Dealing with the Cyber Threat to our National & Economic Security

Dr Paul G. Kaminski

Pittsburgh, PA Jan 10-11, 2013

Notes for talk given in four separate sessions arranged by US Attorney David Hickton: 1) for business and technology leaders, 2) labor leaders, 3)law enforcement leaders, and 4) local press under limitations

.

I first became involved with cyber issues starting in 2009 when I participated in a review as a member of the SSCI TAG. My conclusion from that review was "The more you know about our cyber vulnerabilities, the more you worry". My objective today is to allow you to know more about this so you too will worry more, but far more important than just worrying is doing something about it. We need leadership from both private and public sectors and public-private partnerships to deal with this challenge. My first objective is to help you become better informed. That will enable you to better assess the severity of the threat to our national security and to our economic security as well. Finally, I will offer my thoughts on developing and executing a strategy to deal with this threat.

Before I begin, I must issue some disclaimers. I serve on the PIAB (President's Intelligence Advisory Board), I Chair the Defense Science Board, I serve on The Director of National Intelligence Senior Advisory Group, and I have served for several years on the FBI Director's Advisory Board. My service on these advisory groups has provided me with detailed classified information on US cyber capabilities and similar classified information on the threat posed by others to the US. I will not be able to share that detailed classified information with you today. But I believe I can provide you with the big picture view without providing all the supporting details. I will also make reference to quotes, speeches and public documents that I hope will support the big picture I am presenting.

I am also not in a position to represent or speak for the President, the PIAB, the DOD, the Defense Science Board or the DNI on these issues. I am speaking only for myself and offering you my personal assessments and opinions. So I do not wish to be quoted as Paul Kaminski speaking as a member of the PIAB, the DSB, or the DNI SAG.

Let me begin informing you about the problem by quoting from an Op Ed written by a friend and colleague, Mike McConnel VADM USN Ret, former Director of the National Security Agency (NSA) and former Director of NationaI Intelligence. This was published in the Washington Post on Sunday Mar 7, 2010. And I quote:"

- The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking.
- The problem is not one of resources; even in our current fiscal straits, we can afford to upgrade our defenses. The problem is that we lack a cohesive strategy to meet this challenge.
- The stakes are enormous... If an enemy disrupted our financial and accounting transactions, our equities and bond markets or our retail commerce -- or created confusion about the legitimacy of those transactions -- chaos would result. Our power grids, air and ground transportation, telecommunications, and water-filtration systems are in jeopardy as well.
- These battles are not hypothetical. Google's networks were hacked in an attack that began in December and that the company said emanated from China. And recently the security firm NetWitness reported that more than 2,500 companies worldwide were compromised in a sophisticated attack launched in 2008 and aimed at proprietary corporate data. Indeed, the recent Cyber Shock Wave simulation revealed what those of us involved in national security policy have long feared: For all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts."

Mike McConnel's use of the term "cyber-war" has been criticized as being excessively flamboyant. That may be true. Mike was trying to ring the alarm after having worked during the Bush administration on launching the "CNCI" the Comprehensive National Couinter-Cyber Initiative, and having worked hard again during the transition of the first Obama administration, and becoming frustrated with the lack of real progress. As you can tell I share that frustration.

But Mike was successful in causing the problem to be recognized.

Looking at speeches and press releases, it’s apparent that our present and past Presidents both recognized the importance of these cyber issues. After meeting with McConnel, President Bush did launch the Comprehensive National Cyber Initiative (CNCI) in National Security Presidential Directive 54 on Jan. 8, 2008. President Obama gave a very impressive speech on May 29, 2009 and I quote a few excerpts from that speech:

“For Immediate Release May 29, 2009

REMARKS BY THE PRESIDENT
ON SECURING OUR NATION'S
CYBER INFRASTRUCTURE

It's been estimated that last year alone cyber criminals stole intellectual property from businesses worldwide worth up to $1 trillion.($ 1 TRILLION)

In short, America's economic prosperity in the 21st century will depend on cybersecurity.

And this is also a matter of public safety and national security. We count on computer networks to deliver our oil and gas, our power and our water. We rely on them for public transportation and air traffic control. Yet we know that cyber intruders have probed our electrical grid and that in other countries cyber attacks have plunged entire cities into darkness.

Our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Al Qaeda and other terrorist groups have spoken of their desire to unleash a cyber attack on our country -- attacks that are harder to detect and harder to defend against. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption.

For all these reasons, it's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation.

It's also clear that we're not as prepared as we should be, as a government or as a country. In recent years, some progress has been made at the federal level. But just as we failed in the past to invest in our physical infrastructure -- our roads, our bridges and rails -- we've failed to invest in the security of our digital infrastructure.

No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should -- with each other or with the private sector. This status quo is no longer acceptable -- not when there's so much at stake. We can and we must do better."

I couldn't agree more with the President's statement of the problem and its urgency. But I do believe that we need to move more quickly and aggressively to deal with it than we have been doing.

What's the problem here? There's lot's of talk – but too little action that will make a real difference. This is a serious matter, so I hesitate to illustrate the problem with a joke. But this joke does it so well that I believe it will provide you will a key take-away from my talk.

Having had continuing problems with her brakes, a young woman driver pulled into a dealership and told the service manager that there seemed to be a problem with her brakes, and that she was concerned about her safety. After a several hours, the frustrated head mechanic appeared, agreed that there was a problem, and announced that after several hours of work he couldn't fix the brakes, so he made the horn louder.

We need to develop and execute a strategy to fix the brakes rather than rely only on the horn.

So let me provide a little more information about the problem, then transition to describe the criticality to our national security and to our economic security. If the cyber threat were a disease, I would tell you in medical terminology that there is an acute aspect of this disease, and there is also a chronic aspect.

Let me begin with the acute aspect which is easier to comprehend. As our societies have progressed, we have all become more specialized, focusing on our specialty areas and relying upon others to support our basic needs. We have become dependent upon critical infrastructure – electric power grids, water supplies, transportation systems, and financial systems to name a few. Our personal well-being and our economic and national security are all dependent on these critical infrastructure systems. We can see the enormous impact when we lose these systems locally in massive storms like Katrina and Sandy.

I recall a discussion I had with Haley Barber, then Gov of Mississippi after hurricane Katrina. He couldn't restore power because the cable trenches were filled with water. He couldn't pump out the water because there was no power. His communication system was shut down, so he was using messengers on bicycles. Imagine what would happen if these critical infrastructure systems were taken down at a national level! Unfortunately, many of these systems connect to the internet and have been demonstrated to be vulnerable to cyber attacks. There are severe vulnerabilities associated with the SCADA systems (Supervisory Control and Data Acquisition) developed years ago that have been widely deployed to remotely monitor and control industrial equipment critical to power grids, utilities and some transportation systems. We have demonstrated the ability to remotely destroy critical elements of this infrastructure using our basic cyber tools, and we have seen evidence of intrusions into to these networks by others that could do so as well. So we have demonstrated the vulnerabilities ourselves, and now see others taking the steps needed to exploit them.

This is the acute aspect of the cyber threat. We have completed a Defense Science Board report on Cyber dealing with metrics to describe the resilience with which we can perform military missions that are dependent upon our cyber infrastructure. The report is complete, but in final security review and I will provide you access to that report on the DSB web site when the unclassified version is available very soon. That report defines 6 levels of cyber threats, ranging from level 1 – an individual hacker exploiting known vulnerabilities that can be found via the internet, to level 6 - the existential threat posed by a few nation states (the US is one) who have devoted substantial resources ($B) and time (several years) to discover and exploit weaknesses. Some of our critical infrastructure today is vulnerable to level 1 or 2 threats. Most of it will be seriously vulnerable to level 6 threats.

While see evidence of the intrusions required to conduct such attacks, we have seen little evidence to date of actual serious attacks, and limited evidence of less serious attacks. One of the recent attacks on our financial system (banks in this case) described in Jan 7, 2012 press accounts involved distributed denial of service (DDOS) attacks. These DDOS attacks have largely been dismissed as crude tools that are easily countered. Fortunately, they were countered with minimal disruption by excellent cooperation among the banks with helpful government support. But these recent attacks, attributed to Iran, raised some serious concerns based upon the scale and finesse employed.

So in sum, our acute problem is the existence of threats that would likely be very effective in disabling our critical infrastructure if attacked by level 6 threat nation states, with serious concerns about even lower level threats posed by terrorist organizations or sophisticated criminals.

Next is the chronic problem – cyber espionage. This problem is insidious. It is happening today and has been happening for years. The effects aren’t visible today, but they will become apparent in varying degrees in the future as our competitive positions (and jobs) are eroded by competitors stealing our intellectual property. General Keith Alexander, Director of NSA and Commander of Cyber Command has called this “the greatest transfer of wealth in our history”.

Let me illustrate the threat to our national security by providing an example. We have seen the theft of top level system specs for our F-35 Joint Strike Fighter program. That data was then used to identify critical subsystems and components. The attackers then went to the suppliers (smaller companies with more limited cyber protection) to get detailed performance predictions and discover the limitations in our systems. This is the type of intelligence data that I longed for on Soviet systems when I was director of the stealth program. For years we have relied on our technology edge to offset massive forces deployed by potential adversaries. Do you think this strategy will be effective if our adversaries are provided with detailed copies of our designs and their capabilities and limitations before our systems are fielded?

We face a similar problem with the theft of design, development and production data for leading commercial products. There are further concerns related to theft of data revealing pricing, business plans and negotiating positions. If allowed to continue, this cyber espionage threat will degrade our ability to compete commercially and undermine our economic security and ability to create jobs.

So those are the problems. Now the issue is what to do about them. We are doing a number of good things, but we are not doing enough and are not moving fast enough to keep up with the threat. This is a result of many challenges. Let me name a few:

1. Fundamental asymmetries that are being exploited
    a. We own lots of IP – we are a rich target
    b. We do not use espionage to enhance the competitive position of our private companies – others do
    c. Cyber offense beats defense
2. Privacy concerns associated with monitoring and sharing data
3. Difficulties in attribution
4. Authorities to act and coordinate among public agencies, among private entities and between public and private entities
5. The ability to react quickly at scale.

So a strategy to address our problems must deal with these challenges. Thanks to many constructive actions by this administration including our capable Cyber “Czar” Michael Daniels, we have several key building blocks in place (e.g., NCIJTF, NTOC, DIB, and CERT at CMU to name a few). Our challenge now is to form the necessary partnerships among these elements and the relevant private sector stakeholders. We need to “connect the appropriate dots”.

To react quickly at scale, I believe that we need to work directly with our key ISP’s. They already operate at a scale that would be challenging to most of our government agencies. But they need to be supported with key intelligence data on threat signatures and practices, and research from institutions like UARCS (e.g., CMU), FFRDC’s or national labs to improve robustness of our internet architecture in the medium to long term. We need to bring our best and brightest to bear on the problem.

To provide authorities to act and coordinate, we need policy documents such as HSPD-7, Executive Orders, and legislation to deal with anti-trust concerns, privacy concerns, and provide immunity for certain protective actions to be taken by ISPs and others.

To deal with attribution we need to improve our identity management systems and improve threat sharing.

To deal with privacy issues, we need to better inform the public about the threat, and develop policies to balance the risks of monitoring by US government entities with the risk of growing intrusions on privacy by foreign, terrorist and criminal actors. President Obama has asked for a National Intelligence Estimate of the economic impact of cyber-espionage, and that document (now in the final stages of review) will help to better inform the public.

In many cases we can observe cyber crimes in progress (e.g., data leaving a private firm in the US and arriving at a foreign entity), but do not stop those crimes in progress because of privacy issues, legal restraints, or concerns about losing sources and methods. We can make good use of modeling and simulation tools to examine the benefits and risks of alternative policy and legal constructs that will enhance our ability to stop cyber espionage in progress. We can also build on the DIB program for defense companies and the continuous monitoring initiative to be undertaken by HLS to protect “ .gov”, using these programs to develop the data and experience needed to balance the risks associated with monitoring and sharing of threat data to protect “.com”.

To deal with the 3 asymmetries I described, we need to exploit corresponding asymmetries associated with those who threaten us. While we seek an open internet, many others seek a closed and controlled internet. Our abilities to open their internet at times and places of our choosing can serve as a deterrent to their espionage practices. We can also add cost and complexity to their ability to exploit data by making better use of encryption, and by altering critical design data in files that we expect to be taken. This can undermine their confidence in relying on stolen IP, and increase their cost and risk of exploitation. We can also deter by declaring a company “non-grata” policy, preventing companies from doing business in the US when we have evidence of their use of stolen US IP in their products or services.

We can reduce our risks to critical infrastructure attacks by strengthening defenses against the level 1-4 attackers through the use of best business practices and the development of codes analogous to fire codes in existence today. This approach can be used to avoid excessive government regulation and allow economic incentives (e.g., reduced insurance costs) to improve security practices. For the Level 5-6 threats, we need the capability to respond as a nation in both cyber and kinetic domains with consequences that the Level 5-6 nation state attackers would not be prepared to risk.

Will these actions be without cost and challenge? - Certainly not. But I believe they can be done, they can be affordable, and they can have a significant payoff in protecting our economic security and our national security. But we will need strong leadership and effective private-public partnerships enabled by legislation that will fix the brakes rather than blow the horn.