IRANIAN CYBER THREAT TO THE U.S. HOMELAND

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

AND THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

APRIL 26, 2012

Serial No. 112–86

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PRINTING OFFICE

77–381 PDF 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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY

PETER T. KING, New York, *Chairman*

LAMAR SMITH, Texas
DANIEL E. LUNGREN, California
MIKE ROGERS, Alabama
MICHAEL T. MCCAUL, Texas
GUS M. BILIRAKIS, Florida
PAUL C. BROUN, Georgia
CANDICE S. MILLER, Michigan
TIM WALBERG, Michigan
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
PATRICK MEEHAN, Pennsylvania
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
BLAKE FARENTHOLD, Texas
ROBERT L. TURNER, New York

BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
HENRY CUELLAR, Texas
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
DANNY K. DAVIS, Illinois
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
HANSEN CLARKE, Michigan
WILLIAM R. KEATING, Massachusetts
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
VACANCY

MICHAEL J. RUSSELL, *Staff Director/Chief Counsel*
KERRY ANN WATKINS, *Senior Policy Director*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE

PATRICK MEEHAN, Pennsylvania, *Chairman*

PAUL C. BROUN, Georgia, *Vice Chair*
CHIP CRAVAACK, Minnesota
JOE WALSH, Illinois
BEN QUAYLE, Arizona
SCOTT RIGELL, Virginia
BILLY LONG, Missouri
PETER T. KING, New York *(Ex Officio)*
BRIAN HIGGINS, New York
LORETTA SANCHEZ, California
KATHLEEN C. HOCHUL, New York
JANICE HAHN, California
VACANCY
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

KEVIN GUNDERSEN, *Staff Director*
ZACHARY D. HARRIS, *Subcommittee Clerk*
HOPE GOINS, *Minority Subcommittee Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

DANIEL E. LUNGREN, California, *Chairman*

MICHAEL T. MCCAUL, Texas
TIM WALBERG, Michigan, *Vice Chair*
PATRICK MEEHAN, Pennsylvania
BILLY LONG, Missouri
TOM MARINO, Pennsylvania
PETER T. KING, New York *(Ex Officio)*
YVETTE D. CLARKE, New York
LAURA RICHARDSON, California
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
BENNIE G. THOMPSON, Mississippi *(Ex Officio)*

COLEY C. O'BRIEN, *Staff Director*
ZACHARY D. HARRIS, *Subcommittee Clerk*
CHRIS SCHEPIS, *Minority Senior Professional Staff Member*

CONTENTS

IRANIAN CYBER THREAT TO THE U.S. HOMELAND

Thursday, April 26, 2012

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON COUNTERTERRORISM AND INTELLIGENCE, AND
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
WASHINGTON, DC.

The subcommittees met, pursuant to call, at 10:06 a.m., in Room 311, Cannon House Office Building, Hon. Patrick Meehan [Chairman of the Subcommittee on Counterterrorism and Intelligence] presiding.

Present from the Subcommittee on Counterterrorism and Intelligence: Representatives Meehan, Cravaack, and Hahn.

Present from the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: Representatives Lungren, Higgins, Clarke, Richardson, and Richmond.

Also present: Representative Green.

Mr. MEEHAN. Good morning, the Committee on Homeland Security Subcommittees on Counterterrorism and Intelligence and Cybersecurity, Infrastructure Protection, and Security Technologies—this is a joint committee hearing—will come to order. Subcommittees are meeting today to hear the testimony regarding the threat of a cyber attack to the United States homeland from the Islamic Republic of Iran. I will now recognize myself for an opening statement.

I would like to begin today by thanking Chairman Lungren and Ranking Member Clarke and all of the Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies for joining us here today to examine the threat posed by Iran in the cyber arena. The combination of our expertise on counterterrorism and intelligence, and your expertise on cybersecurity will inform and enhance our discussion. I look forward to hearing from you, and our panel.

I believe the joint hearing represents the attitude we must have when confronted with emerging threats that may not be adequately understood. In my view, the adaptability, flexibility, and willingness to erase institutional barriers called for in the 9/11 Commission Report is on display here, with each of us bringing our own expertise to study a threat which crosses borders and cannot easily be put into a box. While Chairman Lungren and his colleagues on the CIPST Subcommittee have studied the ins and outs of pro-

tecting our Nation's critical infrastructure from cyber attack, the membership of the CT&I Subcommittee have spent a lot of time examining the threat posed by Iran in the world's largest state sponsor of terrorism, and its proxies, of course, principally including Hezbollah.

For the Subcommittee on Counterterrorism and Intelligence, this hearing is a continuation of our previous work examining the threat from Tehran. Last year our subcommittee examined the Hezbollah presence in Latin America that detailed the recently exposed Iranian government plot to conduct a brazen attack here in Washington, DC. I have also recently returned from the region, where I met with defense and intelligence officials and government leaders in Israel and Turkey and Jordan. After in-depth conversations and briefings including with Turkey president Abdullah Gul, Israeli Prime Minister Benjamin Netanyahu, and His Majesty King Abdullah of Jordan, it became increasingly clear that Iran is the most destructive and malicious actor in the region, and will persist in antagonizing the United States and our allies, especially the State of Israel.

As Iran's illicit nuclear program continues to inflame tensions between Tehran and the West, I am struck by the emergence of another possible avenue of attack emanating from Iran—the possibility that Iran could conduct a cyber attack against the United States homeland. Now, many will discount this threat just as many ignored the possibility that Iran would conduct any kind of attack on American soil. Well, this assumption was proven woefully wrong when last year's plot to kill the Saudi Ambassador was uncovered. Now we are adjusting to a realistic understanding of Iran's intent to conduct terror attacks and to kill innocent Americans in the U.S. homeland, we cannot blind ourselves to this new threat. After all, if Iran is willing to blow up a Washington restaurant, and kill innocent Americans, we would be naïve to think that Iran could never conduct a cyber attack against the United States homeland.

Earlier this year, in testimony before the Senate Intelligence Committee, Director of National Intelligence James Clapper clearly stated that Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity. What I view as a private-sector validation of the cyber threat posed by Iran, Google executive Chairman Eric Schmidt recently stated the Iranians are talented in cyber war for some reasons we don't fully understand.

In the event of a military strike against Iranian nuclear facilities, former director of the National Counterterrorism Center, Michael Leiter, assessed that a cyber attack conducted by Iran—Tehran against the United States, would be reasonably likely.

The threat of cyber warfare may be relatively new, but it is not small. Iran has reportedly invested over $1 billion in developing their cyber capabilities, and it appears they may have already carried out attacks against organizations like the BBC, and Voice of America. There have been reports that Iran may have even attempted to breach the private networks of a major Israeli financial institution. Iran is very publicly testing its cyber capabilities in the region, and in time, will expand its reach.

Other nations such as Russia and China may have more sophisticated cyber capabilities, but there should be little doubt that a country that kills innocent civilians around the world, guns down its own people, and calls for the destruction of the State of Israel, would not hesitate to conduct a cyber attack against the United States homeland.

That is why today's hearing is so important.

I want to thank you for joining us today, and I look forward to hearing from our witnesses.

[The statement of Mr. Meehan follows:]

STATEMENT OF CHAIRMAN PATRICK MEEHAN

APRIL 26, 2012

WELCOME

I would like to begin today by thanking Chairman Lungren and Ranking Member Clarke, and all the Members of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies for joining us here today to examine the threat posed by Iran in the cyber arena. The combination of our expertise on counterterrorism and intelligence and your expertise on cybersecurity will inform and enhance our discussion, and I look forward to hearing from you and our panel.

IMPORTANCE OF JOINT HEARING

I believe this joint hearing represents the attitude we must have when confronted with emerging threats that may not be adequately understood. In my view, the adaptability, flexibility, and willingness to erase institutional barriers called for in the 9/11 Commission Report is on display here, with each of us bringing our own expertise to study a threat which crosses borders and cannot easily be put into one box. While Chairman Lungren and his colleagues on the CIPST subcommittee have studied the "ins" and "outs" of protecting our Nation's critical infrastructure from cyber attack, the Members of the CTI subcommittee have spent a lot of time examining the threat posed by Iran, the world's largest state sponsor of terrorism, and its proxies, including Hezbollah.

PAST SUBCOMMITTEE IRAN EXAMINATIONS

For the Subcommittee on Counterterrorism and Intelligence, this hearing is a continuation of our previous work examining the threat from Tehran. Last year, our subcommittee examined the Hezbollah presence in Latin America that detailed the recently exposed Iranian government plot to conduct a brazen terror attack here in Washington, DC. I have also recently returned from the region, where I met with defense and intelligence officials and government leaders in Israel, Turkey, and Jordan. After in-depth conversations and briefings, including with Turkey President Abdullah Gul, Israeli Prime Minister Benjamin Netanyahu, and His Majesty King Abdullah of Jordan, it became increasingly clear that Iran is the most destructive and malicious actor in the region and will persist in antagonizing the United States and our allies, especially the State of Israel.

EMERGING CYBER THREAT FROM IRAN

As Iran's illicit nuclear program continues to inflame tensions between Tehran and the West, I am struck by the emergence of another possible avenue of attack emanating from Iran: The possibility that Iran could conduct a cyber attack against the U.S. homeland.

Many will discount this threat—just as many ignored the possibility that Iran would conduct an attack on American soil. This assumption was proven woefully wrong when last year's plot to kill the Saudi Ambassador was uncovered. Now that we are adjusting to a realistic understanding of Iran's intent to conduct terror attacks and kill innocent Americans in the U.S. homeland, we cannot blind ourselves to this new threat. After all, if Iran is willing to blow up a Washington restaurant and kill innocent Americans, we would be naïve to think Iran would never conduct a cyber attack against the U.S. homeland.

SENIOR OFFICIALS WARNING

Earlier this year in testimony before the Senate Intelligence Committee, Director of National Intelligence James Clapper clearly stated: "Iran's intelligence operations against the United States, including cyber capabilities, have dramatically increased in recent years in depth and complexity." In what I view as a private sector validation of the cyber threat posed by Iran, Google Executive Chairman Eric Schmidt recently stated, the "Iranians are unusually talented in cyber war for some reason we don't fully understand." And, in the event of a military strike against Iranian nuclear facilities, former director of the National Counterterrorism Center Michael Leiter assessed that a cyber attack conducted by Tehran against the United States would be "reasonably likely."

The threat of cyber warfare may be relatively new—but it is not small. Iran has reportedly invested over $1 billion in developing their cyber capabilities, and it appears they may have already carried out attacks against news organizations like the BBC and Voice of America. There have been reports that Iran may have even attempted to breach the private networks of a major Israeli financial institution. Iran is very publicly testing its cyber capabilities in the region and, in time, will expand its reach.

DON'T IGNORE THIS THREAT

Other nations such as Russia and China may have more sophisticated cyber capabilities, but there should be little doubt that a country that kills innocent civilians around the world, guns down its own people, and calls for the destruction of the State of Israel would not hesitate to conduct a cyber attack against the U.S. homeland. That is why today's hearing is so important.

I want to thank all of you for joining us today, and I look forward to hearing from our witnesses.

Mr. MEEHAN. Now, I know that co-Chairman, or the Ranking Member Mr. Higgins is expected today at this moment, but until such time as he is able to join us at the hearing, the Chairman would now recognize Ms. Clarke for any opening comments she may have. Thank you.

Ms. CLARKE. Thank you very much, Mr. Chairman. Chairman Lungren, Chairman Meehan, thank you for holding this joint hearing on the Iranian cyber threat. State-sponsored cyber threats from Iran and actual attacks from other countries directed at the United States, have been a hot topic over the past few years. As you know, we have had a number of classified briefings concerning these state-sponsored attacks. Our ability to detect, prevent, preempt, and deter terrorists and malicious state-sponsored cyber attacks reflect on our capability, and our political will to protect our vital National infrastructure from devastating consequences.

I am glad my colleague and fellow New Yorker, Mr. Higgins, has brought some legislation to bear on the issue we are discussing today. His bill would amplify the State Department's report to Congress on the proficiencies of Iran cyber and technological capabilities. This will help us assess Iran's threat in greater detail. This is quite a story to be told about Iran and cyber threats, and I will be interested in hearing the testimony today.

I have seen the report put out by Reporters Without Borders, that places Iran on the list of enemies of the internet, describing the various censoring techniques that Iran used to control the flow of information among its own people.

The report refers to the government-sponsored cyber police function that uses a combination of content filtering and access control. The report also mentions the use of distributed denial of service cyber attack techniques used as a form of political oppression, which it says may or may not be official state-sponsored activity.

Reports on Iranian Cyber Army have raised questions about the regime's cyber attack capabilities and the extent to which these attacks are coordinated by the government. Some have said the Iranian Cyber Army may be a loose confederation of hackers and cyber activists similar to other hacking clusters, and may include cyber crime networks and other groups.

One such known as the Ashiyane Digital Security Team, has claimed responsibility for hacking into and defacing thousands of websites. Both Iranian Cyber Army, and the Ashiyane are alleged to have ties with the Iranian government's revolutionary guard, but who can tell? Given the Iranian regime's control over the internet and attempts to crack down on citizen's internet activity, it would appear to be a sweeping promotion of hacking without any legal or public recourse and suggests a tacit governmental approval of these activities.

Some have said the Iranian Cyber Army resembles a collective of regime-backing hackers acting of their own volition; yet it may be that the regime has actively leveraged and employed the talents of a young population adept with computer tools. In the wake of Iran's presidential election in June 2009, protesters had used Twitter to skirt government filters to promote, to report events, and organize opposition rallies prompting the U.S. State Department to request that Twitter reschedule its planned maintenance activities in order to ensure access to pro-democracy users. But the Iranian regime's brutal crackdown on the protesters seemingly succeeded. Demonstrations are now few and far between, and many of the web-based citizen journalists that have documented the uprising have been killed, imprisoned, or gone underground; their voices silenced.

The most well-known cyber event in Iran occurred late in 2009, when this Central European security firm reported the discovery of a software worm called Stuxnet, that had infected computers controlling centrifuges of several Iranian nuclear enrichment plants. However, these computers were not connected to the internet, and the worm was said to have been injected into those computers using an external device such as a thumb drive. Stuxnet may be proof of Iran's vulnerability and the effectiveness of other nation's state cyber arsenals. However, it would be—it would also be possible for Iran to gain some knowledge of creating a Stuxnet-like virus from analyzing its network effects.

This leads to fear of reverse engineering leading to a capability of the types of cyber attacks on U.S. critical infrastructure that could rise to the level of a National security crisis. We must be prepared for such rogue actions and be prepared on the National defense level, as well as protecting our critical business operations, vital infrastructure functions, and frankly, our daily lives.

The rapid technological advances in cybersecurity threats over the last several years have outpaced our ability as lawmakers to keep our laws up-to-date. The needed coordination of the many Governmental agencies and private institutions, and the implementation of the procedures that would protect our infrastructure, are huge undertakings and will continue to have huge challenges.

We are seeing some of those challenges being played out on the House floor this week, and my Ranking Member, Mr. Thompson,

is talking about some of the most constructive alternatives to the cyber legislation we are considering. Our intelligence community and law enforcement agencies face many challenges to anticipate, investigate, and respond to cyber threats.

Simply, all these challenges must be overcome, and protection of our infrastructure accomplished without violating our fundamental rights of individual privacy that are enshrined in our Constitution. With that, Mr. Chairman, I yield back.

Mr. MEEHAN. Thank you, Ms. Clarke. Before I begin, let me recognize that the gentleman from Texas, Mr. Green, has joined us today, and I would like to ask unanimous consent that he be able to participate in today's hearing. Hearing no objection, so ordered. Welcome Mr. Green. Thank you for being here with us today. The Chairman now recognizes my good friend, the Chairman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, the gentleman from California, Mr. Lungren, for any statement he may have.

Mr. LUNGREN. Thank you very much, Mr. Chairman. I want to thank all of my colleagues for being here, particularly those from our companion subcommittee to meet on a very important subject. Those of us in the Congress know that we have an obligation to proceed with legislation on important issues such as cybersecurity.

We have an obligation to conduct appropriate oversight of the Executive branch to ensure that they are doing that which needs to be done, in concert, or consistent with legislation that has been duly passed, but we also have another obligation, it seems to me, and that is to raise the knowledge of the public on issues of true National and international importance, and cybersecurity is one of those subjects, and we hope that this hearing provides insight into possible legislation, insight into oversight, and particularly, helps us to raise the public knowledge of this important issue.

As we all know, communicating through cyber space, is now an integral part of the international marketplace, and the global economy. Businesses of all sizes, increasingly depend upon it in their daily operations as well as for market growth. Individuals utilize it on a daily basis. Many people enter into the commercial market by way of the internet these days and other uses of cyber space.

These innovative cyber technologies help U.S. businesses to achieve great efficiencies and to run their vital infrastructures. But the tremendous opportunities provided by cyber space, are accompanied by obvious vulnerabilities. For instance, along with all of the other benefits, with all of the benefits, cyber space is replete with nefarious actors, including organized criminals, industrial spies, foreign governments taking inappropriate advantage of a cyber environment open to all users. The very openness of cyber space contributes to its vulnerability, and its possibility of abuse.

We have been warning about cyber threats in this committee for a long time. It has been a bipartisan effort to warn of these threats. The Nation's top Government, intelligence, and military leaders often cite the cyber threat as the issue that worries them the most. The reason is that a successful cyber attack on a power grid, transportation system, or communication networks could cripple our economy and threaten our National security. Any doubt about the physical damage that could be caused by a cyber attack

should have been eliminated by the Stuxnet virus. I am happy the Stuxnet virus was used by somebody who was a friendly, and it is probably the best example of the cyber and physical worlds intersecting.

Like Aurora, Stuxnet demonstrates that vital critical infrastructure can be physically disabled or destroyed by a capable and motivated enemy, and as we know in those attacks, they were done with a certain stealth element to them. That is, the destruction took place before the operators that were supposed to protect against such destruction were able to even understand that they were under attack.

In addition to these National security concerns, cyber threat thefts are also robbing us of our intellectual property. We have had examples already of how this has cost U.S. jobs and jeopardized our economic future. Cyber threats are real. They are growing in number and sophistication. In assessing the Iranian threat to the U.S. homeland, we need to examine their motivation, their opportunity, and their capability. As the victim of two recent cyber attacks nuclear and oil infrastructure, and multiple U.S. embargoes, Iran, it would seem, would have motivation to strike out against those they think are responsible, or anybody associated with those they think are responsible, or anybody who would stand on the sidelines and cheer those efforts.

The opportunity arises as U.S. critical infrastructure companies have been slow to harden their assets against cyber attacks. Unfortunately, cyber attacks can be launched from any place in the world, because cyber space does not recognize borders. The important question when assessing Iran as a cyber threat is their cyber capability. American Security Contracting Firm issued a report in 2008 rating Iran cyber capability among the top five globally. A December 2011 report indicated that Tehran was investing $1 billion in new cyber warfare technology.

So let me underscore a point made by the Chairman of our other subcommittee. According to the DNI Director Clapper, Iran's intelligence operations against the United States including cyber capabilities, have dramatically increased in recent years, in depth, and complexity.

Since Iran appears to have the necessary cyber capability, we can only hope that they will fear attribution and the overwhelming U.S. response that would surely follow such an Iranian cyber attack against our Nation. I look forward, along with my colleagues, to the testimony of the distinguished panel this morning on the nature of the cyber threat from this rogue Iranian regime. Thank you very much, Mr. Chairman.

[The statement of Mr. Lungren follows:]

STATEMENT OF CHAIRMAN DANIEL E. LUNGREN

APRIL 26, 2012

Communicating through cyber space is now an integral part of the international marketplace and the global economy. Businesses of all sizes increasingly depend upon it for their daily operations as well as for market growth. These innovative cyber technologies help U.S. businesses achieve great efficiencies and run their vital infrastructures. However, along with all the benefits, cyber space is replete with nefarious actors—including organized criminals, industrial spies, and foreign governments taking inappropriate advantage of a cyber environment open to all users.

We have been warning about cyber threats in this committee for a long time. The Nation's top Government, intelligence, and military leaders often cite the cyber threat as the issue that worries them the most. The reason is that a successful cyber attack on our power grid, transportation systems, or communication networks could cripple our economy and threaten our National security. Any doubt about the physical damage that can be caused by a cyber attack should have been eliminated by the Stuxnet virus. Stuxnet is the best example of the cyber and physical worlds intersecting. Like Aurora, Stuxnet demonstrates that vital critical infrastructure can be physically disabled or destroyed by a capable and motivated enemy.

In addition to these National security concerns, cyber thefts are also robbing us of our intellectual property, costing U.S. jobs and jeopardizing our economic future. Cyber threats are real and growing in number and sophistication.

In assessing the Iranian threat to the U.S. homeland, we need to examine their motivation, opportunity, and capability. As the victim of two recent cyber attacks (nuclear and oil infrastructure) and multiple U.S. embargoes, Iran clearly has motivation to strike us.

Their opportunity arises as U.S. critical infrastructure companies have been slow to harden their assets against cyber attacks. Unfortunately, cyber attacks can be launched from any place in the world because cyber space doesn't recognize international borders.

The important question when assessing Iran as a cyber threat is their cyber capability. An American security contracting firm issued a report in 2008 rating Iran's cyber capability among the top five globally. A December 2011 report indicated that Tehran was investing $1 billion in new cyber warfare technology. According to DNI Director Clapper, "Iran's intelligence operations against the U.S., including cyber capabilities, have dramatically increased in recent years in depth and complexity".

Since Iran appears to have the necessary cyber capability, we can only hope that they will fear attribution and the overwhelming U.S. response that would surely follow such an Iranian cyber attack against our Nation.

I look forward to the testimony of our distinguished panel this morning on the nature of the cyber threat from this rogue Iranian regime.

Mr. MEEHAN. Thank you, Mr. Lungren. The Chairman now recognizes the Ranking Minority Member of the Subcommittee on Counterterrorism and Intelligence, my good friend, the gentleman from New York, Mr. Higgins, for any statement he may have.

Mr. HIGGINS. Thank you, I would like to thank both Chairman Lungren and Meehan for holding this important hearing. It is also a pleasure to hold this hearing are Ranking Member Clarke, a fellow Member from New York. I would also like to thank the witnesses for appearing here today. Cyber threat is a threat that knows no limit, and has no boundaries. We know that Iran poses a threat to our cybersecurity. We also know that our information technology has massive vulnerabilities. We know that our dependence on technology is pervasive and growing. We know that our moving forward as a Nation depends on our having a robust, comprehensive cybersecurity policy in place. Therefore, we must have legislation and policies that not only examine the threat, but also protect critical infrastructure and promote research and development that will ensure that we have the proper protocols in place to prevent a cyber attack. I look forward to hearing the testimony and I yield back.

Mr. MEEHAN. Thank you, Ranking Member Higgins. Other Members of the committee are reminded that opening statements may be submitted for the record. Now we are pleased to have a distinguished panel of witnesses before us today on this very, very important topic. Let me first give the biography of Mr. Frank Cilluffo. He is the associate vice president and director of the Homeland Security Policy Institute at George Washington University, where he directs the homeland security efforts from policy, research, edu-

cation, and training on a wide range of homeland security matters including counterterrorism and cyber threats.

Before joining the staff at GW, Mr. Cilluffo served as the special assistant to the President for Homeland Security. Shortly following September 11, 2001 terrorist attack, Mr. Cilluffo was appointed by President Bush to the newly-created Office of Homeland Security, and served as the principal advisor to Governor Tom Ridge.

Prior to his White House appointment he spent 8 years in senior policy positions for the Center for Strategic and International Studies where he directed numerous committees and task forces homeland defense.

We are also joined by Mr. Ilan Berman, Mr. Ilan Berman is the vice president of the American Foreign Policy Council in Washington, DC. Mr. Berman is an expert on regional security in the Middle East, Central Asia, and the Russian Federation. He has consulted for both the United States Central Intelligence Agency, and the United States Department of Defense, and provided assistance on foreign policy and National security issues in a range of Governmental agencies and Congressional offices. He is a member of the associated faculty at Missouri State University's Department of Defense, and Strategic Studies.

Last, we are joined by Roger Caslow. He is an executive cyber consultant for Suss Consulting. Prior to joining Suss, Mr. Caslow served as the chief of risk management and information security programs for the chief information officer of the intelligence community. In this role, he is responsible for the development, implementation, and oversight of multiple risk management policies, security programs, and technology solutions supporting the intelligence community, and DoD. He has led the intelligence community in partnering with the National Institute of Standards, at all phases of planning, development, and delivery of significant body of Federal security guidance. He has held a number of positions with the DoD and intelligence community, including senior policy and plans leader for the chief information officer.

I welcome each of the witnesses today, and the Chairman now recognizes Mr. Cilluffo to testify.

STATEMENT OF FRANK J. CILLUFFO, ASSOCIATE VICE PRESIDENT AND DIRECTOR, HOMELAND SECURITY POLICY INSTITUTE, THE GEORGE WASHINGTON UNIVERSITY

Mr. CILLUFFO. Chairman Meehan, Chairman Lungren, Ranking Members Higgins and Clarke, thank you for the opportunity to appear before you today. As you will note from my prepared remarks, it is difficult to compress such a complex set of issues into 5 minutes, coupled with the fact that I have never had an unspoken thought, but hopefully we can delve into some of the specificities during the Q&A.

First, I don't think it is a newsflash to underscore that we as a country still have a lot of work to do on the cyber front. I think it is appropriate and fair to suggest, while an imperfect analogy, that our cyber community is where our homeland community was shortly after 9/11.

Second, compounding the specific challenge before us, you cannot effectively evaluate, assess, and ultimately address the Iranian

cyber threat through a counterterrorism, homeland security, cybersecurity, or infrastructure protection lens alone; rather, the complexity demands that we look at it through a prism that incorporates all of these views. Let me just also applaud both Chairmen that you saw the need to do some cross-committee pollination on some of these issues.

Iran through its Islamic Revolutionary Guard Corps, associated Quds Force, and its proxies have long had the United States in their cross-hairs. Up until 9/11 it was Iran's chief proxy, Hezbollah, that held the mantle of the deadliest terrorist organization, having killed more Americans up to that point than any other terrorist group.

The current climate is particularly challenging and concerning, however, because the level of tension appears to be rising. We have seen an uptick in attempted and actual attacks on and assassinations of Israeli, Jewish, U.S., and Western interests from Beirut to Baku, to Bangkok and, of course, the recent assassination attempt on the Saudi Ambassador on the U.S. soil.

Against this backdrop, getting ahead of the Iranian cyber threat to the United States is all the more relevant and all the more timely. The reach of Iran's proxies have gone global. Hezbollah activities now stretch from West Africa to the tri-border area of Argentina, Brazil, and Paraguay. Within the United States, there have been 16 arrests in 2010 of Hezbollah sympathizers seeking stinger missiles, M–4 rifles, and night vision equipment. Based on this recent activity, the Los Angeles Police Department has elevated the government of Iran and its proxies to a tier 1 threat.

Notably, the city of Los Angeles, contains the most active Hezbollah presence in this country, and Los Angeles happens to also be home to the largest ethnic Iranian population outside of Iran itself.

Law enforcement officials have also observed a striking convergence of crime and terrorism, a trend highlighted, I might note earlier this week by Defense Secretary Panetta, and further reinforced by SOUTHCOM Commander General Fraser. Hezbollah's nexus with criminal activity is greater than that of any other known terrorist group. These links, including with gangs and cartels, generate new possibilities for outsourcing, and new networks that can facilitate terrorist travel, logistics, recruitment, and operations, and I might note, including cyber.

Moreover, authorities have noted significant terrorist interest in the tactics, techniques, and procedures of smuggling drugs and people into the United States. These developments suggest that our long-standing frames of reference, our so-called red lines, have shifted. First and foremost, whereas previously Iran and it proxies targeted U.S. interests and personnel abroad, the cleave between here, our homeland, and overseas is wearing away as these two fronts merge. As you know in cyber, where we particularly know no borders, this has great resonance.

As you mentioned, the Director of National Intelligence, General Clapper, was very bold in stating now that Iran is now more willing to conduct an attack in the United States. I might note that his assessment has been echoed by many others in the National security and law enforcement community of late.

Let me state a couple of very quick words, specifically on Iran cyber attack capabilities. As has been mentioned, Iran is investing heavily in building its cyber warfare capabilities, including standing up the Iranian Cyber Army, which is in addition to their more conventional and traditional electronic warfare capabilities, which were quite sophisticated to begin with. Recent open-source and public incidents demonstrate a growing level of sophistication.

Ms. Clarke, you mentioned many of the examples earlier today, but I might note there is one that you did not mention, that I thought demonstrated the highest level of sophistication, and that was the recent hack of a security certificate company in the Netherlands, a Dutch company, that demonstrated not only their hacking skills, but their ability to manipulate data as well.

Prior to the official pronouncements regarding the Iranian Cyber Army, numerous hacker groups have operated pro-regime groups in Iran. These range from the broader Basige, to the recent stand up of the Cyber Hezbollah, and perhaps the most sophisticated group from a trade craft perspective, the Ashiyane. It in increasingly becoming clear, however, that the IRGC is not only cultivating, but also guiding, and I think trying to assume control over these various organizations.

These developments aside, the good news is that if you were to rack and stack the greatest cyber threats in nations, Iran is not at the top of the list. Russia, PRC, and others are. The bad news is is what they lack in capability, they make up for in intent, and are not as constrained as other countries may be from engaging in cyber attacks or computer network attacks. Given Iran's history to employ proxies for terrorist purposes, there is little, if any, reason to think that Iran would hesitate to engage proxies to conduct cyber attacks against perceived adversaries.

To paraphrase Mark Twain, whereas history may not repeat itself, it tends to rhyme. If they did it in the kinetic and the physical world, you can assume that they will be looking to cyber capacities as well. I know I am over my time, but a couple of very quick points. Another thing to think about is cyber basically levels the playing field. It provides asymmetry that can give small groups disproportionate impact and consequence. Whereas they may not have the capability, they can rent or buy that capability. There is a cyber arms bizarre on the internet. Intent and cash can take you a long way, and that is what I think we need to be thinking about. I might note that many have assumed and looked at the cyber threat more from a contingency or preemptive action that one of our allies may have in Iran. I don't think that bar is there. I think that they already feel, as has been mentioned by Mr. Lungren, and yourself, Mr. Chairman, and Mr. Higgins as well, that they are taking the gloves off right now in a cyber environment. I might also note that specifically, the fact that they have tried to demonstrate such a capability with the drones, which I don't necessarily believe at all, but they need to demonstrate that capability or they potentially lose all credibility. So I think now is the time to act.

[The prepared statement of Mr. Cilluffo follows:]

PREPARED STATEMENT OF FRANK J. CILLUFFO

APRIL 26, 2012

Chairman Meehan, Chairman Lungren, Ranking Members Higgins and Clarke, and distinguished Members of the subcommittees, thank you for the opportunity to testify before you today. The subject is one of National importance—we, as a country, still have work to do in order to best respond to, and get ahead of, threats on the cybersecurity front. Indeed, with regard to cyber, the United States is in a position akin to where the homeland security community was shortly after 9/11. This is problematic in terms of both cybersecurity and infrastructure protection, as well as counterterrorism and intelligence. There are many points of intersection and overlap between these two "lenses"; and if recent history has taught us anything, it is that bureaucratic stovepiping can have fatal consequences. Your demonstrated commitment to tackle the subject under study jointly is therefore all the more commendable, and indeed a model for moving the Nation forward on the truly difficult interdisciplinary challenges that characterize the current National security ecosystem.

Iran (its Islamic Revolutionary Guard Corps, and associated Quds Force; the Ministry of Intelligence and Security; etc.) and proxies have long had the United States in their cross-hairs. Up until 9/11, in fact, it was Iran's chief proxy, Hezbollah, that held the mantle of deadliest terrorist organization, having killed more Americans up to that point than any other terrorist group. The October 23, 1983 bombing of the U.S. Marine Barracks in Beirut, Lebanon, cost the lives of 241 soldiers, marines, and sailors.

The current climate is particularly concerning however, because the level of tension appears to be rising. We have seen an uptick in attempted and actual attacks on and assassinations of Israeli, Jewish, U.S., and Western interests. This past February saw apparently coordinated bomb attacks against the embassies of one ally, Israel, in the capitals of two others—India and Georgia. February also saw Iranian agents in Bangkok prematurely detonate explosives, while preparing devices, resulting in injuries only to the perpetrators. Consider also the recently thwarted Iranian plot to assassinate Saudi Arabia's ambassador to the United States.

While Iran has sought to distance itself from the incidents described above and denied responsibility for them (not credibly mind you), the reach of Iran's proxies has gone global. Hezbollah's activities now stretch from West Africa to the Tri-Border Area of Argentina, Brazil, and Paraguay. Within the United States, there were 16 arrests of Hezbollah activists in 2010 based on Joint Terrorism Task Force investigations in Philadelphia, New York, and Detroit; and the organization has attempted to obtain equipment in the United States, including Stinger missiles, M–4 rifles, and night vision equipment.[1] Based on recent activity, the Los Angeles Police Department has elevated the Government of Iran and its proxies to a Tier One threat. Notably, the city of Los Angeles contains the most active Hezbollah presence in this country (Detroit is their "traditional" U.S. base of operations). Los Angeles also happens to be home to the largest ethnic Iranian population outside of Iran itself.

Law enforcement officials have observed a striking convergence of crime and terror. Hezbollah's nexus with criminal activity is greater than that of any other terrorist group. These links, including with gangs and cartels, generate new possibilities for outsourcing, and new networks that can facilitate terrorist travel, logistics, recruitment, and operations. Authorities have noted significant terrorist interest in tactics, techniques, and procedures used to smuggle people and drugs into the United States from Mexico. According to Texas State Homeland Security Director, Steve McCraw, Hezbollah operatives were captured trying to cross the border in September 2007.[2]

---

[1] Immigration and Customs Enforcement, DHS. "Indictment charges 4 with conspiracy to support Hezbollah 6 others charged with related crimes," press release, November 24, 2009. Accessed 4/23/12 *http://www.ice.gov/news/releases/0911/091124philadelphia.htm*; Mike Newall, "Road to terrorism arrests began at Deptford Mall, Moussa Ali Hamdan's meeting in 2007 with an undercover FBI informant led to the indictment of 26 with alleged Hezbollah ties," *The Philadelphia Inquirer,* January 25, 2010. Accessed 4/23/12 *http://articles.philly.com/2010-01-25/news/25210171_1_hezbollah-fbi-informant-indictment*; and Anti-Defamation League, "Four Men Indicted in Philadelphia for Attempting to Support Hezbollah," modified 6/16/2010. Accessed 4/23/12 *http://www.adl.org/main_Terrorism/philadelphia_hezbollah_indictment.htm*.

[2] "Terrorists have been arrested on the border, security chief says," *Associated Press,* September 13, 2007.

Law enforcement officials also confirm that Shia and Sunni forces are cooperating to an extent. For instance, Shia members of Lebanese Hezbollah and Sunni (Saudi/Iraqi) militant forces are drawing on each other's skills. That said, competition persists even within Shia circles, including between Lebanese Hezbollah and Iran's Quds Force.

These developments suggest that our long-standing frames of reference and the "redlines" they incorporated have shifted. First and foremost: Whereas previously Iran and its proxies targeted U.S. interests and personnel abroad, the cleave between here (the homeland) and overseas is wearing away, as the two fronts merge. The Director of National Intelligence recently stated that Iran is "now more willing to conduct an attack in the United States."[3] His assessment does not stand alone. In a recent hearing before the House Committee on Homeland Security, the NYPD's Director of Intelligence Analysis asserted that "New York City and its plethora of Jewish and Israeli targets could be targeted by Iran or Hezbollah in the event that hostilities break out in the Persian Gulf."[4] At the same hearing, the committee heard from a former Assistant Director of the FBI that Hezbollah's fundraising infrastructure in the United States could serve as a "platform" for launching attacks against the homeland.[5]

With Iran's nuclear program under scrutiny and sanctions, the potential for escalation is heightened. As a result of his policy choices, President Ahmadinejad is under increasing pressure both internationally and domestically.[6] The complexity of the situation is increased by the tendency of Iran and its allies to conflate the United States and our ally Israel in the context of Israeli contingency and attack plans. Events from Baku to Bangkok (referenced above) have been characterized by some analysts as a "shadow war".[7]

The conflict is not limited to the kinetic or to the physical world. In 2010, the Stuxnet worm disabled Iranian centrifuges used to enrich uranium. Attribution for this attack remains unresolved, although speculation has centered on Israel and the United States. The possibility that Iran may feel aggrieved and seek to retaliate, even in the absence of proof of attribution, is not to be dismissed—particularly against the backdrop of ever-tougher U.S. and global sanctions, and historically turbulent (at least as measured in decades) bilateral relations with the United States. The recent SWIFT sanctions have proven particularly effective in crippling Iran's financial system, adding further pressure.[8] Iran is also grappling with Duqu, a worm which seems "designed to gather data to make it easier to launch future cyber attacks."[9]

With Stuxnet, the virtual and real worlds collided, as the worm caused physical damage to infrastructure. Former head of the CIA and the NSA, General Michael Hayden, has (rightly I would suggest) characterized Stuxnet as both "a good idea" and "a big idea"—suggesting also that it represents a crossing of the Rubicon in that "someone has legitimated this type of activity as acceptable."[10] The vulnerability to cyber attack of critical systems, including nuclear facilities and supervisory control & data acquisition (SCADA)/industrial control systems—with concomitant possibility of loss of life, and less than fatal but still serious and widespread con-

---

[3] Testimony of James R. Clapper before the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the U.S. Intelligence Community,* January 31, 2012, Washington, DC. Accessed 4/18/2012 *http://www.dni.gov/testimonies/20120131_testimony_ata.pdf*.

[4] Testimony of Mitchell D. Silber before the U.S. House of Representatives Committee on Homeland Security, *Iran, Hezbollah, and the Threat to the Homeland,* March 21, 2012, Washington, DC. Accessed 4/16/2012 *http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Silber.pdf*.

[5] Testimony of Chris Swecker before the U.S. House of Representatives Committee on Homeland Security, *Iran, Hezbollah, and the Threat to the Homeland,* March 21, 2012, Washington, DC. Accessed 4/22/2012 *http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Swecker.pdf*.

[6] Rick Gladstone and Alan Cowell, "Iran's President Unfazed in Parliamentary Grilling," *The New York Times,* March 14, 2012. Accessed 4/18/12 *http://www.nytimes.com/2012/03/15/world/middleeast/iran-ahmadinejad-questioned-before-parliament-majlis.html?_r=1&page-wanted=all*.

[7] Andrew R.C. Marshall and Peter Apps, "Iran 'shadow war' intensifies, crosses borders," *Reuters,* February 16, 2012. Accessed 4/17/12 *http://www.reuters.com/article/2012/02/16/us-iran-israel-security-idUSTRE81F1E720120216*.

[8] Corey Flintoff, "New Sanctions Severely Limit Iran's Global Commerce," *NPR,* March 19, 2012. Accessed 4/18/12. *http://www.npr.org/2012/03/19/148917208/without-swift-iran-adrift-in-global-banking-world*.

[9] Yaakov Katz, "Iran Embarks on $1b. cyber-warfare program," *The Jerusalem Post,* December 18, 2011. Accessed 4/16/12. *http://www.jpost.com/Defense/Article.aspx?id=249864*.

[10] "Fmr. CIA head calls Stuxnet virus 'good idea,'" *60 Minutes,* March 1, 2012. Accessed 4/20/12. *http://www.cbsnews.com/8301-18560_162-57388982/fmr-cia-head-calls-stuxnet-virus-good-idea/*.

sequences—raises a host of implications for U.S. National and homeland security. Potential targets are many and varied, and extend to critical sectors such as finance and telecommunications. Assistant to the President for Homeland Security and Counterterrorism, John O. Brennan, has stated that U.S. water and power systems are under cyber attack almost daily.[11] Press reports also suggest that the U.S. nuclear industry has experienced up to 10 million cyber attacks.[12] Even if only one attempt were to succeed, the magnitude of the impact could significantly undermine, if not shatter, trust and confidence in the system. In addition, cyber capabilities may be used as a force multiplier in a conventional attack.

The good news is that Iran is not as sophisticated as China or Russia insofar as computer network exploitation (CNE), cyber attack, and warfare capabilities are concerned (to be distinguished from intent). As yet, Iran has not shown itself to be a similarly advanced or persistent threat.[13] This is not to give Iran a pass. To the contrary, U.S. officials are investigating "reports that Iranian and Venezuelan diplomats in Mexico were involved in planned cyber attacks against U.S. targets, including nuclear power plants." Press reports based on a Univision (Spanish TV) documentary that contained "secretly recorded footage of Iranian and Venezuelan diplomats being briefed on the planned attacks and promising to pass information to their governments," allege that "the hackers discussed possible targets, including the FBI, the CIA and the Pentagon, and nuclear facilities, both military and civilian. The hackers said they were seeking passwords to protected systems and sought support and funding from the diplomats."[14]

Cyberspace largely levels the playing field, allowing individuals and small groups to have disproportionate impact. This asymmetry can be leveraged by nation-states that seek to do us harm, by co-opting or simply buying/renting the services and skills of criminals/hackers to help design and execute cyber attacks against the United States. For example, do-it-yourself code kits for exploiting known vulnerabilities are easy to find and even the Conficker worm (variants of which still lurk, forming a botnet of approximately 1.7 million computers) was rented out for use.[15] In short, no comfort can be taken from the fact that Iran lacks the sophistication of nations such as China, Russia, or the United States. Proxies for cyber capabilities are available. There exists an arms bazaar of cyber weapons. Adversaries do not need capabilities, just intent and cash.

Iran has a long history of demonstrated readiness to employ proxies for terrorist purposes, drawing on kinetic means. There is little, if any, reason to think that Iran would hesitate to engage proxies to conduct cyber strikes against perceived adversaries. To paraphrase Mark Twain, history may not repeat itself, but it does tend to rhyme. Elements of the IRGC have openly sought to pull hackers into the fold;[16] and the Basij, who are paid to do cyber work on behalf of the regime, provide much of the manpower for Iran's cyber operations.[17] As in the physical world however, we must keep in mind when crafting security solutions and response mechanisms that Iran is not monolithic: Command-and-control there is murky, even within the IRGC, let alone what is outsourced. The attribution challenge associated with cyber space is therefore all the more complicated where Iran is concerned. Smoking keyboards are hard to find. Cyber space is a domain made for plausible deniability.

In addition to hired or acquired cyber capabilities, the Government of Iran is, according to press reports, investing heavily ($1 billion) to develop and build out its

---

[11] John O. Brennan, "Time to protect against dangers of cyberattack," *The Washington Post,* April 15, 2012. Accessed 4/23/12. *http://www.washingtonpost.com/opinions/time-to-protect-against-dangers-of-cyberattack/2012/04/15/gIQAdJP8JT_story.html.*

[12] Jason Koebler, "U.S. Nukes face up to 10 miilion cyber attacks daily," *US News & World Report,* March 20, 2012. Accessed 4/24/12. *http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily.*

[13] But note Google executive Eric Schmidt's statement: "Iranians are unusually talented [at cyber warfare] for some reason we don't fully understand." "Google admits Iranian superiority in cyber warfare," *Payvand,* December 18, 2011. Accessed 4/17/12. *http://www.payvand.com/news/11/dec/1189.html*

[14] Shaun Waterman, "U.S. authorities probing alleged cyberattack plot by Venezuela, Iran," *The Washington Times,* December 13, 2011. Accessed 4/18/12 *http://www.washingtontimes.com/news/2011/dec/13/us-probing-alleged-cyberattack-plot-iran-venezuela/?page=all.*

[15] Conficker Working Group, "Conficker Working Group: Lessons Learned," accessed 4/18/12 *http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_-_Lessons_Learned_17_June_2010_final.pdf*

[16] Golnaz Esfandiari, "Iran Says it Welcomes Hackers Who Work for Islamic Republic," *Radio Free Europe,* March 07, 2011. Accessed 4/18/12. *http://www.rferl.org/content/iran_says_it_welcomes_hackers_who_work_for_islamic_republic/2330495.html*

[17] "The Role of the Basij in Iranian Cyber Operations," *Internet Haganah,* March 24, 2011. Accessed 4/17/12. *http://internet-haganah.com/harchives/007223.html.*

own cyber war capabilities, both offense and defensive.[18] There is evidence that at the heart of IRGC cyber efforts one will find the Iranian political/criminal hacker group "Ashiyane."[19] In late 2009 and early 2010, hackers calling themselves the Iranian Cyber Army struck Twitter and the Chinese search engine Baidu.[20] The group also appears to have struck Iranian websites managed by the opposition Green Movement, with deleterious results for the opposition's ability to coordinate its activities.[21] The high visibility of these attacks suggests that the Iranian Cyber Army and similar groups might be utilized as proxies by Iran's Islamic Revolutionary Guard Corps. In the event of a conflict in the Persian Gulf, similar attacks on public-facing websites could provide Iran an avenue for psychological operations directed against the U.S. public. Though fluid, hacker groups could be cultivated and guided—if not directly managed—by the IRGC. Iran's ability to conduct Electronic Warfare, including the jamming and spoofing of radar and communications systems, has been enhanced through its acquisition of advanced jamming equipment. In the event of a conflict in the Persian Gulf, Iran might hope to combine electronic and computer network attack methods to degrade U.S. and allied radar systems, complicating both offensive and defensive operations. [22]

There is also an Iranian "cyber police force"[23] that blocks "foreign websites and social networks deemed a threat to national security," with overall policy guidance provided by "The Supreme Council of Virtual Space."[24] Interestingly, a distributed denial of service (DDoS) attack against the BBC this year happened to "coincide with efforts to jam two of the service's satellite feeds in Iran."[25] There has also been considerable speculation about Government of Iran involvement in a number of hacking incidents including against Voice of America, and a Dutch firm in the business of issuing security certificates. Fallout from the latter was significant and affected a range of entities including western intelligence and security services, Yahoo, Facebook, Twitter, and Microsoft.[26]

Not surprisingly, Iran is trying to make its cyber capabilities appear truly muscular. When a U.S. drone fell into Iranian hands in December 2011, Iranian officials were quick to claim that it was brought down by "electronic ambush of the armed forces."[27] The facts surrounding this incident are not all known, but from what U.S. authorities suggest, it seems that the drone likely malfunctioned, and perhaps was also affected by jamming efforts. Regardless, the fact that Iranian officials went public about their supposed capabilities suggests that they plan to do something significant by cyber means, or else they risk losing credibility.

In June 2011, Hezbollah too entered the fray, establishing the Cyber Hezbollah organization. Law enforcement officials note that the organization's goals and objectives include training and mobilizing pro-regime (that is, Government of Iran) activists in cyber space. In turn and in part, this involves raising awareness of, and schooling others in, the tactics of cyber warfare. Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. Even worse, each such exploit generates additional opportunities to gather yet more data, as new po-

---

[18] Yaakov Katz, "Iran embarks on $1b. cyber-warfare program," *The Jerusalem Post,* December 18, 2011. Accessed 4/18/12 *http://www.jpost.com/Defense/Article.aspx?id=249864*.

[19] Iftach Ian Amit, "Cyber[Crime/War]," paper presented at DEFCON 18 conference, July 31, 2010.

[20] Robert Mackey, "'Iranian Cyber Army' Strikes Chinese Sites," *The Lede* (NYT Blog), January 12, 2010; Scott Peterson, "Twitter hacked: 'Iranian Cyber Army' signs off with poem to Khamenei," *Christian Science Monitor,* December 18, 2009.

[21] Robert F. Worth, "Iran: Opposition Web Site Disrupted," *The New York Times,* December 18, 2009.

[22] Michael Puttre, "Iran bolsters naval, EW power," *Journal of Electronic Defense* vol. 25 no. 4 (April 2002): 24; Robert Karniol, "Ukraine sells Kolchuga to Iran," *Jane's Defense Weekly,* vol. 43 no. 39 (September 27, 2006): 6; Stephen Trimble, "Avtobaza: Iran's weapon in alleged RQ-170 affair?" *The DEW Line,* December 5, 2011. Accessed 4/23/12 *http://www.flightglobal.com/blogs/the-dewline/2011/12/avtobaza-irans-weapon-in-rq-17.html*.

[23] Thomas Erdbrink, "Iran cyber police cite U.S. threat," *The Washington Post,* October 29, 2011. Accessed 4/18/12 *http://www.washingtonpost.com/world/middle_east/iran-cyber-police-cite-us-threat/2011/10/27/gIQA1yruSM_story.html*.

[24] "Cyber-attack on BBC leads to suspicion of Iran's involvement," *BBC News,* March 14, 2012. Accessed 4/17/12. *http://www.bbc.co.uk/news/technology-17365416*.

[25] "Cyber-attack on BBC leads to suspicion of Iran's involvement," *BBC News,* March 14, 2012.

[26] Kevin Kwang, "Spy agencies hit by CA hack; Iran suspected," *ZDNet Asia,* September 5, 2011. Accessed 4/18/12. *http://www.zdnetasia.com/spy-agencies-hit-by-ca-hack-iran-suspected-62301930.htm*. See also Bill Gertz, "Iranians hack into VOA website," *The Washington Times,* February 21, 2011. Accessed 4/19/12. *http://www.washingtontimes.com/news/2011/feb/21/iranian-hackers-break-voa-deface-web-sites/*.

[27] Thomas Erdbrink, "Iran shows alleged downed US drone," *The Washington Post,* December 8, 2011. Accessed 4/18/12. *http://www.washingtonpost.com/blogs/blogpost/post/iran-shows-alleged-downed-us-drone/2011/12/08/gIQAKciXfO_blog.html*.

tential targets are identified, and tailored methods and means of approaching them are discovered and developed.

Given all the above evidence of (both conventional and cyber) capability and intent on the part of Iran and its proxies, the United States requires a robust posture. There are steps we can take to shore up our stance and create a more solid platform for proactive and, if necessary, reactive purposes. From a counterterrorism and intelligence standpoint, it is crucial to focus on and seek to enhance all-source intelligence efforts. Such is the key to refining our understanding of the threat in its various incarnations, and to facilitating the development and implementation of domestic tripwires designed to thwart our adversaries and keep us "left of boom."[28] Disruption should be our goal. Planning and preparation to achieve this end includes information gathering and sharing—keeping eyes and ears open at home and abroad to pick up indications and warnings (I&W) of attack, and reaching out to and partnering with State and local authorities as well as technical and academic communities. Outreach to respected leaders in the community is essential to keep channels open, build trust, and foster mutual assistance. These dialogues should take place across the board, and not just in major metropolitan centers. The history of the Conficker Working Group, captured in a DHS-sponsored lessons learned document, provides examples of the types of relationships that need to be established and maintained.[29]

Searching for I&W will require fresh thinking that identifies and pursues links and patterns not previously established. The above-described nexus between terrorist and criminal networks offers new possibilities to exploit for collection and analysis. To take full advantage, we will have to hit the beat hard, with local police tapping informants and known criminals for leads. State and local authorities can and should complement what the Federal Government does not have the capacity or resources to collect, and thereby help determine the scope and contours of threat domains in the United States. Further leveraging our decentralized law enforcement infrastructure could also serve to better power our Fusion Centers. The post-9/11 shift of U.S. law enforcement resources away from "drugs and thugs" toward counterterrorism is, ironically, in need of some recalibration in order to serve counterterrorism aims. For the last decade, furthermore, U.S. Government analysts have (understandably) focused on al-Qaeda, resulting in a shallower pool of U.S. intelligence on Hezbollah. Recent incidents cited above may provide insight into current tactics, techniques, and procedures, and we should comb through further to mine for and learn possible lessons.

Officials in the homeland security community must undertake contingency planning that incorporates attacks on U.S. infrastructure. At minimum, "red-teaming" and additional threat assessments are needed. The latter should include modalities of attack (such as cyber, and attacks on our critical infrastructures) and potential consequences.

From the perspective of cybersecurity and infrastructure protection, the United States should develop and clearly articulate a cyber-deterrence strategy. Computer network exploitation directed against us is presently a major issue—we are losing billions of dollars in intellectual property as a result. Even more ominous are adversary efforts underway to engage in the cyber equivalent of intelligence preparation of the battlefield, again to be used against us.[30] There is simply no other explanation for the nature and extent of the activity that we have seen so far. Yet, insofar as our response posture is concerned, the current situation is arguably the worst of all worlds: Certain adversaries have been singled out in Government documents released in the public domain, yet it is not altogether clear what we are doing about these activities directed against us.[31] The better course would be to undertake and

---

[28] Frank J. Cilluffo, Sharon Cardash, and Michael Downing, "Is America's View of Iran and Hezbollah Dangerously Out of Date?" *FoxNews.com,* March 20, 2012. Accessed 4/18/12 *http://www.foxnews.com/opinion/2012/03/20/is-americas-view-iran-and-hezbollah-dangerously-outdate/*.

[29] Conficker Working Group, "Conficker Working Group: Lessons Learned," accessed 4/18/12 *http://www.confickerworkinggroup.org/wiki/uploads/Conficker__Working__Group__-Lessons__Learned__17__June__2010__final.pdf*.

[30] Nick Hopkins, "Militarisation of Cyberspace: how the global power struggle moved online," *The Guardian,* April 16, 2012. Accessed 4/17/12. *http://m.guardian.co.uk/technology/2012/apr/16/militarisation-of-cyberspace-power-struggle?cat=technology&type=article*; and *http://m.guardian.co.uk/technology/2012/apr/16/us-china-cyber-war-games?cat=technology&type=-article*.

[31] See Bryan Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (Report, U.S.-China Security and Review Commission, 2011); Office of the National Counterintelligence Executive, *Foreign Spies Stealing U.S. Secrets in Cyberspace: Report to Congress on Foreign Economic Collection, 2009–2011* (Washington, DC: NCIX, 2011) for the espionage activities of China and Russia in particular.

implement a cyber-deterrence policy that seeks to dissuade, deter, and compel both as a general matter, and in a tailored manner that is actor/adversary-specific. A solid general posture could serve as an 80 percent solution, neutralizing the majority of threats before they manifest fully. This would free up resources (human, capital, technological, etc.) to focus in context-specific fashion on the remainder, which constitute the toughest threats and problems, in terms of their level of sophistication and determination. To operationalize these recommendations, we must draw lines in the sand or, in this case, the silicon. Preserving flexibility of U.S. response by maintaining some measure of ambiguity is useful, so long as we make parameters clear by laying down certain markers or selected redlines whose breach will not be tolerated. The entire exercise must, of course, be underpinned by all-source intelligence. Lest the task at hand seem overly daunting, remember that we have in past successfully forged strategy and policy in another new domain devoid of borders, namely outer space.

Sometimes, however, the best defense is a good offense. Yet the U.S. cyber offense to defense ratio, at least as represented in the public domain, has skewed overwhelmingly to defense.[32] There are some signs of late that this may be changing, including newspaper reports suggesting that rules of engagement regarding cyber attacks are being developed, and that the Department of Defense is seeking to bolster its arsenal of cyber weapons.[33] These are encouraging developments, if true, because having a full complement of instruments in our toolkit, and publicizing that fact (minus the details), will help deter potential adversaries—provided that we also signal a credible commitment to enforcing compliance with U.S. redlines. Again history provides guidance, suggesting two focal points upon which we should build our efforts. One is leadership—we must find the cyber equivalents of Billy Mitchell or George Patton, leaders who understand the tactical and strategic uses of new technologies and weapons. The other is force protection—not only must we develop offensive capabilities, but we ought to make sure we develop second-strike capabilities. We cannot simply firewall our way out of the problem. U.S. Cyber Command must both lend and receive support, if our cyber doctrine is to evolve smartly and if our cyber power is to be exercised effectively.

While it is up to the Government to lead by example by getting its own house in order, cybersecurity and infrastructure protection do not constitute areas where Government can go it alone. With the majority of U.S. critical infrastructure owned and operated privately, robust public-private partnerships are essential, as is a companion commitment by the private sector to take the steps necessary to reinforce national and homeland security. Government and industry must demonstrate the will and leadership to take the tough decisions and actions necessary in this sphere.

Lest the incentives to do so not be clear to all by now, consider the words of the FBI's then-executive assistant director responsible for cybersecurity, Shawn Henry, who said: "We're not winning." He illustrated his conclusion by citing a company that, due to hackers, lost 10 years of effort (R&D) and the equivalent of $1 billion.[34] While we cannot expect the private sector to defend itself alone from attacks by foreign intelligence services, we need to do a better job (as a country) of making the business case for cybersecurity. Failure to shore up our vulnerabilities has National security implications. Yet crucial questions remain open, such as how much cybersecurity is enough, and who is responsible for providing it?

The facts in this case support the need for standards, as identified and self-initiated (along with best practices) by the private sector, across critical industries and infrastructures, together with an enforcement role for Government, to raise the bar higher—in order to protect and promote, not stifle, innovation. The economic and intellectual engines that made this country what it is today are, arguably, our great-

---

[32] For comments by GEN James Cartwright, USMC, to this effect, see Julian E. Barnes and Siobhan Gorman, "Cyberwar Plan Has New Focus on Deterrence," *The Wall Street Journal,* July 15, 2011. Accessed 4/23/12 *http://online.wsj.com/article/SB10001424052702304521304576446191468181966.html*

[33] Cheryl Pellerin, "DOD Develops Cyberspace Rules of Engagement," American Forces Press Service, March 20, 2012. Accessed 4/23/12 *http://www.defense.gov/news/newsarticle.aspx?id=67625*; Zachary Fryer-Briggs, "U.S. Military Goes on Cyber Offensive," *Defense News,* March 24, 2012. Accessed 4/23/12 *http://www.defensenews.com/article/20120324/DEFREG02/303240001/U-S-Military-Goes-Cyber-Offensive*. See also Testimony of GEN Keith Alexander, USA, before the U.S. House of Representatives Committee on Armed Services, *Fiscal Year 2013 Budget Request for Information Technology and Cyber Operations Programs,* March 20, 2012. Accessed 4/23/12 *http://armedservices.house.gov/index.cfm/hearings-display?ContentRecord_id=92823c77-38f0-4c20-a3ee-36729e8e19a3*.

[34] Devlin Barrett, "U.S. Outgunned in Hacker War," *The Wall Street Journal,* March 28, 2012. Accessed 4/18/12 *http://online.wsj.com/article/SB10001424052702304177104577307773326180032.html*

est resource. They will power us into the future too, so long as we act wisely and carefully to foster an environment in which they can continue to thrive and grow. To be blunt, legislation of the type described is needed, and it is needed now, in order to remedy crucial gaps and shortfalls, and hold critical infrastructure owners and operators accountable, by focusing on behavior rather than regulating technology.

At the same time, a mix of incentives is needed, to include tax breaks, liability protections, and insurance premium discounts, for private owners and operators of critical infrastructure to take the steps needed to help improve our overall level of security. These measures must also be accompanied by a mechanism to enable and encourage information sharing between the public and private sectors. In addition, as former director of national intelligence, Admiral Mike McConnell, has suggested, the information exchanged must be "extensive, . . . sensitive and meaningful," and the sharing must take place in "real-time" so as to match the pace of the cyber threat. There must be "tangible benefits" for those yielding up the information.[35]

In conclusion, now is the time to act. For too long, we have been far too long on nouns, and far too short on verbs. Again, I wish to thank both subcommittees and their staff for the opportunity to testify today, and I would be pleased to try to answer any questions that you may have.

Mr. MEEHAN. Thank you, Mr. Cilluffo. That might be something you want to develop further in your—in your response to questions. Mr. Berman, we now recognize you for 5 minutes. Thank you.

STATEMENT OF ILAN BERMAN, VICE PRESIDENT, AMERICAN FOREIGN POLICY COUNCIL

Mr. BERMAN. Thank you, sir, and let me start by thanking you, Mr. Chairman, and thanking Chairman Lungren for holding this hearing. Like my colleague, I am appreciative of the fact that this is a synergistic problem and it is one that lends itself to a synergistic solution rather than simply holding one-off events. Let me also say by way of starting, that I am a subject-matter specialist in Iran, rather than infrastructure protection or cybersecurity, so I am going to focus my remarks on the political and the strategic aspects of the emerging Iranian cyber threat.

Let me start by saying that I think the question that is being posed increasingly here within the Washington Beltway is whether or not Iran poses a real and immediate cyber threat to the United States, and the conventional wisdom here is that it doesn't because Iran is squeezed by increasingly harsh economic sanctions from the United States and the European Union and others, and also because Iran, as a result, is weathering significant domestic socioeconomic malaise. But for those very same reasons, I would make the argument that Iranian action against the United States, particularly asymmetric action against the United States, is more rather than less likely. If you look at the Iranian—the way the Iranians approach cyber space, they are essentially looking at two geopolitical drivers that are animating their focus and their attention. The first has to do with domestic repression. The Iranian regime is erecting what President Obama recently called an electronic curtain around its population and it is doing so through the construction of a National intranet to essentially supplant and cordon off Iranian access to the world wide web. It is doing so through the passage of new restrictive regulations and rules governing internet usage, public internet usage. It is doing so through the passage of

[35] VADM J. Michael McConnell, USN (Ret.), remarks given February 22, 2012 at Homeland Security Policy Institute, The George Washington University, Washington, DC. Transcript and video accessed 4/23/12 *http://www.c-spanvideo.org/program/CyberSecurityL.*

penalties relating to content that is deemed inappropriate by the Iranian regimes—Iranian regime, and is doing so through the installation, acquisition, and installation of technologies, foreign origin technologies, such as Chinese origin technologies for the monitoring, filtering, and limiting of access to the internet.

This focus on the part of the Iranian regime, began in earnest after June 2009, when the fraudulent re-election of Iranian President Mahmoud Ahmadinejad catalyzed a groundswell of opposition from the Iranian street. The Iranian opposition elements at the time leveraged the internet extensively in their protests, and as a result, the Iranian regime responded in that domain as well.

It has been successful. If you look over the last year or so, it is very clear that the Iranian Green Movement as it is called, has migrated into the ether. It has migrated into the internet, and the regime has followed them there. If you look at the new restrictions that are being passed by the Iranian regime in terms of access to Facebook, and Twitter, and other accounts, it is very clear that the competition and contest between Iran and its opposition is much more virtual now than it is actually on the streets, but it is still there.

This focus, though, has been confirmed by what has happened in the Middle East over the last year. The Arab Spring has been touted by Iran as a victory for the Ayatollah Khomeini Islamic Revolution, but in practical terms, the anti-regime sentiment that is embodied by the turmoil that has taken place in Tunisia, and Libya, and Egypt is taking place now in Syria and elsewhere, poses a mortal threat to the Iranian regime on a number of levels. As a result, the Arab Spring has confirmed to them the need to clamp down domestically and isolate their population from these outside sources.

The second, and for the purposes of this committee, I think more important geopolitical driver of Iran's interest has to do with the asymmetric conflict that is already occurring over Iran's nuclear program. We heard earlier in the opening statements about the application of Stuxnet, and Stuxnet is one of at least three, possibly more, cyber attacks against—discrete cyber attacks that have taken place against the Iranian nuclear program over the last 2 years or so.

In policy circles in Washington the question of attribution, where Stuxnet and these other malwares came from, who has deployed them, is still an open question. But from the Iranian perspective, it is not. It is very clear for Iran, that the west writ large has launched an asymmetric attack on the Iranian nuclear program and it is mobilizing as a response, mobilizing through the creation of a $1 billion program to ramp up its cyber defense and cyber offense capabilities, the construction of a cyber army of sympathetic hacktivists, and leveraging attacks against entities such as Twitter, such as the Chinese search engine Baidu, such as the BBC. This all shows a very clear pattern of increasingly aggressive behavior, and it underscores, I think, a fundamental point, which is that Iran appears to be moving increasingly from defense to offense in terms of how it thinks about cyber space.

In the opening remarks, Chairman Meehan, you referenced the assessment of General Clapper, about how Iran has become increasingly bold in its strategy. I would make the argument that

this represents nothing less than a seismic shift in terms of how Iran thinks about the U.S. homeland. In his testimony, General Clapper talked about the fact that Iranian officials, probably including the Supreme Leader Ali Khamenei himself, have changed their calculus and are now willing to conduct an attack on the United States. This has salience with regard to the attempted foiled attack in October 2001 against the Saudi Ambassador in Washington, but increasingly, it is likely to manifest itself in other ways as well, including in the cyber realm. Here Iran has significant capability, and significant intent.

Last summer, for example, a hard-liner Iranian newspaper affiliated with the Revolutionary Guard, warned the United States, that America no longer has the "exclusive capability in cyber space and it has underestimated the Islamic Republic," and now needs to worry about "an unknown player somewhere in the world attacking a section of its critical infrastructure."

Are we ready for this? This is, I think, the most salient question of all. The past year has seen a dramatic expansion on the part of the United States in terms of Governmental awareness of cyber space as a domain for conflict. But this attention is still uneven, I would argue. It focuses largely on network protection and resiliency, particularly in the military arena, and on threat capabilities from China, and from Russia. Serious institutional awareness of the threat from Iran and the cyber warfare potential of Iran, has lagged behind the times and so has the Governmental response to it.

So why does this matter? I would argue that it matters for three reasons: First of all, it matters because operationally, an Iranian cyber attack may look similar to a Chinese cyber attack, or a Russian cyber attack, but there are key differences. The first is with regard to targeting objects. Iran has, in both its public statements and its writings, talked extensively about U.S. critical infrastructure.

Mr. MEEHAN. Mr. Berman, can I do this? I am going to pursue that specific line of questioning with you as soon as I have an opportunity. I want you to articulate more on that. Allow me to move with Mr. Caslow at this point in time, and we will return to that.

Mr. BERMAN. Absolutely, thank you, sir.

[The prepared statement of Mr. Berman follows:]

PREPARED STATEMENT OF ILAN BERMAN

APRIL 26, 2012

Congressman Lungren, Congressman Meehan, distinguished Members of the subcommittees: Thank you for the opportunity to appear before you today to address the cyber warfare capabilities of the Islamic Republic of Iran, and the threat that they pose to the U.S. homeland.

Conventional wisdom suggests that the Iranian regime, now being squeezed significantly by sanctions from the United States and Europe and grappling with significant domestic socio-economic malaise, is far from an imminent threat to the American homeland (even if it does present a vexing foreign policy challenge for the United States and its allies). Yet, over the past 3 years, the Iranian regime has invested heavily in both defensive and offensive capabilities in cyber space. Equally significant, its leaders now increasingly appear to view cyber warfare as a potential avenue of action against the United States.

IRANIAN CAPABILITIES IN GEOPOLITICAL CONTEXT

Iran's expanding exploitation of cyber space can be attributed to two principal geopolitical drivers.

The first are the Iranian regime's efforts to counter Western influence and prevent the emergence of a "soft revolution" within its borders. In his March 2012 Nowruz message to the Iranian people, President Obama alluded to the growing efforts of the Iranian regime to isolate its population from the outside world when he noted that an "electronic curtain has fallen around Iran."[1] That digital barrier has grown exponentially over the past 3 years, as Iran's leadership has sought to quell domestic dissent and curtail the ability of its opponents to organize.

The proximate cause of this effort was the fraudulent June 2009 reelection of Mahmoud Ahmadinejad to the Iranian presidency, which catalyzed a groundswell of domestic opposition that became known colloquially as the "Green Movement." In the months that followed, Iran's various opposition elements relied extensively on the internet and social networking tools to organize their efforts, communicate their messages to the outside world, and rally public opinion to their side. In turn, the Iranian regime utilized information and communication technologies extensively in its suppression of the protests—and thereafter has invested heavily in capabilities aimed at controlling the internet and restricting the ability of Iranians to access the world wide web.[2]

This focus has only been reinforced by recent revolutionary fervor throughout the Middle East and North Africa. For while Iranian authorities have sought to depict the so-called "Arab Spring" as both the start of an Islamic awakening and an affirmation of their regime's worldview,[3] the anti-regime sentiment prevalent in the region actually represents a mortal threat to their corrupt, unrepresentative regime. As a result, the past year has seen a quickening of the regime's long-running campaign against "Western influence" within the Islamic Republic. These efforts include:

- The construction of a new, "halal" national internet. This "second internet," which will effectively sever Iran's connection to the world wide web by routing web users to pre-approved, Iranian-origin sites, is currently expected to come on-line by late summer 2012.[4]
- Installation of a sophisticated Chinese-origin surveillance system for monitoring phone, mobile, and internet communications.[5]
- The passage of new, restrictive governmental "guidelines" forcing internet cafes to record the personal information of customers—including vital data such as names, national identification numbers, and phone numbers—as well the installation of closed-circuit cameras to keep video logs of all customers accessing the world wide web.[6]
- Movement toward the formation of a new government agency to monitor cyber space. Once operational, this "Supreme Council of cyber space," which will be headed by top officials from both Iran's intelligence apparatus and the Revolutionary Guards, will be tasked with "constant and comprehensive monitoring over the domestic and international cyber space," and be able to issue sweeping decrees concerning the internet that would have the full strength of law.[7]

The second geopolitical driver of Iran's interest in cyber space relates to the expanding conflict with the West over its nuclear ambitions. Since the fall of 2009,

---

[1] White House, Office of the Press Secretary, "Remarks of President Obama Marking Nowruz," March 20, 2012, *http://www.whitehouse.gov/the-press-office/2012/03/20/remarks-president-obama-marking-nowruz.*

[2] See, for example, Saeid Golkar, "Liberation or Suppression Technologies? The Internet, the Green Movement and the Regime in Iran," *International Journal of Emerging Technologies and Society* 9, no. 1 (2011), 50–70, *http://www.swinburne.edu.au/hosting/ijets/journal/V9N1/pdf/Article%204%20Golkar.pdf.*

[3] "Khamenei Credits Iranian Revolution With Fuelling Egyptian Revolt," *Reuters,* February 4, 2011, *http://www.thenational.ae/news/world/middle-east/khamenei-credits-iranian-revolution-with-fuelling-egyptian-revolt;* Robert F. Worth, "Efforts To Rebrand Arab Spring Backfires In Iran," *New York Times,* February 2, 2012, *http://www.nytimes.com/2012/02/03/world/middleeast/effort-to-rebrand-arab-spring-backfires-in-iran.html?pagewanted=all.*

[4] See Steven Musil, "Iran Expected To Permanently Cut Off Internet By August," *CNET,* April 9, 2012, *http://news.cnet.com/8301-1023_3-57411577-93/iran-expected-to-permanently-cut-off-internet-by-august/.*

[5] Steve Stecklow, "Special Report: Chinese firm helps Iran spy on citizens," *Reuters,* March 22, 2012, *http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B8-20120322.*

[6] *Radio Free Europe,* January 4, 2012.

[7] Ramin Mostaghim and Emily Alpert, "Iran's Supreme Leader Calls for New Internet Oversight Council," *Los Angeles Times,* March 7, 2012, *http://latimesblogs.latimes.com/world_now/2012/03/iran-internet-council-khamenei.html.*

Iran has suffered a series of sustained cyber attacks on its nuclear program. The most well-known of these is Stuxnet, the malicious computer worm that attacked the industrial control systems at several Iranian nuclear installations, including the uranium enrichment facility at Natanz, between late 2009 and late 2010. At the height of its effectiveness, Stuxnet is estimated to have taken 10 percent or more of Iran's 9,000 then-operational centrifuges off-line.[8]

Stuxnet has been followed by at least two other cyber attacks aimed at derailing Iran's nuclear development. "Stars," a software script targeting execution files, was uncovered by the Iranian regime in April 2011.[9] Subsequently, "Duqu," a malware similar to Stuxnet and aimed at gaining remote access to Iran's nuclear systems, was identified in October/November 2011.[10]

Publicly, the origins of these intrusions are still an open question. Israel has steadfastly denied any role in the authorship of Stuxnet or other cyber attacks, despite widespread speculation to the contrary. The United States, too, has remained silent on the subject, although suspicions abound that the CIA played at least some part in putting together and deploying Stuxnet (and perhaps other malware as well).[11]

For the Iranian regime, however, the conclusion is clear. War with the West, at least on the cyber front, has been joined, and the Iranian regime is mobilizing in response. In recent months, it reportedly has launched an ambitious $1 billion governmental program to boost national cyber capabilities—an effort that involves acquisition of new technologies, investments in cyber defense, and the creation of a new cadre of cyber experts.[12] It has also activated a "cyber army" of activists which, while nominally independent, has carried out a series of attacks on sites and entities out of favor with the Iranian regime, including social networking site Twitter, Chinese search engine Baidu, and the websites of Iranian reformist elements.[13]

CYBERWAR AND IRANIAN STRATEGY

In his testimony to the Senate Select Committee on Intelligence this past January, General James Clapper, the director of national intelligence, alluded to what amounts to a seismic shift in Iranian strategy. In response to growing economic sanctions and mounting pressure from the United States and its allies, he noted, "Iranian officials—probably including Supreme Leader Ali Khamenei—have changed their calculus and are now willing to conduct an attack in the United States."[14]

Gen. Clapper was referring, most directly, to the foiled October 2011 plot by Iran's Revolutionary Guards to assassinate Saudi Arabia's envoy to the United States in Washington, DC. But, as the international crisis over Iran's nuclear ambitions continues to deepen, Iran's cyber capabilities should be a matter of significant concern as well. Experts have warned that, should the standoff over Iran's nuclear program precipitate a military conflict, Iran "might try to retaliate by attacking U.S. infrastructure such as the power grid, trains, airlines, refineries."[15]

The Iranian regime appears to be contemplating just such an asymmetric course of action. In late July 2011, for example, *Kayhan,* a hardline newspaper affiliated with Iran's Revolutionary Guards, issued a thinly-veiled warning to the United States when it wrote in an editorial that America, which once saw cyber warfare as its "exclusive capability," had severely underestimated the resilience of the Islamic Republic. The United States, the paper suggested, now needs to worry about

---

[8] David Albright, Paul Brannan, and Christina Walrond, "Stuxnet Malware and Natanz: Update of ISIS December 2, 2010 Report," Institute for Science and International Security *ISIS Reports,* February 15, 2011, *http://www.isis-online.org/isis-reports/detail/stuxnet-malware-and-natanz-update-of-isis-december-22-2010-reportsupa-href1/*.

[9] "After Stuxnet: Iran Says It's Discovered 2nd Cyber Attack," *Reuters,* April 25, 2011, *http://www.jpost.com/IranianThreat/News/Article.aspx?id=217795.*

[10] "Iran Says Has Detected Duqu Computer Virus," *Reuters,* November 13, 2011, *http://www.reuters.com/article/2011/11/13/us-iran-computer-duqu-idUSTRE7AC0YP20111113.*

[11] Ralph Langner, "Cracking Stuxnet, a 21st Century Cyber Weapon," TED Talks, March 2011, *http://www.ted.com/talks/ralph__langner__cracking__stuxnet__a__21st__century__cyberweapon.html.*

[12] Yaakov Katz, "Iran Embarks On $1b. Cyber-Warfare Program," *Jerusalem Post,* December 18, 2011, *http://www.jpost.com/Defense/Article.aspx?id=249864.*

[13] Farvartish Rezvaniyeh, "Pulling the Strings of the Net: Iran's Cyber Army," PBS *Frontline,* February 26, 2010, *http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/02/pulling-the-strings-of-the-net-irans-cyber-army.html;* Alex Lukich, "The Iranian Cyber Army," Center for Strategic & International Studies, July 12, 2011, *http://csis.org/blog/iranian-cyber-army.*

[14] James Clapper, testimony before the Senate Select Committee on Intelligence, January 31, 2012.

[15] Brian Ross, "What Will Happen to the US if Israel Attacks Iran?" ABC News, March 5, 2012, *http://abcnews.go.com/Blotter/israel-attacks-iran-gas-prices-cyberwar-terror-threat/story?id=15848522#.T4g5tqvY9Ll.*

"an unknown player somewhere in the world" attacking "a section of its critical infrastructure."[16]

In keeping with this warning, over the past year infrastructure professionals in the United States have noted that Iran's "chatter is increasing, the targeting more explicit, and more publicly disseminated."[17] The Islamic Republic, in other words, increasingly has begun to seriously contemplate cyber warfare as a potential avenue of action against the West.

Iran has significant capacity in this sphere. A 2008 assessment by the policy institute Defense Tech identified the Islamic Republic as one of five countries with significant nation-state cyber warfare potential.[18] Similarly, in his 2010 book *Cyber War,* former National Security Council official Richard Clarke ranks Iran close behind the People's Republic of China in terms of its potential for "cyber-offense."[19] These capabilities, moreover, are growing. In his January 2012 Senate testimony, General Clapper alluded to the fact that Iran's cyber capabilities "have dramatically increased in recent years in depth and complexity."[20]

PREPARING FOR CYBER WAR WITH IRAN

Where does the United States stand with regard to a response? The Obama administration has made cybersecurity a major area of policy focus since taking office in 2009, and the past year in particular has seen a dramatic expansion of Governmental awareness of cyber space as a new domain of conflict. But this attention remains uneven, focused largely on network protection and resiliency (particularly in the military arena), and on the threat capabilities of the People's Republic of China and, to a lesser extent, of the Russian Federation. Serious institutional awareness of, and response to, Iran's cyber warfare potential has lagged behind the times.

Indeed, personal conversations with a range of experts inside and outside of Government reveal a troubling lack of clarity about the Iranian cyber threat—and the absence of serious planning to counter it. While some parts of the Federal bureaucracy (namely U.S. Strategic Command and the State Department's Nonproliferation Bureau) have begun to pay attention to Iran's threat potential in the cyber realm, as yet there exists no individual or office tasked with comprehensively addressing the Iranian cyber warfare threat. The U.S. Government, in other words, has not yet even begun to get ready for cyber war with Iran.

It should. After all, it is not out of the question that the Iranian regime could attempt an unprovoked cyber attack on the United States. As the foiled October 2011 plot against Saudi Arabia's ambassador to the United States indicates, Iran has grown significantly bolder in its foreign policy, and no longer can be relied upon to refrain from direct action in or against the U.S. homeland. Far more likely, however, is a cyber warfare incident related to Iran's nuclear program. In coming months, a range of scenarios—from a renewed diplomatic impasse to a further strengthening of economic sanctions to the use of military force against Iranian nuclear facilities—hold the potential to trigger an asymmetric retaliation from the Iranian regime aimed at vital U.S. infrastructure, with potentially devastating effects.

At the very least, it is clear that policymakers in Tehran are actively contemplating such an eventuality. Prudence dictates that their counterparts in Washington should be doing so as well.

Mr. MEEHAN. Mr. Caslow, I now want to recognize you for your 5 minutes.

STATEMENT OF ROGER L. CASLOW, EXECUTIVE CYBER CONSULTANT, SUSS CONSULTING

Mr. CASLOW. Good morning, and thank you for inviting me to share my testimony today. I do want to emphasize that my background is primarily in the realm of cybersecurity as it relates to computer and network defense. I am not an Iranian subject-matter expert, but I do know how to secure something and lock it down. It is an honor to appear before the joint subcommittee to testify

[16] "STUXNET has Returned Home," *Kayhan* (Iran), July 27, 2011. (Author's collection).
[17] Author's personal communication, August 17, 2011.
[18] Kevin Coleman, "Iranian Cyber Warfare Threat Assessment," Defense Tech, September 23, 2008, *http://defensetech.org/2008/09/23/iranian-cyber-warfare-threat-assessment/*.
[19] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to do About It* (New York: Harper Collins, 2010), 148.
[20] Clapper, testimony before the Senate Select Committee on Intelligence.

about the Iranian cyber threat to the U.S. homeland, and I do hope that my testimony is of benefit to create a better defensive posture against this stated threat.

My colleagues here have already identified the threat. They scoped it out for us. That is good. Looking from a pure vulnerability perspective and how we go forward and how we attack that, according to the 2012 Data Breach Investigations Report from Verizon, 97 percent of all reported data breaches were avoidable through basic level security controls implementation. Now, let me just state, that in order to protect our way of life, we must be prepared to return to the basics of security, not the flashing glitz of a Duqu or a Stuxnet, which I could talk if we wanted to about that, but rather the foundational aspects of cybersecurity.

Once we have secured the basics across all sectors, then and only then can we have the greater certainty that the weakest link is not as exploitable by those who seek to do us harm. Within the field of cybersecurity, this requires ensuring the foundation is secure by knowing what is on and connected to our networks, what our basic security posture is, and what it should be, and ensuring the right people with the right skill sets are building, maintaining, and protecting these assets and data. Furthermore, within the cybersecurity discipline, we require a strong governance structure. Governance is far from the most exciting area of cybersecurity, but it is foundational to ensure better management of our vulnerabilities against our threats. For this to work, we must have clearly defined language, write what is meant, and leave little room for negotiation as possible.

Good governance is required for best performance of our National, State, local, and industrial activities. Good governance supports better integration of cybersecurity and information technology architectures, building in the security requirements up front. Good governance supports the adoption of risk-management-based decisions, which are only as good as the information available to the decision makers responsible for the defense of our interconnected networks, both public and private. I am going to mention Executive Order 13587, which was the structural reforms to improve the security of classified networks. That was a good start, however, I believe it required more teeth, but it also required better integration across all levels to include our industrial partners, less the bureaucracy overrun the implementation.

Another not-too-exciting area, is the emphasis on education, training, and awareness. Education emphasis, not merely on the hard technology engineering skills, but also on the basic critical thinking skills which are lost in many technology disciplines. With respect to training as a Nation, our standards need to be fully matured and established across all sectors.

We can make improvements by leveraging the private-sector security-based and -focused training organizations which are aware of the threats, vulnerability, and respective countermeasures. Basic awareness of the threats posed to all sectors and elements to our society is also important. We still have too many people who are ignorant of the threats, and become caught in phishing, spear phishing, social engineering, and other types of manipulation, exploitation, and exfiltration schemes.

Again, all sectors are important and require some level of targeted awareness campaigns. I consider it more of an op-sec, or an operational security against a cyber attack. Now, there is a National initiative for cybersecurity education which evolved from the Comprehensive National Cybersecurity Initiative, was intended to address many of these education training and awareness issues, but has not taken root. I fully understand the concept of measure twice and cut once, but when we face the threats we do as a Nation, the 85 percent solution should be enough to start. More focus on results and accomplishments, less talking, will better serve this initiative in our overall cybersecurity posture regardless of the threat vector.

Finally, when to seek out and leverage by name, when and where possible, specific people, tailorable process, integratable security technology solutions. We must allow the security—the subject-matter experts to research, propose, implementable processes and technology solutions and then put them in place with minimal delay. Bureaucracy is not our friend in this arena.

Now, there are no easy solutions, and we have been speaking to these topics for a number of years, but if we are serious about protecting our Nation's interests, we must first secure the basics before moving into more advanced methods and techniques. Thank you again. I look forward to any questions you might have for me.

[The statement of Mr. Caslow follows:]

PREPARED STATEMENT OF ROGER L. CASLOW

APRIL 26, 2012

Good morning and thank you for inviting me to share my testimony today. My name is Roger Caslow [1] and I am an executive consultant with Suss Consulting. My background is primarily in the realm of cybersecurity as it relates to computer and network defense. It is an honor to appear before this joint subcommittee to testify about the "Iranian Cyber Threat to the U.S. Homeland" and I hope that my testimony is of benefit in to creating a better defense posture against this stated threat.

According to the 2012 Data Breach Investigations Report,[2] 97% of all reported data breaches were avoidable through basic levels security controls implementation. Allow me to state that in order to protect our way of life we must be prepared to return to the basics of security. Not the flashy and glitzy but rather the foundational aspects of cybersecurity. Once we have secured the basics, across all sectors, then and only then can we have greater certainty that the "weakest link" is not as exploitable by those who seek to do us harm. Within the field of cybersecurity this requires ensuring that the foundation is secure by knowing what is on or connected to our networks, what our basic security posture is and what it should be, and ensuring that the right people with the right skill sets are building, maintaining, and protecting these assets and their data.

Furthermore, within the cybersecurity discipline we require a stronger governance structure. Governance is far from the most exciting area in the field of cybersecurity but it is foundational to ensure better management of our vulnerabilities against our threats. For this to work we must have clearly defined language, write what is meant and leave as little room for negotiation as possible. Good governance is required for best performance of our National, State, local, and industry activities. Good governance supports better integration of cybersecurity and information technology architectures, building in the security requirements up-front. Good governance supports the adoption of risk-management-based decisions, which are only as good as the information made available to the decision makers responsible for the defense of our interconnected networks, both public and private. Executive Order

[1] Roger Caslow Bio.
[2] 2012 Data Base Investigations Report, Verizon.

13587,[3] *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* is a good start but it requires more "teeth" and better communication across all levels, to include our industry partners, lest the bureaucracy overrun the implementation.

Another, not-too-exciting area, is the emphasis on education, training, and awareness (ETA). Education emphasis, not merely on the hard technology engineering skills but also on basic critical thinking skills, which are all but lost in many technology disciplines. With respect to training, as a Nation our standards need to be fully matured and established across all sectors. We can make improvements by leveraging the private-sector security-based and -focused training organizations, which are aware of the threats, vulnerabilities, and countermeasures. Basic awareness of the threats posed to all sectors and elements of our society is also important. We still have too many people who are ignorant of the threats and become caught in phishing, spear phishing, social engineering, and other types of data manipulation, exploitation, and exfiltration schemes. Again, all sectors are important and require some level of targeted awareness campaigns. Consider it as operational security against the cyber attack. The National Initiative for Cybersecurity Education (NICE)[4] which evolved from the Comprehensive National Cybersecurity Initiative was intended to address many of the ETA issues but it has not taken root. I fully understand the concept of "measure twice and cut once" but when we face the threats we do as a Nation, the 85% solution should be enough to start. More focus on results and accomplishment, with less talking; will better serve this initiative, and our overall cybersecurity posture.

Finally, we must seek out and leverage, by name when and where possible, specific people, tailorable processes, and integratable security technology solutions. We must allow the subject matter experts to research and propose implementable process and technology solutions and then put them in place with minimal delay; bureaucracy is not our friend in this arena. Also, we must not be afraid to embrace the hacker community, but in order to do so we must leverage a different type of recruiter. Our talent recruiters going to this community via to the major hacker conferences, also known as "CONS", will have little success in three-piece suits. They must be people who have the look, feel, and knowledge to speak with this community at the social and technical levels. This is critical to securing the skill sets and knowledge base from a community with a greater knowledge of the offensive side of the battle. It's a known fact in sports, combat, and security that knowledge of the offensive tactics, techniques, tools, and procedures are of utmost importance in further bolstering our defensive posture, and in the case of cybersecurity, securing our networks.

There are no easy solutions, and we have been speaking to these topics for a number of years, but if we are serious about protecting our Nation's interests we must first secure the basics before moving onto more advanced methods. Thank you again and I look forward to any questions you might have for me.

Mr. MEEHAN. Thank you, Mr. Caslow. Thanks to each of the panelists. The Chairman will now recognize the other Members for questions. The Chairman will recognize Members for questions in the order in which they were here today. I now recognize myself for 5 minutes of questioning.

I thank all of the panelists for your compelling testimony and I believe as we work together as a panel, will explore a number of these areas. I could jump in with anybody, but let me begin with you, Mr. Berman, because you were touching on some issues that I think are important to develop. First, that was a pretty strong statement to say that we have experienced a seismic shift in how Iran not only views the United States, but its willingness to carry out actions against the United States.

So I would like to have you tell me how you have come to that conclusion, and then where you see our cyber capacity as being a likely target. Then if you have a moment, I am interested as well

[3] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,* Signed October 7, 2011.

[4] National Initiative for Cybersecurity Education Strategic Plan, August 2011.

in the idea of what we have talked about in which, you know, we spent our time with Russia, and China, and so worried—this concept that we don't even know what is coming from Iran; the use of proxies, which is part of the MO. I think I have given you a little bit to jump with, so I would love you to just take off.

Mr. BERMAN. Well, thank you, sir, that is a little bit of a tall order. I am going to try to do my best to address it. The question first of the seismic shift. I think it is very clear, and I don't know if you recall, but I was a witness before this panel last summer looking at Hezbollah activity in the Western Hemisphere, and at the time, myself, and a number of the panelists that were with me, made the point that Latin America, and the Western Hemisphere generally, is seen as a staging area, an area of opportunity for the acquisition of funding for illicit activity that provide revenue to the Iranian regime.

Mr. MEEHAN. I note this testimony was prior to the point where we were aware of what happened in Mexico.

Mr. BERMAN. Exactly right. What you see—or at least what I have seen in the months since has been an evolutionary approach that Iran has taken towards how it positions itself, vis-à-vis, the U.S. homeland. Previously, it would have been very difficult to imagine a scenario where the Iranian regime, in any part, would authorize such a brazen attack as it did in October—tried to carry out in October 2011. There have been many commentaries that have cast aspersions on that account with regard to the complexity of the plot, the amateurishness of its execution, but the folks that I have spoken to, maintain that this was a credible plot. It was one that was, perhaps not executed properly, but it is one that signaled intent. That intent is, I think, key to this discussion here today. Because when you look at the potential for an Iranian cyber attack, you have to marry capability and intent. With regard to intent specifically, I would argue that Iran has more potentially.

Mr. MEEHAN. But you are talking about intent. In fact, capability here, that required that they had to penetrate the United States physically. Here we are talking about a global network which they can access, not only from Iran, but from anywhere the world.

Mr. BERMAN. I think that is exactly right, and when you look at cyber space, as Mr. Cilluffo said, cyber space is, you know, it is flat. It has the advantage being sticky. It is a field that advantages asymmetric actors. Iran can reach out and touch us in the U.S. homeland via cyber space much more easily than it could via, say, Latin America. As a result, the capabilities are an issue, but the intent, I would argue, is more of an issue. Here, Iran has an overabundance, because unlike the scenario in our foreign policy that we have with China, and with Russia now where conflicts do exist, where we have a stable diplomatic relationship, we have a series of scenarios that are potentially coming down the pike, a renewed diplomatic impasse over Iran's nuclear program as a result of the negotiations, new economic sanctions, potentially even a military conflict that could trigger an attack on the part of the Iranian regime as an asymmetric retaliation.

Mr. MEEHAN. Mr. Cilluffo, do you agree that that the United States is now the cyber network, as was identified by Mr. Leiter, is a traditional terrorist attack target right now?

Mr. CILLUFFO. Unequivocally, when you are looking at Iran, and a couple of other points that make cyber space unique. Mr. Chairman, you had just asked a question along those lines of Mr. Berman. But anonymity, who is behind that clickety-clack of the keyboard breaking into your system? Are you dealing with a pimply kid, or are you dealing with a foreign intelligence service, an organized crime, an economic competitor? You simply don't know much of the time at the breach itself. So attribution, while we are making progress, smoking guns are hard to find in the counterterrorism environment; smoking keyboards are that much more difficult. I would also note that cyber space is made, I mean, it is made for plausible deniability.

So what we have seen, and the reason I am concerned about the Russias and the Chinas is we have seen a sophistication level that is very high. But they are in the business right now of CNE, computer network exploits to steal secrets. If their intent changes, they could just flip the switch and it becomes an attack tool. I might note that what we have seen that I think is most concerning, and certainly to Mr. Lungren's subcommittee is, we have seen adversaries map critical infrastructures.

I don't see what the value of that, the cyber equivalent of intelligence preparation in the battlefield. I don't see what that intent could be other than to potentially use in a time of crisis.

Mr. MEEHAN. So there is a lot of presence within the network right now. It is just that they haven't flipped the switch. Right now it is obtaining information, but they haven't turned it in a proactive sense into delivering some kind of an attack.

Mr. CILLUFFO. I might note that we tend to look at this only through a tech lens. The more sophisticated actors realize that it is the convergence of human intelligence, and technical intelligence, and that is where we should be worried.

Mr. MEEHAN. Well, my time has expired. At this point, I would like to open it to questions to the Ranking Member Mr. Higgins.

Mr. HIGGINS. Thank you, Mr. Chairman. You know, I sense from both the substance and the tone of your testimony, there is an underlying frustration that perhaps we are not doing as much as we need to do in order to defend ourselves against a potential threat. So let me start with Mr. Caslow. According to the former director of the National Counterterrorism Center, Michael Leiter, the United States, he says, can likely defend itself against the types of cyber attacks of which Iran is capable. Given what you know about the vulnerabilities of both the governments, and the private sector cyber infrastructure in the United States, do you agree with the former director that the United States is capable of handling a cyber threat from Iran?

Mr. CASLOW. If I might say, that at the time this statement was made, there may have been certain assumptions made as well, about the understanding of our networks. The vulnerabilities, as technology shifts, vulnerabilities shift. Also, the threat vectors shift. I don't say that I disagree with him, but at the time he was probably correct. As of today, I would believe that it would be less correct, only because, as my colleagues here have already mentioned, the capability and intent is important. Those feed into the risk equation of what threat is. But the other parts of that are

equally important. They are not weighted of one more important than the other. The other parts of that are the big V of vulnerability, the likelihood, or probability of those things happening, and ultimately, the impact of those occurring.

My personal viewpoint from the years I have been doing this is that we can't consider ourselves looking at one threat vector unless we understand our own vulnerabilities. We have to know ourselves first and foremost. I do know with certainty from speaking with my colleagues across industry and across the Government that it is not all boats rising at the same. Unfortunately with the interconnection of our networks from the TS all the way through that we have the—be careful here—we have the known vulnerabilities for a boat that is not as high in the water as the others could negatively impact some of the higher-level boats, to take that analogy further. Again, I frequently use analogies with my colleagues who aren't on the technical side, of a house. You have a house, you build your structure. You are considered—sir, I am sure you are considered with the furniture, or the paint of the color or the varnish on the trim, or how the chair rails go in the dining room or what type of appliances are inside your home. How often do we investigate how deep the footer has been dug. Or is the footer the appropriate depth or width, is it maybe the right construction material. All these other things are actually ultimately more important in many aspects of you having a home that will keep you secure and your family secure over the lifetime. The United States of America is my home. So I want to make sure that we do secure the foundation, the foundation and the building materials and everything that goes into that.

Mr. HIGGINS. I think the other thing that is often missed in terms of counterterrorism is the importance of remaining agile. It seems as though, first of all, no technology advances more quickly in our society than the technology of killing. Every day new weapons of mass destruction are being created to kill more people more quickly, and it is a big problem. I just think that there is a tendency to think terrorism 10 years ago is the same terrorism we have today. What you have is a new generation of terrorists that are more aggressive, that are more technologically savvy and thus more dangerous to their potential targets. As has been stated here, when you consider the testimony that was been given several months ago about the Hezbollah, which acts as a proxy for Syria, for Venezuela, for Iran, having not only a presence in the 20-country region of Latin America but also having a presence in American cities. Their activities we are told is limited to fund-raising. Well, I don't make that distinction. Fund-raising is a component of terrorist activity. What are you raising funds to do? It doesn't have a beneficial impact on society.

So I think this is a threat obviously that is very important that all of you have emphasized the importance of it, and I appreciate your testimony here today. Thank you, I yield back.

Mr. MEEHAN. Thank you, Mr. Higgins. The Chairman now recognizes the Chairman from California, Mr. Lungren.

Mr. LUNGREN. Thank you very much. Mr. Berman, only a few weeks ago a former director of National Counterterrorism Center, Michael Leiter, said or indicated that because of strict financial

sanctions facing the Iranian regime they might target international financial systems in a cyber attack. Would you agree that our financial institutions would be a prime target for Iran based on motivation?

Mr. BERMAN. That is an interesting question, sir, and I think I would have from what I know about how Iran is weathering the international financial sanctions regime, my answer would be "not yet". If you look at what Iran is doing, the attack that Iran has allegedly carried out against financial institutions such as Israel's Banque Poaley, signaling Iranian's ability to reach out and touch and affect and manipulate these financial institutions. Iran as a result of the sanctions that have been levied since the start of the year by the Obama administration and more recently by the European Union is increasingly dependent on utilizing that financial system in places like Venezuela, for example, to circumvent, to skirt, to attain another avenue to access international markets as these sanctions truly begin to bite. As such Iran at least for the moment doesn't have the incentive or the motivation to attack in a catastrophic fashion and take down financial institutions. Will it later? Perhaps. If there is an all-out military conflict over its nuclear program. But as of right now I don't think that threat is mature.

Mr. LUNGREN. Mr. Cilluffo, I have heard it said that with Stuxnet or the public recognition of Stuxnet we have crossed the Rubicon; that is, we now have seen expressed in a prime example of the ability not only to enter into another's computer system or network but to control it in such a way to cause physical destruction. Would you say that is a fair statement?

Mr. CILLUFFO. Absolutely. I do think it did cross a Rubicon and certainly serves as a harbinger of what we are going to be looking to in the future. I might note that I personally feel it was the right thing to do. Let me suggest though that those that may have been hit may not be as discriminate as perhaps Stuxnet was to affect centrifuges. I think the same vulnerabilities that were exploited through our various systems could have catastrophic effect on some of the various critical infrastructure in the United States. So I think we need to inoculate ourselves from a whole host.

Mr. LUNGREN. When we talk about asymmetric warfare it is interesting because one way of looking at it is that the "underdog", the small guy, the one that is less powerful has an opportunity to do harm to the stronger adversary at lesser capital investment, lesser requirement for manpower, et cetera. At the same time it seems to me we ought to look at asymmetric warfare in the terms of the war on terror; that is, asymmetric warfare with the purpose of doing what? Not just destroying property but causing psychological damage to the adversary.

So when we talk about critical infrastructure, one of the things that comes to mind with me is our health system is a critical infrastructure. If I were to attack the United States one of the things it seems to me that would be very effective in an asymmetric way would be to attack the health system. If you could invade the information systems of several health systems of the United States such that no one could depend on the accuracy of the information contained therein, someone lying on the surgical table and getting the

wrong blood type, information indicating that you ought not to take certain medications and it indicating that you ought to take them. If you did that in a series of attacks, you wouldn't have to be successful with too many of them to cause a psychological damage to the United States.

So, I would ask both Mr. Cilluffo and Mr. Caslow whether that kind—do we need to appreciate that kind of a difference in terms of perhaps the target and the impact? As opposed to our sense of conventional warfare view of asymmetric warfare, if that makes sense.

Mr. CILLUFFO. Chairman Lungren, I think it does make sense. I mean cyber has extended and expanded the battlefield to incorporate all of society. So what we used to look through in a more traditional targeting kind of sense, vis-à-vis the military C4ISR now has potential to be against us from a critical infrastructure perspective.

Let me just note though that I feel we have nearly limited vulnerabilities, limited resources and let's not forget we have a thinking predator and actor that bases their actions on our actions. So the best we can really do is get to the point where we are managing risk. I very much agree with Mr. Caslow's view, let's get to the 80 percent solution and then focus on specific actors, because Iran is not China. You have got different sets of tools that need to be brought to bear. Russia is not DPRK, or North Korea.

So I feel that one biggest missing element of our strategy is we don't have a cyber deterrent strategy. We need to clearly articulate one, we need to identify bright red lines in the sand or maybe in the silicon more apt and we need to identify what is unacceptable. Oh, by the way, we can't firewall our way out of this problem. We need to start talking about offensive cyber capabilities and capacities.

Mr. LUNGREN. Mr. Caslow.

Mr. CASLOW. I fully agree. Your analogy of the health care system brings to light a scenario that we tried to scheme out where the health care system connected at one point. If I were to target a hospital near a major military installation, let's take Jacksonville, North Carolina, and maybe I was able to target with something like either a Duqu, which they believe to be the precursor for Stuxnet, we are not quite sure about yet, something that has the ability to attack the SCADA, you tell people it is terminator, it really is because now you actually have computers telling machines what to do. We have had that capability a long time but now we have the adversaries trying to use it in different areas, and granted it was a good thing it was used against someone who means us well, but the minute it is flipped around on us that is a bad thing. They target that hospital with the basic generator backup, they take out a power grid around that area as well. They are also able to take and attack the water system, parts per million of chlorine goes up down depending, and again the read-out says it's right because that is what Stuxnet does. All of a sudden now we have hundreds of thousands people sick in an area where we have troops who are deployed overseas. The ultimate end-game here is not to make those people sick. The ultimate end-game is to terrorize our troops overseas so that our Marines who are deployed in combat

zones can no longer do their mission because they are worried about their children, their wives, their grandmothers, whatever, who are now ill back on the home front because they are communicating with them and now they know they are sick.

Now that does deplete and impact our ability to carry the war out in a physical and kinetic manner overseas. So you are right on target, sir, we do have to be worried about that, but again we do have to ratchet things down to make sure we do have that strong defense, because the tactics, techniques, procedures, a strong defense is necessary in sports and necessary in the cyber world, but in order to do strong defense we have to have the offensive capabilities together as one.

Mr. CILLUFFO. And linebackers in between.

Mr. MEEHAN. An appropriate analogy for draft day. The Chairman now recognizes the gentlewoman from New York, Ms. Clarke.

Ms. CLARKE. Thank you very much, Mr. Chairman. My first question goes to Mr. Caslow. There are reverse engineering possibilities associated with the downing of U.S. drones in the advent of the Stuxnet virus that presents a possibility of advanced cyber weaponry being developed in Iran. In your opinion, is Iran close to developing the cyber attack capabilities that present a threat to U.S. critical infrastructure? Do you believe that other countries with already well-developed cyber weaponry capabilities are aiding Iran?

Mr. CASLOW. Again, ma'am, I am not an Iranian expert, I am a pure computer network cybersecurity person.

Ms. CLARKE. Right.

Mr. CASLOW. However, to answer your question as best as I possibly can, any number of countries, we will go back to the P–3 downing in China, the reverse engineering capability with their inability to fully discharge all of the equipment on that platform and a number of other areas. Any time that we can get someone who has a knowledge base to reverse engineer something that could potentially create a threat. Now that threat is against a specific targeted area, it could foreseeably do that. I would never take away that possibility, but it is the art of the probability because there are a lot of technical aspects involved with the downing of that Pacific platform as well as downing of a lot of other platforms. So not only that, but also the back chatter and how organizations station—the state actors and non-state actors share data and information. We do know this—it was quoted, I guess, the axis of evil and previous administration quoted that, used that term. The reality is it is beyond an axis, the data streams everywhere, the data flows, the internet can go everywhere. I can still go to a dark reading room on the internet and download any number of very bad, nasty little critters that are out there and then use those same critters to attack a network or system. I can buy those capabilities, I can download some of them for free.

So I say, yes. But again this stuff keeps me up at night, it doesn't have to keep you up at night.

Ms. CLARKE. Thank you. Let me just sort of put this in context because this week the House is considering several cybersecurity bills, including the Cybersecurity Intelligence Sharing and Protection Act. I believe that none of these bills that are being considered

will provide the country with a comprehensive cybersecurity strategy, vesting cybersecurity authority in a single domestic Federal agency and include robust privacy protections.

Given the testimony here today on the cyber threat from Iran, what would you recommend as the basis for real cybersecurity legislation that addresses these concerns?

Mr. CASLOW. Thank you for asking that, ma'am, I have been doing a lot of reading on CISPA, and as I mentioned before in my testimony we do have to ensure that we have the governance piece in place. That is important. Integration with industry is exceptionally important. I do believe I also mentioned the fact that we require some level of emphasis on education, training, and awareness, which CISPA is lacking in a lot of areas.

To get away from the privacy aspect, I came from a world where it was about the data—the security and the sharing, now I am in a world where it is about the privacy and the security. So I understand those areas fairly well.

Putting it all in one person's plate, integrating it, it all depends on how it is executed. The old adage goes, the best plan in the world poorly executed is not as good as the worst plan in the world executed with superiority. So we really need to make sure it comes down to the execution. Again as I mentioned, we need to specifically state what the intent is. What do we need to get across, not allow others to try to misarticulate the intent as in some laws and some Executive Orders, it gets down to the actual tactical level at the implementation and they are going it must have been 10 of this and my experience is it is this far away, it is not even close to what the intent is. So we need to make sure that that is clearly stated. Here is exactly what we need. I know that may take longer, I understand that, but I think that is what is needed.

Ms. CLARKE. Let me just ask Mr. Berman, over the past decade have been proposals within the United Nations and other international forums for treaties and convention that would ban the development and use of information weapons. Critics counter that as a form of cyber arms control and would stifle innovation and favor an international norm building approach and code of conduct.

What international internet governance regime would you recommend for countering the Iranian cyber threat? Along those same lines how are the State Department's global internet freedoms initiatives deconflicted with NSA and USCYBERCOM's intelligence gathering and warfighting mission?

Mr. BERMAN. Well, ma'am, thank you for the question. Since it is draft day I may mercilessly punt this over to my colleagues. But let me just point out again I am not a cybersecurity specialist. I am not in the position to speak about that. I can tell you very that parenthetically in my understanding of how the cyber community has dealt with the Iran threat specifically, not the cyber threat writ large, there is a gap in understanding between the operational, what Iran may do, and the political and strategic, what Iran is likely to do if something happens in the real world. That seems to me to be a gap that needs to be closed.

Beyond that in terms of what rules, what standards need to be applied, I would like to turn it over to my colleagues.

Mr. CILLUFFO. Ms. Clarke, thank you for the question. I am pretty vocal in terms of my views on this. I would vehemently not support a U.N. arms control approach to deal with cyber. If you think back to nuclear and it is not a perfect analogy, but as Ronald Reagan said, trust but verify. Given some of the attribution challenges here and given that the two countries advocating this approach, China and Russia, have been known to be active in this space, I think we should be very cautious in terms of what their intentions are. We are not obviously not going to compromise our sources and methods even if we get to 100 percent verification. So I would push back on some of those proposals.

Now, the flip side is that the Council of Europe has a cyber crime treaty. Here I think you have got the behavioral level that everyone can agree when you are dealing with child predators, you are dealing with child pornography, some of the tools that we have used in other confines and environments can be brought to bear in this environment, and I think we ought to consider some of those, but I have very little confidence in the U.N. approach. Quite honestly I feel we need to get more proactive in some of our offensive capabilities because we are not going to firewall—at least to demonstrate a capability to signal that we are serious and we will respond.

Ms. CLARKE. Thank you, Mr. Chairman.

Mr. MEEHAN. Thank you, Ms. Clarke. At this point in time the Chairman recognizes Mr. Cravvack from Minnesota.

Mr. CRAVAACK. Thank you, Mr. Chairman. I appreciate it. Being an old Navy helicopter pilot, this is a brand-new battlefield, a virtual battlefield if you will. But some of the things that can go back to the basics is the best defense is probably a good offense.

So my question would be: How can we not only as a Government agency but unleash the private sector as well and be able to go proactive on if they receive a cyber attack, how can they have a counter offense in identifying where this comes from and beat these back. Can you give me a comment on that?

Mr. CASLOW. Is this punt the football again? If I could I have actually in my written testimony something along those lines.

Mr. CRAVAACK. I apologize I was late. I was in another meeting.

Mr. CASLOW. No, I didn't actually speak to that part, it was just purely written. So I am glad. I wanted to cut my time down and make sure I was within the 5-minute window.

Mr. CILLUFFO. Which was amazing by the way.

Mr. CASLOW. Thank you. I tried to get that right.

Your point is 100 percent correct. We in our community, both the Federal and the industrial side, do have to take a better effort towards embracing the hacker community. Now there is a lot of places I could send you to and hopefully you have your firewall set up the right way so you don't take any nasty critters out with you. But lots of places that we have to leverage those. But in order to leverage those properly we have to send in a different type of recruiter. This recruiter cannot be looking like us in a 3-piece suit or in a suit and tie, walk in there and go, "Hey, guys, how are you doing? I am from the Government, I am from Boeing, let's give you a job." No. These types have to understand the people, they have to have the look, the feel, they have to have the knowledge to

speak to this community at the social and technical levels. Again I emphasize the word "social" because they do think differently. These people understand the hacker community more than anything. This is everything from the 13-year-old kid sucking down Mountain Dew and eating Hot Pockets in their parents' basement to some of the more astute ones like—I will give a name like Dark Tangent who is out there and who is known inside the cyber community, but we have to be able to leverage those as resources. Many of these people are patriots, I will tell you that right now, as was seen when it came to the Anonymous attack. A lot of Americans, United States American hackers came and said, "wait a second, you can't do that to us, only we can do that to us." So we do need to—only my dog, only I can kick it, right? But the reality is we need to embrace those more.

So on that side, again you are right about the offensive nature of the game. As a former fleet Marine Force Navy Corpsman, I have a grunt mentality towards a lot of these issues. I believe in warheads on foreheads. That is a great way to solve a lot of problems. This way we do have to embrace the people who actually are able to pull the trigger. In this case those people, acknowledged as the snipers so to speak, are this hacker community and some of these others. But again we are not going to go in recruiting them looking like this.

Mr. CRAVAACK. My Dad was a Navy guy, 3rd Battalion, 3rd Marines.

You know it is so important what you are saying is that at the United States Naval Academy now they have major, cybersecurity. I mean that is how important that the Government is finally getting this. To be honest with you, if you told me about cybersecurity 5 years ago I would have said, huh? So I am slowly coming around. This is a new virtual battlefield. The implications of which are so massive, providing with the right attack, that the ramifications are unbelievably massive, shutting down grids, you name it.

Now I look at it from a National security aspect that we really have to start focusing on this effort. So I commend you for what you are doing. I am schooling myself up quickly on jumping on this bandwagon saying that we definitely have to do this.

Now I am very concerned about Iranians. A small force can overpower just like you said and overcoming a Nation and that concerns me greatly. So the bottom line, I have got 18 seconds, but the bottom line is: Do you believe in that philosophy, a better offense is probably the best defense?

Mr. CILLUFFO. I wrote that in my testimony. So yes, I dissuade——

Mr. CRAVAACK. Great minds think alike then.

Mr. CILLUFFO. I also think, not to take away from the Navy is fine service, but we need the equivalent of Billy Mitchell to work at cyber. We have a lot of tactics masquerading as strategy. We have to be confident to be able to take these issues in a strategic kind of way, and that includes the computer network attack. We need to demonstrate capabilities, we need to be visible. What good is having a doomsday weapon if no one knows you have it? At the end of the day to me it is part of the solution, it is by no means the end-state, we still need to build up our defensive capabilities

but recognize that the attacker has the advantage here, and we need to always be in the front edge of this.

Mr. CRAVAACK. Thank you, sir. I yield back, Mr. Chairman.

Mr. MEEHAN. Thank you. The Chairman recognizes the gentlelady, Ms. Richardson.

Ms. RICHARDSON. Thank you, Mr. Chairman and both of our Chairmen for having this hearing today. First of all, I would like to ask the question, back in 2008 the CSIS Commission for Cybersecurity for the 44th Presidency made 25 recommendations for a National cybersecurity strategy. To my knowledge, those have not been implemented to this point or at least from a legislative perspective. Do you have any thoughts on that or where you would suggest that we go first?

Mr. CASLOW. I am glad you mentioned that because I did reference CNCI and we do have the inability to pull the trigger. In my previous position, and again I do not represent those opinions of the Office of Director National Intelligence. I am a civilian, make sure I am perfectly clear on that, but in a previous edition I did have a lot of discussion on those. Unfortunately it was a lot of discussion. Again we are too busy about trying to measure twice, cut once versus trying to just pull the trigger in an 80 to 85 percent solution. A lot of those efforts should be, I believe, my personal opinion, that they should be enforced from CNCI, 4, 5, 6, 7, 8, all the way through and we should take a better look at those again, bring in a group of subject matter experts, find out how we are going to get it done, potentially craft the legislation that makes it happen, and then fund that activity, because while we have got a lot of other battles on our front this is very important. It is not just important for us but it is important for our children and grandchildren, lest we don't have an infrastructure American way of life to share with them later.

Ms. RICHARDSON. Would either of you other gentlemen like to comment on the specifics of the 25 recommendations?

Mr. CILLUFFO. I don't remember all the recommendations, but it is fair to say in a sound bite, long on nouns, short on verbs. I mean, we have talked a lot about the challenge. It is about implementation and execution and I don't want to sound overly dramatic, but in 1862 President Lincoln came before Congress with further storm clouds on the horizon and claimed as our time is anew we must think anew and ultimately act anew. We are there now. We know what some of the challenges are. There are great pieces of legislation, many others have put forward pieces of legislation. Now is the time to actually get into that, identify what really needs to be done and pass legislation. This can't be done through the private—first, the Government has to act to get its own house in order first and foremost. Then we have to look at what is the right incentive and other approaches to get the private sector in.

Ms. RICHARDSON. I understand. My question was were there any specific points that you wanted to make regarding the recommendations in particular that you felt should have more of a priority or address?

Mr. CILLUFFO. Act.

Ms. RICHARDSON. Okay, got it.

Mr. CASLOW. If I could, I'm sorry, but if I could, CNCI 8 which was the education, training, and awareness which I did speak to, that to me is of the utmost importance. Because if we are not communicating and training and we are not making sure we have the right skill sets in place, all the technology in the world doesn't matter for anything.

Ms. RICHARDSON. My last question for the three of you gentlemen, are any of you working with any stakeholder groups within the Department of Homeland Security or any other Federal agency?

Mr. CASLOW. No, ma'am.

Ms. RICHARDSON. So you do your work completely from the outside? So you are not being sought after to share your thoughts and ideas of what should be considered?

Mr. BERMAN. Ma'am, not at the moment, no.

Ms. RICHARDSON. Sir.

Mr. CILLUFFO. I stand where I sit, I am not formally involved, but of course we share our ideas with every entity, including Congress and the Executive branch.

Ms. RICHARDSON. No, my question is: Is there a specific stakeholder group that you participate in sharing your ideas and the information and knowledge that you have?

Mr. CILLUFFO. Not anymore.

Mr. CASLOW. Not since leaving the Government on February 27 of this year.

Ms. RICHARDSON. Thank you, gentlemen. I yield back.

Mr. MEEHAN. Thank you, Ms. Richardson. The Chairman would be delighted to ask Mr. Green and thank him for his attendance and his continuing interest in this area and would be delighted to accommodate any questions you might have if you do.

Mr. GREEN. Thank you, Mr. Chairman, I thank you for allowing me to continue to participate. I am an interloper but I do have great interest in what is going on. While I cannot "Roger" what my colleague from the Navy said, I would like to as a veteran of the ghetto wars "Right On" what he said. I totally agree. I would like to focus if I may for just a moment on the phrase "we can't firewall our way out of this." I do understand botnet. I understand Zombie Armies, Trojan horses programs, and I have done some reading on Stuxnet, but I would hope that you are saying that while we can't firewall our way out of it, we can at least use the firewall to get us to that 80 percent that you are talking about and perhaps maybe more at some point in the future because firewalls are an absolute necessity in doing whatever we can to prevent this.

So let me just hear more on this question of how firewalls will help us to produce some degree of salvation.

I would also add this, with reference to the plausible deniability, I would like someone to give me a comment on how we will at some point have to use as much empirical evidence as available to us. I am trying to do as my friend did earlier, select my words carefully. I want my diction to be superb because as we move closer and closer to having to deal with Iran in what may become an unpleasant way, plausible deniability cannot become a barrier to acquiring enough empirical evidence to act.

So would you please start with the firewall concept and how we have to deal with that and then plausible deniability as a means of preventing us from acting.

Mr. CILLUFFO. Sure, and I didn't intend to pick on firewalls in particular. It was more meant to suggest that defensive measures alone, while important and we need to get to that 80 percent solution, in itself you can't expect a corporation to defend itself against foreign intelligence services, for example, that are going to use a mix of technical means, with human means, and an insider. Those are the sorts of challenges. Technology, while important, is agnostic but won't take us all the way. Ultimately the people connection is important and we need to be able to share that information.

So I did not mean to say don't use your firewall. Please use your firewall. But that in itself is not going to take us where we need to go. If you think in a counterterrorism environment, Homeland Security critical, we needed to work the various issues but if we didn't have that pointy end of the spear, if we didn't have the days like we had in Abbottabad or other sorts of actions, we would never be able to ultimately prevail in some of these sorts of challenges.

So I simply meant to suggest that we need to get, raise the bar, raise it high, but recognize that anything above and beyond that you can't incent, you can't expect the corporations to be able to defend themselves against that. So that was the purpose of my point.

Also to suggest that we need to start investing and publicly discussing our offensive capabilities because they are there.

In terms of plausible deniability, that just makes one of the challenges in terms of the attacks we are seeing. If I were to suggest one technical area to invest in, attribution, attribution, attribution.

Mr. GREEN. Yes, sir.

Mr. BERMAN. Sir, if I may jump in quickly, again I am not a cybersecurity specialist but to sort of to revert back to the topic of the hearing, I think what is interesting is something that Mr. Cilluffo alluded to in one of his answers, which is a cyber deterrent strategy, a strategy that marries concepts of deterrence with the idea that if someone reaches out and touches us it wouldn't be good for them, it wouldn't be healthy for them.

I would point out that over the last 8, 9 years as the international community has grappled with the Iranian issue we have had an abject lack of a deterrent strategy for dealing with Iran in terms of nuclear acquisition, in terms of its actions asymmetrically in places like Iraq and Afghanistan, and I would argue that we are now facing an area also that is crying out for the need for a more robust deterrent strategy so the Iranian regime understands very clearly that there are red lines that if they cross in the cyber realm would rebound to their profound detriment.

Mr. CASLOW. If I could, too, the concept of firewalls, let's go to the technical side of this now, unfortunately you can say you have a firewall. When he said we can't firewall our way out of this, I understood exactly what he meant. A firewall is only good as how you establish the firewall. Me, I believe we should put across the main solutions all over the place because they are much more active. A firewall is a passive mechanism and if not established appropriately and properly, then you can say you have a firewall but I will tell you right now more than likely if you had a home network

I will hack you, I will get you. If I can't get you, someone else will, especially if you are not maintaining your firewall and ensuring the right security controls are in place the right way.

So it is not only the technologies which you speak of but it is also the implementation of those technologies to ensure they are properly implemented and secured in accordance with the standards that we have to put in place. So again they are only as good as you use them. Just like a gun, it is only as good as the person shooting it, right?

Mr. GREEN. Thank you, Mr. Chairman. I am over my time. Thank you and I yield back.

Mr. MEEHAN. Thank you, Mr. Green, and for your presence here. I know that the panel is ready to conclude, but I am going use my prerogative as the Chairman to ask one follow-up which is you have both—all three of you at separate times have developed this concept of an offensive not just capability but I am also interpreting if I am getting it correctly as the utilization of some kind of offensive action in this environment. I certainly recall the days of assured mutual deterrence with the nuclear threat, but of course we never really used a nuclear weapon. So what is the predicate that would allow us to in a country like ours where we are hesitant to deliver some kind of an aggressive offensive action unless and until we believe we have been attacked? So how do we—would you develop this concept of offense in this world where the conclusion seems to be we are not going to be able to exclusively simply defend ourselves from the consistent probes that may turn into an actual attack from Iran or China or Russia. What is offense?

Mr. CILLUFFO. Mr. Chairman, that is an excellent set of points, and I think before we lean too forward in this direction we do need to have the tough doctrinal sets of questions. We have a lot of strategy, we have a lot of tactics, but there is nothing pulling these pieces together. In the midst of that you also need to clearly define rules of engagement, which have not been done thus far. But I might suggest there are ways to demonstrate capability, such as nuclear tests, short of actually delivering such a capability through various platforms on a particular actor.

I might also note that we do need to start thinking of the homeland implications. I mean, one of the challenges with cyber weapons, you use them, you use them once, they can be used against you. A, you can reverse-engineer it and use it against you; B, you are compromising your golden bullet potentially that you may want to use when you really need it. So ultimately we have got to start embedding computer network attack and cyber thinking into traditional National security and military thinking. Right now we treat it a bit as a black art, ooh, ah. At the end of the day if we start discussing it as we do every other platform system and TTP that can be deployed, then it takes some of that out and we are going to want to play to our strengths, because ultimately the greatest threat is not cyber unique, it is cyber as a force multiplier to kinetic or whatever else it may be. That is also what we need to be worried about defensively in terms of higher-end actors.

My whole point is if we don't create these bright lines in the silicon or in the sand, there is nothing to dissuade, deter, or compel people from engaging in the space. We need to start finding the

critical infrastructures. If people are mapping that there should be consequences. What other reason could they use to map that other than to potentially use that as part of a broader attack plan? To me that is where the line needs to be crossed. In the exploit business, we are all in the exploit business, so that is a little more difficult, but once it starts going to some of these critical infrastructures we need to be thinking about that.

I might also note your committee I think has an obligation and the responsibility to be involved in these discussions because there are homeland implications if we start moving proactively that we need to be ready for defensively. Before we engage in certain military activities, I want to make sure our homeland is protected from some of those.

So these are tough questions, cuts across all committee structure, all Executive branch, and truth is we don't have the doctrine right now. We need to start developing it and I would argue discussing it, because right now we are kind of in the worst of both places.

The Office of Director of National Intelligence, the National Counterintelligence Executive, NCIX, recently came out naming names, calling out Russia and China, stealing billions and tens of billions of dollars of our intellectual property. Now we are saying: They are doing it, what is the disincentive for them to continue doing that? What would an Iran interpret if they see we say it is happening and we are not doing much to visibly defend ourselves. So I think we need to start having these conversations.

Mr. BERMAN. Sir, one parenthetical point, sort of going back to the topic of the hearing, I think it is important and both of my colleagues alluded to it as part of their remarks, is that not all threat actors are created equal. In this context, specifically in the Iranian context, politics matter. In fact they matter a lot. In order for us to have a predictive cyber strategy that marries defense and offense, that includes deterrence, we have to not only think about the operational capabilities of these threat actors but also what is happening in the real world that might incentivize them to act whereas others would not. I think whether you look at, specifically thinking about the military, when you look the at the Pentagon's recent work on developing something resembling a cybersecurity blueprint, they have been grappling with precisely this question: At what point do you draw a red line that would activate sort of a cascading series of events that might end up in a real military conflict? This may be a peripheral issue or a conceptual issue for dealing with Russia or China, at least at the moment, it may be a much more actual one with regard to Iran because of what is going on in the real world.

Mr. CASLOW. Sir, if I might add to that, let's go to the establishment of U.S. Cyber Command, darn good idea, great function. DIRNSA, its great leader, I have much respect for the man. Unfortunately, there is one bad aspect of that, something called posse comitatus. The U.S. military cannot exert their arm over domestic United States. Right? We all know this, this is the law, that is the way it is. The Department of Homeland Security has that purview. Homeland Security and NSA as U.S. Cyber Command have integrated in some aspects, but that is a relationship integration, it is not a formal integration. To my knowledge there is no area where

this thing has been crossed. While we can do all we can to defend the National security systems, both unclassified all the way to the TS/SCI, the fact still remains it is our partners who are outside of those realms that are sitting on the regular networks, our friends of Boeing, Lockheed, wherever all this intellectual property is being stolen from, Microsoft, Google, you name it, they are just as at risk. There is no way for Cyber Command to exert their force and what their ideas are to help that other than the fact that if the Google SISO, Information Security Officer, goes to NSA and says: Hey, we would like your input on this, how do you recommend we do it? But there is no massive, as my colleagues stated, this strategy, this deterrent strategy could articulate some of these things and put those in place so we could show these relationships. We could make sure we put things out, that we enforce these to make sure.

Again we can protect the U.S. Government's infrastructures. I have no doubt about that. However, they are going to get us somewhere else. They are going to get us on the back side, they are going to get us on our weak spot. You don't—you attack the bear from the belly, you don't attack it from the teeth, and that is what is going to happen. So I would encourage the look at, and not too long of a dialogue, as in some cases have occurred, but the look at and the discussion with subject matter experts in all relevant arenas, not just the Government personnel and CEO and SISOs of these companies, to get together to try to dialogue and discuss how to do it. Again not just one vector, we need to address all the potential vectors. Because it very well may come from another side that we are not looking. We are treating against termites and all of a sudden it is those darn little fire ants from Florida that gets us instead. Oh, what do we do now? So we need to ensure that we do take precautious action to ensure that we address as many as possible. In order to do that we have to dialogue, we have to put it in writing, put it down, tap it down, and to discuss it. Then we start moving the flag. Once we put the flag in the sand, then we can start moving it around to somewhere we all can agree on and then we take action.

Mr. MEEHAN. Your testimony has been compelling. I thank you not only for your presence here today and the work you have done but for your continuing work of each of you in this critically important area. I think I speak for all of my colleagues on both sides of the aisle by virtue of the attention that we are trying to pay into this issue too that we value and gain a great deal from your perspective and look forward to working with you in the midst of what is a very real and a very genuine, not just challenge, but threat to the safety and security of the United States and its interests.

Thank you so much. I thank the witness for their testimony and the Members for their questions. The Members might have some follow-up additional questions and if they do and they forward those, I will ask if you could be responsive within the 10 days.

So without objection, the committee stands adjourned. Thank you.

[Whereupon, at 11:45 a.m., the subcommittees were adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN MICHAEL T. MCCAUL FOR FRANK J. CILLUFFO

Question 1a. Although Iran is the world's largest state sponsor of terrorism, it is difficult to fully assess Iran's ability to carry out attacks on-line. However, over the last 5 years it has become increasingly clear that Iran's cyber capabilities are becoming more sophisticated and rank among the best in the world.

How likely is it that Iran's leaders would collaborate and/or fund their developing cyber capabilities with foreign states like North Korea that are antagonistic to the United States, or pass on offensive cyber capabilities to terrorist proxies like Hezbollah?

Answer. Those countries that have the United States in their cross-hairs—including Iran, Cuba, North Korea, and Venezuela—and their proxies (notably Hezbollah, in the case of Iran) are assuredly of concern in the cyber context. However, there is a need to think differently about cyber, instead of simply invoking traditional frames of reference for military cooperation. Models for joint or combined defense planning and cooperation must be adjusted to the cyber context. Where cyber is concerned, tools and techniques, exploits, lessons learned, reconnaissance results, and information on targets and vulnerabilities may be (and are) shared frequently between and among states and groups—but that does not necessarily signal formal sanctioned cooperation. Nevertheless, this type of informal collaboration, particularly among parties whose posture is antagonistic to the United States, is an issue of significant concern.

By contrast, formal cooperation in the stricter sense of the term is a less likely prospect. Indeed, there are several reasons that Iran may not seek that type of cooperation to develop their cyber capabilities jointly with other states hostile to the United States. Perhaps the most compelling is that there is little need to do so because there is a convenient alternative: The equivalent of a cyber arms bazaar already exists. Many individuals and organizations stand ready to rent or sell sophisticated cyber attack capabilities, including bots that could be used to steal information or shut down key elements of physical infrastructure. Moreover, the type of collaboration proposed would require a level of trust between the state parties that would seem difficult to achieve, if not unattainable. (The most sensitive information is unlikely to be shared though sharing in more general terms is likely, as outlined above). Keep in mind that each party could potentially turn the capabilities in question on or against the other. Further, neither party could prevent the other's use of the capabilities against a third entity, and once used the value of the weapon drops or may even evaporate, as targets will be able to craft defenses. The significance of each of these potential hurdles should not be underestimated.

Sharing capabilities with proxies like Hezbollah is an even more likely scenario. The exchange could also run in both directions, as Hezbollah has shown itself to be an innovative organization, and because cyber capabilities are of special interest to sub-state actors, since these tools can help level the playing field. In June 2011, Hezbollah established the Cyber Hezbollah organization; and Hezbollah is deftly exploiting social media tools such as Facebook to gain intelligence and information. It is worth underscoring that Iran has a long history of demonstrated readiness to employ proxies for terrorist purposes, drawing on kinetic means. There is little, if any, reason to think that Iran would hesitate to engage proxies to conduct cyber strikes against perceived adversaries.

Question 1b. A hacker group identified as the Iranian Cyber Army (ICA) has received credit for a number of hacking incidents over the last few years. According to reports, the Iranian Cyber Army has used social engineering techniques to obtain control over internet domains and disrupt the political opposition in Iran.

What is the command-and-control relationship between the Iranian Revolutionary Guards Corps and this Iranian Cyber Army?

How does the Iranian Cyber Army fund, train, and recruit hackers?

Answer. Certainly there is a desire, as manifested in attempts referenced and seen in recent reporting and trends, to assert a degree of centralization. However Iran is not monolithic. Command-and-control there is somewhat murky, even within the Iranian Revolutionary Guard Corps (IRGC), let alone what is outsourced. The attribution challenge associated with cyberspace—a domain made for plausible deniability—is therefore all the more complicated where Iran is concerned. Yet, elements of the IRGC have openly sought to pull hackers into the fold; and the Basij, who are paid to do cyber work on behalf of the regime, provide much of the manpower for Iran's cyber operations. There is evidence that at the heart of IRGC cyber efforts one will find the Iranian political/criminal hacker group Ashiyane. The high visibility of attacks seen to date (including the Iranian Cyber Army's strike against Twitter, the Chinese search engine Baidu, and websites managed by the opposition Green Movement) suggests that the Iranian Cyber Army and similar groups might be used as proxies by the IRGC. Though fluid, hacker groups are being cultivated and guided, if not always directly controlled, by the IRGC.

Question 2a. The Iranian government recently held a conference in Tehran announcing the creation of the Iranian Cyber Defense Center within their military forces. The head of Iran's Passive Defense Organization, Brigadier General Gholam Reza Jalali, indicated that the new center may be responsible not only for defensive cybersecurity, but also for offensive cyber attacks.

How likely is it that this center will begin to coalesce the various hacking groups (such as the ICA) into a single entity controlled by the IRGC? What are the known priorities of the new Iranian Cyber Defense Center and how are they developing their cyber workforce?

Answer. As outlined in my prepared remarks, we have seen efforts on the part of elements of the IRGC to pull hackers into the fold to do work on behalf of the Iranian regime. The likelihood of these expedient partnerships coalescing into a (single) cohesive, coherent, and effective unit is questionable, however, particularly if Iran's history offers any guide to the country's future.

Open source reporting on the Iranian Cyber Defense Center is quite scant. Stated priorities include countering threats (of cyber attack), training, "controlling access to computer networks and establishing cyber defense centers in institutions."[1] Workforce development in the cyber domain could prove challenging for Iranian authorities. Monetary inducements have proved useful for enlisting the skills of the Basij, but the supply of talent within the country may well have important limits. The young, clever, creative people that truly thrive in this domain may, on balance, not be sympathetic to the regime or its aims. This problem is exacerbated by the fact that Iran simply does not have the numbers (population base and potential recruitment pool) that say, China does.

Question 2b. Iran's leaders have made concerted efforts to develop friendships with other foreign leaders antagonistic to the United States. What is the likelihood that foreign countries such as Cuba, Venezuela, North Korea, and others, might collaborate with Iran in developing cyber warfare capabilities?

Answer. Cuba, Venezuela, and North Korea undoubtedly constitute a troika of concern. As detailed above in my reply to Question 1, however, there are several reasons that Iran may not seek to formally develop their cyber capabilities jointly with other states antagonistic to the United States—but friendships between and among these parties could increase the likelihood of cooperation or coordination, designed to execute attack(s). As detailed in my written testimony, press reports have alleged "that Iranian and Venezuelan diplomats in Mexico were involved in planned cyber attacks against U.S. targets, including nuclear power plants." U.S. officials are investigating, but media reports have indicated that the hackers who briefed the Iranian and Venezuelan diplomats on the planned attacks "sought support and funding from the diplomats," who in turn pledged "to pass information to their governments." Iran has also shown itself to be ready and willing to partner with non-state entities on kinetic plots, such as the recently thwarted one to assassinate Saudi Arabia's ambassador the United States, drawing on the assistance of a Mexican drug cartel. Given this history, it would not be a stretch for Iran to collaborate with other parties hostile to the United States, whether state or non-state entities, with the intent of causing harm to the United States. Even a limited goal, meaning an attack intended to inflict harm short of defeat of the United States, could still have serious repercussions. For example, a cyber attack (or worse, multiple cyber attacks) executed against U.S. targets at the same time as one or more of our adversaries make a move in the physical world, such as a push to seize key land or shipping lanes, could slow or complicate U.S. response so that we are unable to marshal

[1] *http://forum.internet-haganah.com/showthread.php?399-The-woods-are-lovely-dark-and-deep* and *http://www.mehrnews.com/en/newsdetail.aspx?NewsID=1472234*.

our power fully and effectively. The result could be "a fait accompli" in the adversary's favor.

The ability to achieve synergy between the physical and cyber dimensions, and to embed that capability into political/military strategic planning, would take Iran to the next level. Moving forward, therefore, the United States should pay special attention to discerning and appreciating developments in this area.

QUESTIONS FROM CHAIRMAN MICHAEL T. MCCAUL FOR ILAN BERMAN

Question 1a. Although Iran is the world's largest state sponsor of terrorism, it is difficult to fully assess Iran's ability to carry out attacks on-line. However, over the last 5 years it has become increasingly clear that Iran's cyber capabilities are becoming more sophisticated and rank among the best in the world.

How likely is it that Iran's leaders would collaborate and/or fund their developing cyber capabilities with foreign states like North Korea that are antagonistic to the United States, or pass on offensive cyber capabilities to terrorist proxies like Hezbollah?

Answer. The full extent of Iranian capabilities is, by its nature, difficult to ascertain. So, too, is the question of whether the Islamic Republic is currently actively collaborating with foreign partners on the development of its cyber potential. However, it is worth noting that Iran has in the past worked with countries such as North Korea on a number of strategic programs (to include nuclear testing and the development of ballistic missiles). As well, Iran's efforts to isolate its population from the world wide web are consonant with China's attempts to limit access to internet content on the part of its citizenry. As such, at least some degree of cooperation in the cyber arena can be expected to be taking place between Iran and its strategic partners.

Similarly, Iran is the chief sponsor of Hezbollah, and has aided the Lebanese militia in its armament, its political activities, and its expansion beyond the Middle East. Iranian assistance to Hezbollah in the development of cyber capabilities thus cannot be ruled out, although little is as yet known about Hezbollah's cyber warfare potential.

Question 1b. A hacker group identified as the Iranian Cyber Army (ICA) has received credit for a number of hacking incidents over the last few years. According to reports, the Iranian Cyber Army has used social engineering techniques to obtain control over internet domains and disrupt the political opposition in Iran.

What is the command-and-control relationship between the Iranian Revolutionary Guards Corps and this Iranian Cyber Army?

How does the Iranian Cyber Army fund, train, and recruit hackers?

Answer. The command-and-control relationship between the Iranian Cyber Army (ICA) and the IRGC is not presently clear. Formally, the ICA has depicted itself at least in part as a self-organizing group—akin to patriotic "hacktivists" present in places such as China. However, the ICA's operations closely mirror regime objectives, and its targets are overwhelmingly those out of favor with the Iranian regime, suggesting tacit official sanction and possibly direction.

I do not have knowledge about the methods with which the ICA carries out its training or recruitment. With regard to funding, however, the connections with official regime entities (such as the IRGC) suggests that at least a portion of the ICA's funding is derived from governmental sources.

Question 2a. The Iranian government recently held a conference in Tehran announcing the creation of the Iranian Cyber Defense Center within their military forces. The head of Iran's Passive Defense Organization, Brigadier General Gholam Reza Jalali, indicated that the new center may be responsible not only for defensive cybersecurity, but also for offensive cyber attacks.

How likely is it that this center will begin to coalesce the various hacking groups (such as the ICA) into a single entity controlled by the IRGC? What are the known priorities of the new Iranian Cyber Defense Center and how are they developing their cyber workforce?

Answer. Such organization is a real possibility. To the extent that the Iranian regime would see benefit to uniting various hacker groups and exerting even greater control over their activities, a "consortium" may be the logical end-result. Such a grouping would, by its nature, lend itself most closely to the activities and direction of the IRGC.

Question 2b. Iran's leaders have made concerted efforts to develop friendships with other foreign leaders antagonistic to the United States. What is the likelihood that foreign countries such as Cuba, Venezuela, North Korea, and others, might collaborate with Iran in developing cyber warfare capabilities?

Answer. Such collusion is already taking place, at least on a low level. A documentary by the Spanish-language television channel Univision late last year exposed efforts by the former Venezuelan consul to Miami, Livia Antonieta Acosta Noguera, to recruit hackers for attacks on U.S. targets—an initiative that was carried out at least partly with Iranian assistance. The incident suggests that Iran's efforts to find common cause with anti-American regimes (including in the Americas) extend to the cyber realm—and that Tehran and its allies are actively contemplating cyber attacks on targets within the U.S. homeland.

QUESTIONS FROM CHAIRMAN MICHAEL T. MCCAUL FOR ROGER CASLOW

Question 1a. Although Iran is the world's largest state sponsor of terrorism, it is difficult to fully assess Iran's ability to carry out attacks on-line. However, over the last 5 years it has become increasingly clear that Iran's cyber capabilities are becoming more sophisticated and rank among the best in the world.

How likely is it that Iran's leaders would collaborate and/or fund their developing cyber capabilities with foreign states like North Korea that are antagonistic to the United States, or pass on offensive cyber capabilities to terrorist proxies like Hezbollah?

Question 1b. A hacker group identified as the Iranian Cyber Army (ICA) has received credit for a number of hacking incidents over the last few years. According to reports, the Iranian Cyber Army has used social engineering techniques to obtain control over internet domains and disrupt the political opposition in Iran.

What is the command-and-control relationship between the Iranian Revolutionary Guards Corps and this Iranian Cyber Army?

How does the Iranian Cyber Army fund, train, and recruit hackers?

Answer. The likelihood of the nation-states collaborating could be measured by the current analysis available through the intelligence community assessments on proliferation. While most counter-proliferation has been focused on CBRNE efforts this could be used as a gauge for overall technology transfer. With respect to the non-state actors such as Hezbollah, the best litmus for this may reside in HUMINT reporting. Computer network attack capabilities are for the most part known, within one circle or another. To gain a better understanding of these I would highly recommend that further discussions, behind closed doors, be had with organizations such as the Open Information Security Foundation.

I have no unclassified knowledge of the command-and-control, funding, training, or recruiting for the Iranian Cyber Army.

I wish that I could be of more assistance but given that I still maintain a TS/SCI I am reluctant to discuss any of these issues via this media.

Question 2a. The Iranian government recently held a conference in Tehran announcing the creation of the Iranian Cyber Defense Center within their military forces. The head of Iran's Passive Defense Organization, Brigadier General Gholam Reza Jalali, indicated that the new center may be responsible not only for defensive cybersecurity, but also for offensive cyber attacks.

How likely is it that this center will begin to coalesce the various hacking groups (such as the ICA) into a single entity controlled by the IRGC? What are the known priorities of the new Iranian Cyber Defense Center and how are they developing their cyber workforce?

Question 2b. Iran's leaders have made concerted efforts to develop friendships with other foreign leaders antagonistic to the United States. What is the likelihood that foreign countries such as Cuba, Venezuela, North Korea, and others, might collaborate with Iran in developing cyber warfare capabilities?

Answer. Response was not received at the time of publication.