August 3 Hudson/CSIF Event on Cyber-Enabled Economic Warfare-Transcript

Audio File URL	http://s3.amazonaws.com/media.hudson.org/2015.08.03CyberEnabledEconomicWarfareAnEvolvingChallenge.mp3

Samantha Ravich: Good afternoon. I'm Samantha Ravich, the principal investigator on this project. I want to thank everyone for attending. In particular, I really want to thank the Hudson Institute and the Foundation for Defense of Democracies for co-hosting this event. I also want to thank the co-authors of the monograph. Some are going to be speaking today, Juan Zarate and on the following panel, Mark Dubowitz and Michael Hsieh but some may be in the audience. Abe Shulsky, Annie Fixler and Tiffany Rad. I don't know if Tiffany is her but if you haven't seen it, Tiffany was quoted extensively in a recent Washington Post series on the cyber vulnerabilities of the auto sector.

A few housekeeping notes before we get started. The first panel will begin momentarily. About 1:00, we'll roll right into the second panel, finish around 2:00. There is a short survey that I would ask if you could. If you haven't taken it already, we'd really appreciate it. It's anonymous, it's short. You can fill it out and leave it in that box. It will really give us a better idea about how people are thinking about cyber-enabled economic warfare and where resources should be put to it. We will be publishing both a synopsis of this seminar and the results of the survey. Stay tuned.

All right. Let me set the stage for a few minutes on how the project on cyber-enabled economic warfare really got started. It really had its genesis back in the mid 1990s in discussions with incredibly smart people like Marin Strmecki and Nadia Schadlow at the SmithRichardson Foundation that have sponsored this work about the intersection of economics and security.

In 1997, the Asian Financial Crisis hit, if you remember, began at Thailand and the contagion quickly spread to Indonesia, South Korea, Malaysia, other countries throughout the region. Foreign debt to GDP ratios rose over 180%. During the worst of the crisis, riots occurred, governments fell. The causes of the crisis were varied but most experts think it was the combination of crony capitalism and economic bubble flooding the market with cheap money and simultaneous slump in semiconductor prices with the rise in the value of the US Dollar.

From our perch in Westport, Connecticut, we discussed how economic destabilization in Southeast Asia could potentially affect larger regional securities. What would it mean to prostrate relations, China and Taiwan? What would it do to radical Islamists and separatist groups like [Gom 00:02:48] in Indonesia or Abu Sayyaf or MNLF in the Philippines but it was the Malaysian prime minister at the time, Mahathir Mohamad what he was saying that really got us thinking. Mr. Mahathir directly pinned the blame on international financiers, saying that they had purposely sabotaged the Malaysian economy. He used the words attacked and said that the economic fires were no accident but a Western conspiracy to rule the world and tell other countries how to run their affairs.

We discounted the Malaysian specific diatribe and rhetoric and it's thinly veiled anti-Semitism, if you remember that part but we did think about the broader issue of how a country or countries can use economic means to undermine and adversary or change its policies. We thought back on America's use of economic warfare against the Nazis, then again against the Soviet Union. We began to think if and how the US would need to think differently about these threats and capabilities as the world financial markets became more automated and more integrated.

Over the next decade, the conversation waxed and waned but came roaring back as evidence began piling up on the scale and scope of cyber-attack against US banks, US defense contractors, US intellectual property, our electric grid, our health care system and most sensitive parts of our government. Were we seeing something new?

Again, there's always been economic warfare where 1 side in a conflict goes after the economy of another to affect and weaken its overall strength but the rise of the global electronically-networked economy and the growing cross-border integration and inter-dependence of its constituent parts has produced sizable opportunities for various actors to develop new methods and strategies of economic warfare.

Both state and non-state actors increasingly could contemplate new possibilities for using pernicious cyber penetration of critical economic assets and systems in order to cause harm to a target state's security capabilities.

We label this new class of security threats cyber-enabled economic warfare. The attempt at achieving political and security goals through cyber-enabled economic aggression. In this type of warfare, the United States is particularly vulnerable. As former DNI Mike McConnell said, "If we were in a cyberwar today, the United States would lose. This is not

because we do not have talented people or cutting edge technology. It is because we are simply the most dependent and the most vulnerable."

We started this project with few organizing questions. One, within the escalating cyber-attacks on US public and private organizations, is there lurking a new type of action, some form of concerted strategy to undermine the US economically. Two, that there are adversaries whose strategies are specifically designed to cause economic harm that could weaken or significantly debilitate US security capabilities. Three, is the US prepared to identify and address such strategies effectively? Four, if not, what can and should be done?

We did not attempt to provide definitive answers in the monograph and through this seminar. Rather, what we wanted to do was start a robust, much-needed debate on this topic. The chapter authors and those who have participated in some of the seminars we have held have also been willing to put novel and creative approaches on the table. Some are workable. Some might not yet be workable but it is critical for new ways of thinking to be explored to address this problem because to a person, we are certain that US intelligence, defense, Treasury and Homeland Security departments and agencies appear to be inadequately constructed or attuned at present to address the way these threats are evolving.

The US system for detecting, evaluating and addressing cyber-enabled economic threats seems structurally inadequate and insufficiently focused on the matter. This raises concerns about America's preparedness for identifying and responding to existing economic warfare threats and even more so about its ability to match the rate of their evolution.

With that, I want to turn to our first panel that examines the evolving nature of this debate. We're honored to have 3 highly knowledgeable and well-regarded individuals. Our format is that each will speak for about 10 minutes. Then, we will open it up to Q&A for another 20 or 30.

First up is the honorable Juan Zarate, my good friend. Juan served as the first ever Assistant Secretary of the Treasury for Terrorist Financing and Financial Crimes. He also served as the Deputy Assistant to the President and Deputy National Security Advisor for Combating Terrorism. His phenomenal book, Treasury's War and I recommend it to everybody explores the evolution and importance of this new era of economic warfare. Juan also serves as chairman and senior council for the senate center on sanctions and illicit finance so thank you.

Juan Zarate: Sam, thank you very much. Thanks to all of you for coming. This is a wonderful turnout and a wonderful event. I want to thank the Hudson Institute, I want to thank FDE, Mark Dubowitz, Ken Weinstein for hosting today. Sam, I want to thank you for your leadership for shepherding the authors and the production of this very important piece of work, I think. I commend all of you in the room and those watching online to make sure to pick it up and to read it because the contribution, at least from the other authors in this compendium, are incredibly important. I'm honored to be here today, especially with Steve and Mike to discuss these issues.

I want to thank Sam, too, because she gave me an opportunity to write a bit more about some of the issues that I began to explore at the tail end of my book that I think are critical as we look forward. What I want to do is discuss with you and maybe open up the discussion for the panel to talk about the convergence of financial and cyberwarfare because Sam's laid out 1 of the interesting dynamics of the 21st century is how dynamic, how fluid, how interconnected both the global financial and cyber domains have become and how interdependent they are.

The reality is, the more dependent that the US and Western economies become on those globalized, interconnected cyber systems, the more vulnerable we also become to the potential asymmetric impact and effects of those who may try to attack if not affect US interests.

What I'd like to do is talk a little bit about what that convergence looks like, starting first with the discussion about the nature of the threats and then what this means strategically because I think where we are now is we're facing a very dynamic and shifting threat landscape but also a dynamic and shifting strategic landscape where the threat of asymmetric capabilities is really upon the US and has really been identified by the DNI and others in the US Intelligence community.

Let me start first with the threat landscape itself and in particular the actors involved in the space. It's clear that actors around the world, be they state or non-state actors, have realized that there's asymmetric advantage in using cyber tools, using tools of financial or economic warfare to their advantage, that many ways it provides a low barrier to entry and asymmetric advantage to think about the use of these tools in a much more aggressive way to attack US interests.

In many ways, Sam has laid out the 20th century and the beginning part of the 21st century was really dominated by not just the Bretton Woods system and American economic and financial dominance but really a dynamic where the US found creative and innovative ways to use

financial power and influence and reach insuasion to isolate rogue actors and activities from the global, commercial and financial system.

We're seeing this play out obviously in the negotiations with Iran. We're seeing this play out to a certain extent to the debate around Russia. The ability to use financial and global tools to isolate rogue behavior has largely been the province of the US government and US policy but US competitors and threatening actors realize that those very same tools, those very same mechanisms, some of the same strategies can actually be used against the US for asymmetric advantage.

You see a full spectrum of actors playing out in this space, realizing this dynamic. Super empowered individuals, hackers and hacktivists for political or other reasons, profit often, using these tools to go after the financial system, in particular banks. Sophisticated organized crime groups using deep expertise found easily on the internet, beginning to infiltrate banks and the financial system. Intelligence services figuring out how to use these tools for state and non-state advantage, again for profit and for political purposes. Finally, nation states, some of them major powers like Russia and China, others marginalized like Iran, Syria and North Korea, figuring out ways to use these very same tools to influence. We've seen plenty of examples of that.

One of the advantages to these actors is the low barrier to entry. As we often say, it's not very costly to get into this game or to be on the offense, it's incredibly costly to be defending against these but there's a supply of expertise available on the internet, often sold to the highest bidder. There is the Dark Web that provides access to those willing to play in those dark alleys of the internet and to connect with those with expertise. There's open source protocols and programs that allow individuals and small groups to have global reach. There's weak defenses globally, whether it's at OPM or in other systems around the world where small or relatively weak actors can gain access to prized information.

You have a spectrum of actors with a spectrum of capabilities that provides a low barrier to entry and begins to challenge the US system and dependencies.

The tools of disruption and potentially even destruction are manifold. You have spear phishing techniques and attacks which are common in the cybersecurity space. You've seen DDoS attacks increase in sophistication and frequency. You've seen malware begin to evolve in some pretty dramatic and important ways and, in particular, attacking

the financial sector. You've seen Trojan horse attacks which may portend potential destructive malware and botnet attacks.

These are not just wild imaginings or hypotheticals. We've begun to see them. The JPMorgan attack last summer, effecting 76,000,000 households. A good example of the potential for vulnerability as well as just for destruction. The DarkSeoul attack in March of 2013 lead by the North Koreans, effecting South Korean banks and operations. The denial of service attacks lead by the Iranians and Syrians against Western banks which continue to this day. The Gauss attack against Middle Eastern banks in 2012. The NASDAQ hack which has not been fully determined or attribution figured out in October 2010, matched with significant infrastructure attacks like Aramco and others, portends a real series of adaptations and attacks on the financial system in a way that is strategic, systemic and important.

Now, let me just move very quickly to discuss why the financial system, in particular banks, have become such an interesting and important part of this landscape. As I have often said, in many ways, the international global banks are now at the center of the cyber storm. That's for a few reasons. One, banks in the financial system where the money is. If you want to profit, if you're an organized criminal ring that just wants to make money, want to engage in fraud, that's where you hack, that's where you attempt to get access to data and to money. It's also where intellectual property, sensitive data may exist, both reputational data that's important to banks but also intellectual property that's important to deals and to companies that are engaged in mergers and acquisitions and attempts to enter new markets. That information becomes valuable to a whole host of actors.

Banks over the last 15 years have also become protagonists in many of the national security issues and debates that affect rogue actors and countries. The very isolation of Iran, for example, from the global financial system has been driven in part by what the Western banks have decided to do or not do in terms of business with the Revolutionary Guard or Iranian companies and fronts.

Also, actors in this space, the full spectrum that I described, understand that banks and the financial system are part of the key vulnerability and a systemic risk for the West and for the United States. Some actors, no doubt the most destructive among that spectrum, would find it incredibly advantageous if not helpful to try to bring down the system in some way or to destroy the trust that is at the core of the international financial system, what Hank Paulson called, "The magnificent glass house."

The banks, the financial system find themselves in the middle of the cyber storm at a time when the asymmetric environment is evolving and evolving in some interesting ways as Sam has mentioned. As the report plays out, US vulnerabilities increasing over time, not decreasing with our defenses not keeping up, with hybrid warfare and gray zones of warfare beginning to evolve as parts of national doctrines. We see this clearly with Russians and how they're thinking about the use of proxies as well as cyber capabilities. You see this as well in the environment where there is much more fluidity than in the past with rogue actors able to interact, enable and profit with and for each other. The Chinese government able to use non-state actors to hack and to claim deniability of those attacks. The Syrians and the Iranians developing their own capabilities perhaps relying on others and the North Koreans clearly developing capabilities as seen in the Sony hack and attack of last year.

There are enormous adaptations happening in the environment due to the technologies, due to the global connectivity of the system but also strategically with these rogue actors, with these challenging states, thinking aggressively about how to use these tools. I know the next panel's going to get into some of the defensive dimensions of this, Sam but I do think it's worth mentioning at least some of the ideas that I put forth in my piece and that I know we will discuss here because there has to be a new way of thinking about this strategy, there has to be a new way of thinking about these tools and ways that not only puts us on the defensive but also on the offensive and thinking about more aggressive public/private partnerships and paradigms that allow us to create not only defense and death but also denial, strategies of deterrence which we've yet to do using financial tools like the President's executive order from April 1.

Perhaps some tailored hack back capabilities, in particular instances, perhaps with cyber warrants when the government gives license to the private sector to protect its systems, go and destroy data that's been stolen or maybe even something more aggressive. Then, finally, developing the redundancy of our systems so it becomes less attractive as a strategic tools for our adversaries.

With that, I hope that's a helpful way of framing the issues. It's a much more dynamic environment, not just in terms of the threats and the technologies but also the strategically as we look at the landscape.

Samantha Ravich: That's fantastic. I look forward both in the Q&A from this panel and rolling into the next 1 to discuss some of those things that Juan laid out at the end, particularly the hack back which is a very interesting topic.

Next up, we have Steve Chabinsky, who's General Council and Chief Risk Officer for the cybersecurity technology firm CrowdStrike. Prior to joining CrowdStrike, Mr. Chabinsky served for over 15 years with the FBI where he helped shape many of America's most significant cyber and infrastructure protection laws and strategies.

As deputy of the FBI's Cyber Division, Mr. Chabinsky helped oversee FBI investigative strategies, intelligence analysis, budget and policy development and execution and major outreach efforts and focused on protecting the United States from cyber-attack.

Mr. Chabinsky, Steve.

Steve Chabinsky: Thank you.

Samantha Ravich: Excellent.

Steve Chabinsky: Wow! Those remarks are so good that all you've left me to do is actually pull some of the threads you've brought up because it … Really, what a tour de force as an overview. Where you ended is where I'm going to start. It has to do with strategy. Where are we? Where should be we?

We actually have a failed strategy right now. The way we know this is we keep putting more resources, more people, more effort, more policies in place. The problem keeps getting worse, right? By no stretch of the imagination can someone says it's going well. Even our best efforts to the extent that we say we're doing well over time, it doesn't compare to where the threat's going. That differential keeps getting further.

I want to address why I think we're there but first I really wanted to summarize in my view what those are doing to use from an economic warfare perspective. What we're actually doing to ourselves in response that's making it worse and what this portends for our future and hopefully what we can learn from that. What others are doing to us as Juan has mentioned goes across a full spectrum of activities that range from stealing confidential information, some highly sensitive information, intellectual property that gives our businesses not only a fair market condition but over time, we've seen allowed us to become economically powerful enough to sustain our military capabilities and private information about individuals that we're seeing can be used both to defeat consumer and citizen confidence as well as used against some people depending on how sensitive the information can be used for espionage purposes and blackmail and extortion.

The ability to capture information also shows the ability to change information and to destroy information. Juan brought up a couple of those. The Aramco case in which company in the Middle East wakes up to find 30,000 computers essentially destroyed overnight.

It's not only about data. It's also about physical systems that are being run. If you change the integrity of nuclear enrichment for example which we've seen capabilities that can be used which also can be used against us or manufacturing products, changing integrities to chips, components that go into military fighters, which we've seen through supply chain attacks.

What that shows you is that there are a number of ways for an adversary both to react, to come at us and how they get into systems. It could be remotely. You hear a lot about phishing attacks and we talked about, it could be supply chain as we mentioned. Products are being created all over. It could be either in the design, the manufacturing, the delivery stage. It could be insiders that are sent to our country which is fairly liberal in terms of work visas and the diversity of our workforce. The vulnerabilities are enormous.

Now, let me step back to how we've responded to that because economically, we responded in the worst possibly way. What we've done is we've sunk billions of dollars of our budget into the least probable method of success for a cyber strategy. What we've done is we've focused almost entirely on vulnerability mitigation. We are expanding our surface area through the internet of things and we're hearing biomedical devices can be hacked. One brand that just the other day, The US government told all hospitals to stop using a particular type of infusion pump because they're worried that through the hospital's enterprise network, hackers could get in and start changing the delivery of medicine to patients. We saw, of course, the demonstration of a car being taken wildly off course.

Vulnerability mitigation is a fool's errand if you think that that will work against a determined, persistent, sophisticated, all-spectrum actors of the types that we are up against. It doesn't work in the physical world. What we do in the physical world is we do a certain amount of vulnerability mitigation. You lock doors, you lock windows, you maybe change the quality of your doors and windows but there's a point where if an adversary wants to get in badly enough, whether it's repelling through the roof, cutting through the ground, they will. We change our strategy quite quickly to threat deterrent which Juan also mentioned.

The idea that we concede the ground. We say, "It is possible for you to get in but no longer will this be about me protecting myself. It will be about me going after you." The principles of threat deterrence involved detection. You don't know they're there, it's pretty hard to deter them. We're seeing routinely, organizations, agencies, corporate industries that are very mature, taking an excess of 200 days to even know that there's an attacker on their system. You have to be able to detect them. You have to be able to attribute it, either based down to the person or who's behind it, a responsibility model is perfectly acceptable. We don't know if it's you but you're responsible for stopping it because it's coming from your area. Then, penalties, some penalty based deterrence. The worst that could happen to a hacker currently for most of what we're seeing in the advance space is they get caught and they get to try again. They don't succeed at first but they try, try again.

That model has to change. In the physical world, we put up alarms and so that immediately says it's for detection. You put up cameras for attribution. When your alarm rings at 2:00 in the morning and it goes to the monitoring company, the monitoring company calls the police, they don't call the locksmith to come over because it's about penalty-based deterrence.

You'll note from an economic perspective that what we've done to ourselves in response, we are bleeding ourselves dry financially with our response because it has lead to 2 concepts. One is diminishing returns on our cybersecurity investment, meaning every dollar that we're spending on cybersecurity now is no longer worth the same amount as when you start off. At the beginning of a program, just like in the beginning of physical security, the dollar you spend might be worth $100 of protection or even more, maybe $100,000 worth of protection. It inches slowly and slowly towards having a dollar represent a dollar's worth of security. That's the diminishing return aspect that we're seeing through vulnerability mitigation.

Far worse is we are actually now in the system of negative returns, meaning every dollar we're spending is actually making things worse because it's proliferated and escalated the problem. We see this every day play out in the newspapers, those of us who are seeing victim clients, that the bad guys when you defeat them, they don't give up. They don't just say, "Okay, I used to have a life of crime. Now, let me see. Life of laws. (Is that a phrase?) A life of law." It doesn't happen. They find alternate routes. We just heard about nation state using steganography, codes based in pictures through Twitter accounts to control botnets. It doesn't stop.

What we've done is we've spent our money. It's resulted in an escalation of the problem. Similar, for example, if somebody were to, if someone were to break into your place of business and the response was, "Why don't you put up a 10 foot wall at a price of $1,000,000 around your complex?" Then, they go out and purchase a 15 foot ladder for $30. Then, the response is, "You know what? Fifteen foot ladder. Time for you to make it a 20 foot wall." We all know what's going to happen next but that is happening to us here.

Not only are we falling victim economically to the fact that our intellectual property is being stolen, fair markets are being distorted, our back end finance system itself is vulnerable as is the rest of critical infrastructure but then our response has actually furthered our economic dependencies at a loss of viability for our security.

Where do we go from here? That's really where the second panel is going to answer the questions but certainly, I think that threat deterrence has to be the predominant focus, using all elements of national power, diplomatic, informational, military, economic, law enforcement. Typical [dineley 00:29:27] and consideration of the private sector's role. For that, we have a global private sector, can be very influential. This is not just a US problem, of course.

As we think about that strategy, the other thing that we really have to be concerned with is how the political and economic warfare that we're facing can result in a crisis of confidence in our country, which could of course be as severe or more severe than actual consequences. I think we're facing the real potential of a crisis of business confidence, the ability to be protected in today's global economy, consumer confidence, the ability actually to do anything online any longer, to take advantage of technology like infusion pumps, insulin injection pumps, automobiles.

The economy that's being driven through technology can face a consumer confidence backlash and unfortunately citizen confidence, if we feel that the country cannot protect us and is actually subject to extortion at any given time. In this country, we have police forces who routinely are being extorted through ransomware in which organized criminals are breaking into police force computer, not only police force computers and telling them, "If you don't pay us our ransom fee, we'll delete or destroy or just not allow you ever to have access again to all of your records," and police forces are paying extortion to foreign criminals. What happens when that happens at a nation-state level against us? Is it already happening and you just haven't been appraised of it?

With those remarks, we'll pass it off to the distinguished congressman.

Samantha Ravich: That's fantastic.

Steve Chabinsky: Time for a drink!

Samantha Ravich: It's after noon. Yeah, right.

We are really pleased to have Chairman Mike Rogers addressing us today. As a former member of the US Congress representing Michigan's 8th Congressional District, member of the US Army, FBI special agent, Mike really is in a unique position to shape the national debate on a wide variety of issues including this one. He hosts the nationally syndicated Something to Think About with Mike Rogers on Westwood One. From his time in the US House of Representatives where he chaired the powerful House Intelligence Committee and was a member of Energy and Commerce, Mike built a legacy as a tireless and effective leader on cybersecurity, counter terrorism and national security policy. We welcome you, Mike.

Mike Rogers: Thank you, Samantha. What I've learned today is Steven is an FBI agent that apparently was designed to catch smart criminals. I was the FBI agent apparently supposed to catch the dumb ones. When they need a [door, 00:32:21] Steven, they called me. When they needed to catch the guy in Russia in his mother's basement on the computer, they called you, which tells you how much smarter it was. Matter of fact, I've had the opportunity to meet and spend some time with all your panelists you'll see today and all of the authors of the book. I highly recommend that. Believe me, I've read a ton. This is to the point, provide you some unique talking points that is a little bit different, it's a little out of the box and I love that thing. I spent this weekend reading it.

When I walked into the room today with all the panelists, it struck me that the IQ of the room on average went down 15 points. I don't know why that happened. Oh, come on, people. Lighten up, for god sakes. I know it's pretty serious. Two things have happened in the last decade that we just don't talk about. We don't want to talk about it. We have had a strategic erosion in our dominance in both cyber and space. You think about in 2007 when the Chinese launched a rocket. It took out a satellite humming around our Earth at about 11,000 miles an hour and hit their target. Thankfully, it was their own. You think that from that day forward and then a whole host of other activities including what some would call killer satellites, Americans dominance in space came to an end. We no longer were uncontested in space. You think about how reliant we

are in space for everything we do in our economy. That was a fundamental change and that meant policymakers like us had to start figuring out how we counter that. How do we step up and reach encounter that? Now, you have to launch a satellite that can do its mission set but can protect itself. That is a whole new ballgame when it comes to space. About half of all the satellites up there don't belong to the United States. Some of them are up to some pretty nasty things.

Then you take cyber. We've watched this problem happen year over year over year and here's the thing. Here's the good news about the former DNI McConnell's comment that if we were in a cyber war, we would lose. If we were in a cyber war, we would lose. That's the good news. Here's the bad news. We are in a cyber war in the United States. We're not winning. It's that bad and it is getting worse.

You think about where we are today. Most of our financial system is under attack. Some successfully, some not. We now know and you'll hear from other panelists about how the new generation of technology which we pride ourselves in making a car do amazing things is now susceptible. Airplanes have been hacked. They're susceptible. Our electric grid has been penetrated. It's susceptible. What they don't tell you in the second part of that is, "Don't worry, nothing to see here. Move along. We got it fixed." Why? Because we don't.

The FBI just came out with an interesting report that year '13 over year '14, there was a 53% increase in economic targeted American business espionage. Fifty-three percent increase over 1 year and the bad news was it was outrageously bad the year before. Why? No consequence. They have been absolutely been able to get away with it. China has built an entire economy on stealing intellectual property, not only from us but from our European allies and other Asian allies, anybody that has a company that has intellectual property is subject to getting it ripped off and likely, they have.

We have watched this problem get worse and I get worked up about this. I just read today where Department of Homeland Security has issued a letter in opposition to the 1 piece of legislation the Senate is ready to move here called SISA. For those of you who are familiar with our bill called CISPA, all of that tells you we got problems, right, with acronyms in Congress. For the 1 reason that it allows companies to directly go to certain intelligence agencies to share malicious threat code which, by the way, has been happening intermittently in the past.

The 1 thing that we looked at in Congress and said, "Here's the biggest problem. We have to foster sharing," so everybody says, "Sharing is the key word. If we can share malicious source code in real time, machine to machine, zeros and ones at light speed, we might, MIGHT, be able to put a dent in this." What you're seeing and why we have watched it happen year over year is now there's a bill out there that I think can be very, very productive, allows and protects those relationships so companies can feel comfortable knowing that their information is safe and saying, "We have this malicious source code. You have to help us with this. We don't know where it came from."

Now, our own government is going to work against itself for god only knows how long again over the details of how we come up with this cybersharing regime in the United States. In the mean time, I think the first bill was passed in 2013 by Dutch Ruppersberger and myself in a big bipartisan vote in the house, so we're going on certainly 2 years, going to likely be 3 years. We still can't come together. The White House can't talk to the Congress. The Senate can't talk to the House. The House can't talk to the Senate. In the mean time, how many trillions of dollars have we lost in both potential economic gain and real dollar loss? Billions, billions and billions and billions of dollars. The 1 trump card that they will throw down and they did it in the DHS letter to stop the legislation is, "We have privacy concerns." That stops everything.

In the meantime, the Russians, the Chinese, the Iranians. Unfortunately now the North Koreans, we could list about 15 other nation states, are already on your networks. They're stealing your information pretty much daily at ease, again, with no consequence.

Think about where we are today versus where we were 10 years ago. Space, we are no longer the dominant player in space. It is now contested. Now, our technology is better clearly in many cases but now we have to worry about the safety and security and the survivability of many of those old systems including some of the relatively new systems that we launched into space. Big problem for any business anywhere in the world, let alone how tight we are in the economy. On cyber, getting our clocks cleaned. Now the intelligence community is going to set up its own version of a cyber center to try to police up its act and by the way, I think it's probably a really good idea.

We didn't even know all the capabilities among our own intelligence folks. Why? People kept throwing down the privacy note and we stopped everything for 2 years. We couldn't get the intelligence community together to share information in a real and meaningful way real time

again, machine to machine, nobody's reading emails, in order to push back on what we know is a serious and growing threat to the United States. Couldn't quite get ourselves there.

The last part of this in 2014 is a real policy shift that we all, as Americans yawned and moved along. We had 2 nation states, not the most capable on our list of nation states we worry about, make the calculated decision that they were going to use their nation state capability to exact an economic punishment of a single United States business.

Now, normally, if somebody went in and blew up somebody's warehouse and they fired a missile or sent some sabotage group from somewhere across the world into the United States to do that, it'd be an act of sabotage, it'd be an act of war or an act of terrorism. A political entity using destruction to further its political gains. Clearly fits in the definition of terrorism, at the very least.

We saw a nation states in 2014 and both of those cases now are public. One is the Sands Resort Casino and the other is the Sony case. Both of those involve nation state cyber capability and cyber actors. The problem and I think all the panelists have said today is where is the deterrence to doing this. There is no deterrence. They're not going to stop. They're going to actually increase their ability to have the capability to conduct those kind of attacks. They will continue to pick companies of which they find vulnerable to do economic and real destructive harm.

If you think about the Sands Resort Casino, was similar type arrangement where the CEO gave a speech about why Iran should not get a nuclear weapon. They decided that was an affront enough that they would use their nation state capability to attack the Sands Resort Casino, took them a long time and they ended up penetrating a casino out in Pennsylvania and worked their way back to their headquarters. Took them a long time to do it. They were determined before they did millions of dollars worth of damage at that headquarters for a political purpose. America's response, not much.

We have yawned at this notion that we have this problem but as long as I can get to Starbucks with my app and I can pay for my parking on my iPhone, everything must be okay. The problem is, every day, we erode our ability to protect a growing and more complicated system.

Lastly, we are getting ready to add 28,000,000,000, BILLION, new applications to the internet. The internet of things. Everything from your garage door opener … I don't know about you but every time I walk by

my refrigerator of my house, I think it's working against me already, let alone now thinking it's on the internet working against me as well. This is a huge problem for us. I think you'll hear a little bit about this on the second panel, especially with the automotive focus. We're going to add all these devices, not 1 ounce of security prevention has been planned in any of it. One of the biggest things that happens to you when you have an application on your network is if you talked to your security folks is they probably don't know that application is on their network. There are good companies coming out now understanding how you adequately map in real time and network. It is harder than it sounds. Nobody has completely 100% mastered it. There are a couple that are close but that means on your networks, your private sector networks, there are huge vulnerabilities built in that even the best security company.

You ask, "Why does a serious financial institution on the West Coast get penetrated?" The spend $250,000,000 a year on cybersecurity alone. Two hundred and fifty million dollars, they get penetrated. Why? It's because the complicated nature of network and how you manage the network and even understanding what application is on it. I always say that this is not just a technology problem. It's an anthropology problem, too. It's a people problem.

If you wonder why the Chinese have stolen as much data that isn't related necessarily to a criminal act, Anthem Medical and the list is pretty long. We could be here an hour going down the list. Certainly the OPM, you think of it, lots of really detailed personal information. Why would they do that? Eighty-five percent of all the success rate of a Chinese penetration of your network comes from a phishing email. Imagine the email I can create if I know everything about you for the last 10 years and I mean everything. I also know when the last time you went to the doctor and exactly what you had done at the doctor and what your building status is.

Imagine that email that comes to you at work that says, "Last week, Mike, you had your knee looked at. You had it x-rayed. I think I screwed up on the billing cycle. Would you verify that this was your, YOUR, x-ray not the guy after you?" "Yeah, I was there last week. Yes." The email came from my doctor. At least it looked like it came from my doctor. I click on it. They're in. Eighty-five percent of the Chinese success rate. They've just increased their targeting by 53%. I'm not the smartest guy in the room but in the FBI, we would call that a clue. We got problems abrewing.

I appreciate the discussion and thanks for including me. Appreciate it.

Samantha Ravich: That's fantastic. We have about 15 minutes or so to really open up for questions, focusing on the evolving threat and from this panel, it became clear that the evolving threat is both from our adversaries and frankly from ourselves against ourselves as well. I don't know if someone has a mike or small enough room. Sir?

George Murnel: Hello. My name is George [Murnel. 00:45:07] My question is, is there any difference in approach to cyberwarfare between the public and the private sector? Can we even just say all private sector goes in 1 way, all public sector goes the same way? Is there any difference in approach to that? Thank you.

Samantha Ravich: Want [inaudible 00:45:26]

Mike Rogers: I have, I think, a little bit of a different perspective from some of my panelists so this should be an interesting discussion. I worry about this. Eighty-five percent of the networks in the United States are private. Contrary to popular belief and the National Security Agency is not on those networks. They're not unless they have a warrant to be there and that is highly unlikely. What happens is you have this intelligence service overseas trying to collect information, trying to protect the government. What we want to do is share that information in real time so the private sector can protect themselves.

That's where we are today. It's not working very well. Sharing is terrible No one wants to do it for liability reasons. A whole host of good reasons why not to share which hopefully we can fix. Here's the problem with the private sector saying, "To heck with it. I'm going to go and flick whoever I think did this." Determining who and attributing that attack to a certain nation states or international criminal organization, there are capabilities all over the map. Some can do it very, very well. Some think they can do it very, very well. Some don't have a clue how to do it but wouldn't stop them from doing it anyway.

The government would then be in the responsibility, "How do I protect 25 businesses from what would be the second order impact?" If I attack you, you come flick me in the forehead. I'll guarantee you they're not going to sleep on it overnight. They're going to come back. Why? Because they've already been trained that there's not much of a consequence to doing this. How do you contain that?

If we don't have a good policy on this. I argue, you got to have a good defense before you go out and do something bad to your neighbor. I always say, "If you're going to punch your neighbor in the nose, hit the

weight room for a few months first because he's likely to hit you back." The problem is, we have no good defense today for that 85% of the networks. The companies that are really good at it, they would be fine. It is a lot of companies I wouldn't have any problem doing that. The problem is what do you do when they take out the 15 companies that are their suppliers that can't withstand a cyber attack at all? Now what do we do? Now, we have an engaged private sector against a nation state of which we're watching happen as a government entity. What do you do? How do you stop the escalation?

Now, from a government entity, we have all kinds of ways to stop, to de-escalate any event. You have none of that in cyber space. That's what I worry about. We have to get all of that right before we allow them to have it.

Juan Zarate: Just real quickly, I just love being on this panel with these gentlemen. It's awesome. Three problems and you've identified a critical question. One, the adversaries we're talking about don't differentiate between public and private. They, in many ways, the autocratic states, in particular totalitarian states, it's all 1 thing. Their economic power and influence is a part of state power and influence. The Chinese have actually identified their banks as a strategic asset so starting principal is our adversaries in this space don't differentiate. Secondly, if we think about national defense, resilience, health. Our health system, our financial system, our infrastructure's a part of that.

In some ways, the clear divide between public-private in many ways in this environment doesn't make a lot of sense. Third point I'd make is I think 1 of the challenge and Mike referenced this is how we interact between the public and the private sector. Information sharing is a leading edge of that question but also it's a fundamental question of our national security architecture. How do we actually enlist the private sector in a way that enables them, defends them and makes us part of a national resilient campaign when there's a clear blend?

One way of thinking about this and maybe that's where Mike and I disagree. I do think there's a way of thinking about this a bit more aggressively. A cyber privateering model frankly takes straight from our Constitution. The founding of our republic came at a time when there was much unease about maritime security. We have a provision in the Constitution for letters of mark and reprisal for the government to actually leverage privateers in the maritime security domain, precisely because there was this blend of threats and this blended environment.

I think we need to look a little more aggressively because the environment itself doesn't differentiate between public and private. We don't want to do damage to our Constitution or the way we foster the private sector and protect it but we also can't ignore the fact that the private sector whether it's Sands, Sony, JPMorgan are a part of our national resilience and economy.

Samantha Ravich: You want to hear 1 other question, then you …

Steve Chabinsky: Actually, I wanted to add 1 thing on this matter. It's something that both Chairman and Juan talked about when discussing the differentiation in our country with what's government owned and what's private sector owned but it goes past that and our country and most of the Western countries, there's a very hands off view to the internet. You have to allow technology to innovate and governments actually have it as a philosophy to not get overly engaged in the infrastructure. That's not happening everywhere in the world.

The companies that we already mentioned that get thrown out, Russia, China, North Korea. They are vulcanizing the internet. You just don't realize it. They have filtering in place. They own the infrastructure. They're monitoring the infrastructure. They can take it up, turn it down, have resilient approaches. That relationship that we have with the private sector where we're hands of but at the same hand, it's not resulting in secure outcomes, isn't being followed everywhere. What we're seeing is, as the rest of the world, those who tend to be the aggressors are really locking down their infrastructure. We're going in exactly the opposite direction in a way that really would not be considered I guess obvious when we do other things.

For example, if I were to say, I could develop 1 cell tower that has so much power that all you need is 1 cell tower, you'll always have your 4 bars wherever you are in the country. The only problem is it'll give you cancer, everyone said, "That's a ridiculous invention. It's no good. Don't use it." If I said, "I can build a car that can go 2,000 miles an hour, you'll be in California before you know it. The only problem is our roads aren't set up for it," everyone would say, "That's the most ridiculous, ludicrous idea I've ever heard." In technology, you can develop and sell almost anything regardless of the security and economic consequences to our country.

We really have to start thinking about what we're permitting and that relationship between the private sector and the government has to really shift in common cause to health and safety and security.

Samantha Ravich: Great. Thank you. We'll take a couple of questions. I just want to reference in the monograph, both in Juan's chapter and in Michael Hsieh's chapter, there are discussions about letters of Mark. In fact, there's really interesting footnotes about some law school articles that have been written specifically about letters of Mark in cyber that I commend you to …

Keith Smalley: Good afternoon, Keith Smalley. Just want to follow up on your last comments, Mr. Chabinsky. A lot of the focus is, how do we make the network more defendable, more robust, more resilient. How do we attribute the threat act or who actually hacked the system. At what point do we flip the model that you were just alluding to and start holding the actual manufacturers accountable because they guarantee you in most of these intrusions, whether it be Sony or elsewhere, it may have come in by a spear phishing attack but it was utilizing a vulnerability in Adobe or Flash or some other vendor software that is running on that network. What time do we start holding them accountable and start cleaning our own house?

Samantha Ravich: We'll start with Steve, yeah, and then others.'

Steve Chabinsky: I think it's the wrong perspective, frankly. We don’t demand perfect security in any other aspect of our life. I would never dream that if my house got burglarized, I should start going after the architect and the contractors and saying, "Someone was able to tunnel through the ground." Our market right now is incentivizing the purchase of low cost, quick to market products that don’t have that level of security but never will. I'm not saying that there can't be a better job in coding and there are some companies who have done an excellent job. I'm all for it but the fundamental issue we're talking about today would not change, that nation states and organized crime groups that are persistent and determined will always be able to break in sooner or later because it is impossible based on vulnerability mitigation efforts to secure a dynamic inter-operable environment which is what we have in the internet.

The only time you see it in the physical world is something like a bank or a fortress. It doesn't move and it doesn't change much over time. You can really secure it but once you say, "We're actually going to meet up with everybody and we're going to change all the time through updates, upgrades and connections," that's the fool's errand.

The real choice here is how are we going to start taking some of this money and putting it into a robust conversation and an intellectual analysis, bring actual analytic standards to options analysis. When these

things happen, how do we build platforms that were necessary, are not necessarily better at being secure but are a lot better at detection, attribution and then figure out what our policy choices are. We might find out despite, I think you took the card. I'll make it this 1 that some of the systems that we need the best security for coincidentally and a good coincidence have the least privacy concerns like the electric power grid.

If you worked for … Forget about [inaudible 00:55:19] for a second but the standard electric power grid, everybody there that owns it wants to have perfect knowledge of who's on it at every single time, very low privacy demands. That's where I would start, not necessarily from cleaning up the house from a mitigation point of view, which god bless you if it could be done but figuring out how to build in detection attribution and real policy choices to give to our leaders in those areas that matter most.

Samantha Ravich: One, 2 things.

Juan Zarate: Yeah, just real quickly. I think there's a different dimension of liability here that's important because what we haven't enabled is frankly the private sector bar and the plaintiff's bar to actually be a force in this environment. With the attribution revolution, I think there's actually an opportunity to think about class action lawsuits, key tem actions, victims of cyber malignant cyber-attack that allow victim companies, individual shareholders to actually go after companies that are taking advantage of the environment.

Chinese SOEs that are using stolen data, why aren't they subject to not just government action but potentially even private litigation. The question of liability's an important 1 but I think we need to flip the model a bit more and empower the private sector to actually be an actor and deterrent.

Samantha Ravich: Mike, do you have … I think we have time for 1 quick question. Michael, quick?

Michael: [inaudible 00:56:47] just to get you all on the record on this, just to get you all on the record on this, could you …

Steve Chabinsky: How fast the tables change!

Michael: Yes. Is it fair to say that the US private sector in cyber has no right of self defense, according to the law, that that is our policy? We have no right to self defense? In the same way there's a duty to retreat, we have no right

to self defense. I think I'd like to begin with Juan because you advise banks on this when you listen to the lawyers and the lawyers seek to work with you on this, do they feel that the bank has a right to defend itself when it comes under attack by either criminals or by nation states?

Juan Zarate: I think part of this is how unifying defense, right, because if you can define defense passively, and say, "Of course we've got the right to defend. We've got the right to create layers of redundancies," and lot of the criticism is they haven't done those. They haven't done a lot of the cyber hygiene that they need to do in terms of employee awareness, et cetera. They would say, "Certainly we can do that."

There's also a lot of reticence of the private sector to the chairman's point to actually getting involved too actively. There are a lot of companies that really don't want the very idea of hack back or to be active defenders of systems. They want the government to do it. They want more information to be able to do it themselves. In that sense, if you define defense broadly, yes, they do. Do they have an active defense role to play at this point and is there a legal structure for that? No.

Mike Rogers: Defense of personal property is a justification so it's an otherwise illegal activity. I think it's very unserving. We haven't seen prosecutions against companies. That might be prosecutorial discretion. We don't know what happened if there were a case that was taken up.

Unfortunately, a lot of this is theoretical but what I certainly would say is there's no certainty in this area. Businesses, unlike individuals who are more likely to roll the dice, businesses hate uncertainly and we're a nation that can't even get a national data breach law. We're stuck with dozens upon dozens of individual state laws in the area of data breach notification. What's the chance of a company figuring that they have certainly of action, even within the United States no less how that might be observed outside of the country, where they are likely doing business. I think the short answer is, do they? There's no clear answer to that but that factor is enough to make it that big businesses that are responsible are not going to touch it.

Samantha Ravich: That's great.

Steve Chabinsky: Yeah, when you start talking about extra territorial aggressive defense, I think that's a loser from the point go. If you do not have proper legal authority, I think it's a disaster, mainly because in the stand your ground circumstance, you're dealing with a personal threat to your life. In the way the law is written is it has to fit that criteria. This you could never

make that legal argument in here, number 1. Number 2, again, when you decide you're going to breach territorial jurisdiction and go after someone, you have opened up a can of works of which is well beyond the scope of your threat. That's where we have … Our policy is not there. We don't even in the United States have a good offensive policy.

I think it was Admiral Rogers not that long ago, within the last few months, said just as much as that, that we don't have a good cyber offensive policy. We talked about it ad infinitum in classified settings for the entire 10 years I was on the intelligence community. We could never get consensus to move to the next place on what that cyber offensive is.

By the way, just as a personal note, I just saw the administration says they're going to make China pay for the consequence for the OPM hack. I can't wait. I cannot wait to see what the heck that thing is. Candidly, I'm not too excited about what's going to be. We haven't crossed that threshold to bring everybody in a room and try to work through this problem. Long answer to your question but I don't believe they have the right to go extra territorial to protect what they perceive to be a threat at that point.

Samantha Ravich: Fantastic. Thank you. Thank you so much if we can get a hand for our speakers. It's just great. You can see how we can take many hours talking about that but we're going to roll right into the next panel on capabilities needed to protect and defend in a cyber enabled economic war.

While we're getting our seats before I turn it over to the panelists for this discussion, I want to read a very short paragraph. "There's an intellectual no man's land where military and political problems meet. We have no tradition of systematic study in this area and thus few intensely prepared experts. The military profession has traditionally depreciated the importance of strategy or politics are important as compared with tactics. Now, we are faced with novel and baffling problems to which we try to adapt certain ready-made strategic ideas inherited from the past. If we examine the origin and development of these ideas, we may be better able to judge whether they actually fit the present and future."

This was written in 1959 by Bernard Brodie in his treaty, Strategy and the Missile Age. It is a prescient piece. I recommend it to all his calls for new ideas and scholarship to deal with the atomic age helped the US create the doctrine and capabilities that guided us for the last half century at least.

I would add to Brodie's assessment that there is an intellectual no man's land where political, military and economic problems meet and that we have no tradition of systematic study in this area.

Within our monograph and in our earlier seminars, I have turned to earlier work that I and others did on the nuclear kill chain and thought about its applicability to this evolving threat of cyber-enabled economic warfare. There are indeed vast differences, namely the hurdle for development, acquisition and use but also what I call in 1 of the previous panels, somewhat referenced it, could we be in a war and not notice metric.

I think it would be hard to ignore the use of a nuclear weapon but as we heard in our last panel, we are fully engaged in a cyber-enabled economic war. The kill chain of needed capabilities, so to speak, may have to be thought about differently but nonetheless, it's basic elements, intelligence and warning, deterrence, detection, forensics, interdiction, battle management, consequent management and recovery serve as a useful way to gauge our current capabilities and create the doctrine and technologies that we need going forward.

At this point I want to welcome our 3 amazingly talented individuals that we'll talk about the nexus of policy and technological developments. The first is Mark Dubowitz who's executive director of the Foundation for Defense of Democracies where he leads projects on Iran, sanctions and non-proliferation. He's an expert on sanctions and has testified before Congress and advised the US administration, Congress and numerous foreign governments on Iran and the sanctions issues. He heads the foundation, FDT Center on Sanctions and Illicit Finance and is the co-author of more than a dozen studies on economic sanctions against Iran. Mark, off to you.

Mark Dubowitz: Great. Great. Sam, than you very much. First of all, Sam, I hope you will keep me to my 5 minutes. Maybe give me a nudge if I'm over 5 minutes. I'm going to try to make my remarks short. I want to thank Sam very much for involving me with this project. Been a fascinating project. Amazing people to be involved in. Ken, thank you much for hosting this and allowing FTD to co-host this. Mark and Michael, pleasure again to be with you.

Also, I want to pay a special note to the young woman who co-authored this report with me, Annie Fixler who's based in New York who is 1 of those remarkable people, next generation of economic warriors. I know Juan knows her very well, Samantha knows her very well and it's

certainly, I think, satisfying for the 3 of us than when we're off playing golf in our retirement, someone like Annie is going to be continuing the fight.

Let me talk a little bit about the paper that we wrote together. I want to put this in context. The paper is called Cyber-Enabled SWIFT Warfare. We call it SWIFT warfare because the case study that we dealt with as part of the analysis is the SWIFT financial messaging system which is the global standard that if I want to wire money to Juan, my Citibank has SWIFT codes and Juan's account at Chase Manhattan has SWIFT codes. It's the way our 2 financial institutions talk to each other so I can wire money to Juan which I do often.

No, no. Absolutely. The key looking at SWIFT is SWIFT really was the high point of the US government's economic warfare campaign against Iran. It reminds me there was a point and time where we were actually engaged in economic warfare against Iran. This is coming at a particularly troubling moment for me, spending a lot of time working on Iran to see the US government now dismantle the entire sanctions infrastructure that we put in place in pursuit of this nuclear deal but that's a topic for another panel.

Certainly for periods of time but as David Sanger said in the New York Times, the US Treasury Department where Juan worked and under Juan's leadership and Stuart Levy's leadership, David Cohen's leadership and now Adam Szubin, the US Treasury Department was described as President Obama's favorite non-combatant command and for good reason. It had become the locus for economic warfare against the Iranian regime and really was a decade of escalatory measures that began under President Bush, the designation of key Iranian banks and Revolutionary Guard entities and it actually culminated in the passage of sanctions legislation by Congress, Congressman Rogers certainly played a key role in that.

It was fascinating because as these sanctions escalated, you saw over time a dramatic impact on the Iranian economy and on Iranian decision making. Some of the key events along the way, included the US Treasury departments, USA Patriot Act 311 where they actually was a finding that the entire jurisdiction of Iran, the financial sector of Iran was the jurisdiction of primary money laundering concern. It was legislation that was passed by Senators Menendez and Kirk which legislatively designated the Central Bank of Iran as the key pillar of that jurisdiction of primary money laundering concern.

Then, in 2012, again Congress over the objections of the Administration and the Europeans, actually passed legislation threatening sanctions against the board of directors of SWIFT. That legislation encouraged the Europeans and eventually SWIFT to expel dozens of Iranian banks from the SWIFT system. It was unprecedented. It was the first time in SWIFT's history that there was a wholesale deSWIFTing of a country's financial institutions. It ultimately cut off Iran from the global financial system, made it impossible for the Iranians through the formal system to move money, to finance trade, to repatriate their foreign exchange earnings.

Now, it was certainly a tool of very effective coercion but it was something that our adversaries have learned from. I would note that when it comes to SWIFT, we see calls from the US Congress, from the British government, in fact, from pro-Palestinian organizations to use SWIFT, again, as this ultimate instrument of economic coercion. In fact, last year, pro-Palestinian organizations acts SWIFT to de-SWIFT Israeli banks, particularly those banks that had branches in the disputed territories.

The British government had asked for SWIFT to deSWIFT Russian banks. That lead to a response from the head of 1 of Russia's largest banks, VTB Bank who said, "That deSWIFTing of the bank would be an act of war, an act of economic war."

We've seen our adversaries try to take our playbook on Iran and use it in other ways. In Russia, the Russians are using economic warfare against our allies in central Europe and Eastern Europe. There they're using energy warfare. The dependence that our European allies have on Russian national gas for example. There's been a whole series of measures, both offensive measures against Russia because of its annexation of Crimea and invasion of Eastern Ukraine but also retaliatory measures by the Russians against our allies and against the United States leading to the need for defensive measures.

If you move to the Asia Pacific region, the Chinese have used economic warfare and political warfare against Taiwan, for example, for years to persuade the international community that Taiwan should not be recognized as an independent state. The Chinese cut off the expert of rare earth minerals for a couple of months when there was a dispute with the Japanese. Those rare earth minerals were very important, were actually critical to key industries of the Japanese economy. As everybody knows in the south China sea there have been significant territorial dispute between China and the Philippines and Vietnam and Japan and

other countries. The Chinese have matched their naval maneuvers with economic coercion.

What you're seeing essentially is our adversaries learning from us that the power of economic warfare, the power of economic coercion as a dominant instrument of course of statecraft.

Now, the United States and certainly our allies in the Middle East, in Asia and in Europe are lucky because the United States still remains the dominant global financial superpower. Eighty-one percent of global transactions are done in the US dollar, 60% of foreign exchange reserves are held in the US dollar. Forty-five percent of global financial transactions are done in the US dollar. Because of the US dollar's dominant position in the global financial system, we still wield tremendous power but make no mistake. That is changing. It's changing in some fundamental ways.

The Russians and Chinese for example are creating an alternative to the SWIFT financial messaging system. It's in a nascent form right now. It's unlikely to track to support that SWIFT has today with 10,500 financial institutions using the SWIFT system but over time, it may erode the global dominant position of SWIFT. The Chinese have a combination credit card/Interac card which is available in 100 plus countries around the world. It has a market position that represents 45% of the total number of cards in global circulation and something like 25 to 30% of the global transaction value. Quite extraordinary.

For the Chinese, it's very useful and the Russians because it's delinked from New York. When we were imposing sanctions on Russian banks, the Chinese moved in after MasterCard and Amex and Visa moved out and offered this card to Russian banks who then offer an Interac card and a global credit card delinked from New York and therefore not susceptible to our sanctions.

The Chinese have set up the Asian Infrastructure Investment Bank which is an alternative bank for infrastructure financing which has attracted significant global support including for most US allies.

As a final example and there are many others, the Chinese have gone to the IMF and asked that the, something called the SDRs, which are special drawing rights, which essentially represent a global asset, a foreign exchange asset. That asset is linked to a basket of currencies including the US dollar and the Chinese Yuan. The Chinese have been pressuring

the IMF to actually change the allocation, the percentage allocation in that basket so the Yuan is more highly represented.

These are just 4 examples of how over time, the Chinese are trying to erode our global dominance. We may be witnessing the creation of a parallel financial system over time that diminishes the power of the US dollar.

Let me end on this, with this specific recommendations. Andy and I conducted lots of interview with folks in the US government, lot of former Treasury officials, state officials, people in Europe and Asia because what we really wanted to find out was what kind of defensive measures were we actually taking? We've been very good on the offense but how good have we been on the defense? What we discovered particularly in the US is that there hasn't been as much thinking about defense of economic warfare. How do we create an economic defensive shield to protect the US and our allies from the use of offensive weapons by the Iranians, the Russians, the Chinese and others against our closest allies?

You'll see in the monograph, came up with some specific recommendations but specific recommendations within the US government changes institutional changes within the interagency. The idea of creating number 1, an office of policy planning at the US Treasury Department. State has an office of policy planning, our recommendation is a Treasury Department should have an office of policy planning where they're really thinking about these kind of defensive measures and they have the time, unlike our friends, the Treasury who are drinking from a fire hose every day to think through what kind of specific measures we can put in place to defend the United States and our allies.

Number 2 is actually standing up an economic warfare directorate or subdirectorate at the NSC. Our sense from the NSC is those folks have a lot of strong planning on the economic side. They understand markets, they understand financial markets but the idea of having people at the NSC who understand sanctions and illicit finance and the use of economic warfare would be useful.

Three was actually establishing a doctrine on the use of economic warfare. We have doctrines about everything. We have doctrines from the nuclear age. We have doctrines about missile defense and we certainly have a new cyber doctrine that folks have spoken about. An economic warfare doctrine would be very useful. How should we be using it offensively, how should we be using this defensively?

Then, maybe a controversial recommendation but the idea of setting up an economical warfare command, all right? We actually have commands in the US government. Most of them, I believe, are at the Pentagon but this idea would be an economic warfare command that would draw the best and the brightest and the necessary resources across the inter-agency. Our recommendation was to locate a treasury. I'm sure there'll be a lot of debates about that.

Those 4 specific recommendations on both doctrine and on institutional changes so that we can actually protect our allies against the use of economic coercion.

I'll finally end with this. Israel's been an interesting example because the boycott, divestment and sanctions, movement against Israel suggest that we are seeing the canary in the coal mine. We're seeing that here is a small democracy, liberal democracy, an ally to the United States where all of a sudden, economic warfare is being used against Israel to achieve political objectives of those who oppose Israel's position in the territories.

Whatever position you take on the territories, whatever position you take on these regional disputes, my assessment, my conclusion is we should be protecting our allies with cyber defenses, ballistic missile defenses, military defenses and economic warfare defenses regardless of our assessment of who's right with respect to a regional dispute. This is the canary in the coal mine. As terrorism once came to our shores, economic warfare will 1 day come to our shores. We have to start thinking through the kinds of methodologies, doctrines and institutional changes to create that economic defensive shield.

Samantha Ravich: That's great. The only thing I would take issue with is economic warfare has reached our shores. I think Mark and Annie would agree. In their chapter, they really do delve down into, "All right. If we're going to be serious about this, then let's be serious." What does that mean in terms of organizational changes that may be necessary in the US government?

Our next 2 speakers focus on where really the rubber meets the road in terms of the technologies that are going to be needed, how we think about that because ultimately, we're going to have to be able to back up our words of deterrence with our technologies.

The first speaker is Doctor Michael Hsieh, who's a program manager in the Information Innovation Office at DARPA which for those who may not know is the Defense Advance Research Project Agency. His focus is on

quantitative and cryptographic techniques for establishing provable security and big data in software. Previously, he was a research scientist at SAIC and a scientific consultant at Booz Allen Hamilton. He holds a PhD in chemistry from Princeton. Michael?

Michael Hsieh: Okay. First of all, thanks. I think I speak for Mark as well, too, when I say that those of us who work on the technology side of the house found this to be a very useful and fun exercise to think about the broader context in which a lot of our work lives.

As a prefatory remark, I should say that all the opinions I express today since I'm still in government are my own and not those of DARPA or of the US government.

I'm actually going to begin on a slightly downbeat note. Today, you can barely turn on your news browser without seeing a fresh story of yet another US firm victimized by some kind of economic espionage or intellectual property theft. What is vexing about today's state of affairs is there does not seem to be a clear path out of this very bad equilibrium. The purpose of my article in the monograph is to hopefully provide some new thinking that may help us out of the state, 1, by taking a historical perspective on economic espionage as really a timeless instrument of competition between nation states. Number 2, a scientific perspective on technology that can potentially help us flip the script on the economic spies and IT pirates that are targeting our national industries and undermining our national economic strength.

To begin, we have through history that can help us here. The notion of intellectual property actually evolved over centuries as an enshrinement of a system of economic reward to the inventors of valuable ideas. The United States economy is particularly sensitive to the climate in which such rewards are protected because in a 2012 report by the US Patent and Trademark office, 75 out of 313 US industries are categorized as IP Intensive. They account for more than 27,000,000 jobs and more than 18% of all employment in the US in 2010.

According to the 2013 report by the commission on the theft of American intellectual property, the US loses over $300,000,000,000 a year in IP theft. The report stated that if IP were to receive the same protection overseas that it does here, the American economy would add millions of jobs and encourage significantly more R&D investment and economic growth.

Now, unfortunately, not all countries in the world are serious about protecting a rule of law based IP right regime but perhaps 1 of the great ironies of history is that United States has been here before in this problem although on the other side of the problem.

In the immediate aftermath of America's war for independence from the UK, our young republic itself engaged in no holds barred campaign of privately conducted but officially tolerated IP theft against British industry in order to supercharge the young American manufacturing economy.

Now, the British response to this was quite rigorous. They were fully aware of the stakes of this type of conflict. They exposed export controls on machines and designs, restrictions on skilled immigration and sometimes acts of arson against US factories employing stolen British IP.

I know there's been some talk about hack backs in the previous panel and this isn't really what we have in mind but the idea of hack backs is not terribly new actually. It's been tried.

Arson aside, the British strategy would not look unfamiliar to American officialdom today yet by any reasonable accounting, the British policy completely failed to snatch the diffusion of their most sensitive manufacturing IP into the factories of its unfriendly transoceanic rival which went onto eclipse the UK as the world's manufacturing leader.

Now, all of this must sound distressingly familiar to all of us today. In 2015, it's obvious that it is America that is playing defense in this game. To exemplify the struggles of all of our IP sensitive industries, I will focus on the software industry not only because they are the largest by export value but because they are also new ideas pertinent to that industry that might inspire new thinking for other industries protections as well.

To give a partial illustration of what our software industry struggles with, in a report by the Business Software Alliance, 19% of the software sold in the US is pirated but in China as 1 other example, 77% of the software transacted is pirated but beyond the simple crime of making and running unauthorized pirate copies, there is actually the deeper and far more insidious theft made possible by prying into the source code of software to extract the proprietary algorithms and ideas that are created through vast sums in research and development dollars.

How do we stop something like this? Through the lens of how we might protect our software industry, we developed a new model for thinking

about how to protect our IP based not only on law and diplomacy but on technology and economics as well. That may change the dynamic between attacker and defender in this IP conflict.

The status quo in defending our nation's IP interests in general tilts towards the kind of diplomatic and legal remedies favored by the British. As we have seen through historical experience, there are fundamental limitations to this kind of approach. It is useful to pull back a step and think about the problem at a more basic level.

IP theft is fundamentally as much an economic as it is a criminal phenomenon. We have seen through again historical experience that laws and diplomacy are limited in their ability to deter criminals from this kind of crime. The question is can we use technology and economics to deter economic decision makers from deciding to steal as opposed to not steal? Can we raise the technical cost of stealing to such high levels that it no longer becomes worthwhile to do so?

The good news is that the answer is yes but there are some major caveats. Today, commercial software is effectively defenseless against being robbed of its deep IP by reverse engineers because the state of the art in defending software against such theft largely consists of inserting passive [jut 01:24:16] code to inveigle the attacker by essentially giving him more code to read and to understand.

However, this security through obscurity approach can almost always be defeated in under a day with standard software tools. It's almost universally regarded as ineffectual among software security experts.

The good news here is that a recent mathematical breakthrough by UCLA computer scientist Amit Sahai and collaborators has opened up the door to making new kinds of software that can baffle even the best resource reverse engineers. The new approach entails writing the source code in such a way that unwrapping it's inner commercial secrets is equivalent to computing a mathematical problem whose solution provably requires lifetimes of effort even with the most powerful supercomputers and algorithms known today.

This is exciting because this is the kind of technological breakthrough that could be the impetus for imagining a future where IP rights are protected not by the laws of governments or nations but the laws of mathematics. Here there are some huge caveats. Realizing such technologies not only for software but maybe for other products as well, too, will very likely require radically new scientific ideas that will take years if not decades of

sustained research and effort but if these efforts are successful, such efforts could ensure economic leadership far into the future.

To pivot to another problem, 1 of the issues that we have in the cyber threat today is that victims are caught up in a very pathological dynamic in which they actually have sometimes an interest in concealing their own victimhood. We talked about this in the context of cyber threat sharing.

One of the other interesting things that has emerged in the academic research over the past 30 years is the field called secure multi-party complication. This really began as something of an academic problem about a little bit more than 30 years ago. This is called the millionaire's problem by which 2 millionaires want to see which one of them has more money but they don't want to reveal exactly how much money each of them has, basically. I don't know how millionaires think but it's a neat problem.

The bottom line is that this might seem like a contrived problem but from a cryptographic and mathematical perspective, it's not trivial at all, actually. A whole field of cryptography built up specifically around this that morphed into what we call SMPC today.

Now, given that that was a relatively contrived problem 30 years ago, what this has evolved into 30 years later is a very valuable and practical technology in a very real problem. In space today, there is some dozens or if not scores of space-faring nations. They all have their satellites going at very high speeds. Every country and every agency and every company has an interest in not having satellites collide. The problem, though, is when you reveal your trajectories, you're giving away sensitive commercial information or even national security information. How do you share information about your satellites without giving away those kinds of secrets? Where the research has gone is from that very contrived millionaire's problem some 30 years ago to actual technology to actual software today. That could actually help the likes of national space agencies and companies share their information without revealing private information.

This is obviously exciting because these are not trivial problems. For the math geeks out there, these are 200 degree integrals, actually, over space and time for objects going at near relativistically relevant speeds, basically. It's a hard problem and computationally very difficult but there again exists software after 3 decades of investment that actually gets us closer to that problem. It's not hard to see how this maps onto a lot of the kinds of sharing problems that we have within the cyber threat realm

which actually has a non-trivial and very important privacy component as well, too.

To conclude, I think it's very fitting that the ingenuity of the American economic system that has produced so many value creating, world-changing ideas could be at the end of the day, a source of defenses to protect those very ideas. Thank you.

Samantha Ravich: Thank you, Michael. Doesn't it make you feel good that he's in the government protecting us?

Male: [Inaudible 01:28:28]

Michael Hsieh: Yes.

Samantha Ravich: Yeah, he is tremendous. The modern day, I think, problem of the millionaires problem now is to actually figure out how much money does Donald Trump actually have. I think that's what it's evolved to.

Finally, Mark Tucker is the founder and CEO of Temporal Defense Systems and founding board member of the Cyber Insurance Company of America. At TDS, he leads a team of experienced white hat hackers and technologists that are redefining the technology, security paradigm to safeguard competing devices and networks in the cyber war era.

Rick, welcome.

Mark Tucker: That was a mouthful. Thank you, Samantha and thank you for inviting me. I think this is a great way to look at the problem because this problem is a complex problem and it's really not quite understood but when you marry those 2 terms of cyber war with economic cyber war, it brings multiple notions that help cross pollinate and define the problem.

Before I go into a few things and ideas I think might help correct the problem, I think we're still at the point where we need to quantify and basically understand the problem's dynamics.

When I heard a few things in the previous panel, I was diametrically opposed but I was down there and couldn't talk. I've held those things. I understand why the comments were made. The comments were made because of these trends and these economic things happening and trying to understand the essence of what's going on here is what forums like this are about.

When you look at cyber economic warfare, you're like, "What is it?" It's war. It's not crime. There's a difference between having a war environment and a criminal environment. Crimes happen in war but I think it's very safe to say that if we get some actionable assumptions and say, "Okay, maybe it's not provable 100% but a preponderance of evidence means that this assumption is pretty good and we can start making some action plans around it," because ultimately, I think America needs a cyber action plan. We've got the Department of Cyber Command now. We've got multiple departments of everything but the core of the problem is still a little bit elusive. I think a few things in the first panel were perfect and spot on.

Let's say actionable assumption, cyber war is here and upon us. I would go so far as saying, "When did cyber crime become cyber war?" What inflection point and time did that happen? That's happened in the Stuxnet attack. That was the shot heard around the world. That is when cyber war became a bit like the turning point of criminal gangs and all these activities happening to something that became a physical damage was caused. It caused geopolitical outcomes because of it. That 1 thing is shot heard round the world, we can assume that cyber war is here.

Then, we start looking at, "Well, what is the dynamic of cyber war look like?" It looks like a low intensity conflict in war terms, to me. It doesn’t look like the power balance between the nuclear war era where everybody built up these huge offenses and nobody struck. Why? Because there's proliferation has already occurred. That dynamic doesn't exist in cyber because there's too many actors, there's too many people. It takes 1 individual. That would be equivalent to saying, "Well, if we think about it like trying to do a nuclear power arms race buildup of offensive cyber weapons, it just won't work because we can't control it. There's too many points of attack basically heading through," but if you look at it like a low intensity conflict, you can pretty much say, "Okay cyber war is here to say for a long time."

There's going to be interesting things that happen. The playing field is basically, if I can compare a few examples of where a low intensity conflict is occurring, we look at Iraq in 2004 when all of a sudden, America comes in. We take the country over. I was there, by the way, so the ground truth I had then is equal to the ground truth I have now on the problem. I've seen it from all different levels.

When I was first there, there was a bomb here and there and it went off. Yeah, it was scary but in essence, it was a power void because Saddam

was gone and nobody knew what to do. The criminal gang started to move first and there was a little bit of activity happening.

What happens when those types of low intensity conflicts evolve, the next stage is coordination, where all of a sudden, there's 6 bombs going off and they're going off at the same time and the frequency's going up. When we look at the threat horizon over a 20 year period on cyber war, basically what we're seeing is a negative threat. For 20 years, a negative trend that's occurring.

Now, when most of that occurred in … Think of it as cyber crime era, Now, in the cyber war era, we've seen the curve steepen. In essence what's happening is if you look at the battlefield. The battlefield's interesting in cyber war because it's all around all of us and its global, so you're saying, "What's going on?" The frequency of attacks are occurring and the battlefield is being softened.

When we see all these attacks happening on the banking systems, on the transportation systems and all these negative economic pieces, we haven't seen anything yet. This is just the normal course of a low intensity conflict.

The next stage is basically coordination. When coordination occurs, people are going to get worried and scared and plan is completely required. Now, what we should be doing is learning from these types of discussion points so that we can make this plan and get ahead of the curve.

If we take the assumption that we're in the cyber war era, it looks like low intensity conflict, we've got a power void because nobody's controlling what's going on. Then, we're saying, "Okay, well, maybe we need to come up with some assumptions of how we got here." Why is security so bad? You can borrow economic principles to understand that. It's pretty easy.

The question that was asked is why don't the manufacturers share in the liability? You want to know why? It's because Bill Gates' dad was an attorney and a very smart attorney. Every time you load software, you hit an okay button. You basically take the liability and shift it over to you or if you're a company, you shift the liability over to your company.

Now, it makes total sense that we've got so many security holes because the economic incentive is not with the manufacturer of these products. A part of what Steve was talking about, while I disagree with him, I

understand how he got to those notions because it's like, "Well, you can't fix the problem," so all we have is offense.

I would suggest this, that we can fix the problem. The defensive problem is fixable but like any problem, we have to be able to quantify it. If we don't quantify the problem and we can't measure the problem, we don't know if it's improving or getting worse. We can see the attacks move up and down but we don't know how to compare 1 technology against another technology. What is the security of this industry? What is the baseline? We don't have any of those metrics right now.

One of the technologies that will shift that. Maybe it won't shift the liability back to the manufacturers but it'll change purchasing habits when people know what operating system scores a 3 and another operating system scores a 4 in security. What that will do is allow economic principles to basically take the security responsibility and allow the consumers or the companies or the purchasing managers to basically buy more secure stuff.

Once we know how to measure it and that technology is in existence now, then all of a sudden we can start to say, "All right, we're going to basically change the evolutionary path of technology," because now that we can measure it, it's no longer good enough to say, "I have good security. I have a firewall. I have antivirus and I have an intrusion detection system." What'll actually happen is you'll say, "Well, your security's a 3. You may have all those things but those things aren't basically raising your level of security."

By basically creating the standard use of measure for technology which is called QSM which is 1 of our company's products that we've worked with at George Mason University over the last 4 years to basically solve is a huge building block to basically changing this shifting liability landscape and allowing the security level to go back into technology.

When we look at these problems and we go, "Okay, so there's an okay button. Wow! That okay button sure did a lot." Yes, it did but there's also other things it did a lot to technology. Moore's Law, for example, every 2 years, a chip gets twice as fast but there hasn't been any interesting, profound observational laws even but if we've got this 20 year negative trend where the threat's keep going higher and high and now at an increasing point. If we can get ahead of that curve by let's say just 2 years. Now, all of a sudden, we've got the ability to measure technology security and we can start to use America's creativity and America's production force and harness the country's resources on a technological

basis that's now focused toward better security, we come up with maybe the [Ribot's Law 01:38:24] and say, "Well, if America stays 2 years ahead on security, then we're basically going to hit an inflection point where that trend starts to go down. As long as we stay 2 years ahead, then, all of a sudden we're headed in the right trajectory for defensive security."

I would also advocate, yeah, in this American cyber action plan, we've got to say, "Okay, 85% of the resources or some number, 85% defense, 15% is offense, for example. We have to come up with those measures and those metrics and then we basically have to coordinate as a country to utilize our resources to win. We're America. We own the technology market. We may not own the manufacturing base but it's still our ideas. Why do you think they're stealing our IP? Because we're ahead.

Let's use the thing that America can basically take to market and the fact that our vulnerability is the fact that we're connected but that's also our greatest strength. If we harness what put us here and we just look at it in a little bit different way, then I think we can make an improvement on the defensive side.

I think on the offensive side, if we start thinking of the problem like low intensity conflict and we create things to beat cyber insurgencies which is basically what's happening, we look at the surge, we can have a banking industry surge to basically take the fight back to them and to create those deterrent portions but it's not going to be police type of effort because there's no laws being enforced and there's the ability to basically bring someone to justice is very difficult. It's going to look like a low intensity conflict cyber war environment.

Anyway, my times up. Thank you.

Samantha Ravich: Thank you. Thank you, Mark.

Before we go to the questions, I just wanted to mention when we started this project, we really wanted to create a larger group of people that are interested in this topic that take different pieces of the research on to move it forward. We never wanted it to be that this was the be all and end all.

There's a lot to go forward on this. One of the things that I think this panel and the last 1 really showcased are the needed places where policy and new technologies come to bear. On that, I was Hudson, Hudson Institute's co-founder Herman Kahn wrote the 6 Desirable Characteristics of a Deterrent. He wrote that, "A deterrent, to be successful, must be

frightening, inexorable, persuasive, cheap, non-accident prone and controllable." If we just even start with those 6 things and you can imagine having both the policy makers, the war fighters, the technologists around a table saying, "All right, look. Here's the problem. How do we create a deterrent that both rests with sound policy doctrine and the technologies to be able to do what Kahn recommended, I think we would really move this conversation ahead.

Okay, my interjection …

Male: [Inaudible 01:41:45]

Samantha Ravich: Wait, wait 1 second.

Steve Chabinsky: Yeah, the new FDDs, center of sanctions illicit finance, great, thought-provoking panel, both panels actually. There was something that was said in the first panel that provoked a question that I think is appropriate for you all which was the reference to us losing the space race. It made me think about President Kennedy decades ago, he set the goal and he set the goal post in terms of getting to the moon and the space race.

The undercurrent of course our competition with the Soviet Union and the tremendous threat that was there but over that decade, he really galvanized with the country, galvanized with this goal that was inspiring, it was very positive. If we were to look at the cyber war, the cyber race, what would be the goal or the goal posts? Is there a way to galvanize this next generation of young people and others within our society to target a specific goal so that we could win the cyber race which we're losing.

Samantha Ravich: Mike, you want to take this first?

Michael Hsieh: Okay. I think that's analogy that's often drawn. Of course, it's problematic because with the space race, there's clearly defined goal posts as to progress, sending a man into space, setting a man on the moon, sending a device to Mars and beyond and so on and so forth.

The problem with cyber, though, is that the agenda's much more diffuse as you imagine. Cyber's a lot of things. There are the kinds of cyber problems that exist on machines and networks and there is as chairman Rogers mentioned in the previous panel, anthropological problems around cyber as well, too.

I think 1 of the things that tends to be a distracter in the cyber debate is an over emphasis on the technological dimensions. There is a

tremendous human dimension involved here as well, too, because it's a security problem. All security problems are human problems.

Just looking at the statistics of the kind of compromises that occur because somebody opens and email or somebody opens an attachment or goes to a link. Then, all hell breaks loose after that. At the end of the day, you're not going to get away from that because we don't design software and networks for machines. We design them for ourselves.

I think where we could possibly direct 1 area of research actually is to say that, "Well, we should stop blaming the human," because we are human. We should be able to open up a link or an attachment or go to a cite without trembling in moral fear that it's going to compromise the entire enterprise. Whereas I think there's going to be a much more diffuse kind of agenda for the cyber problem, I think there are some problems that can still be very ambitiously stated, very much like the problems of the space race as well, too. That's 1 of them but I'm sure there's others as well, too.

Samantha Ravich: That's good.

Mark Dubowitz: I would just add to this. Maybe this is too simplistic but I think when it comes to cyber, the whole notion of winning is something that we're cautious about it. We're careful about it. We don't actually want to win in cyber. We just want to survive. In historical terms, we invent the cannonball. We don't want to win using the cannonball. We just want to survive if the other side gets 1. We invent missiles. Again, we don't want to just win using missiles. We want to create missile defense shields just in case the other side develops bigger missiles than we have.

There seems to be some hesitation when it comes to cyber. I don’t work in the cyber field but I sense it in the language. I would say, the goal should be we're going to win this cyber war. Any country that launches a cyber-attack against us is going to be met with fearsome retaliation. Again, I don't know what we're going to do against the Chinese because of OPM. No idea but I don’t hear in the rhetoric of the President a commitment to actually win. I think that we need to send a message that we're the United States of America and whether you hit us with cannonballs or missiles or cyber-attacks, we are going to retaliate in a fearsome way and our goal is going to be to win in the cyber world as we won, I think, in missiles and we won in cannonballs. I think it's a commitment at that level before we get into exactly how we do it on a technical level and how do we reorient the US government on an institutional and a doctrinal level in order to do so.

Samantha Ravich: Mark?

Mark Tucker: I also think that there's major goal posts along the way. For example, when we hit this turning point and the 20 year trend ticks down, what is going to actually happen? If we say, "Well, what's going to happen on the PLA side or the China side," unit 61398 all of a sudden, all the millions of agents that they're watching on their screens and monitoring go dark. That's actionable. When that happens, you know what we're going to see? We're going to see that unit freak out. We're going to see him go back into the drawing board. We're going to see him working day and night. They're going to be start sending minions out to get new points so they can basically reinsert new types of agents. This is what I mean by we've got to be able to stay 2 years ahead because if we can stay 2 years ahead, the effects are dramatic.

Right now, what we've done is we've basically just stayed complacent and let all these agents and things and supply chain infections just permeate everything. I think just like that where we're saying, "All right. When the turning point hits, how will you know?" Because that unit, that is the biggest unit in the world right now that's basically 1 unit against us, they're basically, their agents go dark. Then, we're going to see actions because of it. I also think that we can measure the number of cyber events that will occur and I think we can measure the amount of money that's stolen from the bank or credit card so I think we can come up with measurable are we winning metrics.

Mark Dubowitz: Here's just a quick addition to that. Here's an indication of how you're losing. I was reading through the Iran deal the other day and every day it's a new surprise. My yikes moment of last week was I discovered that the United States and our allies, we commit to protect the Iranian nuclear program against sabotage. In effect, what we're saying is we're going to protect the Iranian regime's nuclear program against the ability of the United States, Israel, other allies to use cyber offensive weapons against Iran's nuclear program regardless of what happens with that nuclear program. In 10 years, 15 years time, it'll be of industrial scale with near 0 breakout, easier clandestine sneak out. They'll have an ICBM and a powerful economy. Even then, we will commit to defend Iran's nuclear program against cyber sabotage.

That's not the shot to the moon. That's not a commitment to winning. That's actually, we're going to harden our adversary's cyber defenses.

Samantha Ravich: Sir?

Rich Wilhelm: My name is Rich Wilhelm. I recently retired from Booz Allen where I ran all of our business with the intelligence agencies but 20 years ago, I had a job similar to yours on Vice President Gore's staff, Samantha, where we did round 1 of all of this.

We're so much farther ahead now but I'm struck by 1 thing. Yes, we are much farther ahead. We understand the threat much better and there's a lot more technology out there but I'm struck by how little progress we've made in solving the central policy issues that are going to be required to actually move ahead.

My thinking over the years, I think had matured somewhat. It seems to me that we're essentially trying to solve a problem where boundaries don't count on illegal policy and organizational and bureaucratic framework where boundaries really do count. I'm not just talking about geographic boundaries. I'm talking about the difference between private and public sector responsibilities between domestic and foreign, if you look at the intelligence community. We need some new framework.

This is a question really for you, Mark. The government response has been to create new organizations but not fundamentally alter the existing boundaries that exist in law of our existing agencies. What do you think the likelihood is that we can solve that problem over the long run and that there is a new paradigm that will emerge so that the interfaces between the various agencies operate a hell of a lot more smoothly than they do right now?

Mark Dubowitz: Great. Thank you for that question and for your service on these issues. I would say that I'm somewhat optimistic. I've seen it from the outside on the offensive side. I think we've done a pretty good job and a lot of credit to Juan and the folks at the Office of Terrorism and Financial Intelligence Treasury. Who had even heard of TFI or OFAC a decade ago or 15 years ago. I hadn't but I'm sure lots of folks in this room hadn't.

What Juan and his colleagues did at TFI and OFAC had been around a long time is that they took institutions, agencies in the US Treasury Department and they turned them on offense. I think did a really remarkable job not just leveraging government but leveraging markets because the real secret sauce of our financial coercion on offense was not what we did to governments. It's actually what we did to companies and financial institutions in changing their risk reward assessment with respect to doing business with rogue regimes or terrorist organizations. It was putting in a fundamental choice. "You could do business with our $17,000,000,000 economy or you can do business with Iran's

$350,000,000 economy and if you do business with their $350,000,000 economy, you're going to be doing business with the Revolutionary Guards and a number of very bad actors who are engaged in a range of illicit financial activities." That was the genius of that program.

Congress played a significant role in it. Other agencies played a significant role in it but I would say it's been a very successful program. I'm obviously very skeptical about whether we have actually used those incredible resources and achievements towards the right diplomatic ends but at the end of the day, we certainly hone the instruments. Our paper tries to look at it from the other point of view.

Now, with those instruments honed on offense and other countries and adversaries using some of those same powers, how can we reorient the government to start thinking about creating a defense of economy shield? We started to make some movements on the cyber. We have cyber command. I'm learning a lot about some of the deficiencies we've got in that area but in an economic warfare perspective, the folks at TFI don't have the time to actually think through defensive shields which is why an Office of Policy Planning would be useful for the Treasury. It would be useful to have that directorate at NSC. It would be useful to have an economic warfare command with all the powers to work at an inner agency level, to actually think through both on the cyber side and on the traditional economic warfare side, how do we defend the United States?

I'll end with this. Here's a good news story to me. The state of South Carolina just passed legislation. The legislation simply says that any country that actually uses economic warfare against 1 of our allies will be denied state grants from South Carolina and that the state pension fund of South Carolina will have to divest from any companies engaged in economic warfare against 1 of our allies.

That's interesting. At the state level, it's the state of South Carolina. It's effectively saying, "You use economic warfare against the United States or our allies, don't come do business in the state of South Carolina." You're starting to see this spread across the country. Illinois just did something similar and other states are contemplating. That's creating a defensive shield at the state level which I think could actually be created at the federal level through executive orders, legislation and creating a defensive economic architecture lead by many of the same people who've been so successful on offense.

Samantha Ravich: That's great. For me to take 1 last question. Just so that you political scientists or IR theorists out there don't think there's a place for you in this robust debate and moving forward and it's just a place for economists and technologists, we need a better understanding of how the different adversaries view their strategy towards us, right? There is absolutely no reason to think that what the Russians are doing or how they're organizing is in any way similar to what the Chinese are doing or what the Iranians are doing or the North Koreans are doing.

An understanding of those states and how they view strategy and how they view tactics is a must in all this piece. One telling point on this is that in the weeks before the Sony hack, the North Koreans were speaking out at every opportunity, had screaming that the movie that Sony was going to release, The Interview, was an existential threat to North Korea. The North Korean watchers knew that the North Koreans may possibly be gearing up to take retaliatory action. Of course, when the Sony hack hit, they were some of the first ones to say, "Look over at Pyongyang."

All right. I think last question. Sir?

James Say: James [Say. 01:56:08] Doctor Hsieh used the phrase, "Cryptographically sound." It reminded Juan that parts of the US government, somewhat allergic to cryptographically sound practices which raises the question about how serious the US government is about the whole idea that being cryptographically unsound has advantages to US government and any technology that you have, there other guy will get in a year or 2 afterwards what you show is possible. Any comments?

Michael Hsieh: Again, I should preface all this by saying that today, I'm speaking just as an individual and not as a representative of either my agency, department or the US government at large but I think I should also preface or append to my earlier comments that I'm essentially talking about things that still live very much in the research space. Obviously cryptography means very different thing when you're talking about RSA and mature technology versus a lot of the kinds of things that still happen in academic circles, secure multi-party computation, privacy preserving computation and so on and so forth.

When I use terms like security in this cryptographic context, actually, maybe the better word to use is provable security rather than cryptographic security in the sense that we can quantify how much security we're getting, given a certain protocol and given certain parameters and given certain settings. I think that probably is a more accurate way to characterize that.

Samantha Ravich: That's wonderful. I think with that, I'm going to wrap up unless 1 last question? Okay. All right. I thank you so much for giving a round of … Again, stay tuned for the synopsis of this seminar, the survey results. Again, I encourage you all to take it if you haven't. It's fast and anonymous. Thank you again. Have a good day.