime happening by a bunch of Internet trolls in China. China controls the Internet better than any country on earth. I know that from strong personal experience. I guarantee you that if they can find my emails to dissidents they can certainly track down a giant organized cyber attack happening in their own territory.

China does not view the U.S. as a valued trading partner and a model for progress. We have got to give up on this naive perception that China is doing everything they can to move forward to become the United States. They are not. They view us as a ideological adversary who they see as weak and foolish and something that needs to be controlled.

The Internet was developed by the United States Government at United States taxpayer expense. We in the United States and in the U.S. military have every right to expect special privileges in the Internet, and we need to make sure that it is not debased by either hoodlums or nations who do not appreciate the rule of law. It shouldn't be used by tyrants to repress their citizens, and we shouldn't allow those same tyrants to attack our corporations and our infrastructure. The Chinese Government can't think of enough things to do with the money that they have been earning from the economic warfare that they have been executing against the United States.

While we are frustrated over a 2-percent cut, the Chinese are launching moon missions, building maglev trains, launching the biggest military buildup that we have seen since the 1930s. Meanwhile, these cyber attacks against the United States are in the same financial class as the 9/11 attacks. They are costing clearly, billions, and I believe, hundreds of billions of dollars, and this translates to real effect on American individual workers, and this results in loss of life to Americans as well.

And so I ask, why does China get a pass on this scurrilous behavior and every other form of scurrilous behavior that they engage in from economic abuse to human rights? I believe that if Unit 61398 were a segment of the Iranian Republican Guard located in

Tehran that that building would be a smoldering pile of rubble before I got a chance to testify, yet there seems to be something going on with China.

And I think that the problem is, frankly, that a lot of American corporations are co-opted by the Chinese regime. They have such a huge interest in the production capabilities and the ability to exploit Chinese labor and the Chinese environment to lower their costs, and they are chasing the delusional promise of this giant market that they are someday actually going to be given access to that they don't dare offend their Chinese host.

They are like the abused partner in an abusive spousal relationship. They are not going to call the cops on the Chinese, and they are really not going to do it when they know that the cops don't show up and that the cops don't have any guns, which is the situation that we are in now.

This is not a technical challenge, it is a military one. No amount of locks or alarms could protect your home if there was no belief that the police would show up or that the prosecutors would do anything if you had burglars working in broad daylight against whatever security you had put in place.

We need to do some serious actions. And I strongly recommend, first of all, that we have a tariff on Chinese technology that accounts for our governmental cost in cybersecurity to defend against the Chinese, and for the damages that we estimate against our corporations, until there are no further signs of this sort of activity. We should have a ban on the import of any Chinese networking hardware, and specifically I mean Huawei. We need to stop the revolving door at the State, Treasury, and Commerce Departments where officials from those Departments come directly from doing business with China or look forward to doing business with the Chinese as soon as they get out of government service.

Finally, we need to stop educating our adversary. Our computer science departments and engineering departments are full of mainland Chinese students, the majority of whom return to mainland China. Why are we educating these students of a country who are using that technology that we are handing them to oppose our interests? Thank you.

[The prepared statement of Mr. Autry follows:]

Testimony of Greg Autry
Senior Economist, Coalition for a Prosperous America, American Jobs Alliance

On

Cyber Attacks: An Unprecedented Threat to U.S. National Security

Before the

Subcommittee on Europe, Eurasia, and Emerging Threats

Committee on Foreign Affairs

U.S. House of Representatives

March 21, 2013

Good afternoon Mr. Chairman and members of the Subcommittee. My name is Greg Autry. I am the co-author, with Peter Navarro, of the book *Death by China*. I also serve as Senior Economist for the Coalition for a Prosperous America and the American Jobs Alliance. I teach macroeconomics at Argyros School of Business at Chapman University in Orange, California. I have previously worked as a software and network engineer and have earned certifications from Novell (CNE), Cisco (CCNA) and Microsoft (MCSE).

I am testifying on my own behalf and the views expressed here are not necessarily the views of any organization.

My testimony will focus on the economic consequences of China's persistent cyber assault against America's citizens, firms, government and critical infrastructure.

The recent report from Mandiant Corporation has made perfectly clear what everyone in the cyber security community already knows – there is a giant sucking sound in the world economy and it is coming from China. The government of that nation has long been engaged in a massive hacking campaign aimed at Western firms, governments and infrastructure. The military origin of these attacks, the obvious economic cost, and the threat implied by intrusions into our critical infrastructure, mark this as a 21st century act of war.

These attacks are not an isolated case of industrial espionage but rather part of an integrated military-economic-cultural assault on America, a nation that China views not as a benefactor and valued trading partner, but rather as an ideological adversary who must be subdued by any means necessary. Chinese senior military strategists have discussed such multidimensional warfare for years[1]. While the Chinese economic assault on the U.S. manufacturing base is painfully visible to our unemployed, the Mandiant report shows that China views this as a military operation. In the process China has debased the Internet, a gift to the world developed at U.S. taxpayer expense.

As a former software and network engineer, I am undeniably impressed by the skill, thoroughness and audacity of several private sector organizations whose counterintelligence work has brought the Chinese hacking threat into the light. Canada's Information Warfare Monitor report on the Gh0st RAT threat, McAfee's work on Aurora, Dell Secure works investigations into Chinese military connections and now Mandiant's brilliant demonstration that Unit 61398 of the People's Liberation Army is APT1 have done our nation and the world a great service.

However, it is reasonable to assume that our national security, military, and government officials have aware of this for sometime. Why is the Chinese regime never held accountable for of any manner of bad behavior? If 61398 were an Iranian Republican Guard unit located in Tehran the U.S. military would have reduced their HQ to a smoldering pile of rubble long before I presented this testimony.

---

[1] i.g. Liang and Xiangsui, *Unrestricted Warfare*, 1999.

How does an economist estimate the cost of Chinese cyber warfare? The evidence suggests these revelations are merely the tip of the iceberg. The FBI admits, "As a result of the inability to define and calculate losses, the best that the government and private sector can offer are estimates."[2] A full accounting of the damage done to the U.S. is impossible to compile, because most of the victims will never detect the Chinese intrusions or will decline to admit to their losses.

The discrepancy between expert estimates and the value of crimes actually reported makes this under reporting obvious. For instance, Symantec estimated 2011 individual and small business cybercrime losses at $388Billion[3], while the FBI's IC3 summary of actual reports that totaled a mere $485million[4]. McAfee even tossed out a $1Trillion estimate a few years ago. Using the more conservative number only a little more than a tenth of one percent (0.0125%) of these crimes by cost were reported. Even if Symantec overstated the problem by an order of magnitude we still have more than 98% of cybercrimes going unreported.

In any case, how do we place a value on something like Google's source code? The firm trades at 25 times its annual earnings, suggesting most of its value is in future revenues. Conservatively assuming that half of Google's market capitalization of $248 billion reflects the value of its technology (other factors might be labor force, brand equity and assets) this implies a property worth $124 billion has been compromised. While assessing the total cost over time has too many unknowns to model, Google has clearly suffered at the hands of its Chinese competitor Baidu. Google has lost $ billions in the Chinese market alone prompting Google's co-founder Eric Schmidt to brand the Chinese government a "menace." He has wisely noted that "The disparity between American and Chinese firms and their tactics will put both the government and the companies of the United States at a distinct disadvantage." In other words we don't cheat and steal well.

Assuming that most American firms are less savvy than Google when it comes to cyber security, it is easy to justify some very large losses. If Mandiant was able to identify 141

[2] http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism
[3] http://us.norton.com/content/en/us/home_homeoffice/html/cybercrimereport/
[4] http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf

victims, there are thousands of compromised firms. If we set Google's losses at just $10 billion and assume that to be fifty times larger than the average of two thousand major victims we end up with a $400 billion figure. In any case, the losses are clearly in the hundreds of billions of dollars. Putting an exact number on the damages should be no more important to our reaction than calculating the precise losses from Al Qaeda attacks. The point is that *the Chinese government is currently using its military to intentionally inflict enormous damage on the American economy.*

Consider that the economic costs of the September 11 attacks (excluding the military reaction) have been estimated at around $175Billion[5]. The *annual* cost of Chinese military hacking to the US economy is therefore in the same range as 9/11. Every $100 billion implies a loss of about one million American jobs[6]. *Chinese military hacking has left millions of American workers unemployed.* And although we've been spared the specter of horrible televised deaths, the suicide and death rates for the unemployed are substantially higher than the national average[7]. The statistics would suggest that over the years, *Chinese military hacking has killed thousands of Americans.*

The membrane between the black-hat hacker community and the professional security services of China is very permeable. Internet trolls with handles like "UglyGorilla" have access to millions of American emails and passwords via their PLA connection. American workers often use their business computers and email for personal financial transactions. Many of them use the same password at work as they do on their bank. The American public should be in an uproar.

Technical protections against cyber intrusion have consistently proven to be insufficient because most initial system compromises are achieved via exploitation of human beings with "social engineering" tricks like spear phishing. The criminal

---

[5] The New York times suggest $55billion in physical damage and $123billion in attenuated economic impact. The cost of invading Afgahnistan and Iraq in reaction are separate and larger; though they are surely much less than the cost of using a traditional military response to China – something that is probably not a wise option. http://www.nytimes.com/interactive/2011/09/08/us/sept-11-reckoning/cost-graphic.html?_r=0

[6] Estimating revenue of $100,000 per job

[7] http://www.nytimes.com/2012/11/05/health/us-suicide-rate-rose-during-recession-study-finds.html, http://news.yale.edu/2002/05/23/rising-unemployment-causes-higher-death-rates-new-study-yale-researcher-shows

consequences of getting caught are minimal. A report from Cambridge recently suggested, "we should spend less on anticipation of cybercrime (antivirus, firewall, etc.) and more in response . . . hunting down cyber-criminals and throwing them in jail."[8] Internet crimes must have punishments, even when the criminal is the Chinese government, or there is no rule of law online. As an analogy consider that if the police don't respond and the courts don't enforce the law, all the alarm systems and locks on Earth could not keep your home safe.

When businesses in lawless regions are left at the mercy of criminal elements they must: fail, relocate or reach an accommodation with the criminals. Consequently, victims of Chinese cyber attacks are actually helping to conceal the extent of this problem. They wish to avoid public humiliation, negative stock market reaction and the liability associated with the loss of customer data. What makes the silence more worrisome is that most large American corporations have been, for all practical purposes, coopted by the Chinese government. They are so dependent on low-cost production in China and strategically committed to the promise of the "world's largest market" that exposing the criminal behavior of their notoriously vindictive host is unthinkable. With the noble exceptions of Google and the New York Times, an American Corporation is no more likely to "call the cops" on China than are the victims of abusive relationships likely to testify against their spouses.

Remedies proposed by the administration suggest that nothing will happen until a victim proves exactly what China took it and how they used it. What CEO wants to take another beating from China's state manipulated economy and the stock market while trying to convince the U.S. government and the WTO of their victimhood?

Worse, many officials in the departments of State, Treasury and Commerce upon whom we depend to make China play fair come straight from doing business with China or proceed to do so as soon as they leave government.

---

[8] Measuring the Cost of Cybercrime:
http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf

What is most important is recognizing the systemic nature of the China problem. None of China's offenses, including cyber attacks, occur in isolation. They are part of an integrated, asymmetric *war by other means* policy. Yet, America deals with trade cheating, space debris, and espionage as though each were a completely disconnected phenomena.

We are executing an "Asian Pivot" strategy to confront China's increasingly belligerent military posture in the Western Pacific, while our consumption of Chinese goods finances a massive PLA arms build up. The administration promises to tackle PLA cyber assaults in a similarly schizophrenic manner. Nothing could possibly make China's master strategists happier.

The fundamental problem is that the Chinese government is not a normal government but an immoral regime conducting an *active and planned assault* against our political and economic institutions. These cyber attack revelations are simply the latest manifestation of that war in progress.

Do we believe that China's corrupt, state dominated economy is actually beating American private enterprise in a fair contest? While Shanghai booms and Chinese billionaires sprout up like rice in the spring, 25% of Americans are unemployed or underemployed. This is the root of our intractable fiscal dilemma. While we cut and tax, the Chinese government can hardly think of enough new things to do with the vast wealth our consumers and corporations transfer to them – from maglev trains and moon missions to a frightening military buildup. This is what losing a 21st century war looks like.

I propose the following remedies.

Get Real about China: It is time to publicly admit that our engagement policy has completely failed to produce a democratic, peaceful China and is empowering an aggressive dictatorship. We must engage our allies in this new approach.

Systemic Penalties for a Systemic Problem: Take the burden off demonstrating damages off the victims and put the pressure on the perpetrator to stop. The PLA has been proven guilty of intending to undermine American firms and it does not enjoy constitutional rights in the US. A significant tariff should be placed on Chinese manufactured technological goods until there is no further evidence of these activities.

Technology Sanctions: The import of any Chinese computer and telecom networking hardware or software into the U.S. should be restricted. Specifically: Huawei, a technology firm founded by a Chinese military officer and routinely implicated in intelligence work.

Recover Costs of Defense from China: An import tariff equal to America's cyber defense costs should be attached to Chinese imports. (A similar tariff should be assessed for our expense of missile defense and the "Asian Pivot" costs.)

Return Costs to Multinational Corps: It is time to stop rewarding American corporations for transferring capital, technology and jobs to an enemy state by modifying our corporate tax system to favor American based manufacturing.

Stop Conflicts of Interest: Halt the flow of US officials to and from engagement in business with China. Encourage the Senate to make the investigation of Chinese business dealings a priority in confirmation hearings for officials at State, Treasury, and Commerce.

Stop Educating Our Adversaries in Military Technology: Ban the admission of computer science student to the U.S. from nations whose militaries engage in cyber attacks against America and her allies. We are educating a massive pool of Chinese talent in our computer science and engineering schools, where they displace tens of thousand of American citizens and allies.

Encourage U.S. Education in Computer Science: Direct the majority of student aid to STEM majors and specifically graduate degrees in computer science and engineering.

Protect and Reclaim The Internet: The Internet is an invention of the American government funded by U.S. taxpayers. The U.S. government and the U.S. armed forces are reasonably entitled to demand special privileges in its use. Any attempt to transfer further administrative oversight of the Internet to international regulatory bodies must be most strongly opposed. Any opportunity to *regain* U.S. control of the Internet would be in the interest of all people, most notably the citizens of China. Specifically ICANN and control of the DNS root must remain in the U.S. Root servers currently in the U.S. must remain there. The location of anycast servers should be restricted to friendly nations.

Closing Note: I want to be clear that my remarks are in no way meant to disparage the admirable nation of China nor its hardworking people. My criticisms are aimed entirely at the corrupt, nominally communist plutocracy that is repressing them and at the failed American policy of engagement, which has enriched and empowered that loathsome regime a thousand fold.

Mr. ROHRABACHER. Thank you very much.

Now we have 10 minutes before the vote is actually taking place. What we could do is we will have the testimony from Mr. Mazza. We will then recess. As soon as the votes are over we will come back and have a few questions for the panel, if that is all right. We apologize, but we don't have the control over when the votes come.

Mr. Mazza, you have 5 minutes, and then we will have 5 more minutes to get to the floor.

Go right ahead.

STATEMENT OF MR. MICHAEL MAZZA, RESEARCH FELLOW, AMERICAN ENTERPRISE INSTITUTE

Mr. MAZZA. Chairman Rohrabacher, Ranking Member Keating, members of the subcommittee, thank you for the opportunity to testify before you today on China's use of cyber capabilities.

China, I argue, sees cyber capabilities as a tool of statecraft, and like any such tool, it can and should be put to use in the pursuit of national interests. What are those interests? In brief, the primary goal of the Chinese Communist Party, or CCP, is to stay in power. No longer securing its legitimacy on a foundation of Marxist ideology, the Party now relies on delivering economic prosperity and on its claim to a nationalist mantle to ensure its continued rule.

And in my remarks here I am going to focus on the more traditional aspects of security implications rather than economics. China's continued rise is crucial if the CCP is to validate its claim that it and it alone can lead the country back to what it sees as its traditional and rightful place atop the Asian hierarchy. And to do so, Beijing must restore sovereignty over territory supposedly wrongly taken from it. Doing so would not only allow Beijing to complete what it sees as an historic mission, but to enhance its own security. Controlling islands in the East and South China Seas would grant China greater strategic depth, allow it to more easily safeguard or control sea lanes, and permit it to more easily access the Pacific and Indian Oceans.

But of course, these waters are also home to U.S. treaty allies, long-standing security partners, and new friends. And it is in these littoral regions where tensions have been running high, where conflict is most likely to break out, and where U.S. and Chinese interests clash. Differing visions of what Asian and perhaps global order should like have led China and the United States into what is shaping up to be a long-term strategic competition. For China, cyber capabilities are tools to be used in waging this competition and in securing its interest in the Asia Pacific. And in particular, I hear that China uses cyber capabilities for three related but different purposes.

First, Chinese hackers will engage in espionage activities in the pursuit of both strategic and tactical intelligence. Such activity is unwelcome but shouldn't be unexpected. The United States and China are going to spy on each other. Second, the People's Liberation Army, or PLA, will use cyber warfare as part of its suite of anti-access/area denial capabilities, or A2/AD. The PLA has been developing systems aimed at keeping U.S. forces distant from Chi-

nese shores, complicating in particular the U.S. Navy's ability to operate freely in the Asia-Pacific Theater and thus making U.S. intervention in the Taiwan Strait or other conflict more difficult. In the event of a conflict, PLA cyber forces would likely aim to disrupt U.S. military command and communications networks, essentially trying to blind, deafen, and silence U.S. forces.

Third, and in my opinion, most worrisome is China's development of what might be called strategic cyber weapons. Recent revelations of Chinese cyber intrusions into U.S. critical infrastructure are especially troubling. That an attacker a half a world away could threaten our electrical grid or transportation security is of course a frightening thought, but in my opinion, even more concerning is that China's development of these capabilities is potentially destabilizing. Because the weapons lack the ugliness of nuclear arms, Beijing may come to see them as more usable than nuclear weapons. And with such weapons likely to be seen as adding an intermediate step on the escalation ladder, Beijing may come to see armed conflict as less dangerous than it otherwise would have.

Fortunately there are steps the United States can take to arrest China's use of cyber capabilities and ensure American national security going forward. These steps fall into three broad categories—legal, diplomatic, and military and that they all be suggestions that require further thought, certainly. In the legal realm there may be need for new legislation. My colleague Dan Blumenthal has recently argued that Congress should adopt a cyber attack exception to the Foreign Sovereign Immunities Act to allow for civil suits against foreign governments acting illegally in the cyber realm. This is something that we have done in the realm of terrorism.

Diplomatically, there are several paths to take. Ideally, of course, China will be willing to join in some broad based international effort to establish norms and rules of the road in the cyber realm, but as you have pointed out, China will need incentive to do so. The Obama administration has suggested that cyber threats will threaten the overall U.S.-China relationship, but it needs to start elucidating just what that means. What are the risks? Potential options include limiting access to the U.S. market for Chinese state-owned enterprises or pursuing action at the WTO.

In the military sphere the United States should be clear about how we will respond to the use of strategic weapons on American soil. The Department of Defense should explore whether it is possible to conduct cyber exercises that will effectively demonstrate U.S. capabilities, much as conventional exercises are used, for example, to deter North Korea. If the United States limits itself to just playing defense in cyberspace, it is likely to find itself on the losing end in a competition with China. Playing offense, not just militarily but in the legal and diplomatic fields as well, will allow Washington to impose costs on Beijing when necessary and enhance national security. Thank you.

[The prepared statement of Mr. Mazza follows:]

Statement before the House Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, and Emerging Threats

Cyber Attacks:
An Unprecedented Threat to U.S. National Security

March 21, 2013

Michael Mazza
Research Fellow
American Enterprise Institute

Chairman Rohrabacher, members of the subcommittee:

Thank you for the opportunity to testify before you today on China's use of cyber capabilities and how the United States might respond.

The cyber realm is a relatively new one and thus one that we are still working to understand. Offensive cyber capabilities are particularly worrisome for a number of reasons. These unconventional weapons may be used by state or non-state actors and, when used, their origin may be difficult to trace. Appropriate responses to their use remain a matter of debate.

In some ways, the advent of cyber warfare calls to mind the early days of the Cold War, when there was little agreement on how nuclear weapons should be used. Were atomic weapons simply big bombs or did they represent a revolutionary capability, something new and different? Would they most effectively be used against civilian populations, conventional military targets, or the enemy's own nuclear weapons? Was it possible and affordable to defend against long-range ballistic missiles armed with nuclear weapons and, if so, would such defenses be stabilizing or destabilizing? It took decades of intellectual efforts from political scientists, economists, physicists, and others to satisfactorily address these questions, some of which are still debated today.

I raise this analogy for two reasons. First, the analogy suggests that we are only in the early stages of what will likely be a long-term effort to understand conflict in the cyber realm.

Second, while the role of nuclear weapons in national security has long been hotly debated, that debate did come to some consensus that those weapons are tools of statecraft—though perhaps controversial ones—and can be used as such. China, at least, appears to have reached the same conclusion about cyber capabilities. A first

order question, then, is: what are China's ends and how does it operate in the cyber realm to achieve them?

China's Rise and Cyber Statecraft

The primary objective of the Chinese Communist Party (CCP) is to stay in power. No longer securing its legitimacy on a foundation of Marxist ideology, the party now relies on delivering prosperity and its claim to a nationalist mantle to ensure its continued rule.

China has seen sustained, high levels of economic growth over the past two decades, with GDP growth in the high single- and low double-digit rates. As recently as 2007, China experienced 14.2% growth.[1] Growth has slowed somewhat since, with 2012's rate reaching a nadir of 7.9%, the lowest in 13 years.[2] Given the weaknesses inherent in China's economy—poor performing loans, weak domestic consumption, shoddy ownership rights, a shrinking labor force, to name a few—it will be difficult for the country to return to the high-charged growth of past years.

One reform that would help the Chinese economy would be to strengthen domestic intellectual property rights (IPR) protections and enhance enforcement. Such moves would help to spur innovation and make China a more attractive place for multinational corporations to do business. But such reforms still appear unlikely for several reasons, including:

1) There remain vested interests opposed to IPR enhancement.
2) China's relatively low position on the value chain does not lead to the creation of large constituencies in favor of stronger IPR.
3) It is easier to steal knowledge and technology than for China to develop it itself.

That third point is most relevant for our purposes. General Keith Alexander, Commander of Cyber Command and Director of the National Security Agency, has described cyber theft of U.S. intellectual property as the "greatest transfer of wealth in history," citing a cost to U.S. companies of approximately $250 billion per year.[3]

---

[1] "GDP growth (annual %)," The World Bank, http://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG, accessed March 20, 2013.
[2] Kevin Yao and Aileen Wang, "China's economy posts slowest growth since 1999," Reuters, January 18, 2013, http://www.reuters.com/article/2013/01/18/us-china-
[2] Kevin Yao and Aileen Wang, "China's economy posts slowest growth since 1999," Reuters, January 18, 2013, http://www.reuters.com/article/2013/01/18/us-china-
economy-gdp-idUSBRE90H03020130118, accessed March 20, 2013.
[3] Keith Alexander, "Keynote Address," Cyber Security and American Power, American Enterprise Institute for Public Policy Research, Washington, DC, July 9, 2012.

Chinese hackers are surely responsible for a large piece of that and, to date, neither U.S. corporations nor the American government have given China sufficient reason to halt that activity. Unless incentivized to do so, cyber theft from China will surely persist as the CCP aims to ensure that the Chinese economy continues to grow.

An additional benefit for China to the theft of American IPR is that it allows Chinese companies to grow at the expense of their American counterparts, which not only suffer the immediate effects of thefts, but must also must invest their limited resources to repair networks and protect against future incursions. Again, thus far, Chinese authorities have seen little need to halt an activity that may actually make American companies less competitive.

While ensuring the Chinese people continue to grow wealthier is itself a primary goal of the CCP, China's continued rise is also crucial if the party is to validate its claim that it and it alone can lead the country back to greatness. The CCP has long propagated a victim narrative of Chinese history, and nationalist education has been particularly emphasized since the aftermath of the Tiananmen Square massacre. In that narrative, China was Asia's central power, or "Middle Kingdom," for millennia before Western powers brought it down and inflicted upon it a so-called "century of humiliation." It is the CCP who can right those wrongs and return China to its rightful place atop the Asian hierarchy.

To do so, Beijing must restore sovereignty over territories wrongfully taken from it, including Taiwan and disputed islands in the East and South China seas. Doing so would not only allow Beijing to complete what it sees as a historic mission, but to enhance its own security. Controlling these islands and the surrounding waters would grant China greater strategic depth, allow it to more easily safeguard or control sea lines, and permit it to more easily access the Pacific and Indian oceans. Of course, these waters are also home to U.S. treaty allies (South Korea, Japan, the Philippines, Thailand, and Australia further afield), long-standing security partners (Taiwan and Singapore), and new friends (Indonesia, for example). It is in these littoral regions where tensions have been running high, where conflict is most likely to break out, and where U.S. and Chinese interests directly clash.

For China, cyber capabilities are tools to be used in pursuit of its own interests in this region. In particular, China likely uses or will use cyber capabilities for three related, but different, purposes. First, Chinese hackers will engage in espionage activities in the pursuit of both strategic and tactical intelligence. This, of course, is a natural activity in a competitive relationship—the United States and China are going to spy on one another. The question is, what new counter-intelligence tools are needed to meet this relatively new espionage threat? The more traditional tools of espionage are inherently risky—intelligence operatives can be arrested, spy planes can be shot down—but the risks to hacker-spies are not so clear. How can the United States make cyber espionage a riskier proposition for China and others?

Second, the People's Liberation Army (PLA) will use cyber warfare as part of its suite of anti-access/area denial (A2/AD) capabilities. The PLA has been developing systems aimed at keeping U.S. forces distant from Chinese shores, complicating in particular the U.S. Navy's ability to operate freely in the Asia-Pacific theater and thus making U.S. intervention in a Taiwan Strait or other conflict more difficult. Much of the attention to China's A2/AD capabilities has rightly focused on its missile forces, naval capabilities, and air defense systems. But cyber capabilities play a role in A2/AD, as the Defense Department's 2012 report on Chinese military power made clear:

> China's leaders in 2011 sustained investment in advanced cruise missiles, short and medium range conventional ballistic missiles, anti-ship ballistic missiles, counterspace weapons, and military cyberspace capabilities which appear designed to enable anti-access/area-denial (A2/AD) missions, or what PLA strategists refer to as "counter intervention operations."[4]

In the event of a conflict, PLA cyber forces will likely aim to disrupt U.S. military command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) networks. These efforts will complement attacks with more conventional, "kinetic" weapons to essentially blind, deafen, and silence U.S. forces. It should be noted that the 2012 DoD report on China's military included "cyber weapons" among the PLA's "counterspace capabilities" as well.[5]

As with Chinese cyber espionage, these developments are concerning, but they shouldn't be surprising. It is not unnatural for China to adopt military measures aimed at countering U.S. military advantages—in particular, advanced C4ISR capabilities—which also happen to represent critical vulnerabilities. For U.S. military planners, the questions are clear, though the answers may not be. How can the American military enhance defense against cyber attack? Does the PLA have vulnerabilities of its own that are susceptible to cyber warfare? What vulnerabilities do China's cyber forces themselves have to counter-attack, whether cyber or kinetic? Is it possible to take China's cyber forces out of the fight early in a conflict?

More worrying than China's theft of intellectual property, its espionage activities, or its development of cyber weapons for use at the tactical and operational levels, however, is China's development of strategic cyber weapons. Recent revelations of Chinese cyber intrusions into U.S. critical infrastructure are especially troubling. No government can easily tolerate a state of affairs in which its country's electrical grid, water supply, financial stability, or transportation security are held at risk by an anonymous hacker half a world away.

---

[4] "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2012," Department of Defense, May 2012, p. iv
[5] Ibid., p. 9

Yet even worse is that China's development of these capabilities is potentially destabilizing. Because these weapons lack the ugliness of nuclear weapons—there is no radiation and they don't immediately and directly cause widespread death and destruction—not to mention the fact that their origin may be difficult to trace, Beijing may come to see them as more "useable" than nuclear weapons. And with such weapons likely to be seen as adding an intermediate step on the escalation ladder—one preceding the use of nuclear weapons—Beijing may come to see armed conflict as less dangerous than it otherwise would have. Conflict would become even more likely if Beijing believes that the American response to a strategic cyber attack would be one that China can tolerate.

Ideally for China, of course, its possession of such capabilities would ensure it never has to use them. Cyber weapons for A2/AD would keep U.S. forces physically distant from a fight in China's neighborhood, while Chinese strategic cyber weapons would deter the United States from attempting to expand or otherwise escalate the conflict. Meanwhile, effective espionage would allow China to more accurately predict U.S. actions, to gauge U.S. vulnerabilities, and to speed along its own military modernization. At the same time, theft of IP and trade secrets would be making American companies less competitive, putting a drag on the U.S. economy and putting further budgetary pressures on defense spending.

American Policy Options

I knowingly paint a dire picture here, but it is thankfully one that need not be borne out. There are steps the United States can take to arrest China's use of cyber capabilities and ensure American national security going forward. The suggestions below, all of which require further thought, fall into three broad categories: legal, diplomacy, and military.

In a recent article for *Foreign Policy*, Dan Blumenthal, director of Asian Studies at the American Enterprise Institute, applauds the Justice Department for tackling the issue directly through its formation of the National Security Cyber Specialists' Network (NSCS), which is exploring the potential prosecution of cyber criminals and whether that would have a deterrent effect on other hackers. But Blumenthal argues that new legislation is required:

> ...Congress could also consider passing laws forbidding individuals and entities from doing business in the United States if there is clear evidence of involvement in cyber attacks.
>
> Congress could also create a cyberattack exception to the Foreign Sovereign Immunities Act, which currently precludes civil suits against a foreign government or entity acting on its behalf in the cyber-realm. There is precedent: In the case of terrorism, Congress enacted an exception to

> immunity for states and their agents that sponsor terrorism, allowing individuals to sue them.[6]

Blumenthal also cites a paper by Jeremy A. Rabkin and Ariel Rabkin, in which the authors propose that Congress use its constitutional power to grant "letters of marque" to privateers. The idea would be to essentially coopt American hackers—effectively granting them immunity and perhaps funding if they agree to target only those countries or entities approved by Congress. This would allow for less provocative but still semi-official retaliation for attacks on U.S. entities.[7]

Diplomatically, there are several paths to pursue. The Obama administration's recent willingness to repeatedly raise the issue of Chinese cyber incursions, both publicly and privately, is a good first step, which will begin to convey to Beijing how seriously the United States is taking the matter. Ideally, China will be willing to join in a broad-based international effort to establish norms and rules of the road in the cyber realm. But China will need incentive to do so, and at present its experience in the current world of cyber is one of much gain and little pain.

The Obama administration, then, must begin to match its words with actions. In a recent speech to the Asia Society, National Security Advisor Tom Donilon asserted that cyber threats pose risks "to international trade, to the reputation of Chinese industry and to our overall relations." It is time for the administration to begin elucidating just what those risks are. Potential steps could include limiting the access to the U.S. market for Chinese state-owned enterprises and for any Chinese companies determined to have benefited from theft of American trade secrets. The administration could also consider the feasibility of filing suit at the WTO.

The administration can also work with allies and partners to encourage more responsible behavior in cyberspace. For example, like-minded countries could establish a preferential trade agreement, which would require strict adherence to a set of cyber crime legal standards for membership. Alternatively, victims of cyber theft and cyber attacks could establish a shared set of punishments, such as those listed above, that they agree to impose.

In the military sphere, the United States should be clear about how it will respond to the use of strategic cyber weapons on American soil. Beijing should not be confident it can carry out an "untraceable" cyber attack and should have a clear understanding of the consequences in the event of attacks against U.S. critical infrastructure. The

---

[6] Dan Blumenthal, "How to Win a Cyberwar with China," ForeignPolicy.com, February 28, 2013, http://www.foreignpolicy.com/articles/2013/02/28/how_to_win_a_cyberwar_with_china, accessed March 20, 2013.

[7] Ibid.; Jeremy A. Rabkin and Ariel Rabkin, "To Confront Cyber Threats, We Must Rethink the Law of Armed Conflict," Hoover Institution, 2012, http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rabkin.pdf, accessed March 20, 2013.

Department of Defense should explore whether it is possible to conduct cyber exercises that will effectively demonstrate U.S. capabilities, much as conventional exercises are used, for example, to deter North Korea. In his *Foreign Policy* article, Blumenthal suggests that the "U.S. military could set up an allied public training exercise in which it conducted cyberattacks against a 'Country X' to disable its military infrastructure such as radars, satellites, and computer-based command-and-control systems."

But multilateral security efforts can go even further than exercises. Blumenthal argues that "the United States should set up a center for cyberdefense that would bring together the best minds from allied countries to develop countermeasures and conduct offensive activities." Not only would this allow for more effective development of advanced capabilities, but it would enhance deterrence as well. Chinese actions against one country could send all partners into action via the "cyber defense center," and an attack on the center would be an attack on all of the partner nations.

Cyber threats pose serious risks to the U.S. economy, the U.S. military, and American national security more broadly. China, in particular, is making use of cyber capabilities to pursue its interests at the expense of America's own. Working with allies and likeminded partners and, wherever possible, with China as well, the United States should be able to secure itself against these growing threats while hopefully establishing norms of behavior in cyberspace from which all nations can benefit.

Mr. ROHRABACHER. Thank you very much.

Now we have 4 minutes to go down and vote. And Dr. Libicki, I am sorry that we are going to—or are you going to be able to hold off? It will be about a half an hour by the time we get back here.

Mr. LIBICKI. Certainly.

Mr. ROHRABACHER. Thank you very much. So what we will do is I will recess the hearing for 30 minutes, and so we should be back in a half an hour. And let us just note for the record as we recess that we are talking about here a—Mr. Keating, we have heard testimony indicating that the cyber attack has been traced directly back to a unit of the Chinese army, and this is phenomenal that we can actually have evidence of an army of another country involved in this type of criminal activity aimed at Americans and others.

We have also heard testimony about the United States, through our Chinese student graduate program have perhaps educated some of the people in that Chinese army unit, who then took the knowledge back that they gained in the United States, to attack us. And so we will have some questions for our panel along these lines when we come back, and Dr. Libicki will have his testimony. So this hearing is now in recess for 30 minutes.

[Recess.]

Mr. ROHRABACHER. Okay, this hearing is now called to order, and we had a 30-minute break. We will now proceed with the rest with the final witness, and then we will proceed to have some questions, and hopefully we will be adjourned in about a half an hour from now.

Dr. Libicki?

STATEMENT OF MARTIN C. LIBICKI, PH.D., SENIOR MANAGEMENT SCIENTIST, RAND CORPORATION

Mr. LIBICKI. Good morning, Chairman Rohrabacher, Ranking Chairman Keating, and other——

Mr. ROHRABACHER. Someone has tampered with the electronics and you are not coming through on that phone, or maybe you just need to put it over here.

Mr. LIBICKI. Good morning, Chairman Rohrabacher——

Mr. ROHRABACHER. There is a lesson to be learned in that.

Mr. LIBICKI [continuing]. Ranking Member Keating, and other distinguished members of the subcommittee. Thank you for the opportunity to testify today on cyber attacks, an unprecedented threat to U.S. national security.

On September 11th, 2001, terrorists attacked the United States. Three thousand people died and the physical damage was upwards of $200 billion. On September 12th, the country responded. The United States strengthened its homeland security. We went to war twice. Over the next dozen years the United States lost 6,000 in combat, 10,000 to 20,000 were seriously injured. Total additional expenditures exceeded $1 trillion.

I point this out not to criticize the policies that followed but to indicate that even though an attack on the United States may be damaging the cycle of response and counterresponse may be far more consequential. Accordingly, even though a cyber 9/11 may be costly, it would be short-sighted to evaluate the threat in terms of

immediate damage without considering how the United States would manage such a crisis in order to yield an outcome that works best for the American people.

We are right to be worried about a 9/11 in cyberspace, but we also ought to worry about what a 9/12 in cyberspace would look like. Indeed, one of the best reasons for working hard to avoid a 9/11 in cyberspace is precisely to avoid having to deal with a 9/12 in cyberspace. That noted, because a cyber 9/11 or what looks like a cyber 9/11 might happen, it is worthwhile to think about what we do the day after.

The issue of how the United States should manage crisis and escalation in cyberspace is addressed in a recently published Rand document of the same name. I now want to take the opportunity to summarize some of the salient points in the document. The first point is to understand that the answer to the question, is this cyber attack an act of war?—is not a conclusion but a decision. Cyber wars are wars of choice. A country struck from cyberspace has the opportunity to ask, what would be the most cost effective way of minimizing such future suffering? Depending on circumstances it might be to go off to war. Alternatively, it might not be.

The second is to take the time to think things through. Computers may work in nanoseconds, but the target of any response is not the computer, in large part because even if a computer is taken out a substitute may be close at hand. The true target of response is those who command cyber warriors, that is, people. But people do not work in nanoseconds. Persuasion and dissuasion of people are work at roughly the same speed whether or not these people command cyber war or command another form of war.

Third is to understand what is at stake before you react, which is to say, what you hope to gain by making the attackers cease their efforts. This goes for both responding to cyber attack and to responding to what may be deemed intolerable levels of cyber espionage. Fourth is to not take possession of the crisis unnecessarily, or if you do take possession at least do so only on your own terms. That is, do not back yourself into a corner where you always have to respond whether doing so is wise or not.

Fifth is to craft a narrative that facilitates taking the crisis where you want to take it. In some cases, the narrative has to allow the attacker to back down gracefully, which is to say cease what they are doing. Sixth is to figure out what are the norms of conduct in cyberspace, if any, work best for the United States. It may be encouraging that last week both the United States and China agreed to carry out high level talks on cyber norms, but there are a lot of questions to work through. Where, for instance, does one draw the many lines among cyber war, cyber crime, cyber espionage, and violations of international trade law?

Seventh is to manage the cyber escalation wisely. This not only means remembering that the other side will likely react to what you do, but understanding what a crude tool tit-for-tat counterescalation is when it comes time to influencing the behavior of the other side. In sum, while I believe it is certainly a worthwhile effort to prevent the future 9/11 in cyberspace, similar levels of care and thought need to be given to how to manage a potential 9/12 in cyberspace. If not, we may find as with the historical 9/11

that the consequences of the reaction and counterreaction are far more serious than the consequences of the original action itself. Thank you very much.

[The prepared statement of Mr. Libicki follows:]

Testimony

Managing September 12th in Cyberspace

Martin C. Libicki

RAND Office of External Affairs

CT-384

March 2013

Testimony presented before the House Foreign Affairs Committee, Subcommittee on Europe, Eurasia, and Emerging Threats on March 21, 2013

This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. RAND® is a registered trademark.

Published 2013 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Email: order@rand.org

Martin C. Libicki[1]
The RAND Corporation

Managing September 12th in Cyberspace[2]

Before the Committee on Foreign Affairs
Subcommittee on Europe, Eurasia, and Emerging Threats
United States House of Representatives

March 21, 2013

On September 11th, 2001, terrorists attacked the United States. Three thousand people died and the physical damage was upwards of two hundred billion dollars. On September 12th, the country responded. The United States strengthened its homeland security. We went to war twice. Over the next dozen years, the United States lost six thousand in combat. Ten to twenty thousand were seriously injured. Total additional expenditures exceeded a trillion dollars. I point this out not to criticize the policies that followed – but to indicate that even though an attack on the United States may be damaging, the cycle of response and counter-response may be far more consequential.

Accordingly, even though a cyber-9/11 may be costly, it would be shortsighted to evaluate the threat in terms of immediate damage without considering how the United States would manage such a crisis in order to yield an outcome that works best for the American people. That is, we are right to be worried about a "9/11 in cyberspace," but we also ought to worry about what a "9/12 in cyberspace" would look like. Indeed, one of the best reasons for working hard to avoid a 9/11 in cyberspace is avoid having to deal with a 9/12 in cyberspace. That noted, because a cyber 9/11 (or what looks like a 9/11) might happen, it is worthwhile to think about what we do the day after.

The issue of how the United States should manage crisis and escalation in cyberspace is addressed in the recently-published RAND document of that name.[3] I now want to take the opportunity to touch on some of the salient points in that document, as well as follow-on thoughts.

The first point is to understand that the answer to the question – *is this cyberattack an act of war?* – is not a conclusion, but a decision. In physical combat, such a question may be meaningful: if

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.
[2] This testimony is available for free download at http://www.rand.org/pubs/testimonies/CT384.html.
[3] Martin Libicki, *Crisis and Escalation in Cyberspace*, Santa Monica CA (RAND), MG-1215-AF.

your neighbor's tanks are in your backyard heading for the capital, then war is on. But such a question is usually the wrong one to ask about cyberwar. True, cyberwar can disrupt life even on a mass scale. Cyberwarfare can enhance conventional military power. But, it cannot be used to occupy another nation's capital. It cannot force regime change. No one has yet died from it. And, Stuxnet notwithstanding, breaking things with ones and zeroes requires very particular circumstances. A cyberattack, in and of itself, does not demand an immediate response to safeguard national security. Instead, a country struck from cyberspace has the opportunity to ask: What would be its most cost-effective way to minimize such future suffering? If war fits the bill (and other nations understand as much), the victim of a cyberattack could declare that it was an act of war and then go forth and fight. Perhaps making war can persuade the attacker to stop. Yet, war also risks further disruption, great cost, as well as possible destruction and death -- especially if matters escalate beyond cyberspace. Or a country may look at policies that reduce the pain without so much risk – such as by fixing or forgoing software or network connections whose vulnerabilities permitted cyber-attacks in the first place.

Second is to take the time to think things through. Computers may work in nanoseconds, but the target of any response is not the computer – in large part because even if a computer is taken out a substitute can be close at hand. The true target of a response is those who command cyberwarriors – that is, people. But, people do not work in nanoseconds. Persuasion and dissuasion of people work at roughly the same speed whether or not these people command cyberwar or any other form of war. A corollary error is to assume that a confrontation in cyberspace is inherently unstable – thereby necessitating being a quicker draw than the other guy. It is precisely, because unlike with nuclear war, a nation's cyberwar capabilities cannot be disarmed by a first strike, there's not the same need to get the jump on the other guy, just as there is not the same need to match his offense with your offense, when it's your defense that dictates how much damage you are likely to receive.

Third is to understand what is at stake – which is to say, what you hope to gain by making the attackers cease their efforts. This goes for both responding to cyberattack and responding to what might be deemed intolerable levels of cyber-espionage. With cyberattack, what you are trying to prevent is not the initial attack, but the next attack – the effects of which might be larger than the initial attack but may also be smaller. (This is particularly true if the initial attack teaches the immediate victims, that, say, making industrial controls accessible to the Internet may not have been the smartest idea.) As for espionage, we really have no handle on how to evaluate the damage that takes place to the country when other countries see what we don't want them to see.

Fourth is not to take possession of the crisis unnecessarily – or at least do so only on your own terms. That is, do not back yourself into a corner where you always have to respond, whether doing so is wise or not. It is common, these days, to emphasize the cost and consequences of a cyberattack as a national calamity; last week the Director of National Intelligence proclaimed it as the primary short-term threat to the nation. Making such arguments tends to compel the United States to respond vigorously should any such cyberattack occur, or even merely when the possible precursors to a potential cyberattack have been identified. Having created a demand among the public to do something, the government is then committed to doing something even when doing little or nothing is called for. In some cases, it may be wiser to point out that the victim had a feckless cybersecurity posture. In other cases, downplaying the damage may be called for. The more emphasis on the pain from a cyberattack, the greater the temptation to others to induce such pain -- either to put fear into this country or goad it into a reaction that rebounds to their benefit. Conversely, fostering the impression that a great country can bear the pain of cyberattacks, keep calm, and carry on reduces such temptation. Correspondingly, despite good arguments in favor of drawing red lines for deterrence purposes – "if you do this, I will surely do that" – the cost of being credible is that if deterrence fails, such a declaration tends to constrain one into carrying out retaliation. To do nothing or nothing much, at that point, tends to hollow all deterrent postures, and not just in cyberspace. Given the inevitable ambiguities associated with the consequences and causes associated with cyberattacks, inflexibility may also demand a response well before the facts are clear. There are careful tradeoffs that have to be made.

Fifth is to craft a narrative that facilitates taking the crisis where you want to take it. Narratives are, essentially, political morality plays, in which the United States has to select a role that puts it in a good light while retaining basic consistency between the facts of the matter, as well as with its previous narratives. Part of crafting a narrative requires finding the right role: does the United States want to portray itself as a victim of cyberattack? As the righteous enforcer of international norms? As the superpower that demands respect? Narratives also have to find a role for the attacker, and the definition of such a role may, in some cases, have to encourage and accommodate the attacker's graceful and face-saving retreat from belligerence. After all, the odds that an attack in cyberspace arises from , miscalculation, inadvertence, espionage with unintended consequences, or the actions of a rogue actor are nontrivial.

Sixth is to figure out what norms of conduct in cyberspace, if any, work best for the United States. Last week both the United States and China agreed to carry out high-level talks on cyber norms. Although nearly four years of Track II negotiations with the Chinese (in which I participated) have yielded meager results, there are still some grounds for optimism. But, first we have to address some salient questions. To what extent can the Laws of Armed Conflict apply in a domain where

the patterns of collateral damage are poorly understood, where the distinction between civil and military is difficult to discern, where it's getting harder and harder to know where your information sits, and where the transparency required for neutrality simply does not exist? Where does one draw the many lines among cyberwar, cybercrime, cyber-espionage, and violations of international trade rule? Is it in the U.S. interest to make unconstrained espionage a *casus belli*? How well should states be able to monitor (let alone enforce) compliance before it can assure itself that the norms are worth having?

Seventh is to manage cyber-escalation wisely. This not only means remembering that the other side will react to what you do, but also understanding what a crude tool counter-escalation may be for influencing the other side. Consider that with Stuxnet, it took many tries to get the desired effect. The Iranians may not have known they were under attack until they read about it in the *New York Times*. It is also unclear whether we would have had much damage assessment had the centrifuge plant not been under independent inspection. To further illustrate what the fog of cyberwar may mean to escalation control, assume a defender wants to place in an opponent's mind the thought that if he escalates and the defender will counter-escalate proportionally. But in cyberspace what the attacker does, what he thinks he did, and what the defender thinks he did may all be different. The defender can only react to what he thinks the attacker did. That is because the defender's systems are usually different than the attacker's. Equivalence between perception of the attack and the intended response may be inexact. Then there's the similar difference between the defender's response and the attacker's perception of what was done in return. After all this, the attacker may think the retaliation was proportional, understated, or went overboard in crossing counter-escalation red lines -- redlines that were not originally crossed by himself. The effect is akin to playing tennis on a rock-strewn court.

In sum, while I believe it is certainly worthwhile effort to prevent a future 9/11 in cyberspace – and understanding the nature of the threat is an important component of that effort – similar levels of care and thought needs to be given to how to manage a potential 9/12 in cyberspace. If not, we may find, as with the historical 9/11, that the consequences of the reaction and counter-reaction are more serious than the consequences of the original action itself.

Mr. ROHRABACHER. Thank you very much.

Now we have heard some very thought-provoking testimony today, and the complications that you just outlined and the different levels that we have to consider and the timing of consideration, as I said earlier that when we had our first witness from the administration, things are a lot more complicated now than they used to be basically in terms of providing security for our country, but also providing a methodology of dealing with criminal behavior on an international and global scale.

We have heard today about especially when we were talking originally about the Chinese military itself is engaged in cyber espionage and perhaps cyber attacks. Let us note that this is different than just having the Chinese army engaged in some act of aggression against an enemy or against an adversary of China. In this case the Chinese military is engaged in activity that has security implications but also economic implications, mainly for the leadership of China which is an oppressive dictatorship, a cliquism. They may be utilizing this apparatus to enrich themselves as well as their clique.

We also know that this what we are talking about is cyber attacks, we are also talking about cyber oppression. That in China you have so many people who are engaged in cyber operations at the direction of their government, but those directions may not be an attack on the United States or on a competitor, but they also may be aimed at their own people in oppressing their ability to utilize the Internet for a free type of communication.

So we have all of these factors coming to play. Perhaps what ties them all together is the fact that the United States has been the enabler of all of this. Whether it is positive or negative we have enabled this. The Internet is an invention of the United States of America. It has been put in place basically by our technologists. And on top of that, we have trained and continue to train people to have expertise in this new arena of human behavior.

So we have a relatively new arena, the cyber arena, and we have indiscriminately, whether or not the people that we are training are representing a positive force in the world or a negative force in the world, we have been training them at our universities and educating them at the highest level of graduate studies into these type of scientific endeavors that utilize the Internet. We have been training people to go home and use them. For example, when we talk about Chinese military unit, now are we suggesting that that Chinese unit is just a bunch of corporals and privates, or do they have Ph.D.s in that unit that you have tracked down? Are there Ph.D. students that perhaps were trained in American universities?

Mr. BEJTLICH. Sir, we don't have any specific information about that sort of activity. What I will say is that we have seen, and this is all through open source again, documents, submissions to conferences by Ph.D.s who say their job is working for 61398. And when they submit these papers they didn't realize that by saying 61398 someone could later on tie them to that Chinese military unit. In other words, that was a code name that they never thought would be penetrated. So you can find documents on the Internet

talking about different ways to conduct computer security, different ways to write software where the authors will say, I am 61398.

Now I don't know of any case where you have tied that back to say well, where did this person study? Did they study at Cal Tech or something like that? I don't know of anyone who has done that sort of analysis. But clearly you have very well trained people. This unit was very focused on hiring English speakers. That was the goal of this unit. You had to speak English. You had to know computer security, computer science, and as a result they were able to take that expertise and target English-speaking companies.

Mr. ROHRABACHER. I would suggest, and Mr. Autry, I would like your opinion because you are the one who first brought up this issue of actual educated individuals. If you provide a person with the education in this arena of high technology type understandings of physics, et cetera, we are actually arming those people to do good things or bad things. And yet we are not paying any attention as to whether or not those students who we are educating in these graduate level classes, especially the Chinese students, are going to go back to China and participate in oppressing their fellow Chinese or threatening the well being of other countries that are considered adversaries by the Chinese Government. And maybe you could expand upon that thought.

Mr. AUTRY. Yes, thank you, Chairman Rohrabacher. As a lecturer and a Ph.D. student at the University of California Irvine, I have noticed the ever-increasing predominance of Chinese mainland nationals in our classrooms. In the business school it is not unusual for the Ph.D. cohort to be fully 50 percent mainland Chinese students. In the M.B.A. programs I often see a quarter of the classes mainland Chinese students. My understanding is that in computer science and engineering, classrooms with 40 percent mainland Chinese students is perhaps the norm.

This should be of great concern to a nation who prides itself on its technological development to drive its economy and to make its defense second to none in the world. It is a great thing when we open up our schools to students from around the world who wish to embrace American values and learn from us and take them home and emulate what we have done, but I have to say of the Chinese cohort that I work with on a regular basis many of them are at best apolitical. They certainly are not here to embrace our ideological values, and many of them are openly hostile to American ideological values and see any criticism of the Chinese Government to be inappropriate and something that they don't want to see happening.

I believe that limiting visas for students in computer science to countries that do not engage in cyber attacks against the United States is a very realistic option we should consider. Thank you.

Mr. ROHRABACHER. I have been aware of this problem for awhile, and when I have spoken to presidents of major universities like Stanford University, for example, I just get the answer that well, that is for the government to worry about but not for us, not in academics. Security issues should be handled by the Federal Government not by academics.

I would suggest that this is, what we are talking about today is the equivalent of equipping a hostile power, let us say, 50, 60, 70

years ago, but helping to equip a hostile power with the ability to build a nuclear weapon. I mean if you have students from Germany and you say, well, we can't really make a decision about the nature of the regime that controls Germany, or Stalinist Russia, and then we equip graduate students with the knowledge of how to put together a nuclear weapon, that is an insane, suicidal, national suicidal policy, and would have been then and our people certainly recognize that.

I guess it is hard today when China is presenting itself as our adversary wherever they can, allying themselves with the rotten regimes in the world and trying to make hostile territorial claims as well as of course their economic, what I consider to be economic aggression. But as we just heard that the cost of 9/11 was $200 billion. Is that what——

Mr. LIBICKI. Yes, correct, the cost of 9/11, roughly, in property damage. Somewhere between——

Mr. ROHRABACHER. So the cost of 9/11 is $200 billion, but we also heard earlier that your report suggested that there was about $250 billion a year lost to cyber attacks of some kind or another. So what we have here is a huge issue of security that should consider even our major universities as to what kind of knowledge that they are permitting to be provided to people who might do us harm. And I would think and I would suggest that we are not now paying attention to that.

And again, every time you hear about we are going to bring people in, foreign students, and it is all done in the name of taming a potential adversary. But if you are bringing these people in and they are only taking science classes or mathematics classes at the highest level, you are not taming them at all. You are just providing them with technical knowledge and technical know-how. Perhaps we should insist that we do have exchange students coming in from every country including China, but they have to be social science majors, and they have to be aimed at understanding freedom of thought and intersocial interaction and perhaps even economics instead of how to make bombs and how to destroy people through the cyber system.

Let me see, some of the other questions that I had here for us today. So let me just say, I would like to make this statement for if the Chinese people are listening. I would like to say something directly to the Chinese people and the Chinese cyber intelligence personnel. Intelligence gathering among nations has been going on for thousands of years, and I understand that and everybody on this panel understands that.

But what differs with what governments did in the past and what they are doing and what is being done now by the leaders of China and other countries, is they are using the nation's intelligence apparatus to enrich themselves. You have an elite in China using the intelligence system including the cyber potential to enrich themselves, yes, to to give their country leverage, but for the first time we see the enemy has a personal motive in committing this aggression and having the ability to do so. The elites' use of China's intelligence agency is like having a private corporate detective, and basically you can have a private detective working for you

if you have a company, but if you are using it for a personal reason you are cheating your company.

The people of China are being cheated in that the apparatus that has been set up to protect them is being used to enrich the elite, and at the same time put China into a hostile relationship with the United States and other free countries of the world. And on top of that, the elite in China are using this not to protect China, not to make it more prosperous, but also to repress their own people. And do people that work for the Chinese Government, do they want to be a cog in a system that is designed to destroy the potential for freedom of all of their fellow Chinese?

The elite in China, their vanity and their desire for more wealth and power has led China down a wrong path, and I would urge those people in China, which is the vast majority, the people of goodwill there, to push this elite that is running their country that is raping their country and putting us on a path to conflict, to push them out of power and to reach out to the United States with a hand of friendship as we would reach out and want to reach out to them. In the cyber field this is vitally important.

And what I will do is give the witnesses each 1 minute more to comment and then we will probably close the hearing. We will start at this end because you had to wait for a long time to start, so go right ahead.

Mr. LIBICKI. I think we need a better understanding of the impact of Chinese economically motivated cyber espionage on the United States' economy. We hear a lot of numbers being thrown around. We don't really know how they are derived or how consistent they are with how we know economics works.

We are fairly confident that terabytes of data go from the United States and end up in China. We have very little visibility about what happens when they go to China and supposedly go to people who can make use of them. So I would suggest, in fact, that it is an important issue, because just to throw random numbers around here, if it is a trillion-dollar problem we treat it one way, if it is a billion-dollar problem we treat it another way. Our relationship with China is extremely complicated, has many facets, and it is useful for us to get our priorities correct, and that kind of information will help do so.

Mr. ROHRABACHER. Mr. Mazza?

Mr. MAZZA. Thank you, Mr. Chairman. In my remarks today and others have cited this as well, that what is really needed is sort of a, I guess a whole-of-government approach you could call it, really using all of the arms of American power to achieve our ends. But I think it can't be understated how important the U.S. military is in this effort. As we heard, the PLA is playing a very direct role both in the commercial espionage as well as the more traditional in military activities, and a military response is needed. We need to consider whether or not that needs to be purely cyber in the future or not, and what options we will have in the event of conflict to put a stop to cyber activities emanating from China.

Mr. ROHRABACHER. Mr. Autry?

Mr. AUTRY. I concur that it would be great to know more about this, but I think that we know enough already in that there is hundreds of billions of dollars in damage, which means thousands if

not millions of American jobs, and consequently, American lives lost in this issue. It is not our burden of responsibility to prove exactly what the damages is, but it is our responsibility to stop this hostile and overt action by the Chinese military against the United States of America.

Mr. ROHRABACHER. Mr. Bejtlich?

Mr. BEJTLICH. One of the key elements of our report was the finding that this particular group was, on average, present inside Western companies for a year before anyone was able to find them. There are some cases that stretch up to 5 years. I would encourage, when Congress is considering legislation, to go beyond just the idea of continuous monitoring. That is a term that means essentially checking baselines, looking for configuration flaws, and instead go to a more operational model where you are looking for intruders on your network.

You need to have teams of people equipped with the sort of privacy-friendly intelligence that is in the Mandiant report, using that information, looking for intruders on the network and then dealing with them once you find them. It is not enough to just be patching your flaws, to have good software. The intruders will find a way in. You have to be out there looking for them in order to succeed. Thank you.

Mr. ROHRABACHER. And so let me finish it off with it is not enough to know that we are willing to go out and find those people who are hacking the system, whether it is an organized group out of China that represents a government aggression upon the other nations and other people or whether it is just individual hackers or criminals around the world who are engaged in trying to get into people's bank accounts and take money or in some way to mess with the system.

So it is all of these elements, but identifying them is not just, we have to also understand what we are going to do in response. And I will have to say that so far especially from our first witness who is not here to make a further comment although I would give him that opportunity now, but I am sure that he is doing his job but I don't believe that the United States Government is doing its job in making sure that we are prepared to deal with a threat as expansive as this threat, which is going to get even worse and worse as we become more and more dependent on this cyber world for us to remain an effective society and a safe society. But at this point I have not heard what we will do once we find out all of that information.

Now we know there is a building and we know there is People's Liberation Army people in the building and we know that that is the source of cyber attacks or cyber oppression coming out of that building, so what are we going to do about it? Well, I think it has got to be more than well, we are just going to—what was the wording we had earlier about raising, basically raising the level of rhetoric. And I would suggest that raising the level of rhetoric does not mean anything to bullies and gangsters. And if you are dealing with bullies and gangsters there has got to be some form of retaliation. And we have not had any examples of what we can actually do, except Mr. Autry, I think, explained something about we can

determine what the price tag is and maybe put a tariff on goods coming in from China or other countries.

But remember what happened today. What happened today was we thought that South Korea, which has been attacked, their banking system and other parts of their economy have been attacked, today identified not North Korea but China as the aggressor in this situation. So you may have China hiding behind North Korea, which it has done in many cases, or various groups hiding and portraying themselves actually as these attacks are coming from someone else.

Well, we need to know. It is getting more complicated. It is not going to get less complicated. But one thing is for sure, our Government is not prepared to deal with this threat. We are unprepared. And when something happens, if it is of a huge magnitude or someone fiddles with the air traffic control system or the grid, as Steve Stockman mentioned, even the oil industry now they could hack into that and screw up our entire production of energy, of oil and gas. If something big like this happens and if it is a well thought out plan, if a small group of fanatics can organize an effort that caused $200 billion of damage on 9/11, one can imagine that a country run by a criminal element could do even more damage.

So we are not prepared to meet this threat. We need to have more discussions like this. I want to make sure that all of you that we keep in touch, because we will have another hearing like this probably in about 6 months to 1 year to see if we have made any progress in that 6 months. And I will be asking you to tell me what you have seen if, there has been any progress made.

With that said I would like to thank the witnesses and thank my staff. I appreciate that Mr. Keating, the ranking member, had an Appropriations hearing that he had to go to, but his participation earlier was much appreciated. So thank you all very much and this hearing is adjourned.

[Whereupon, at 11:37 a.m, the subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

SUBCOMMITTEE HEARING NOTICE
COMMITTEE ON FOREIGN AFFAIRS
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, DC 20515-6128

Subcommittee on Europe, Eurasia, and Emerging Threats
Dana Rohrabacher (R-CA), Chairman

March 19, 2013

TO: MEMBERS OF THE COMMITTEE ON FOREIGN AFFAIRS

You are respectfully requested to attend an OPEN hearing of the Subcommittee on Europe, Eurasia, and Emerging Threats in Room 2172 of the Rayburn House Office Building (and available on the Committee website at www.foreignaffairs.house.gov):

DATE: Thursday, March 21, 2013

TIME: 9:00 a.m.

SUBJECT: Cyber Attacks: An Unprecedented Threat to U.S. National Security

WITNESSES: Panel: I
Mr. Christopher Painter
Coordinator
Office of the Coordinator for Cyber Issues
U.S. Department of State

Panel: II
Mr. Richard Bejtlich
Chief Security Officer and Security Services Architect
Mandiant Corporation

Mr. Greg Autry
Senior Economist
Coalition for a Prosperous America

Mr. Michael Mazza
Research Fellow
American Enterprise Institute

Martin C. Libicki, Ph.D.
Senior Management Scientist
RAND Corporation

By Direction of the Chairman

The Committee on Foreign Affairs seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202/225-5021 at least four business days in advance of the event, whenever practicable. Questions with regard to special accommodations in general (including availability of Committee materials in alternative formats and assistive listening devices) may be directed to the Committee.

COMMITTEE ON FOREIGN AFFAIRS

MINUTES OF SUBCOMMITTEE ON *Europe, Eurasia, and Emerging Threats* HEARING

Day *Thursday* **Date** *3/21/13* **Room** *2172*

Starting Time *9:07 am* **Ending Time** *11:37 am*

Recesses [*1*] (*10:24* to *11:08*) (____ to ____) (____ to ____) (____ to ____) (____ to ____) (____ to ____)

Presiding Member(s)

Chairman Dana Rohrabacher

Check all of the following that apply:

Open Session [✓]
Executive (closed) Session [ ]
Televised [✓]
Electronically Recorded (taped) [✓]
Stenographic Record [✓]

TITLE OF HEARING:

Cyber Attacks: An Unprecedented Threat to U.S. National Security

SUBCOMMITTEE MEMBERS PRESENT:

Ranking Member Keating, Congressmen Duncan, Stockman, Marino, Cook, and Lowenthal.

NON-SUBCOMMITTEE MEMBERS PRESENT: *(Mark with an * if they are not members of full committee.)*

None

HEARING WITNESSES: Same as meeting notice attached? Yes [✓] **No** [ ]
(If "no", please list below and include title, agency, department, or organization.)

STATEMENTS FOR THE RECORD: *(List any statements submitted for the record.)*

Prepared Statement of Mr. Christopher Painter
Prepared Statement of Mr. Richard Bejtlich
Prepared Statement of Mr. Greg Autry
Prepared Statement of Mr. Michael Mazza
Prepared Statement of Martin C. Libicki, Ph.D.

TIME SCHEDULED TO RECONVENE _____
or
TIME ADJOURNED *11:37 am*

Subcommittee Staff Director