I.

THE BROOKINGS INSTITUTION

DETERRENCE IN CYBERSPACE:
DEBATING THE RIGHT STRATEGY WITH RALPH LANGNER AND DMITRI ALPEROVITCH

Washington, D.C.
Tuesday, September 20, 2011

PARTICIPANTS:

Introduction and Moderator:

PETER W. SINGER
Senior Fellow and Director, 21st Century
Defense Initiative
The Brookings Institution

Panelists:

DMITRI ALPEROVITCH
Former Vice President, Threat Research
McAfee

RALPH LANGNER
Founder and President
Langner Communications

* * * * *

P R O C E E D I N G S

MR. SINGER: Hello. I'm Peter Singer. I direct the 21st Century Defense Initiative here at Brookings. And we are delighted that you've all come out on this wonderful weather day to talk about a topic as happy as cyberdeterrence. So we very much appreciate you coming out. This is an exciting event for us. We're looking forward to it.

To give some background, just a generation ago cyberspace effectively didn't exist beyond the nascent links between a limited number of universes -- I remember the very first time I accessed the Internet. I remember the very first time using e-mail. When I was in college, e-mail was designed effectively just for sending jokes around to each other. That's how we used it. Today, the centrality of cyberspace to our entire global pattern of life is almost impossible to fathom, and the numbers involved are so big that they sound pretty much imaginary. There are as many as 4 billion people behind the roughly 50 billion devices that have connected to the Internet at some point, conducting more than 2 trillion transactions involving 50 trillion gigabytes worth of data. Domains that range from commerce to communications to war, to the critical infrastructure that powers and protects our modern day civilization all depend on the safe and secure operation of this globalized network of networks.

And yet, the malevolent threat landscape has increased hand-in-hand with the growing scale and use of the benevolent side of cyber domain. Each day, tens of thousands of new pieces of malware are found, hundreds of thousands of computers are compromised and pulled into botnets, and scores of malicious websites are created.

But more important than these numbers may be the evolution in this threat landscape. It's gone from one being dominated by individual hackers, often just looking for attention, to one of complex organized groups that range from international criminal networks to private and state-related espionage and military efforts. The result is just as the positive side of the cyber domain is rippling outwards into the physical domain, so, too, is the potential negative side of it. The Internet may have no formal state boundaries, but it is increasingly a place that state entities both operate in and deeply care about. And perhaps of greatest concern is the rapidly rising nature of the Internet and cybersecurity as a source of friction between great powers.

The result is that we have a strange dichotomy. On one hand, stories about suspected attacks on U.S. and allied interests in both the public and the private domain have become an almost daily occurrence in the media and a source of regular discussion in the policy sphere. This has taken on a new level of concern and publicity with the recently reported intrusion into American government, military, corporate, university, NGO, and think tank networks, such as Operation Aurora, Operation Night Dragon, and the recent disclosure of Shady RAT, in which in that case successfully targeted more than 72 governments, international institutions, corporations, and think tanks.

In the United States, the scale of these growing cyber threats has been used as a justification for a host of new legislative efforts and the Pentagon's new cyber strategy, which sought to lay out the makings of a new cyberdeterrence doctrine, importantly leaving open the door for escalation to traditional military means. But this dialogue, this debate also has an international aspect to it. Nearly every nation out there has described itself as being under cyber siege, from our allies in the United Kingdom, which saw their Parliament's computer network penetrated by -- compromised by a worm whose origin still remains unclear, to the Chinese government, which has stated that it has suffered from some 34,000 cyber attacks emanating from the United States.

This period has also seen the sophistication of these attacks grow. Most notably, the Stuxnet episode, which was viewed by some as a potential success for allied cyber efforts in that it hampered an arguably illegal production of WMD at an adversary and in a highly focused manner without any casualties, but it's been described by others as an indicator of a new level of threat and consequence in this realm.

And yet, this trend is both countered and exacerbated by a second problem that we don't talk about enough. There is perhaps no issue that is growing of importance as fast as cybersecurity, but also is least understood. This is not just a matter of my mother asking me about the interweb. It's also something that strikes leaders and policymakers who make the most important decisions, including in cyberspace, or sadly as one Pentagon leader I recently saw described "this cyber stuff." For example, the FBI views cybersecurity as the third most important national security threat to the United States behind only WMD and 9/11-scale terrorism and yet the director of the FBI did not have either an e-mail account nor a computer in his office as late as 2001.

It's a realm where we also see hype and hysteria reign, whether it's the chairman of the Joint Chiefs of Staff describing it as a "existential threat." Call me crazy, but I reserve existential threat for things like alien attack or a thermonuclear war. Or the Chinese Academy of Military Sciences that released a report earlier this year that stated, "Of late, an Internet tornado has swept across the world, massively impacting and shocking the globe. Behind all of this lies the shadow of America. Faced with this warm up for an Internet war, every nation and military can't be passive, but is making preparations to fight the Internet war." The point that I'm making here is that this is an issue that is both important, but also one that needs deeper discourse and debate, especially by professionals, not by posers and not by profiteers.

That's why we're so excited today to be joined by two key figures from the realm of cybersecurity to talk to us about their thinking on the issues of deterrence and strategy in this realm. We'll first hear from Dmitri Alperovitch, who is one of the most prominent cybersecurity experts out there. He is the former vice president of Threat Research at McAfee where he led the company's Research and Internet Threat

Intelligence and Analysis. Most notably, he's the author of the recent report on the Shady RAT attacks, which revealed cyber intrusions into more than 70 different entities over a period of year and before that he led investigations into Operations Aurora and Night Dragon among others.

Then we'll hear from Ralph Langner. He's the founder and president of Langner Communications, a German software and consulting IT firm that's focused on industrial information technology, especially in the issue of control system security and critical infrastructure protection. He received worldwide attention for his analysis of the Stuxnet malware that was discovered in Iran, effectively leading the team that was the first to discover that Stuxnet was, in fact, a cyberwar weapon meant to damage the Iranian nuclear program.

So, and then we'll open it up after that to discussion and Q&A with all of you.

So I'd like to welcome Dmitri up to the podium.

MR. ALPEROVITCH: Thank you very much. Thank you, Peter. It's an honor to be with you.

I'd like to start with a disclaimer. I'm now an independent security researcher and the opinions I will express today are my own and not any organization I may have represented in the past. I speak for myself and only myself.

Today I will argue that strategic cyberdeterrence is not only feasible, but that a declaratory cyberdeterrence policy is a prerequisite for peace and stability in today's very dangerous cyber domain. To start with, what is deterrence? It is essentially a mind game, a psychological game of chicken. The point of deterrence is to influence the cognitive state of your potential adversary and prevent them from embarking on a course of action that they may wish to take.

Here's how the U.S. Department of Defense defines it. It is prevention from action by fear of consequences. Deterrence is a state of mind brought about by the existence of a credible threat of unacceptable counteraction. That sounds fairly simple, but how can we actually enforce this in the uncertain domains such as cyberspace?

Well, let's start with trying to figure out what action we're actually trying to deter. It is clearly not everything. We're not going to deter every possible cyber attack. That's an impossibility. We cannot do that because of laws of armed conflict, which dictate that retaliation must be proportional to the harm suffered in the attack. Thus, if someone is launching a massive swoop invasion across your border, you have the full right to retaliate in full force; but if instead they're throwing stones or sneaking people across, then clearly your options are much more limited and the threat of counteraction may no longer have a deterrable consequence.

Thus, we need to consider the impact of the attack in our calculus for developing a deterrent strategy. We need to define the red lines to determine our strategic cyber defense priorities as a country and apply the just war theory to determine what deterrent response is available in our arsenal.

To do that, we need to consider the taxonomy of cyber attacks. We can use the CIA information security model to classify all cyber attacks into three categories -- those that attack confidentiality, integrity, and availability of either information or information systems. Almost every single cyber attack or exploitation will fall into one of these categories. This model does not include psychological operations using cyber means that countries such as Russia and China would consider cyber attacks in their information warfare doctrines, but here in the U.S. we do not consider those operations to be strategic threats to our open societies.

Nation-state sponsored attacks on confidentiality, otherwise known as cyber espionage, are a significant threat to the U.S. and its allies. These incidents are becoming more numerous as we better understand how to detect and identify them.

However, these are acts of theft with intruders primarily suspected of originating from China, a rising superpower with a strategy of global economic domination are exfiltrating intellectual property from governments, enterprises, and nonprofits. Nearly all the targeted attacks we see these days fall into this category. Today, economic espionage is performed on a massive scale with nearly every industry successfully and persistently compromised and organizations throughout our country losing their most valuable intellectual property on a daily basis.

While this activity represents a significant national security risk due to potential for future limited GDP growth, loss of industrial competitiveness, and global market share, our options for retaliation are highly limited. Laws of armed conflict and international norms take the destructive retaliatory option off the table and it is very difficult to find another solution that has an equivalent, unacceptable counteraction deterrent value. Our only hope is to raise the economic costs on the adversary through the use of such tools as sanctions, trade tariffs, and multilateral diplomatic pressure to impact their cost benefit analysis of these operations.

Political and national security-related espionage on the other hand is not deterrable and has now become an acceptable international norm with all powerful nations engaging in it in various ways. Retaliation options are typically limited to diplomatic arguments, deportation of embassy staff, and arrests a spy, none of which are sufficiently costly to change the cost benefit analysis of these actions.

Cybercrime by and large is about theft and now destruction as well. Cybercriminals want to compromise the confidentiality of your bank account, your credit card number, your personal information, but they’re not modifying your data or destroying it on your computer except for a few relatively rare situations, but which do not rise to the level of strategic cyber threat to our nation.

Next we have attacks on integrity of data. These are much more insidious than confidentiality attacks and are designed to achieve tactical or strategic advantage over an adversary by sabotaging an operation of their critical civilian or military information systems. The act may involve manipulation of data inside information systems that can degrade or distort your virtual or physical situational awareness capability by spreading misinformation in your intelligence systems. The goal may be to achieve either a specific tactical objective to obscure or hide specific activities or to achieve a strategic surprise in preparation for an all-out attack. It can also involve subversion of physical devices and processes that are guided or operated by information systems. The Stuxnet worm, whose analysis was led by my esteemed friend Ralph Langner here, was clearly an example of this activity, as would be manipulation of weapons guidance systems that cause them to fire off target.

These types of cyber attacks are quite dangerous and can potentially impact our way of life when launched on large scale and with devastating impact to national or economic security. However, that scale and impact is very important for our deterrence considerations. Someone hacking into a website and defacing it is not a strategic attack. It’s annoying and has some costs associated with it, but that does not have a large impact on our way of life. Turning off our electricity for a significant period of time -- a five-minute regional brown out probably does not count -- or compromising the water or food supply would clearly fall into that category.

I would argue that even Stuxnet, which at best only achieved a moderate length delay in an Iranian enrichment program, the widely suspected target of sabotage, did not rise to the level of being considered a strategic threat to the Iranian nation that required overt retaliation.

Integrity attacks look very much like covert action operations, and while they may be tolerated on a minor scale, such as an operation to kill Osama bin Laden hiding in Abbottabad, Pakistan, for example, or limited scale sabotage of USAF’s nuclear weapons program, significant destructive operations will not be tolerated by any self-respecting nation state.

Finally, we have availability attacks, which are those that attempt to bring information systems offline in order to shut down or destroy critical physical or virtual processes or prevent access to information. Once again, scale and impact are absolutely key. A denial-of-service attack against a website is a big deal to you if it's your website, but is not a strategic threat to our country. A prolonged D-DOSS attack that is not easily mitigated and which shuts down critical parts of our nation's infrastructure may very well be strategic and something we want to try to deter.

Although sometimes short duration attacks that are surgically targeted, for example, intelligence collection and analysis capability that can blind a nation's ability to see an immediate strategic conventional or broader cyber threat by denying defenders access to that vital situational awareness or intelligence resources may very well fall into that category as well.

Now that we've discussed what types of attacks we want to deter, let's talk about the how. For deterrence to be effective and credible we need to build and demonstrate a credible threat detection system that will also protect our ability to counterstrike. Of course, we do have a serious problem in the cyber domain that with advance of obfuscation and polymorphic techniques, an attack can actually remain stealth and avoid detection for prolonged periods of time as Stuxnet had done, for example.

However, as you recall, if we're trying to deter catastrophic or strategic attacks it'll be much easier to detect them as the impact should be visible in most cases. Integrity attacks do pose a particular challenge because of their stealthy nature, so critical data and systems must be redundant and with constant integrity or operational checks that will help to detect an attack.

At any rate, as you recall, deterrence is all about psychology, so our detection does not necessarily need to be perfect, but good enough to sow doubt in the adversary's mind that they will be detected and that retaliation will be swift and powerful.

Counterstrike retaliation may not necessarily be limited to cyber, of course. The right weapon, which could be kinetic, should be selected to inflict a proportional amount of damage on the adversary. We do have a problem to date, one that is not likely to last more than a few decades, in that there are plenty of potential adversaries who have very limited cyber vulnerabilities. Countries like North Korea, for example, have virtually no reliance on cyber at all, so if you limit your retaliation operations to the same threat vector with which you had been attacked, this asymmetry in offense and defense will prevent effective deterrence. In other words, if your water dam blows up because of a cyber attack, you can use J-dams or cruise missiles on your adversary's water infrastructure to achieve the same impact in the case of a limited cyber vulnerability of their water sector or for other considerations as well.

The other component of credible capability is preserving the command and control decision-making and counterstrike operational capability in case of an attack. Communication channels from appropriate decision-makers who would make the call to launch a counterstrike down to the weapon operations must survive a catastrophic attack. This means weapons and guidance systems, for example, and communication resiliency is paramount with plenty of redundancy built in for offline or out of band control and communication channels which should not depend on the network being up and running.

Our rapid march toward cyber enablement of virtually every technology we have is a serious problem that increases our vulnerability in this area and something that we need to keep a very watchful eye on to make sure that those redundancies still exist. Frequent exercises must be helped to preserve confidence in those capabilities.

Finally, we must have a demonstrable counterstrike capability. Our adversaries must know that we have the capability to inflict vast damage on their nations and infrastructure in response to a clear and imminent threat. I believe that this means that we need to start talking openly about our offensive capabilities in cyber and their readiness levels just as we discuss our ballistic missile arsenals, air force or submarine fleets. Today, our enemies know and have a healthy appreciation for our kinetic capacity, but have virtually no idea what cyber capability exists in our offensive realm.

I believe that ambiguity is counterproductive and is, in fact, decreasing our deterrence. The will to retaliate is a more nebulous psychological concept that is comprised of both reputation to use offensive weapons and a declaratory first strike or second strike policy. Once again, we must convince our adversaries that we will not hesitate to strike them with full proportional force in the event of an attack and that we can do that in part by declaring that policy openly and clearly.

Attribution is a problem that is often cited as a reason deterrence cannot work in cyberspace. It is indeed very difficult and sometimes impossible to accurately and quickly attribute a cyber attack once you discover it to a specific adversary through technical means alone. The use of non-cyber intelligence resources, such as human intelligence and signals intelligence can certainly help with our goal, but also cannot provide a reasonable level of assurance required for credible deterrence.

Despite this challenge, however, I suggest to you that it is conceivable the deterrence will be effective even without accurate and timely proven attribution. For one, the required level of attribution needed for counterstrike is directly proportional to the degree of criticism our nation state is prepared to endure in the international and domestic course of public opinion and is greatly influenced by the destructiveness of the original threat and a cui bono of benefits-based analysis of attack subjectives. The threshold is not proved beyond a reasonable doubt in a court of law, but been good enough for CNN.

Strategic context in international relations at the time of the attack can offer strong clues as to its origin. For instance, if we're engaged in a highly tense situation in the Taiwanese Straits and we suffer an attack on our military logistics systems in the Pacific region, we don't have to look too far for where blame may need to be placed.

In conclusion, I have presented to you an argument that we need a declaratory policy of retaliation to strategic cyber attacks that clearly and credibly define red lines that will trigger a response. I've also made the case for the need for continued investments and timely detection of strategic cyber threats and most importantly preserving the resilience of our response infrastructure both command and control and communications in order to demonstrate a credible counterstrike capability. Today's defenses and security systems are too weak and undefendable against a dedicated, well-financed, and trained adversary, such as an advanced nation state's military or intelligence apparatus. This is evidenced by the daily barrage of new stories we're seeing about successful and deep penetrations of all sectors of our economy, as well as government systems, and as recently revealed by the deputy secretary of defense, including even disconnected classified networks.

In cyberspace, just as in the physical world, the advantage always goes to the offense and the defense-only strategy will always lag behind and make us even more vulnerable. To be clear, I'm not arguing it is counterproductive to try to make our systems more secure. On the contrary, that only strengthens our deterrence posture. But only focusing on security is a strategy for failure because a dedicated enemy that used the views the cost of launching an attack as minimal as I believe is the Chinese view of their cyber espionage activities today, it will always find a way in.

The deterrence model I presented today does have challenges. I believe it is a good model for nation state deterrence, but it is clearly -- it will clearly not deter a non-nation state actor. The asymmetric threat deterrence, unfortunately, is an unsolved problem to date even in the physical world demonstrated by our primary national security fears being of WMDs being employed by terrorist groups who fear no retaliation and abide by no rules of engagement. I'm afraid I don't have a solution for this problem in cyberspace either. We're very lucky today, however, that most asymmetric actors do not yet have a significant cyber offensive capability or have expressed much interest in obtaining it, but that will no doubt change with time and represents a significant challenge for our future policymakers.

With that I want to thank you and I look forward to the discussion.

(Applause)

MR. LANGNER: Thank you very much for coming here this morning. As an introduction I would like to remind you that I'm not going to talk about -- very much about denial-of-service attacks against websites, et cetera. I'm trying to focus on the hardcore cyberwarfare stuff. The cyberwar attacks, and probably what could evolve into cyberterrorism.

Why are we discussing deterrence in the first place? Certainly to start off, because there was a threat. We recognized that there was a threat. And second --

MR. SINGER: Speak into the mike a little more. We can't hear you.

MR. LANGNER: Thanks. So why are we discussing this deterrence in the first place? First, because we are aware that there was a threat, and second, because we think that we are not properly protected or that protection may even be impossible. The more difficult the protection, the more reasonable it seems deterrence.

Now, the point is our understanding of deterrence is largely influenced by the nuclear threat and by the experience of the Cold War. And as a matter of fact, Dmitri argues that the rules of deterrence in the cyber domain are identical to those in the nuclear domain, which is something that I strongly object. And I would just argue to the contrary that cyber conflict is completely different from conventional military conflict, that it follows different rules, and that cyber actually defines new rules of warfare. And I think that Peter Singer has made a very strong argument for this approach in his book on robotics on the battlefield and I also believe that the paper you have been handed out entitled “The Wrong War” gives some good argument to support this.

So I am going to explain why I believe that such new rules have to be applied by going into some details of real and hypothetical cyber attacks. Let’s start with the problem of attribution that Dmitri touched.

In order to be able to deter you must know whom to deter. So in order to do this you must be able to determine the intent of and the sources of the attack. Now, unfortunately, this might be much more difficult than you think so I assume you’re all aware of the problem that an IP address doesn’t tell you where an attack originated, for example. But it’s actually much more difficult than this. And I think a good example for the problem of attribution can be found in the case of Stuxnet. So just to give you an idea, I’m absolutely convinced that the United States is the leading force behind Stuxnet. Dmitri is not. He says, no, that just can’t be from my experience. And we are not here to actually discuss who did it, but just to give you an idea that even experts in the field who spend weeks or months in analyzing this probably might not agree. And this will be a problem for political and military decision-makers. Whom do you trust? So this is a problem that needs to be addressed.

For example, one of the most respected IT security experts in the United States said in October 2010, “My guess is that Stuxnet authors, and its targets, will forever remain a mystery.” That’s Bruce Schneier’s words. But let me point to one problem that we have here. We might never again have as much forensic evidence as in the case of Stuxnet. So if you believe that Stuxnet is difficult to attribute, in the future it will be -- will probably be much more difficult. So attribution can sever your option of deterrence because you don’t know who to strike.

Now, Dmitri argues that we can substitute such forensic evidence by a cui bono analysis. Let’s get back to Stuxnet. Who benefits from Stuxnet? Is there enough evidence? So certainly the United States benefits. Israel benefits. But then we’ve got Britain, France, Germany, Saudi Arabia, Egypt. Actually, it would be easier to ask, well, who has a problem with Stuxnet? So I believe that there are some situations where a cui bono analysis really doesn’t get you that far because there are so many potential suspects that you might need to hit or that could be behind the attack.

Now, imagine for a minute here a cyber attack against the United States, for example, taking down 10 power plants. Who benefits? Well, certainly, less countries and adversaries than in the case of Stuxnet, but we are still talking about a number that’s bigger than one. Whom are you going to strike? I think that’s very difficult to answer. And this can even be complicated just by technology. So, for example, you all know in the cyber domain geography is completely irrelevant. So there is no use of determining the geo location of some server where, let’s say a denial-of-service attack emerged from because I could just set up this server that I use to launch my attack in the United States. It’s not a problem. I can do that. I can use a server in China. I can use a server in Malaysia or in Brunei. It’s completely irrelevant.

And a tech complexity can also make it very difficult to establish responsibility. So, for example, think about complex cyber attacks on the record such as the denial-of-service attack in Georgia in ’08, when during the Russian invasion Georgia suffered denial-of-service attacks against government websites. The interesting fact back in ’08 was that you could actually launch the attack as a private citizen because you could download the attack to and from the Internet and just attack Georgian websites. So in such a scenario, who is actually the attacker? Who is responsible? The guy who developed the code or the guy who downloaded it from service provider and launched an attack? Or the service provider himself? This is getting very, very fuzzy. Who is responsible?

And in the future it might even get more fuzzy when we take into account that we are going to see cyberwarfare service providers, such as a modern day Xe, formerly known as Blackwater, just selling you a complete cyberwarfare attack for, let's say $10 million. Who is responsible? The guy who pays or the service contractor? In the future we might even ask, well, if somebody threatens to release exploit code against power plants in the wild, does that constitute an act of aggression or not? So it gets complicated by technical measures.

Who do you want to hit? So Dmitri has pointed out that your response capability must be timely. Rapid command and control decision-making and execution in response to a imminent cyber threat is very important for your deterrence. And unfortunately, you can't play a cyberstrike by ear. There is no fire on command. So the only exception for this is what we have seen in botnets, so distributed denial-of-service attacks. These are the only set of cyber weapons that you could have on a kind of launch-ready alert.

So you could launch such an attack within minutes, but for the more interesting cyberstrikes where you are hitting hard targets, they can't be launched within minutes. They might require weeks or even months. Back in '07, Estonia was under a widespread distributed and not a denial-of-service attack against government websites and against the Estonian infrastructure. Estonia is a very modern country that heavily employs the Internet for public communication.

So earlier this year the Estonian president was asked in an interview if this was the beginning of a new kind of warfare. And the Estonian president is not only a super smart guy; he's also very knowledgeable about cyber issues. And his response was what we have seen is not the beginning of a new type of warfare; actually, it's an end. And the thinking behind this was that this is so unsophisticated. We won’t see much of that in the future anymore. What we are going to see in the future will be much more dangerous and probably even lethal.

So the problem is -- the technical problems, sophisticated cyber weapons as we have seen in the Stuxnet case have no immediate effect because there is no online command and control. The significant cyberstrikes work on a midterm scale. And this means that a pre-emptive cyberstrike in response to a credible and imminent threat might technically be impossible.

What are you going to hit? Let’s suppose you found a solution for all the problems mentioned so far. What’s on your target lists? I can tell you what your opponents are looking for. They would intend to strike, for example, military weapon systems, critical infrastructure such as electrical power, water, and transportation. They will try to strike critical industries. I refer to critical industries as industry sectors, which are vital for national economies so you can cripple a national economy using these cyber attacks by attacking these by cyber means. Hazmat facilities: These are chemical facilities that process hazardous materials such as poisonous gas. And last but not least, nuclear power plants: You will certainly have opponents who in their wet dreams think about blowing up a nuclear power plant and to turn it into a cyber/nuclear weapon.

Now, this is what your opponents are thinking about. If you want to deter such attacks, certainly your response would have to be proportional. Unfortunately, many of these targets, you wouldn’t consider hitting many of these targets proportionately because this would be unethical or just plain stupid because when we think about critical infrastructure, for example, such as power plants and water treatment facilities, once you take down power plants and water and transportation you can bet that there will be civilian collateral damage, which is something that the United States forces tried to avoid in the last years to a very great extent.

The same is certainly true for hitting chemical facilities and try to turn them into chemical weapons. You just wouldn't do that for ethical reasons, even if your opponent just managed to blow up the chemical plant. And you certainly wouldn't try to attack a nuclear power plant by cyber because if you want to do a nuclear attack you just fire a cruise missile or an intercontinental ballistic missile.

Other targets would be plain stupid. So for example, taking critical industries such as the financial industry, what sense would that make because it would backfire to you. Richard Clarke, the former anti- --counterterrorism advisor of the United States Government, once said that a couple of years ago they were thinking about just hacking bin Laden's bank accounts, but they refrained from doing that because they feared an international financial crisis because the markets would lose confidence in the financial system.

So this might be just plain stupid to do a proportional response. This will leave only military weapons systems as your best choice of targets, but these are technical rather than strategical. And your opponent will certainly expect it anyway that you're going to attack his weapons systems by cyber. I don't think that future war will be led without any cyber components so I would call that deterrence.

So there is another area of problems that I want to touch in closing and these are related to proliferation. Certainly, for deterrence, your capability to strike must be demonstrated. This is no disagreement between me and Dmitri, but, unfortunately, if you demonstrate -- credibly demonstrate what you are going to do, your opponent has a chance to protect against this threat. At present, this can be done considerably easily in the cyber realm. There was another problem that if you are actually launching a cyber weapon, you're proliferating it by using it. So the funny thing is cyber weapons proliferate by use as we see in the case of Stuxnet. So several months or weeks or probably a year later the code is available on the Internet for dissection by anybody who has the motivation and time to do so. This is certainly different from conventional weapons who would explode on impact. Cyber weapons don’t explode on impact; it remains intact and it can actually be launched against other targets as well if it is not as specific as Stuxnet.

Unfortunately, the safeguarding of cyber weapons is impossible and so is counter-proliferation. Just think about it for a second. Your counter-proliferation efforts in the nuclear realm are focused on the fissile material and not on the know-how. Now, the correspondence in the cyber realm for the fissile material is bits and bytes. And you can’t control the production and transportation of bits and bytes.

So uncontrollable proliferation means that cyber weapons will soon be available to rogue nation states, failed nation states, terrorists, and organized crime. There is no way to prevent this. By its very nature, cyberwarfare will evolve into asymmetrical conflict. Within a few years every nation state will be able to possess cyber weapons and it’s just a question of time until non-state actors, including terrorists, will also have command over such weapons. Don’t always think about terrorists wearing funny clothes, sitting in the desert in caves and they don’t have the capability to develop sophisticated cyber weapons. They probably won’t, but they don’t need it. All they need is the funding. Cyber weapons will be available within I would expect a couple of years on a gray market. You can buy them. You’ll be able to buy them. Future conflicts will involve opponents who don’t fear retaliation or simply are not vulnerable. I think there is no disagreement between Dmitri and me in this area.

And in closing, what I think is very, very important is to understand that most of the important targets, such as critical infrastructure, can be protected. This is quite a disagreement between me and Dmitri. It’s probably due to the different focus that we have. So my focus is not on your average IT system. My focus is on things like critical infrastructure or critical industries.

So these systems, which are usually referred to as cyber physical, they can be protected easily. And as a matter of fact, concepts for protecting these systems have been suggested by the U.S. Government for over a decade. We were talking about this problem and the need to address this problem for over a decade. Proven concepts develop most notably by national labs, such as Sandia, INL, or ORNL are readily available. Unfortunately, the implementation of cyber defense measures has been largely ignored by asset owners, including the military by vendors and by contractors.

It appears to me that the more intelligent approach to cyber defense is working on the problem of failed protection efforts rather than entering into a cyber arms race that only accelerates proliferation and thereby increasing the threat.

Thank you very much. (Applause)

MR. SINGER: Now, normally I would begin with a question to both of you, but Dmitri, what Ralph laid out was in many ways sort of a counter to the vision of deterrence as you laid out. So I wanted to give you a chance to respond directly to that before we kick it into broader Q&A.

MR. ALPEROVITCH: Sure. Well, just really briefly, I don’t disagree with a lot of what Ralph has said. I think when you look at strategic deterrence, which is what I argued, I don’t believe we have seen a cyber attack to this day, including Stuxnet, that has risen to that level. So the examples that Ralph has given to us -- Georgia D-DOSS, Estonia D-DOSS, Stuxnet -- I do not believe rise to the level of impacting a way of life of a country on a prolonged period of time such as to significantly degrade their national security or economic security.

When we do face such attacks, one, they require significant sophistication. Even Ralph himself has said that Stuxnet probably required three or four years of development, significant resources from the human intelligence perspective, expertise that is only available probably in a couple of countries in terms of knowing how to compromise the centrifuges, how to compromise the control systems, understanding how to get into those environments, being able to replicate the testing infrastructure to make sure that the weapon will work as designed, that capability only exists really in a few advanced nation states today and when we're faced with a question of attribution you have to match the capabilities to the intent and that dramatically narrows your list of suspects.

I also disagree with Ralph that it's a problem that there may be more than one potential adversary. Certainly, we have examples in the nuclear deterrence space where, for example, the French in the 1970s had a "tous azimuts" targeting policy whereas they openly declared that should they see a ballistic missile heading for France they will retaliate simultaneously against both the Soviet Union and the United States without trying to figure out where it came from.

So not necessarily arguing for "tous azimuts" policy, targeting policy in cyber, but certainly if you suspect that there are two likely opponents that may have penetrated the strike against you that has tremendous impact to your national security infrastructure I think you have the right to retaliate against both.

MR. SINGER: Before I turn to Ralph on this I wanted to pull one thread that I thought was a very important difference which was the idea that he's putting forward that use equals proliferation, that is, as you put it, to achieve deterrence you didn't want the U.S. or any other actors to remain so sort of unclear about their capabilities, that we have to be more clear about our capabilities. But what he raises is that any time you reveal your capability it's not like testing the Trinity bomb out in the desert. The parallel would be more like shipping the Hiroshima bomb via UPS and leaving the how-to manual out in the streets. And this weapon is one that once you use it, it can be replicated by maybe less sophisticated actors.

Where do you come down on that?

MR. ALPEROVITCH: I disagree in two ways. One is that when I talk about demonstrating offensive cyber capability I don't necessarily mean demonstrating it by releasing it out in the wild. I'm talking about exercises and simulations that can help understand and contain the environment where you're not necessarily revealing the code of what you're releasing, but demonstrating the impact it was cyber attacked to a level that an adversary may think twice about your capabilities.

But the other point is that cyber weapons are essentially single-use. So as we have seen with Stuxnet, for example, Stuxnet code has been available for over a year. We have seen -- we have not seen, to our knowledge, another Stuxnet or anyone using a copycat attack using Stuxnet, primarily because the capability in Stuxnet that attacked the physical infrastructure was very, very specific. The code, the target of the controllers, was targeted at presumably the controllers that only operate the uranium enrichment plant in Natanz and nowhere else. To modify it, to target another system requires a significant degree of sophistication. The vulnerabilities that Stuxnet exploited have since been patched so a lot of the capability can no longer be simply reused.

MR. SINGER: Ralph, do you want to respond to this?

MR. LANGNER: Absolutely. So there is one very important point that I would like to make. Dmitri has argued that to pull off a significant cyber attack you would need the resources of a nation state. In the cyber physical realm this is not true. You should use something like Stuxnet as, for example, your first botnet. And by the way one very strange thing that we discovered is that Stuxnet has no precedence. So in the cyber physical realm, 10 years ago we had the first cyber attack on the record in Australia. It was very unsophisticated. Then followed a period of silence and suddenly we see a weapon of a complexity that just hits through the roof.

Now, most people assume that in order to do something like that it would require the resources of a nation state, but that's not true because I can copy a great deal of the design, just like it would be the first botnet. So let's assume here for a minute that the guy who developed the first botnet was a genius. He spent many months on this stuff. But now it’s out on the street. It’s out on the Internet and you can analyze it. And to build a copy of that, just replicating the concept is much more easier. And this is the biggest problem that we have with Stuxnet. Forget about the centrifuge for a minute. Our problem is, contrary to what Dmitri has just stated, the vulnerabilities on the control system part of Stuxnet are still there. They are not patched. That’s not true. They are still there. And I can tell you why they are still there, because you can’t patch them. They are unpatchable. They are in the design. So the vendor can’t just provide a patch for download on the Internet.

I refer to these vulnerabilities as iDay vulnerabilities as opposed to 0Day vulnerabilities. Your 0Day can be patched, let’s say, the next day once the vendor has discovered where the problem is, and let’s say it’s a buffer overflow. They fixed it and they provide a patch. Your iDay vulnerability stays there for an infinite number of days and that’s what your attacker can count on. So the vulnerabilities are still there and I can just use -- I can exploit these very same vulnerabilities and use the exploits in completely different scenarios. And you could compare this, for example, to the .lnk vulnerability that Stuxnet exploited. The .lnk vulnerability has nothing to do as such with centrifuges. I could have used this exploit against any other target. And the same is true for the vulnerabilities we find on the controller level. Some of these vulnerabilities have nothing to do with centrifuge as such and I could very well use the same exploits to attack, for example, U.S. power plants.

MR. SINGER: Okay. Let’s bring the wider audience into this discussion, and if you wanted to give a retort as part of the Q&A as well we’ll go to that.

So what I’ll ask is wait for the mike to come to you. Stand and introduce yourself. And actually, we’ve got first hand right here.

MR. HUNTS: Thanks. Steve Hunts from Equilibrium Networks.

I want to touch on a theme that you brought up, Peter, in your conversation with Dmitri and I've spoken with Alan about in the past, which is that I know that probably all of us in the room, or at least most of us, would agree that there is an ongoing spate of attacks against U.S. military and critical infrastructure assets and financial assets, a lot of which are reported to come from China. And with that in mind I'd like you to collectively respond to the argument that what is going on and the reason why we're talking about this subject is not because we're worried about, you know, is cyberdeterrence possible, but rather that it's happening to us. And that someone, whether it's the PLA or someone else, is deterring the United States from intervening, whether it be in Taiwan or somewhere else, by constantly pushing the borders and demonstrating the capability.

MR. SINGER: Dmitri?

MR. ALPEROVITCH: Well, I addressed this a little bit in my talk that what we're seeing today primarily is theft of data, cyber espionage, not destructive activity. And there's a challenge in deterring that no doubt because your ability to retaliate in some sort of kinetic or destructive capacity is limited due to proportionality of a response mandated by international law. I put together a case for other types of deterrence in the diplomatic arena and economic arena because what is essentially happening is a massive transfer of wealth in the form of intellectual property from here to presumably China. And that's something that we absolutely need to address because it's a national security concern. But there are other ways to do that.

MR. SINGER: Ralph, do you want to weigh in?

MR. LANGNER: Well, actually, I agree with the suggestion that was included in your question. And I also am worried about the possibility that we might just fall behind. And especially in respect to what I have argued earlier that we are discussing a good cyber defense of, for example, critical infrastructure for a decade and not much has happened. But many things did happen on the offensive side, not right here, but, for example, in China. So I would agree to that.

MR. SINGER: One thing I would toss out is the way this area is often -- it gets the most attention in the media and as a result how policymakers, senior policymakers talk about it is the fictional, most spectacular. It’s the -- to use the Secretary of Defense saying the problem is a “digital Pearl Harbor.” And at least so far the current issue is not a digital Pearl Harbor; it’s death by a thousand cuts. And I think I would agree. You, in your report, added an important adjective to what you described as a, you know, theft of intellectual property. It’s a theft unequaled in history. That is, we‘ve never seen so much of value taken. And again, we frame it normally in bytes, but what’s being taken is billions of dollars worth of R&D investment that’s been made by the original owners of that data and then is being gained by whoever is taking it. And so -- and then in a national security sense it’s not just economic competitiveness. It’s you’re seeing -- you can measure it in terms of years. It’s the years which it takes to develop a sophisticated jetfighter that then we’re seeing at least certain basics of it being transferred across. And so to me that aspect is perhaps more disturbing than some of the critical infrastructure risk that both you were talking about. And I’m frustrated by the fact that we don’t have a good narrative for talking about deterrence in that realm. You know, we can say, oh, we should apply sanctions and the like, but that at least hasn’t been realistic so far. One of the reasons of which is basically institutions that are targeted for whatever reason don’t like to talk about it. And so it’s kept -- we don’t reach the level of a collective will to engage in whatever counteraction or to create a public cost to it as long as we consider being targeted as something that is the victim’s fault. I could see crime parallels to that.

MR. ALPEROVITCH: Well, the other important point is that this is CNE -- cyber network exploitation -- activity, but it is essentially a demonstrable capability for doing CNA -- cyber network attack -- because once you're in a system doing damage to it is just a difference of a few keystrokes as opposed to stealing the data that's sitting on that system. So I think the important point is that, you know, presumably the Chinese are inside all these networks, government networks, enterprise networks, and they haven't done damage yet. But the capability certainly exists there and how we deter them from taking that step.

MR. LANGNER: I would like to underline that every sophisticated cyber attack that would try to achieve some damage starts with collecting information. So it starts with intelligence gathering. And up to now our understanding of sophisticated cyber attacks such as Shady RAT and the similar stuff in the APT area is that the primary goal was to steal information and something like trade secrets. But if you think a little bit ahead, these same attack vectors might be used for different purposes, such as gathering the intelligence to make the subsequent destructive attack possible. So you need that first logical step. You need to gather intelligence before you are able to hit your intended target hard for the cyberstrike.

MR. SINGER: Let's get some more questions. Allan, right there. You've already got the mike.

MR. FRIEDMAN: Allan Friedman from Brookings.

So I wanted to pick up on a strain of discussion you were having on proliferation because I thought that was very interesting. And I wanted to take it into an economic direction.

So in the first part of this decade we had a big public discussion about vulnerability disclosure policy where there are a bunch of people saying we found this vulnerability. We're going to publicize it because we don't think you'll act quickly enough to patch. That's reached a pretty good resolution right now. We have the secondary market of vulnerabilities and there's a whole private sector involved. Yet, Ralph, you mentioned that there is no possibility of disclosure than patch timeline when we're talking about SCADA. So when we have people like Arami from Italy sort of publicizing vulnerabilities and PLCs, what should the policy response to this be? Should we be engaged in trying to damp down all public disclosure of vulnerabilities? Should we be having private markets? Should it stay academic? Should we disclose nothing?

MR. LANGNER: Yeah. I think it's -- before you listen to my answer you will have to keep in perspective that I'm talking from within the security community. And so this might be another side of, let's say, political decision makers or asset owners or vendors. So you might hear a different opinion because I'm in that community.

We have -- we, as the community, have a hell of a problem seeing vendors and asset owners just doing nothing, just sitting on their vulnerabilities. And it's getting up to a point where people like me really can't stand it any longer. Up to the point where I have already said, well, if nothing changes within five years then I'm out of this business. I can't stand it any longer.

And it also has some -- it can lead to some very bizarre discussions. So, for example, is it really a vulnerability disclosure what some people are doing? Let me give you -- let me try to make the point here. Back in 2008, I approached a very big vendor in the control system area about what we think is a critical vulnerability that we have identified. And there was some back and forth so it took some time that the vendor understood what we were talking about, and finally when they got it they replied, well, we wouldn't -- we wouldn't describe this as a vulnerability, period. So they didn't intend to do anything about it. In our opinion, still it is a critical vulnerability.

Now, the point is if I am going to talk about this vulnerability and publicly release information about this vulnerability along with exploit code, I could say this is not vulnerability disclosure because according to the vendor it's not a vulnerability in the first place. (Laughter)

So just to give you an idea how bizarre the situation can get. And again, we professionals in the community are at the point where we are really having a hard time because our clients -- in my case these are mostly asset owners -- where we try to secure facilities. They really don't get the support, for example, from vendors that they deserve. And we were running out of options to make a significant change here. And this is one reason why just recently researchers like Orema or Beresford or even myself or Dave Peterson, he is working on that, too -- are more and more openly discussing this stuff and just telling the vendors, oh, you told everybody it's not a vulnerability and everybody knows it anyway. So let's -- why not discuss this for example with the media?

MR. ALPEROVITCH: Ralph, I want to thank you for making my point that the networks and the systems are not defendable. (Laughter)

MR. SINGER: Okay. Let's give someone actually in the back there. Yeah.

MR. WEINTRAUB: I'm Leon Weintraub, University of Wisconsin.

I'd like to ask a question based in part on the excellent article that was handed out with this piece. Thank you very much.

Dr. Singer, you compare the situation to the 19th century issue of piracy rather than the Cold War analogy. And you said how nation states develop a series of norms and treaties to protect against the issue of pirates. I think in that situation nation states had the recognized legitimacy to do the attacks, to defend the borders, et cetera. In this era -- in this cyber area where there's so much mix between the public attitude of governments and the private sector, I'm wondering who is going to assume that role?

Now there is, for example, an organization -- an international organization, the ITU -- the International Telecommunications Union -- which is a mixture of both public and private. I don't know if -- now, so far, as far as I know, they're mainly involved in allocating frequencies and other things like that. But would this be a viable way to do it? Or do we have to look for a new model since this is such a complex mix of both the public sector and the private sector?

MR. SINGER: It's a great question and I hope you all will weigh in as well. What my co-author and I were trying to do is knock down a little bit that concept that there was a perfect fit to the Cold War, which is a narrative that is very much taken off in D.C. policy circles. I would argue mainly because it's what people are most familiar with already in senior policymaker roles. It's the parallel that it was unsurprising when the Air Force was planning its strategic bombing campaign in Vietnam it wasn't all that stunning that they reached back to how they did strategic bombing versus Nazi Germany because that was what those officers that were now generals knew best.

We used the example of pirates -- more importantly, privateers -- to hit at this notion of attribution that one of the keys in this space is that you may have individual or organized actors that are basically straight acting as criminals. Then you have clear state notions, you know, whether it's cyber command or the PLA, but a large problem, at least in the attacks that we've seen so far, is entities in the middle that may be state affiliated, but not formally the state. Patriotic hackers is how it's often described. My understanding is that the Georgian incident sort of reflected that rather than a formal entity. And that again, there are certain historic parallels for that which was the nature of privateers which, you know, were privates during some periods and then they would get state sanctioned. And the very essence of their identity, that was the appeal of them. And yet you saw an interactional action against it. And one of the key lessons was it was not just developing international treaties, which I think is useful, but also it took action at the private sector at the market level, which is one of the keys that we're going to have to, I think, engage in in this realm.

So the answer isn't just the ITU. It's also my own personal belief the ISPs starting to develop some responsibility and accountability in this network. And again, another parallel for this may not be privateers; it may be how, for example, international banking went from saying I don't have any responsibility for the terrorist money that is in my bank account, I can't control with it, to post 9/11 they suddenly developed accountability for it.

We may need to see a similar parallel in ISPs. They won't enjoy it, but that may need to be developed.

MR. ALPEROVITCH: You know, I don't believe that cyber criminals, terrorists, or hactivists are a strategic threat in cyberspace today to our country. I just don't. I don't believe the capability exists there. I quite frankly don't see the motivation particularly on the part of cyber criminals which are mostly interested in profiting from financial-type of fraud. I don't see them going into the destructive capability which would clearly inflict massive retaliation on them should they do something truly damaging and take them out of business permanently.

So I think the problem today, it may change in the future, but today is nation state activity. And when you think about that it's an interesting model we have where the private sector actually has responsibility against defending themselves against an armed invasion in cyberspace from another country or intelligence agency. Where else do we ask the private sector to defend against another nation state and armed attack either in the physical world or in cyberspace? I think that model fundamentally breaks when you start considering the variety of businesses that are out there. Maybe perhaps your multinationals will have the capabilities and the funds to build secure systems, but your 10 people, utility firm, and some small town obviously has no chance. And I think it's ultimately government responsibility to figure out either deterrence doctrine or defensive posture to help protect against that threat.

MR. SINGER: Ralph, do you want to weigh in?

MR. LANGNER: Just one quick comment. I like the analogy to piracy very much. I think it’s a better analogy than the Cold War analogy. I think one of the biggest problems that we have in discussing cyber attacks is that in a way right now anybody who is trying to achieve cyber capability or acting in this realm is kind of an outlaw, just like a pirate, because there are no laws. They are still in development and this is one very important effort that I see which is carried out by NATO’s Center of Excellence in Tallinn. They are very much concerned with developing international law that sets some rules of how to define and how to interpret certain actions and to set limits for cyberactions.

MR. ALPEROVITCH: Can I just say one quick thing? I do disagree that there are no laws. I mean, there are plenty of laws regulating computer network attacks and intrusions, and the United States itself believes that the laws of armed conflict do apply to cyberspace.

MR. SINGER: One last parallel that again Noah and I at least like about the notion of privateers or piracy is not just the idea that you’re not talking about an interstate Cold War in terms of politics, but you’re talking about a realm of primarily commerce and communication, whether it’s the sea or whether it is cyber, that actors are attempting to, simply put, interdict or steal. And within that space one of the interesting things of the privateering parallel which is important to remember in discussions, you know, folks like us gathered is that it was a very useful tool to the United States. It was actually our most effective military tool that for whatever reason -- we can get into a longer discussion -- we decided not to utilize. So there is a parallel of both the U.S. doing this, which we do in cyber, let’s admit it, whether it’s demonstrable or not, but then also that what you’re talking about is at some point it was a tactic technique broader doctrine that the U.S. decided was no longer valuable. Which, if we’re going to see any kind of end of, at least state level action in cyber, it will have to be states deciding that this vector and type of attack, including using privateer equivalents is no longer valuable. That’s the only way I see it getting used.

Let’s get in the front another questions. Right here. Right here.

MR. SMITH: Thank you. Bruce Smith, Brookings, retired.

A very rich and fascinating discussion. As a tyro in this field I don’t quite know where to start, but on the question of what kind of analogy or arms control disarmament, international regime, legal structure, I think you have three alternatives. You can have a kind of START analogy where you have a binational agreement between two great powers: U.S.-Russia, let’s say U.S.-China. That’s one option. You can have more of a WTO, a total multilateral framework where you work through the U.N. or the OECD or something in an attempt to create a legal regime with all nations. Everybody subscribe to it. Or I think perhaps more realistically you might have something like the old COCOM where you really did have a structure. You preserved international trade, international business activity, but it was within the so-called free world of people who played by the rules and you’re able to pretty effectively, with some leaks, to exclude the Soviet Union and non-signatories, non-acceptors of the rules of the game from participation.

Now, I don’t know if that has any utility to think in those terms, but if you were to think of a modern day kind of COCOM where you’d rule out as not belonging to the international economy or international trade those nations who really didn’t play by the rules, would that -- does that make any sense?

MR. ALPEROVITCH: I don’t know how you exclude China from participating in the international economy today given that they own so much of it. But I think the multilateral model is the only one that can make sense. But the thing that I find very unfortunate is that the gulf in understanding between what even constitutes a cyber attack between us and, let’s say, China or Russia, is just so huge.

I was in a conversation with some officials from the Chinese Foreign

Ministry a few months ago where they basically declared that a rumor spreading on Facebook that causes social unrest in China they would consider a cyber attack. So how do you even begin to have a conversation with them about norms of behavior when clearly we're not going to regulate Facebook, free speech, and everything else? And that's what they consider one of their most strategic threats. So the gulf is huge and, again, the costs of the activity that we believe they're perpetrating in terms of economic espionage are so low that they have no interest in stopping.

MR. LANGNER: I would like to focus on the issue of arms control and again would like to re-emphasize my point that cyber arms control is impossible for technical reasons. And for a minute please don't think about the situation right now. Think about the situation, let's say, in five years. Just to give you some ideas, your cyber arms shop cannot be spotted with satellite surveillance. Your Geiger devices are of no use. It is just not possible to detect any development activity of cyber arms.

Let me try to give you a better idea of how that would work. If tomorrow morning the president of the United States gives me a call and says, okay, Ralph, we need you. We need you to work on our next, let's say, Stuxnet 2.0. And you get any resources --

MR. SINGER: And you ask how much?

MR. LANGNER: And you can have any resources that you want. For example, U.S. Cyber Command, and my response would be just forget about Cyber Command. Just give me, let's say, a bag of money and I'm going to do that with my own team. Let's say we are talking about 10 people that I would need. Right now the cyber arms race is about talent. It's not about the number of people that you have. Right now it's only about talent. So me and my 10 guys would be spread around the globe. We would be working on different parts of the weapon. We can coordinate and check via the Internet, via IP sec lines, so we can put all this together without anybody, including the

CIA, being able to recognize what’s going on.

Okay. I exclude the CIA because I might be in their focus already.

(Laughter)

But just to make the point, so this could be done anywhere. And right now it’s a matter of talent and you can’t do any surveillance on this. Your satellite images are just worthless. Your attacker might be sitting in a hotel room in New York City. Another one might be sitting somewhere in the Bahamas.

MR. SINGER: All right. Let’s give -- actually, right there. Yeah.

MR. LINDSAY: Jon Lindsay, University of California.

An important variable when you’re talking about deterrence is this question of offensive advantage which both of you spoke about a little bit. And it’s kind of a conventional wisdom that, you know, offense is easy in cyberspace. And, you know, that’s clear at the low end, front, whatnot. I wonder if you can talk about the high end where, you know, you also have this problem of, you know, intelligence being necessary for the planning. And, you know, intelligence is hard. It goes wrong all the time and if you have a lot of certainty that’s involved, does that mean maybe the offense might be difficult and therefore the effect uncertain? So you might, you know, not really want to bring that to the bargaining table if you have a weapon that, you know, is highly uncertain.

MR. LANGNER: I would like to go first here. So certainly you do need some intelligence for any sophisticated attack. But let’s put it into the bigger picture. There is always an element of uncertainty in any act of war. Clausewitz once said, “War is the reign of chance.” And the funny thing is, with the evolution of cyber attacks that we receive, I mean, attacks of the Stuxnet caliber, you could well say this is a big field experiment with unknown outcome. I was surprised to see that it obviously worked pretty well. But you couldn’t bet on that. And this will be the case with future cyber attacks.

The attackers are, in a way, in a phase presently where simply experimenting.

MR. ALPEROVITCH: I think if you’re talking about very specific target attacks, let’s say you’re talking particular infrastructure, the Iranian nuclear power plant or some weapons guidance systems, I think you can get a great deal of certainty assuming you have good intelligence and ability to have a testing environment where you can actually try out the attack in the lab before you actually launch it. I think when you’re talking about massive scale attacks, you know, let’s say shutting down the electrogrid in the United States, that’s where things become much more complicated because understanding all the interdependencies between different utilities, the transmission lines, et cetera, is probably -- you probably would be hard-pressed to find a single person in this country who totally understands it. And the fact that you have trees growing in Ohio that are rubbing up against power lines that cause a blackout in the Northeast kind of tells you that very few people understand those interdependencies. That means you can cause accidental cascades that cause significant damage, but it also means that it’s hard to predict what’s going to happen and whether you’ll actually cause damage because these systems are so complex.

MR. LANGNER: Let me please follow up just a minute in respect to Stuxnet. Two topics surprise us. First of all, that the attackers only achieved to take down 1,000 centrifuge from 5,000. And our understanding right now is that this might be due to the fact that their intelligence was just incomplete. So that -- which happens all the time, that the people in Natanz might have wired the actual control systems a little bit different than what was in the specification. It happens all the time. And so your spies managed to get out the documentation, but that’s all you have. And so you’re acting on it.

The second thing that surprised us was to see the worm spreading, for example, to India. I could give you an explanation, but I’m just saying this was certainly not intended by the attackers. This was an element of surprise. And what worries me is for the 2.0 or anything that might come soon, what will the next unintended surprise look like?

MR. SINGER: Okay. We're getting to the witching hour so let's bundle two together and actually, so, wait in answering and let's get both these folks over here. Actually, up front here. Right here. Yeah.

MR. PURDY: Thank you. Andy Purdy with CSC.

I appreciate the discussion. I think there's been a focus on more tactical deterrence or tactical response. I think a deterrence strategy also requires a look at vulnerabilities and defenses. So in the nuclear context, the George Kennan strategy of, okay, they've got to know that we're going to respond heavily is fine. We knew we were vulnerable. We knew we didn't have the defenses. We didn't have Star Wars. So we had to use that kind of deterrence strategy. I think what we're talking about here, we have to go well beyond, particularly because of the problem of attribution, the problems of it's not just governments that are involved. And so I think the singular contribution of Peter and Noah's paper cannot be overstated.

Moving away from the Cold War analogy, whether it's piracy or not, the point is it's public and private. There's an ecosystem. We have to approach it like an ecosystem that's not focused just on attribution, it's focused on the enabler. So you look at that key sentence in this article. "The networks of just 50 Internet services providers account for about half of all infected machines worldwide." So I would ask you, what is your sense about whether we need to take the kind of strategic approach that Peter and Noah are talking about to help inform and make more effective a deterrence strategy?

MR. SINGER: Hold off. And actually just hand that to the gentleman right behind you. Yeah.

MR. CURRY: Thank you. My name is Eric Curry, USAF, retired.

My question is bounded to the criminal non-state actor realm. Arguably, the whole cyber realm is still the wild, wild West. As an industry they have a complete pass. When I get a drug I don't have to sign an end-use license agreement to say if I drop over it's not their fault. There was a time when the automobile industry had that same pass. The pharmaceutical and medical industry no longer has that pass. Their responsibility was safety. When are we going to start to hold the people who produce this realm? As you said in your paper it's a manmade realm driven by profit without, whether it's a SCADA producer, whether it's Microsoft, Adobe Flash. It's first to market. There's no consideration, no responsibility for security. When through product liability national and international regulation are we going to start to control this realm? And I know we don't want to kill the baby in the cradle because there's a lot of jobs and profits there, but a lot of this is manmade and there's been very little responsibility placed on the people who produce this realm in the private sector. So what's the law of -- the role of product liability and regulation to control at least the baseline level of vulnerability in this entire realm?

MR. ALPEROVITCH: The problem you have is that safety and security are not the same thing. You can do risk analysis of a system from a safety perspective. You can estimate the probability of an earthquake or another accident or a natural disaster. You can't do that with a manmade threat because if you have an adversary that's intent to penetrate your network and spend no expense to get into your network, your risk is 100 percent. And they will get in.

Today, and I deal with folks that do penetration testing of all kinds of networks, government networks, enterprise networks all the time, they tell me that they have yet to encounter a system they cannot penetrate and do so quite easily. My argument is that defensive approaches, and I'm not arguing that we shouldn't improve our defenses, but defensive approaches alone will not work. The fundamental architecture of both the Internet and the systems that are on that network are undefendable today.

Now, so unless you decide to rebuild it from the ground up, both the network and the systems, I think you have to deal with a domain where you will be penetrated. You know, the NSA, for example, has a model where you have to assume that your network is always compromised and you have to operate in that environment. We have to start thinking that way on a broader scale.

MR. LANGNER: Okay. First, I would like to comment in the affirmative in respect to the first question raised. So I agree with the proposition made in the paper. And for the second question, unfortunately, I do believe that we need more regulation. I used to be anti-regulation and anti-government, but I don’t see it happening. I don’t see the defense that we really need being established by a private-only effort. So we do have already very good approaches to rules in the industry and I’m afraid they need to be enforced by tighter regulation.

And I would like to make one final comment in respect to what Dmitri just said, like the installed base is so big that it’s impossible to defend it. Please don’t always talk about the installed base. Yes, this is a huge problem, especially in critical infrastructure, but please also keep in mind that every day, let’s say something in excess of a thousand new systems are installed. And what we are doing right now, we are installing the same old legacy systems with the same known vulnerabilities over and over again and we’ve got to first stop this leak. This is why something like regulation for new products makes very good sense.

MR. SINGER: Well, I want to thank both of you for contributing to this discussion. A great deal of substance. It’s been fascinating I think for all of us, and I think what’s important is in many ways this is the start of the discussion. I think you both can agree on that. And so we hope you’ll come back again and continue to work with us on these important topics. And thank you all for joining us. Please -- (Applause)

* * * * *

CERTIFICATE OF NOTARY PUBLIC

I, Carleton J. Anderson, III do hereby certify that the forgoing electronic file when originally transmitted was reduced to text at my direction; that said transcript is a true record of the proceedings therein referenced; that I am neither counsel for, related to, nor employed by any of the parties to the action in which these proceedings were taken; and, furthermore, that I am neither a relative or employee of any attorney or counsel employed by the parties hereto, nor financially or otherwise interested in the outcome of this action.

/s/Carleton J. Anderson, III

Notary Public in and for the Commonwealth of Virginia

Commission No. 351998

Expires: November 30, 2012