Intelligence Squared U.S.
590 Madison Avenue, 30th Fl.
New York, NY 10022

Contact Publicist: Eileen Murphy
T: 917-913-2233
eileen@eileenmmurphy.com

June 8, 2010

They cyber war threat has been grossly exaggerated

For the motion: Marc Rotenberg and Bruce Schneier
Against the motion: Mike McConnell and Jonathan Zittrain
Moderator: John Donvan

RESULTS

Before the debate:	After the debate:
24% FOR	23% FOR
54% AGAINST	71% AGAINST
22% UNDECIDED	6% UNDECIDED

John Donvan:
I'd like to welcome our panelists to the stage. Round of applause.

[Applause]

I'll introduce them in a moment but first I want to introduce the man who has made Intelligence Squared U.S. possible: Mr. Robert Rosenkranz. The Rosenkranz Foundation; he started this four years ago in New York with the purpose of raising the public discourse in New York City. We are a force to be reckoned with there. This is our first foray outside and we are so pleased to be in the nation's capital and so pleased to see so many of you. So I would like to first of all, to welcome Robert Rosenkranz.

[Applause]

Robert Rosenkranz:
My role in these proceedings is to frame the debate, to outline why we think the topic is important and why we feel they're intellectually respectable arguments on both sides. So, in late 2009, computer operators in China gained access to Google's computer network and obtained information about Chinese dissidents and about some of Google's intellectual crown jewels including their development plans and they're passwords and stuff. Chinese military strategy emphasizes cyber espionage to obtain our military and technological know-how. In the event of major conflict, they strive for the capacity to attack our home front, not by conventional arms but by disabling the vulnerable civilian computer systems that are essential to run our power systems, our telecommunications grids and our financial system. And China by and large, has a huge interest in our success. In contrast, terrorist groups have powerful motives to destroy our domestic

infrastructure, particularly if they can do so without a physical presence in the United States, why wouldn't they.

So the extraordinary complexity of our computer systems with their hundreds of millions of lines of code, make them very hard to defend. The attacker needs to find only one weakness and the defender needs to find them all. And then advance. That's why so many of our military's best strategic thinkers consider cyber attacks our single biggest threat. So what's the argument in favor of tonight's motion? Simply put, describing a worst-case does not make that case likely. It may seem a sensible precaution to defend against a dire outcome, but first one needs to assess both risks and costs. Apropos risks: How plausible is it that the Chinese or any other nation would attack our civilian computer infrastructure, even if they had the capacity to do so? By targeting civilians, might their military commanders risk committing war crimes? Wouldn't their strategists assume that we have the capacity to respond in kind? And how plausible is it that terrorists who can barely talk to each other on cell phones are capable of a serious cyber attack? And apropos costs: Consider the potential for the dead hand of government bureaucracy to stifle an invasion or to infringe our privacy. Do we really want to give the folks responsible for airport security greater powers of surveillance?

[laughter]

Robert Rosenkranz:
Is cyber war a threat that we're not taking seriously enough? Or is it one we have exaggerated? It's a very important question for our nation, and we've assembled an extraordinary panel of experts to help you decide. Before we begin, though, I want to say a word of thanks to WAMU in D.C. that's promoted this debate very, very heavily and is maybe responsible for a lot of you who are here tonight. And -- but particularly, I'd like to introduce Jeff Ganek, the CEO of Neustar, which made this evening possible.

And I hope you'll join me in applauding Neustar's generosity.

[applause]

Jeff Ganek:
Thanks, Robert, and thanks to Intelligence Squared for taking this show on the road. We at Neustar are delighted to have coaxed Intelligence Squared away from home in New York for the first time ever, bringing it here to Washington, D.C. Clearly, just the packed house here tonight shows that there's a true hunger for intelligent and civil discourse that's Intelligence Squared's hallmark. There's much the nation's capital can learn from Intelligence Squared, and we're excited for this evening to get started. This is a timely topic, so I won't take up any more time. Instead, I turn the stage over to John Donvan, and our distinguished panelists.

John Donvan:
Can I invite one more round of applause for both Robert and Jeff?

[applause]

John Donvan:
Welcome, everyone, to another debate from Intelligence Squared U.S. I'm John Donvan of ABC News, and once again it is my pleasure and my honor to serve as moderator, as the four debaters you see sharing the stage with me here at the Newseum, and it's our first debate outside of New York City. Four debaters, two against two, will be debating this motion: "The cyber war threat has been grossly exaggerated." Now, you in the audience have a special role, and I just want to divert very briefly while I talk about that. We've already mentioned that WAMU is a partner in this evening, and they obviously did a very, very good job in bringing all of you out here on this evening. And we are aware of the fact that Conan O'Brien who's doing his 30-city tour, this is his night in Washington, and we are aware of the fact that James Taylor and Carole King -- that doesn't happen very often -- they're singing together four blocks away.

And mostly, we are aware of the fact that at National's Stadium, Steve Strasburg is taking the mound for the first time.

[applause]

John Donvan:
So, the fact that all of you are here for a security policy discussion, debate in really, anywhere else but Washington, D.C. -- the words "wonk fest" will not escape my lips, but I do want to congratulate all of you for being here. And here is the reason. This is a debate. It is a contest. There will be winners and losers, and you, our audience, have a special role. You are the judges. By the time the debate has ended, you will have been asked to vote twice: once before and once again after the debate. And the team that has changed the most of your minds on this motion will be declared our winner. Let's go to the first vote now. To the right of your seats, there is a keypad. If you agree with our motion, "The cyber war threat has been grossly exaggerated," if you agree, push number one. If you disagree, or if you're with the side that is arguing against, you push number two. And if you're undecided, push number three. All right, looks like from everybody's faces that we have passed that test. So we'll have the results in a short while. We'll share with you what the opening, what the preliminary vote is, after it's tabulated. And then once again at the end, we'll go to the second vote and that's how we'll choose our winner. So onto round one: opening statements by each debater in turn. Seven minutes each. Marc, you can make your way to your lectern. I'd like to introduce arguing for the motion, that the cyber war threat has been grossly exaggerated, Marc Rotenberg who is executive director of the Electronic Privacy Information Center. He has been, since before most of us were familiar with the Internet, a fierce advocate for our privacy. In fact, he has taken on internet behemoth Google, filing Federal Trade Commission complaints against Google on the grounds of possibly violating privacy. That's the kind of man he is; those are his issues; I'd like to introduce Marc Rotenberg, but I'm curious to know, do we need to worry more about China or you, if we're Google?

Marc Rotenberg:
Thank you so much John, and thank you all for being here tonight. I wanted to begin also by thanking Intelligence Squared and the Rosenkranz Foundation and Neustar for hosting this event. This is an important issue; this is one of those issues that's being discussed here in Washington, in Congress and the White House and your views, your assessment of want the country should do with regard to the threat of cyber warfare is very important and we thank you for being here tonight. We're going to ask you tonight to consider the proposition of whether the threat of cyber war has been grossly exaggerated. Keep in mind the statement of the proposition. We're not talking about cyber attack, cyber concerns, cyber worry, or not being able to boot up your email. This is a debate about cyber war and how serious that threat is. I'd like to share with you a few statements that I uncovered as I was preparing for this debate. One of the leading experts on cyber war said, "Digital Pearl Harbors are happening every day." The person who has been named to head the U.S. cyber command, the current director of the National Security Agency said "U.S. military networks are seeing hundreds of thousands of probes a day." And one of our opponents in the debate tonight has compared the threat of cyber warfare with nuclear war. Now Bruce and I are going to try to explain to you why it is that we believe that these statements overstate the problem. We are certainly aware of the full range of risks to the Internet and there are many different actors out there. Some of them with criminal intent, some of them are spies; some of them are just curious.

We used to call them hackers in the good ole days. All of them pose various types of threat to the Internet as we know it, but if we reduce all of these threats to the catch-all of cyber war, I am concerned that it will take our country in a direction that we will very much regret. But tonight we are not only going to try to persuade you that the threat of cyber war has in fact been grossly exaggerated, we are going to try to explain to you why this has happened. In fact, what you are hearing now about the threat of cyber war is part of a long running campaign here in Washington to move control of the Internet, the technical standards and the openness that we have enjoyed away from its current model to one that would give the intelligence community and the National Security Agency much greater authority to decide what people may or may not do on the Internet. And that effort has been underway long before the stories that you will hear tonight about Russian hackers and Chinese plans to take over the Internet and even attacks launched from North Korea. Back in the 1970s, the NSA worried about the public availability of encryption; the key security standard that today makes possible the routine transactions you engage in when you buy a book on Amazon or download a song from iTunes. NSA didn't want that encryption technology widely available, and they fought against it. Fortunately, computer researchers pressed on, and encryption became widely available and provided a key technique to make possible secure online transactions.

But then, in the 1980s, along came John Poindexter who would later come up with Total Information Awareness, and he worried about unsecured private computer networks -- does any of this sound familiar -- back in 1984. And he wanted the National Security Agency to be responsible for computer security in the United States. Fortunately, the Congress didn't like that idea. They pressed back on Mr. Poindexter and the White House, and we established open standards to safeguard network security, but this is not

the end of the story. Because then again in the early 1990s, as encryption was becoming more widely available and the NSA worried that they could not intercept private communications, they said to Internet users and American business, "You have to use a new technology that we've developed, called Clipper, the escrow key encryption standard. Anytime you want to send a private e-mail, we need a copy of that key that you used to encrypt your communication because we want to be able to know what is contained in your private messages." And again, Congress pushed back and Internet users pushed back, and the Clipper chip proposal put forward by the NSA in the early 1990s was rejected. The story continues. After 9-11, NSA was there again arguing for control of the Internet to try to protect our nation against terror attacks. Now, don't misunderstand our argument tonight. We are aware of these threats, and we are not going to try to persuade you that there are not threats out there that are serious and real and that we should ignore. That is not our argument. Our argument is that we have to be very careful about allowing a single, secret, unaccountable government agency, which has been fighting for 25 years to take control of Internet security, to become the dominant authority for the Internet, which is what will happen if you accept the proposition that the threat of cyber war has not been grossly exaggerated.

So, we urge you this evening not only to side with our side, to agree that this threat has been exaggerated, but also to understand why it has been exaggerated. There are agencies in Washington that want very much to know what's in your e-mail. They want to know when you log online. They want to be able to build big databases and detect patters. And this is the threat that Bruce and I will try to respond to. Thank you.

[applause]

John Donvan:
Thank you, Marc Rotenberg.

[applause]

John Donvan:
Our motion is, "The cyber war threat has been grossly exaggerated," and first up to argue against the motion, I'd like to introduce Mike McConnell. Now, speaking about experience, not only was he a vice admiral in the Navy where he did a significant amount of intelligence work, he went on to become former director of national intelligence, making him the nation's top intelligence officer. Also in his career, he was director of the National Security Agency. Mike, does it get more inside than that?

Mike McConnell:
Well, a few things, not too many.

[laughter]

John Donvan:
But nothing you're going to share tonight.

Mike McConnell:
Well, actually I am going to share a little bit of a story that --

John Donvan:
Terrific.

Mike McConnell:
-- goes with that long history.

John Donvan:
Ladies and gentlemen, Michael McConnell.

Mike McConnell:
The translation --

[applause]

Mike McConnell:
Thank you. The translation of experience is age. The bad news is age. The good news is grandchildren. But let me humanize just a second. A little under the weather. Two grandsons come to see me. The oldest runs into the room and says, "Grandpa, Grandpa, make a sound like a frog." And I said, "Son, what for?" He said, "We're talking to Grandma and she said as soon as you croak, she's taking us all to Disney Land."

[laughter]

Mike McConnell:
That's what age does for you. Let me compliment Marc on his argument. And I want to say up front, I agree with everything Marc said about the essence of what makes us Americans: privacy and civil liberties.

However, I disagree and urge you to vote against this proposition because of how he framed it. Let me just quote, “Our argument is do not let a single authority, the National Security Agency,” agency I was chosen to lead, “control the Internet.” It has nothing to do - it has nothing to do with this debate. Now--

[Applause]

Mike McConnell:
I want to just, if you’ll bear with me for just a second, just a small amount of time here; I want to make reference to people who are informed at the highest level with all of the information: our last three presidents. President Clinton focused on this subject; he had a special panel review it and he concluded that it was critical to the nation that we move to address this set of vulnerabilities. President Bush who I had the pleasure to serve along with serving President Obama, said, and I’ll just quote, “in the last few years, threats in

cyber security have risen dramatically. The policy of the United States is to protect against the debilitating disruption of operations in our information systems for critical infrastructures." Later, when I had a chance to serve on the inside again, I made my case to President Bush and he supported a comprehensive national cyber security initiative. The Congress agreed and a bill was passed. Now, we've got a new administration. The new administration did not agree with the previous administration, huge policy differences in every dimension. We made our case to President Obama and he said, "I will take it under review." After reviewing it for a considerable period of time, he said, one year ago, we meet today at a transformational moment, a moment in history, when our inter-connected world presents at once with great promise but also great peril.

It's the great irony of our information age, the very technologies that empower us to create and to build also empower those who would disrupt and destroy. The key is disrupt and destroy. I'm not talking about hackers. I'm not talking about criminals, lots of statistics. I'm not even talking about China and what China has done to take information out of this country. I'm talking about destruction of data. Let me give you just a way to think about it. The United States economy is $14 trillion a year. Two banks in New York City move $7 trillion a day. On a good day, they do eight trillion. Now think about that. Our economy is $14 trillion. Two banks are moving $7 trillion to $8 trillion a day. There is no gold; they're not even printed dollar bills. All of those transactions, all those transactions are massive reconciliation and accounting. If those who wish us ill, if someone with a different world view was successful in attacking that information and destroying the data, it could have a devastating impact, not only on the nation, but the globe. And that's the issue that we're really debating. We are so inter-connected; we have enjoyed the benefits of the information technology revolution. It's touched everyone in this room. From the time you got up this morning in an air conditioned space; you bought gasoline for your car with a credit card. You do online banking; you have power routed to your home. We're on a path to increase the digitization of the country. Medical care will be improved because of information technology. We can move the information; we can understand trends and we can protect privacy. And the arguments that our opponents are going to mount are this is an argument about privacy and civil liberties; it is not.

We can have both. I was privileged to serve the National Security Agency as its director. I was there for the debate over clipper chip and the other things that were mentioned. What I would encourage you to do, since I'm going to be out of time in just a second, is bring that topic up when we have a chance to have the dialogue with questions from the audience. And I will tell the story from a little bit different perspective. I did serve on the inside; I have served on the outside, so I've had the privilege of seeing it from both sides. That's not fair to you the audience, because I live in a classified world. We have a system of representative government. Those representatives that speak for you are cleared; they're informed; their responsibility is oversight. The equivalent of the National Security Agency was breaking Nazi Germany's code in World War II. Historians argue that that probably shortened the war by 18 months to two years, saved countless lives and incredible resources. Did the American people have the right to know that NSA was breaking Nazi Germany code in World War II? Because if they had

known, the Germans would have known, and all they had to do was take it away by changing the rotors. Secrecy gets a very bad name in our society. American citizens don't like spies in spite of the fact that the first spy master was George Washington. Secrecy is a necessity.

[applause]

Mike McConnell:
And I would summarize by saying we have laws and the key is getting the law correct. If the law is written appropriately and there is the appropriate oversight committee, if you violate the law, you will be held accountable. In a nation as free and as wonderful as ours is, leading the world in human rights and privacy and civil liberties, it's getting the debate framed right to mitigate the risk, to protect the nation consistent with our values and our laws. I urge you to vote against this resolution.

[applause]

John Donvan:
Thank you, Mike McConnell.

[applause]

John Donvan:
So, we are halfway through the opening statements of this Intelligence Squared U.S. debate. I'm John Donvan of ABC News. We have four debaters, two teams of two, who are arguing out this motion: The cyber war threat has been grossly exaggerated. You've heard the first two opening statements, now onto the third. Bruce Schneier has a position in a company and also a position in the culture. He is the chief security technology officer of BT, but he is more than that. If you listen to him on any YouTube video, he is a thinker, he is a philosopher, a man who has taken the topic of security to the human soul, asking questions like what is trust and when do we know it and when do we recognize it. So, he gets the title guru. And I want to ask you since our radio audience can't see you, the ponytail, is that a guru thing, or do you just like it?

[laughter]

Bruce Schneier:
Actually, I think it's an East Coast crypto thing.

John Donvan:
Okay.

[laughter]

John Donvan:
Ladies and gentlemen, Bruce Schneier.

[applause]

Bruce Schneier:
So, we're here today to debate the motion that the threat of cyber war is grossly exaggerated. And I also, in preparing, read a book full of articles and have some choice quotes. Mike McConnell said in an op-ed in the Washington Post in February of this year that the United States is fighting a cyber war today and we're losing. So, cyber war is going on right now in our country. Amit Yoran, who did cyber policy, cyber security under Bush, I believe, said that cyber 9/11 has happened over the past 10 years, but it's happened so slowly that we don't see it. So, 9/11, you know, thousands of people dead, billions of dollars of damage, has happened, and we just didn't notice it like the cyber war we're currently losing. In 2007, Germany -- and it's a great -- this is a great newspaper headline -- "Germany attacks China for starting the cyber war."

This is actually great because when Germany attacks China, they are attacking them by yelling at them because China started a cyber war. Another headline, same incident: "China declares war on western search sites." You can actually declare cyber war on search engines. I don't know if you knew that. An article from an Australian magazine, The Independent, February of this year: "Hackers declare cyber war on Australia." So, cyber war is so easy, even kids can do it.

[laughter]

Bruce Schneier:
This year, London Times, March of this year: "Cyber war declared as China hunts for the West's intelligence secrets." And last year -- actually, Fourth of July last year there was a cyber war in the United States, headlines all over the place. I have one from the Wall Street Journal: "Cyber blitz hits U.S. and Korea." In this instance, there were some denial-of-service attacks against Web sites in South Korea and the United States, which happen, we think, from North Korea. There were a bunch of congressmen actually proposing that we attack Korea in response, except we think the attacks might have come from the U.K., which would have been awkward, or, actually, from Florida, which would have been really awkward.

[laughter]

Bruce Schneier:
Okay, so this is silly, right? I mean, when we talk about cyber war in the headlines, in the rhetoric, we're not talking about war. This is a rhetorical war, right? It's the war on drugs, it's the war on poverty. It's a really neat way of phrasing it to get people's attention, right, and to make an interesting headline. Now, what's going on really is a blurring of the threats. There are a lot of threats out there. Cyber war is one, cyber crime; we've heard about cyber terrorism, cyber-hooliganism, cyber activism. And it often can be really hard to figure out what's happening. And just think about how we respond to these sorts of threats.

When something happens to us, it can be the response from the FBI or from the military or from the Secret Service or from Homeland Security and it depends on who's attacking us and why. And when we don't know who's attacking us and why, it can be very easy to call it war. But in most cases, it's not, right? There's a lot -- and -- I took quick notes, I probably got them wrong, some of McConnell's statements, some of the quotes about, that we need to address the vulnerabilities, that the threats in cyber security have risen dramatically. Again, we're hearing -- yes these are true, there are threats, there are vulnerabilities; cyber security's a big deal, but they're not war threats. Probably in the debate later, we're going to go into some of the examples of cyber war. I just mentioned Korea attacking the U.S. A big one was in Estonia; it's been called the first cyber war. And basically, someone or some country, some believe it's Russia, announced a denial of service attack against a bunch of Estonia websites, so it's kind of like the army marches into your country and then gets in line at the motor vehicle bureau so you can't get your driver's license renewed. That's sort of what that looks like. The only person they've ever found who they can convict of this was a 22 year old Russian living in Tallinn who was annoyed about a statue falling down. So I mean, we're now where we can't tell foreign invaders from bored kids. The other events we talk about, China was mentioned a little bit. I mean yes, there's a huge intelligence threat. China's doing a lot of targeting against Google, against others. Marc mentioned the enormous number of attacks per day against government networks. That number actually is pretty reasonable for all of your computers as well.

We're talking about different worms and viruses; lots of threats, again not cyber war. So, I urge you to really think critically about what we're talking about. Metaphors matter. If we frame this discussion as a war discussion, then what you do when there's a threat of war is you call in the military and you get military solutions. You get lockdown; you get an enemy that needs to be subdued. If you think about these threats in terms of crime, you get police solutions. And as we have this debate, not just on stage, but in the country, the way we frame it, the way we talk about it; the way the headlines read, determine what sort of solutions we want, make us feel better. And so the threat of cyber war is being grossly exaggerated and I think it's being done for a reason. This is a power grab by government. What Mike McConnell didn't mention is that grossly exaggerating a threat of cyber war is incredibly profitable. The last article I saw said there's about $400 million in Booz Allen contracts on cyber war. You don't get those by saying you know, this is kind of dumb. But, it really is. The threats are real; the threats are serious; cyber space is not a safe place, but these are not war threats. For the threat of cyber war to be serious means you believe the threat of war is serious. And if you're not worried about war,

[Applause]

Bruce Schneier:
--you can't be more worried about cyber war; that just doesn't make sense. I guess I'll be back when it's discussion time.

[Applause]

John Donvan:
Thank you, Bruce Schneier. Our motion is, "The cyber war threat has been greatly exaggerated," and now to argue against that motion I want to introduce Jonathan Zittrain who is a professor of Internet Law at Harvard, who a couple of years back, said the great thing about teaching Internet law is that those who study it don't really know what it is yet.

Jonathan Zittrain:
I thought it was that they taught gym.

John Donvan:
I got the quote wrong. Have things changed?

Jonathan Zittrain:
Well.

John Donvan:
Jonathan Zittrain.

Jonathan Zittrain:
Thank you.

[Applause]

Jonathan Zittrain:
Thank you so much. Thank you to the Rosenkranz Foundation, Intelligence Squared, and thank you Bruce for promising not to hack the voting devices that we're using tonight in the program.

[Laughter]

Jonathan Zittrain:
So, here's where we're at so far. Marc says, "Vote for us if you don't want a police state." Bruce says, "Vote for us if you think journalists and their headline writers and sometimes their sources exaggerate," and, "Vote for us if you don't want a military state." So, I stand here proudly before you in the negative, despite the fact that I do not want a police state. I do think that journalists and their headline writers sometimes exaggerate -- is it okay to say that in the Newseum? Is that all right?

[Applause]

Jonathan Zittrain:

Did you see, by the way, if you're particularly a fan of the news, you can live here. There are Newseum residences, which is --

[Laughter]

Jonathan Zittrain:
There's like a bat pole and you can go down and read the headlines. I can't believe I've just used a minute in this opening, but -- and we all agree that the use of the word "cyber" is probably a bridge too far. If you at least agree with that, please send me --

[Applause]

Jonathan Zittrain:
Yes. You can applaud or send me some cyber mail, and I will send you a reply. What we heard from Mike were some scenarios that were kind of the watershed event scenarios, and I don't know about you, but after his rip on the banking system, I might be going to my nearest ATM and purchasing a brand-new hollow mattress.

[Laughter]

Jonathan Zittrain:
I want to give a more gradual view of the vulnerabilities that you'll notice both Bruce and Marc handily acknowledge. "Oh, we're not saying the system works. In fact, we agree it's utterly vulnerable. We just don't like the use of the word 'war,' and we don't like the use of the word ‘war' because it might give people a platform through which to have bad things happen after that, to militarize or to create a police state or something like that." Well, fine. We have to argue against that, but let us be truth-tellers about the state of vulnerability in our networks and our endpoints, and then deal with it from there, neither exaggerating nor understating it.

So, what kind of threat am I talking about? Let me just give you two quick examples. The network itself. The Internet is an utterly bizarre network, and to answer your question, John, the more I study it, the more I am just agog that it functions at all. And there are plenty of Internet engineers who --

[Applause]

Jonathan Zittrain:
-- remain puzzled and say, well, it's just a pilot project. The jury's still out.

[Laughter]

Jonathan Zittrain:
So, for example, to get a piece of data from one end to another, like this pen up to the back of the room, the sane, rational way to do it would be to hire somebody, to have a Newseum employee who would take it up there, and then if it didn't get there, we would

know whom to blame. Call it the FedEx method of getting it there. The way the Internet does it is basically like a big bucket brigade. I pass it to the front row, it goes back, would you mind, would you mind, or for sports fans, kind of like beer at a Red Sox game, right?

[Laughter]

Jonathan Zittrain:
You gain nothing except soiled trousers by doing it, but there is a strong normative presumption that you will pass the beer.

[Laughter]

[Applause]

Jonathan Zittrain:
Now, this also leads to structural vulnerability, because if you drink the beer or if you pass it forward instead of sideways, it doesn't get to where it's going. And it turns out that in 2008, the state of Pakistan, as is its wont, asked its Internet service providers to prevent people in Pakistan from getting the YouTube. There was something there that they didn't like. And one ISP, as kind of a parlor trick, chose to implement that block by announcing within the stands of fans that are ISPs here, that it, in fact, was YouTube. And this is a decentralized system. So, its announcement meant that packets that would otherwise be going to YouTube went to them from their subscribers. And then it resonated like ripples in a pond from one ISP to another like dominoes until with about two minutes, anywhere in the world, if you were trying to get to YouTube, your packets were going to Pakistan and they weren't coming back. Now, that is not only downright weird, it is an example of just a whole genus of vulnerabilities that are extremely difficult to fix.

Now, was that an act of war? Definitely not. Is it a vulnerability such that if you had malice towards a state that relies asymmetrically on this network and decided that you wanted to use this as an instrument of your aggression, could you do so? Absolutely, and I do not believe you will hear them say otherwise. That's why you hear Bruce saying against the straw people of "there's a cyber war already in progress." All right, I don't think there's a cyber war going on right now against us in America, but boy are the vulnerabilities there. So long as there is the vulnerability, all we need is the motivation, and I don't want to rest on the good graces of any state around the world, or for that matter any 12-year-old, that wants to try to take down the net. And, he's not 12, but I did ask Ed Felten, computer scientist at Princeton, once, I said, "You know, if you're in a 24-like scenario and your life depended on it, and you had to bring down huge swathes of the net and you only had a week to do it, kind of planting the seeds in the head I said could you do it. And he thought about it really careful, and he said, could I have two weeks? And that’s the kind of thing that did not make me feel better. Now, Robert Rosencranz, one of our hosts, mentioned GhostNet, our collaborators in the Open Net initiative at Toronto and up at Harvard, worked to expose this network that they named GhostNet

where basically this wasn't run of the mill Trojans that all of us have right now on our machines while we think we're playing solitaire and in fact our machines are spamming each other. This isn't a run of the mill Trojan; these are the ones targeted to particular people and institutions that a government might have interest in, compromising the machines and leaving them open on average for over 200 days, where they've got the keys to the kingdom. They can surveil everything; they can control the machine. How do we know? Because our researchers hacked that system and then could see what they saw. We saw the ministries of foreign affairs of Iran, Bangladesh, Latvia, Indonesia, the Philippines, and Brunei, open to us, if all we wanted to do was grab the files.

The embassies of Germany, Romania, Cyprus, the Associated Press, not the embassy, the Associated Press itself, and NATO headquarters, exposed through our view of this system. That's something that says to me, to the extent that surveillance and spy craft is an instrument of war, war is what you have. So I am concerned as, is I think everybody here about protecting civil liberties, about not having the responses to this problem be too quick, too panicked, too corporate, or too military. There are solutions that I hope we can talk about in the panel, to avoid too far in any of those directions. But let us be clear about the problem. Thank you.

John Donvan:
Thank you, Jonathan Zittrain.

[Applause]

John Donvan:
And that concludes round one of this Intelligence Squared U.S. debate where the motion being argued is the cyber war threat has been grossly exaggerated. And we now have the results of our preliminary vote where you, our live audience are judges in this debate, registered your stance on this motion before the debate began. Here are the numbers. Our motion is the cyber war threat has been grossly exaggerated. Before the debate, 24 percent of you agreed with you motion, 54 percent disagreed, and 22 percent were undecided. That's where things started; we will ask you to vote once again at the conclusion of the debate and the team that has changed the most minds will be declared our winner. Now, on to round two where the debaters address each other directly and answer questions from the audience and from me. We have here in Washington D.C. at the Newseum, two teams of two. We have Marc Rotenberg, the security activist, and Bruce Schneir, the security specialist and internet philosopher who are arguing that the other side's argument really is a red herring intended to lead to a power grab by the military.

The side arguing against is saying that we are terribly vulnerable to a list of vulnerabilities and that the stakes are enormously high if the damage were done, the damage would be something that we almost could not recover from. I'm John Donvan moderating and I have an initial question and my question is to the side that is arguing for the motion. You have heard what the other side has said and you have described what you have heard as not being a situation that deserves to be described as war, but what

kind of collection of vulnerabilities or what sort of action would actually be for you, be an unexaggerated threat of cyber war. What would it take for you to abandon this motion?

Bruce Schneier:
I guess for cyber war, you need war.

John Donvan:
Bruce Schnier.

Bruce Schneier:
So tanks would be nice. Maybe some bombs. It's -- one of the rhetoric we hear is a cyber Pearl Harbor, which is an opening salvo to cyber war. I'm thinking of a fleet; that would work.

John Donvan:
Bruce, the motion isn't there is a war. The motion is about a threat.

Bruce Schneier:
Right, what I would need to see for cyber war; I guess I would need nation hostilities that are warlike. I mean, I would have to be fearful of war. I would have to be fearful that Canada would roll over into the United States. Now if I was worried Canada would do that, I would worry about Canada's cyber command and cyber capabilities, and I would worry about the cyber threats from Canada. As long as I feel safe against war, I just don't think the subset of war is going to bother me. So you're talking about damage we can hardly recover from. A lot of that happens by accident. We saw -- it was a couple years ago, three undersea cables were cut going into Egypt. Now, this was kind of a weird coincidence maybe, or maybe it was some kind of intelligence action.

But that's a pretty big threat. You can imagine that as a war-type threat. And it was something that was recoverable from. The power blackout in 2003 hit I think D.C., the northeast part of the United States, southeast part of Canada. You know, that was a series of events. One of them seems to have been the Blaster Worm. I mean, the guy who wrote the worm couldn't have predicted on a bet that that would have resulted in that.

John Donvan:
Let me bring --

Bruce Schneier:
But [unintelligible] cyber action. But again, it's a war.

John Donvan:
Let me get a response from Mike McConnell on the other side.

Mike McConnell:

Thank you very much, John. When Bruce spoke at the beginning, he said, "Mike McConnell said the U.S. is fighting a cyber war today, and we are losing." That's not in fact exactly what I said. What I said is if we were in a cyber war, we would lose. And I was making that statement somewhat metaphorically. And let's think about the terms we're using: cyber war, Cold War. Did we have a Cold War? For those of you in the audience about my age, you probably really experienced that. The issue is there was a Cold War. We had a nation state who, if the United Nations banged on the podium and said, "We will bury you," there were risks, and we prepared. When we prepared, we prevailed. We won the Cold War. And if I had to do it over again, maybe I would use the word conflict or battle as opposed to war. So I want to highlight we're talking about the threat. There are vulnerabilities. They cannot be denied. Every member of this panel in this debate would agree that there are huge vulnerabilities. So what my partner and I are attempting to be are truth sayers, as he said, provide the warning to cause our citizens to recognize the vulnerability and cause their government, their businesses and their personal behavior collectively to address these vulnerabilities so that if there's a war we would prevail. One last thing, John. Desert Storm shocked the Chinese, shocked them.

They had an army that was totally unprepared. In Desert Storm, one weapon destroyed target. Any time in history with thousands of weapons, from Desert Storm till today, the Chinese are building an army and a capability to take out the cyber capabilities of the United States, take out the eyes and ears, our strategic advantage. That's what is currently going on in this capture of information, moving terabytes of data.

John Donvan:
Marc Rotenberg, I mean, some of this can turn into a little bit of a semantic tangle.

Marc Rotenberg:
Right.

John Donvan:
But Mike McConnell brought up an interesting semantic move when he said cyber war, Cold War. The Cold War didn't turn into actual combat and invasions, and yet we all know what that meant. Respond to that, please, whether that works or not.

Marc Rotenberg:
Yeah, I don't think it works. And I think the point that Bruce was driving at is, look, when we talk about war, war, we're talking about one nation state going after another nation state with the intent to decimate its economy, you know, overrun its land, you know, threaten its people. That's what war is about. And in Washington, even when we're at war, we're reluctant to say we're at war. So we use this word, you know, very, very carefully. And if I could have just one more moment, I'm actually a little bit surprised by some of Mike McConnell's earlier comments about the role of the NSA in all of this. He seemed surprised that I was talking about the NSA in my opening remarks and the context of this debate. But this debate is entirely about the role of NSA. And the Congress knows this because it was the NSA director who recently went before the Congress to be nominated as the head of US cyber command. This person is now

responsible for coordinating the military response for the United States in the area of cyber security. It didn't have to be the NSA. It could have been the Department of Homeland Security. It could have been the commerce department. It could have been -- well, stay with me on this, will you? It's an option, right?

It's an option. But there is an obvious reason. You know, and all of Mike's family and friends who are here tonight siding with him understand what I'm talking about. This argument for cyber war is an argument for the Department of Defense for the National Security Agency to take the lead on cyber security in the United States. And this is a debate we've had now for 25 years. And what I tried to do in my opening statement was to remind all you folks what our experience with that has been. It's the experience of clipper. It's the experience of classified responses.

John Donvan:
I'm going to -- since you're going back to your opening statement, let me interrupt and go to Jonathan Zittrain to respond to what you just heard.

Jonathan Zittrain:
Well, a little bit, there is a little bit of philosophical thing going on here where it's like is this a chair? You know, like, well, it has three legs and not four. And I never saw somebody sit on it, but you could. And I mean, you know, the boundaries of a chair gets fuzzy. So what makes a war a war? Well, we've heard a couple things. Who are the actors involved? If the person initiating the hurling of a stone at someone is a state actor, could it be a war? Well, if the stone hit somebody from another state, if a South Korean soldier in the demilitarized zone hurls a stone at his North Korean counterpart, squarely trying to hit him, is that an act of war? Is that an act of war, Mike?

Mike McConnell:
I think it might be.

Jonathan Zittrain:
I think it might be too.

[laughter]

Jonathan Zittrain:
Let's just say that we should not try that experiment right now. You know? Worse has happened on that peninsula, and it started from lesser things. And then you look, all right, what's the motive and what's the effect? Now, what I hear is, yes, the canonical, platonic form of war is like the digital representation -- this is for a younger generation. In the “Lord of the Rings” series, when all those monsters are going up against each other, all right, that's a war.

[laughter]

Jonathan Zittrain:

Right? That's a Platonic form. But you can take away a leg or two and still have the fundamental truth be, one, are we exposed?

Absolutely. And what are we exposed to? It may not be a bomb coming down our middle chimney of our house, but it could be something that greatly affects our way of life. If you indulge Mike's hypothetical and say what if tomorrow those two banks could be taken out, and suddenly everybody that had some claim to those $7 trillion has no idea to whom it belongs, nor can they prove it. Seems to me that's a predicate with the right actors in place to be an act of war.

John Donvan:
Jonathan, this seems to boil down to -- and I don't want to get into this rhetorical tangle here.

Jonathan Zittrain:
Yeah.

John Donvan:
But the word "threat" is in there, and it seems to --

Jonathan Zittrain:
Yes.

John Donvan:
-- the word "threat" means something that could happen. And the question is you are saying we should be really, really, really, worried about what could happen. And you're saying not so much. And you're saying they have motives for trying to scare us. But are you ever -- and you know what damage can be done. Bruce, that's what you do for a living is protect -- is protect a company. Are you -- are you able to sleep at night in terms of the stuff that could happen?

Bruce Schneier:
So this is actually interesting. As security guys, we tend to think all about the bad stuff. But, I mean, you go out in the audience, your bank account's actually fine, all right? Your identity hasn't been stolen tonight. We talk a lot about the threats. And in my business, we have conferences on the threats. You write papers on the threats. All we do is threats. But actually most of the world works pretty well pretty much all the time. The internet works. The pens go to the back of the room, the beer gets passed, and life goes on. Yes, there are vulnerabilities, but the networks, right, I mean sure -- yes, there's espionage going on. A lot of companies keep a lot of secrets? So, yeah, it's easy to sleep at night because we are safe. By and large, we are safe. Yes, there are threats. There are common threats. I mean, you could look at the number of -- amount of money stolen from identity theft, right, some cyber crime. And it's a big number. But it's a much bigger number, money that isn't stolen. Yes, there's bad stuff going on, but it's rare.

20:27:33

It's in the noise.

John Donvan:
We are safe. Three very important words. Are we -- Jonathan, respond to are we safe?

Jonathan Zittrain:
No, we are not safe.

[laughter]

[applause]

Jonathan Zittrain:
I wanted to put to Bruce the question I said I put to Ed. Bruce, if you had a crack team, NSA left you a team of good spooks, and you have two weeks --

[laughter]

Jonathan Zittrain:
-- not signing them up just yet. You have two weeks, and you have to wreak maximum havoc among the devices in consumer land. The people you just told should feel safe in their homes and businesses. You have to wreak maximum havoc. I know it's against interests to answer it. But tell me just how far could you go?

Bruce Schneier:
So, we talk about this. And actually, after -- in crypto conferences, security conferences, people get beers at the end of the night. And we have these conversations. And --

[laughter]

Bruce Schneier:
-- I mean, there's a side that --

Jonathan Zittrain:
This is just among us here.

[laughter]

Bruce Schneier:
Right. There's a side that says, well, you know, new introduction of a Microsoft operating system is indistinguishable from a big denial of service attack.

[laughter]

Bruce Schneier:

So, you know, you've got these sorts of things happening --

[applause]

Bruce Schneier:
We have these things happening sort of normally. We had an AT&T satellite go out because of software updates, and a lot of people's pagers didn't work. These sorts of things do happen. You can do damage but we recover. We're actually really good at recovering. And I don't think given two weeks and a crack team, you could take down the internet. You could make people real annoyed. You can make -- actually probably get paid overtime -- but the techies who have to fix their computers and networks are going to have a bunch of sleepless nights, but it's not going to take down the -- it's not going to do irreparable damage to our country, to our society. This is not an existential threat. I mean, nothing like that; this is around the edges.

John Donvan:
Okay. I want to in a moment go to questions from the audience, so I want to start that process. We'll get the microphones out there and once again I want to remind you to hold the microphone a fist's distance away from your mouth, to really ask a question that is a question, and to try to keep it on our topic, and we'll come to you in just a moment. But Mike McConnell, I want to give you a chance to respond to what you just heard.

Mike McConnell:
I want to go back to the word, "war," and just remind the audience, Cold War, there were no Russians marching down Pennsylvania Avenue until we won.

[laughter]

Mike McConnell:
And they were on the friendly side. So this -- careful of the use of the word "war." Marc said that's a nation state attacking another nation state, we did not exchange nuclear weapons with the Soviets. We prevailed in that war. It's the metaphor of war. Now, also, Marc, earlier in our introduction, accused me of tapping his telephone, and he also just made reference to me stacking the audience with family and friends.

[laughter]

Mike McConnell:
Now, I would love to have done that however it is against the law -- it is against the law to tap Marc's telephone --

[laughter]

Marc Rotenberg:
You got it.

Mike McConnell:
-- unless he is guilty of a crime, and that goes completely out of the context of the National Security Agency and becomes a law enforcement issue which is controlled by a judiciary process.

John Donvan:
Mike, let me bring to you a question that actually goes to the issues that concern Marc. There is a bill that's sort of sitting in the Senate, a lot of cyber -- to address cyber threat, and one of the provisions in the bill was to give the president the power to disconnect a company or to disconnect even a government agency from the Internet if he thought it was a threat. And ultimately that provision slipped away because of pressure from groups like Marc. Do you think it was a mistake for that provision to go away? If you --

Mike McConnell:
No, I do not. I do not. But let me just add a little more context, there are now 40, 40 -- four zero -- bills, resolutions, or amendments on the Hill circulating, and let me remind you of what Mark Twain said about that.

No man's life, liberty, or property are safe while the legislature is in session.

[laughter]

[applause]

Mike McConnell:
This is a debate that involves you in this room, the citizens, being informed about this process, the scare tactics of the government tapping your telephone; that cannot happen with the right law.

Marc Rotenberg:
Oh, my God.

[laughter]

Mike McConnell:
It cannot happen without the right -- without the law.

Marc Rotenberg:
Does the phrase “warrantless wiretapping" mean anything this evening?

[applause]

Mark Rotenberg:
I mean, come on, Mike, let's be serious. The past administration violated the U.S. Constitution and you pushed for --

[talking simultaneously]

Mike McConnell:
Is it appropriate to be interrupted --

John Donvan:
Yeah. Actually, I --

Marc Rotenberg:
-- that no one would be held accountable.

John Donvan:
-- all of that may be true but it's actually a different debate.

Marc Rotenberg:
That's an incredible statement.

[laughter]

John Donvan:
That's a different debate. And, Mike, I want to go back to the question --

Marc Rotenberg:
But we should go to that debate. That's what this debate is.

[laughter]

John Donvan:
[unintelligible] we'll be back and we'll book it.

Marc Rotenberg:
Notice that --

John Donvan:
I want you to go to my question, why don't you want to give the president the power to do this? Because the president can put troops on the street, he can close down ports, why not give the president the power to --

[talking simultaneously]

Mike McConnell:
Notice that Marc came for a different debate. Now, let me answer your question.

[laughter]

You don't want to concentrate that kind of power with a bill on the Hill that is not thought out. My argument is this is very, very complex. My opposition here made reference to my comments about Cold War and nuclear weapons. The reason I made that reference is we didn't know what to do with nuclear weapons. We didn't know how to control them. We didn't know what our doctrine would be and so on. So in the late '40s, early '50s, we had the best minds in this country -- it was called the Solarium Project -- two things came out of that work, containment and nuclear deterrence. And what it said was never ever use them. It built the framework which allowed us to prevail in the Cold War. And that's the argument I'm making here. It's not about warrantless surveillance, easy to say, hard to refute.

[talking simultaneously]

John Donvan:
All right, I'd like to go to some questions from the audience now and, sir, with the microphone. Thank you for being there.

And I apologize that I didn't meet you before and know your name, but there's a gentleman in a blue shirt, and if you can rise, sir -- thank you. And I just want to wait 10 seconds so that the cameras can find you and I think that's probably good. Okay. Go ahead, please.

Male Speaker:
Good evening. This question is primarily for Mr. Schneier and Mr. Rotenberg. We've heard a lot of examples tonight about nefarious cyberspace activity as the defining event itself, but I think we've seen examples of nefarious cyberspace activities as part a more conventional conflict, when Russia invaded I believe it was Georgia. Is it grossly exaggerated to believe that nefarious cyberspace activities might be used as part of a more conventional conflict against the U.S. or one of our allies and if that is grossly exaggerated, who should be in charge of ensuring that our networks are not overrun in that event?

John Donvan:
At least take part one of that question, yes. Mr. Schneier.

Bruce Schneier:
I think it would be silly of anyone to think that any future war will not include a cyberspace theater, all right? War encompasses all theaters: land, water and air space, cyberspace. War will fill the available space.

Jonathan Zittrain:
This side agrees.

[laughter]

Bruce Schneier:

So yes, so if there is war, there will be a cyber component. Georgia's interesting. So Georgia was an actual tanks rolling in invasion and there were some website deface -- non-service attacks. We don't actually know who did that. You know a lot of what we're talking about, we talk about cyber wars, are kids playing politics. And you see it. You see Israel and Palestine, you saw U.S. and China, you know, when the U.S. spy plane had to land in China a bunch of years ago. I saw India-Pakistan when the sort of nuclear tests were going on. I mean, you see this all the time that it's cyber-activism, it's kids playing politics and we actually don't know. It's sort of odd to think that as you're rolling in tanks you're going to make it so people can't visit some website.

They're probably not paying attention to that right now. But if you're someone who's rooting for your side, that's what you can do. So, yeah, it's hard to know what these things were but any future war will certainly include a cyber component.

John Donvan:
Jonathan, do you have anything to add to that that moves it from where we are?

Jonathan Zittrain:
Well, we actually saw in the recent Russia-Georgia conflict a number of Georgian blocks on the web. We infer that it might be the Georgian government actually trying to keep some of its own people from getting some of the bad news too early but certainly a component of that war was a cyber strategy. And we've seen it in other instances, whether it's disputed elections or other things actually attacking cyber infrastructure because information is really key and if people are confused and they don't know what's going on and they're relying on the Internet, they tossed their television set or they don't know how to work it, that's a problem.

Bruce Schneier:
Right. I mean, Iran's an example of that, the elections in Iran. A lot of the information came out in cyberspace. Iranian government's trying to block it and, you know, activists around the world trying to counter that. I mean, lots of great stuff. Not exactly war, but they were good things.

Mike McConnell:
John, could I add some--

John Donvan:
Mike McConnell

Mike McConnell:
Let me add just a couple of facts about the Russian conflict. That cyber -- those cyber attacks were deliberate. I agree with the way that Bruce is describing it. There was a lot of piling on. But what happened was deliberate, it was rehearsed ahead of time and it was effective in shutting down the Georgian government and the Georgian government was defeated. The Russians achieved their objective and that's an example of how you

would interface in a current conventional conflict the ability to attack the other side's capability to communicate, to coordinate, to integrate their forces. The Georgians lost.

John Donvan:
We have a question in the front row so if you could stand up, and the microphone is on its way.

Male Speaker:
So, Jonathan Zittrain in his opening remarks mentioned that the Internet is broken, that people are running protocols that are insecure, and that's it's easier for a malicious or incompetent service provider in Pakistan to direct all of the world's YouTube traffic to that provider. And I think Bruce and many others would agree that many consumers and people are running out of data protocols on out of date software. We're not hearing, though, any calls for increasing National Science Foundation funding or any calls for --

Jonathan Donvan:
So what's your question?

Male Speaker:
The question is if the problem is that we're running out of date software or the problem is that we have an insecure internet, why are we not calling for secure software and regulation of technology companies rather than giving power to the DOD and NSA who have never done anything to fix the Internet or fix security problems?

[applause]

Male Speaker:
NSA is in the business of finding flaws, not fixing flaws.

Jonathan Donvan:
All right. The part of your question that I want to bring to Mike because it's entirely unfocused is that the government has never done anything to protect the Internet. Is that true?

Mike McConnell:
Let's start with the fact that DARPA invented the internet. So that's a good start place.

[applause]

Mike McConnell:
There are two organizations that --

Male Speaker:
It wasn't their job to secure it.

Mike McConnell:

True, because it was designed to be open and unassailable. However, it is what it is. There are two organizations that make encryption code for the federal government. One is the National Security Agency to protect secrets, and the other is the national institute of standards and technology for unclassified protection. There is an initiative calls CNCI, comprehensive national cyber security initiative, and it does exactly what you just said it didn't do. It is to direct funding into the national science foundation, produce a cyber corps, now it's a word, cyber corps. What does that mean? It means teaching kids double E and computer science and understanding so they can make this process better. If you're old enough to remember Sputnik -- 1957, most of you probably don't remember that. Immediately after, we had a bill that started sending kids to school for double E and computer science.

I went to college on that bill. Otherwise I would have been not able to go. So this debate is about doing what you just said. It's not about accusing NSA of spying and warrantless surveillance or saying DOD doesn't do its job. It's about a debate that causes us to invest the resources and train our people so that we can securely rely on something we have become dependent on.

John Donvan:
Sir, what do you think of Marc Rotenberg's concerns with the sorts of measures that you seem to be asking for when you said the government isn't doing anything about it is the sort of -- would invite the kinds of government interference that he finds scary and terrifying. I'll bring the mic back to you. I'm sorry.

Male Speaker:
Well, I didn't say terrifying, exactly.

John Donvan:
You didn't. And I -- totally, you didn't. And that's a very good point.

Bruce Schneier:
The threat of him saying terrifying has been totally exaggerated.

John Donvan:
And I -- if you can be brief. But he's concerned that the sorts of remedies that I think that you're asking for could be disastrous for privacy.

Male Speaker:
I think Marc is scared of the NSA which is not subject to any oversight. I don't think he's scared of a transparent process to improve internet security.

Marc Rotenberg:
Okay. So let me clarify. Tonight's debate topic's not whether or not Marc's scared, okay?

[laughter]

Marc Rotenberg:
We're not going to go there. We're having a policy discussion, a very important policy discussion. And I'm still having a little difficulty following what Mike McConnell is saying. He said the NSA is not interested. They're not going to get involved, not a big deal. A couple months ago, in The Washington Post, he's writing we need to develop an early warning system to monitor cyberspace, identify intrusions, locate the source of attacks. And we must be able to do this in milliseconds. And then you say we need to reengineer the internet to make attribution, geo location, intelligence analysis and impact assessment, the result more manageable. This is exactly --

John Donvan:
But I think he -- I think he's fessing up to all of this.

Marc Rotenberg:
Yes, but here's the point about it, okay? And this is why this is a very important question.

If the goal were to promote security, reliability, stability the way we talked in the internet community about responding to security threats, we would have unclassified programs. We'd be doing education and training. We'd be responding to user concerns. But that's not the model that we're moving forward now. In fact the model that Mike just described a moment ago, the CNCI is a classified document prepared by President Bush. He was there at White House meeting in 2008. We're still trying to get public disclosure of that document because right now we have a secret cyber security policy. We can't even talk about it. I mean, we can imagine what's in it, but we don't even know what the document says. Mike knows what the document says, but we don't.

Jonathan Zittrain:
Can I just say -- can I just say --

Mike McConnell:
It's posted on the White House website if you'd like to read it.

Marc Rotenberg:
No, not the original document.

John Donvan:
Jonathan, can you be brief, because I want to move on.

Marc Rotenberg:
No, no, no. Don't say that.

John Donvan:
Jonathan Zittrain of Harvard.

Jonathan Zittrain:

On behalf of the negative team for this debate, I whole-heartedly support much more money to universities and research.

[laughter]

Jonathan Zittrain:
Let there be no doubt --

John Donvan:
Then if the gentleman with the green tie and blue --

Jonathan Zittrain:
-- our proposal for a new Maginot Line in cyberspace is moving ahead.

John Donvan:
Gentleman with the green tie and blue shirt in the very middle.

Bruce Schneier:
You'll never get him a microphone.

John Donvan:
This is will add 10 minutes to the debate. Give him a microphone.

Bruce Schneier:
Do it the internet way.

[laughter]

John Donvan:
Sorry.

Bruce Schnier:
Yay. Nobody drink the beer.

[applause]

Male Speaker:
So I'm pleased to announce that the internet works.

John Donvan:
I really hope your question is excellent. Otherwise the internet's failed.

Male Speaker:
This question is for the team against the motion. Mr. Schneier brought up recovery, and I think this is a key difference between real war and so-called cyber war. Would you care

to comment on the difficulties of the two compared to each other, recovery from a physical war and a cyber war?

Jonathan Zittrain:
I guess that's for one of us.

John Donvan:
Who did you --

Jonathan Zittrain:
I'll take a crack at it first, I suppose. First, note that our brethren in the affirmative set the bar at, does this create an existential threat to the country. That bar is too high, otherwise what happened in Grenada I dare say was not a war, although I think Grenada may have thought otherwise; or Panama, or you name other conflicts that need not have existential dimensions. As I understand it, even the war of 1812, yeah, they burned down the White House, but, you know, they didn't actually threaten the entire integrity of our country. So we want to go short of existential threat. When I think of a war, what I think of is a hostile act designed to harm quite often, and typically physically, but not always, the interests, livelihood and, you know, day to day existence of the target. And that is most certainly possible in cyberspace. And when you see it happening because a 12-year-old can do it, it's like, yes, but it's not the Chinese. It's like, well, that does not make me sleep any better at night.

John Donvan:
All right. I have to do a little thing for the radio and television at this point. It will be very brief. I want to remind you, we are in round two of this Intelligence U.S. squared debate. I'm John Donvan of ABC News. We have four debaters, two teams of two. We're Marc Rotenberg and Bruce Schneier who are arguing for the motion, “the cyber war threat has been grossly exaggerated.” And arguing against that motion, Mike McConnell and Jonathan Zittrain. Oh, I mispronounce -- somebody in my ear -- the person who tells me everything to say.

Jonathan Zittrain:
The NSA.

John Donvan:
-- has told --

[laughter]

John Donvan:
I have to do it a second time. I apologize.

Bruce Schneier:
The voices in your head have a friends and family plan.

John Donvan:
There's always been a voice in my head. I slurred. We are in round two of this intelligence US squared debate. I am John Donvan of ABC News, your moderator.

We have four debaters.

Bruce Schneier:
You said “debaters” right. I counted four.

[laughter]

John Donvan:
We are in round two of this intelligence squared US debate. I am John Donvan of ABC -- I have to do it without everybody laughing.

[laughter]

John Donvan:
We are in round two of this intelligence squared US debate. I'm John Donvan of ABC News. We have four debaters, two teams of two who are debating this motion, "The cyber war threat has been grossly exaggerated." And we are going to questions from the audience. Once again, ma'am, right there. You're the only woman in that zone. So stand up, and a microphone will come to you. I mean the only woman raising her hand. And we're actually seeing lots of men raise their hands, and we'd love to hear from some more women in fact.

Female Speaker:
My question is to both teams. And we talked a lot about how this is in fact a policy debate. And I would like to know what policies, concrete policies, each side would propose come out of tonight's discussion.

Marc Rotenberg:
Excellent question.

[applause]

Marc Rotenberg:
So part of the argument on our side has been the need for openness. We believe that the most robust cyber security strategy is one that's based on openness and transparency. You know something? That's also been the key to the growth of the internet. We don't think there should be classified documents. We don't think there should be secret standards. We don't think there should be secret agreements between companies like Google and the NSA over how to set cyber security standards for the users of services. Just to take that step in this area, we think in the long term would provide great benefit for cyber security.

John Donvan:
Mike McConnell, who actually helped make policy.

Mike McConnell:
The nation typically responds to one of four things. Fortunately, the most important is ballots. And even Marc would agree there's no tampering with those. The second thing is crisis. There is a crisis, we react, sometimes in a dramatic way.

The third thing is money. And the fourth thing is law. What I am arguing, or what I propose is we get the law correct. We don't want to wait for crisis. And when I made reference earlier to the debate in the late '40s and the early '50s, it was achieved in a way that I would agree with Marc, openness. It was an open debate where we put the issues on the table, and we talked about it. And we got to the right place with the right strategy. That's when I'm advocating we recognize the vulnerability at a significant level where they would be attacked in war that could cause strategic damage to this country so that we elevate it and get the right policy embedded in law.

John Donvan:
Your teammate, Jonathan Zittrain.

Jonathan Zittrain:
First, let me express complete support and agreement for the fragrant smoke that Marc just blew about openness and transparency. I'm completely in favor of that, too, so if you feel supportive of that, it doesn't mean you have to vote for that side because it's about the remedy, not about the problem. But you asked a great question about the remedy and let me give you a couple thoughts on that, that I think dovetail with openness and transparency. First, yes to Chris' question from the front row; more money to universities and research arms that brought us the Internet to begin with -- that's where the Darpa money went, would be great, and more concretely -- I don't know if anybody remembers SETI at home? This was one of these screensavers you could run instead of the flying toasters back in the day, and it would be crunching numbers from radio telescopes like that movie "Contact," and at some point your computer might be, like, OMG, "We have found extraterrestrial life."

[laughter]

Jonathan Zittrain:
Many people installed that and you ended up being able to do what otherwise would take a super computer by people volunteering cycles of their computer, offered over the network, aid among people with a common goal wanting to serve humanity. And I would love to see essentially what you might call "NATO at home," which is a form of mutual aid in alerting, so if your computer is having issues there's a way it can alert nearby other computers that can learn to drive around that pothole it just hit.

I'm part of a program called Herdict, as in, verdict of the herd. I know the name is terrible, open to other ideas, but the basic plan is as you're surfing the Net and you find

you cannot get there from here for whatever reason, you're trying to get somewhere and it's not working, you can click a button and just report that, not even to the government, to likeminded people who can then get for the first time exactly the kind of dashboard that Mike called for in his editorial so we know where the blocks are. These are concrete ideas in the spirit of mutual aid, and you don't have to --

[talking simultaneously]

John Donvan:
Jonathan, you're rather going on. Thank you. Bruce Schneier.

Bruce Schneier:
So I actually disagree that openness is not a remedy. Openness is a remedy. I mean, one of the problems we have in Internet security is secrecy, that when you have secret systems, you don't know what the vulnerabilities are, you can't assess them, you can't make intelligent buying decisions and use decisions about what to choose. Openness actually is a remedy. And it is a way to improve security. The best security protocols we have in the Internet have been designed openly either by NIS, by the government, in open process, by industry through the IETF, another open process. Protocols that are developed in secret systems in secret tend not to work well. So basically I view security failures on the Internet as market failures; that the incentives aren't aligned for whoever has the ability to secure to do it. And you can see that in identity theft, you can see that in viruses, that the people who can solve a problem don't have the incentive to do it. And when you have those problems and you have market failures, government has to step in and sort of set those right. So I actually agree with Mike that the problem is government needs to get the policy right. We probably violently disagree on what that would look like, but that's what I want to see. I want to see the market fails that prevent these problems, whether they're the worms, the viruses, and all the servers attacks, the Chinese hacking, from happening. I want to see those fixed.

John Donvan:
Okay, I'll go to another question. I just for no particular reason want to go to a part of the room I haven't been to, there's a gentleman -- actually the gentleman who's sitting on the stairs, since you've been enduring that position, I think you've earned the right. Did you say come up to the balcony?

Male Speaker:
I'm on the balcony.

John Donvan:
Do we have a microphone up there? We don't. I apologize. We don't. Do you want to come down? If one of you wants to come down, choose a representative --

[laughter]

Male Speaker:

We really don't need a microphone.

John Donvan:
No, we do for the broadcast. If you'd come on down, I promise -- but you're going to ask a very good question, right?

[laughter]

John Donvan:
Come on down, seriously, and we'll ask a -- sir, go ahead.

Male Speaker:
So the proposition that we're being asked to vote on as the audience is that the cyber war threat has been grossly exaggerated. I'd like to know what each of you would say in response to the question, how do you measure that threat? How do you evaluate that threat?

John Donvan:
I think we might -- I'd like to see you rephrase that question that brings us much closer to the actual motion, because I think we could chew up a fair amount of time on that. And I actually think we've covered it quite a bit, so I'm going to pass on that question with respect.

Bruce Schneier:
That'll be edited out of the broadcast.

John Donvan:
No, no, not necessarily. Did this gentleman come down yet?

Male Speaker:
Right here.

John Donvan:
Sorry?

Male Speaker:
What I have not gotten from either team, I would like some numbers. I don't know whether or not to be afraid, not afraid -- out of our so-called $14 trillion economy; how many of those dollars are currently lost to cyber crime? I don't want a solution that is more expensive than what we're trying to fix either in loss of liberty or in terms of actual dollars. How many times have our defensive systems been attacked? How many of these attacks are simply because of sloppy configurations by corporations or the government?

Again, are there any numbers or facts?

John Donvan:

Okay, good point, very good point. Mike McConnell.

Mike McConnell:
Forty-two.

[laughter and applause]

Mike McConnell:
I'm not making fun of your question. There are lots of numbers, millions of attacks and so on. Let me put it in a little context. I did focus on the financial community because that's one I understand a little bit better. The financial community in the United States spends 500 billion dollars a year on IT, 500 billion dollars a year on information technology support. Now that's moving all those ones and zeroes that represent your money or other company's money and so on. So when you talk about expensive solutions, at least when I talk to the banking community, they are hungry for a set of solutions that allows them to have higher confidence in their transactions. Now let me make my point. Banking is based on confidence. We can't run the globe without it. So when Marc made reference earlier to my suggestion at re-engineering the Internet, I'm all for the wild, wild web as most -- as much as anyone wants to be on it but I'm arguing for when the transactions impact billions of dollars and millions of peoples -- millions of people, you probably should have a level of communicating that is robust and secure. Example: the military sends its secrets over the same physical infrastructure as those of you in this room that text.

John Donvan:
Mike, you don't need to say that. You made that point before and I think the question really was if, you know, if we were, if these attacks were potatoes, how many pounds of potatoes do we have racked up already? Do we know how much damage has been done?

Mike McConnell:
Well, it's a hard question to answer. There are literally billions of attacks. I can give you some numbers like that. Bruce could give you better numbers than I can, but the point is we were in a Cold War and we never exchanged nuclear weapons. We prevailed.

John Donvan:
Well, to answer his question, we don't know?

Mike McConnell:
The answer is there are many ways to answer the question with countless examples.

Terabytes of data have been taken by foreign nation states out of this country that include intellectual property for businesses, it includes information from the Department of Defense, Department of State, the Congress, the aerospace engineering system, weapons designers, huge amounts of --

John Donvan:

All right. Let me go to your opponent, Bruce Schneier.

Bruce Schneier:
So no debate that the threat of cyber espionage is real and cyber espionage happens every day. The question is about war. You asked about the losses due to cyber crime. Unfortunately I didn't bring my cyber crime data and they've forbidden us to use the Internet up here so I can't get it.

[laughter]

Bruce Schneier:
There are lots of numbers on the net and cyber crime is a very fast growing industry. I would argue if we were up here doing that the threat of cyber crime, we tend to under-exaggerate. We know that the federal government spends about $6 billion to $7 billion a year, unclassified, on cyber security. Classified you'd probably want to double that. That's what most people believe but we don't actually know and they won't tell us because after that they'll have to kill us.

[laughter]

Bruce Schneier:
Lieutenant General Alexander when he was testifying for head of cyber command said the Pentagon networks are targeted by hundreds of thousands of probes per day, whatever that means. You do the numbers, you divide up the number of computers that they have, that's about the same number of probes that you and your corporate network are targeted by. These are mostly automatic worms -- there are ways you can make these numbers really sound big. Amount of data in cyber espionage? Sure, it's a lot. A lot of times we don't know. A lot of this stuff goes unreported --

John Donvan:
Let me go to Jonathan Zittrain because we came back to we don't know a lot about it.

Jonathan Zittrain:
Right where Bruce left off, the reason it's hard to come up with numbers is because even the definition of attack varies. If somebody scans your port, have you been attacked? A computer port not a real life port.

Mike McConnell:
You don't even know who it is necessarily.

Jonathan Zittrain:
Exactly, you don't. But let me give two statistics that I think are pretty well agreed upon that to me frame it nicely.

One is that at this point, there is good confidence that over 99 percent of the e-mail sent in the world today is spam. Only one percent or less -- if you dipped into a trough of e-

mail circulating, would actually be a letter to somebody with a human on the other end. That is pretty crazy. And network engineers generally say yes. But three minutes of Paris Hilton on a video is so much more bandwidth than all that email, who cares? Just throw it out on the other end. But it says something about just how far it's been penetrated. Statistic number two, at times, a particular Trojan or virus, a particular piece of malware crafted by one entity has been responsible by having infected lots of machines that then become spammers for over 50 percent of the spam on a given day. And that shows just the extent to which you could have a state change, where one particular well-crafted Trojan could have such an impact on the environment. And that gets back to the question about the threat. I measure the threat by the delta, the difference between the day-to-day world we experience right now in cyberspace and the potential, the plausible potential, not fake, but the plausible potential for a huge change in the way we experience it.

John Donvan:
I want to -- Dan, do he have time for one more question? Okay, we have time for one more. And, sir, beard, tattoos. The only one.

Male Speaker:
So this question is mainly for the folks on the --

John Donvan:
Against side?

Male Speaker:
Yeah. What I wanted to look at here was, the discussion was organizations that are going to control the internet you know, focused in the beginning.

John Donvan:
Can you -- I need you to keep the mic close and also just to get to the point of the question, please. Thanks.

Male Speaker:
Okay. Between the FBI, NSA and the red team, it's true that not one organization is currently or will be running the internet.

But is this war, or is this focused more like cyber crime? Because if we look at that, looking at Heartland Financial Systems and their penetration, you know, there's similar penetrations like Bradley Manning within the DOD where the DOD had --

John Donvan:
But really, what is your question?

Male Speaker:
Do you really, truly feel that this is cyber war, like a cyber war threat and that this isn't just cyber crime that happens to be --

John Donvan:
Do you mean is it really -- is it really a nation trying to take down our functioning as opposed to getting into our bank accounts.

Male Speaker:
Yes.

John Donvan:
Okay. And are those two things necessarily mutually exclusive. Mike McConnell.

Mike McConnell:
It is not cyber war the way you are describing it. But the proposition is threat of cyber war. So we're talking about the potential threat of cyber war. And what I'm alleging is when there is conflict, even of a kinetic nature between nation states, cyber will be a part of a warfare that would be carried out. What my real worry is are terrorists groups that are not deterred, someone who is engaged in the equivalent of suicide bombing, given that they could access, penetrate and cause damage to the United States through cyber means. So take us back to the proposition. It's not war is happening. It's the threat of cyber war being in our future that we must mitigate.

John Donvan:
Okay, Marc Rotenberg, last word in this section.

Marc Rotenberg:
I just want to restate a point that Bruce made early year, which I think goes directly to your question. If you have a threat of cyber war, you have to believe that there's a threat of war. And you have to believe that one country is prepared to destabilize another country, is prepared to see its economy diminish, its trade impacted and whatever diplomatic consequences can follow from that. That's a really big deal.

And in our modern world, it seems increasingly unlikely that countries, even countries that don't necessarily get along, are willing to take that risk. So I think this key point about the relationship between the likelihood of cyber war and the likelihood of war can't really lose sight of it.

John Donvan:
Thank you, Marc Rotenberg. And that concludes round two of this intelligence squared debate.

[applause]

John Donvan:
And so here's where we are. We are about to hear brief closing statements from each debater. They will be two minutes each. And it's their last chance to try to change your minds before you vote again on the proposition. So reminding you of where you all

stood when you voted on this proposition, "The cyber war threat has been grossly exaggerated" at the beginning of the debate. At the outset, 24 percent of you agreed with the motion. 54 percent disagreed, and 22 percent were undecided. You will be asked to vote once again in just a few minutes, but first; round three, closing statements. And we're going to begin arguing against the motion that the cyber war threat has been grossly exaggerated. Mike McConnell; executive vice president of Booze Allen Hamilton and former director of national intelligence and retired vice admiral in the U.S. Navy.

Mike McConnell:
Bruce made the statement that the problem is secrecy, to which Marc agreed. And that's a very interesting point, but it has nothing to do with this debate. This debate is not about self-serving interests. It's not about large government programs. It's not about privacy and civil liberties. This debate is about recognizing the significant vulnerabilities resulting from our cyber interconnectedness which results in interdependence. The vulnerability is our interdependence. When the framers wrote the Constitution, we were pretty self-sufficient. Most of us were farmers, probably in excess of 80, 85 percent. Today in this country, 1 percent of the population is engaged in farming.

The 1 percent feed the other 99 percent. There is huge vulnerability in the fact that you are dependent on electric power, digital money, a supermarket full of groceries. All of those things are interdependent and interconnected. And that's what we're talking about, those vulnerabilities. So if there is a war, if there is a war, cyber attack would be mounted. Now, based on the positions I've occupied inside and outside of government, I can assure you that nation states are preparing for cyber war. Marc said they may be preparing, but they would be unwilling to use it. You could describe that as deterrence. I support deterrence. That's what this debate is all about. What is it we have to do to be able to deter other nation states from engaging in war or engaging in cyber war? I urge you to support our position on this debate and vote against -- against the proposition.

John Donvan:
Thank you, Mike McConnell.

[applause]

John Donvan:
Our motion is the cyber war threat has been grossly exaggerated. And here to offer his summarizing statements for the motion; Marc Rotenberg, executive director of the Electronic Privacy Information Center and adjunct professor at Georgetown University Law Center.

Marc Rotenberg:
Okay. So we've tried to persuade you this evening that this threat of cyber war, key term, has been grossly exaggerated. And I wanted to say that Mike McConnell and I have debated these issues for many years. And I suspect we will continue to debate them on into the future because we know, on both sides, that there are consequences that flow from how you judge the proposition tonight, whether the military plays a greater role in

cyber security, whether internet users are required to identify themselves, whether government agencies are allowed to conduct routine surveillance of communications within the United States.

All of those consequences are on the table, depending on what you conclude regarding our debate. But there's something about the debate tonight which actually surprises me a little bit. And that's the fact that Jonathan Zittrain is sitting at that table and not our table. And the reason I make this argument is because Jonathan has written very persuasively about the generativity nature of the open internet. And he has educated us about the value of the decentralized distributed model that has made possible companies like E-bay and Google and services like Wikipedia, and on the story goes. Jonathan, I can promise you that none of this would have ever happened if the NSA had won the clipper chip debate back in the 1990s. And I'm going to urge you, along with the rest of you, to come over to our side. I'll get a chair for you here. We've got a couple chairs, don't we? We'd love to have you on our side because if you value an open internet, if you believe that innovation and security, just like innovation and commerce, is based on the open competition of ideas, then you have to support our side. You have to support the pro position in this debate.

John Donvan:
Thank you, Marc Rotenberg.

[applause]

John Donvan:
Well, as it happens, summarizing -- up next to summarize his view against the motion, the cyber war threat has been grossly exaggerated, Jonathan Zittrain, professor at Harvard law school and cofounder of the Berkman Center for Internet and Society.

Jonathan Zittrain:
Marc, let me thank you for your kind and genuine offer of asylum over on your side of the room.

[laughter]

Jonathan Zittrain:
Let me tell you why I think instead, both of you guys should be coming over here where the air is clear, and the thinking is equally clear --

[laughter]

Jonathan Zittrain:
-- and where your fears can still be realized over here.

You don't have to give up what you're afraid of to come over to this side because I was surprised, too, because what surprised me tonight was that if there's going to be scare

mongering on some side you would think it would be on the people saying no, no, the threat isn't exaggerated, here's why you need to be afraid, be very afraid. But the fear machine I felt was generated over here because what they were talking about were the worries about the remedy, if we come in and take something that they think isn't all that broke and try to fix it we're going to end up with surveillance we don't want, with a police state, with a military state, et cetera, et cetera. Now, in some respects I share that fear of overreaction should we get a watershed event, and that's why I think we need to be so gimlet-eyed about plausible possibilities that make things different than they are right now. I know the chicken wakes up every day, the free-range chicken, and says, oh, the farmer has come along to feed me again. Life is good.

[laughter]

Jonathan Zittrain:
But sometimes induction doesn't work just from the fact that the farmer's been friendly every day.

[laughter]

Jonathan Zittrain:
So I worry that we'll get an event of some kind and then Bruce and Marc's nightmares will come true because we will end up in a Cold War mentality, a conventional war mentality, about how to deal with it, and that is the wrong mentality, and that's why I stand by my previous writings, Marc, and that's why when you asked for concrete suggestions they're suggestions that rely on openness, on transparency, on goodwill and cooperation among people metaphorically passing the microphone from one to another like an ad hoc mesh network. Creatively we can do this.

John Donvan:
Jonathan Zittrain, your time is up.

Jonathan Zittrain:
And I thank you all.

[laughter]

[applause]

John Donvan:
Our motion is "The Cyber War Threat Has Been Grossly Exaggerated," and now, making his summary statement summarizing his position for the motion, Bruce Schneier, chief security technology officer of BT and author of "The Cryptogram" newsletter and blog, "Schneier on Security."

Bruce Schneier:

So we spent a lot of time on semantics here. I'm going to again read this from the Washington Post, Mike McConnell said, "The United States is fighting a cyber war today and we are losing." This is a position that exaggerates the threat. It's a valuable one, $300 million in contracts of Booz Allen this year, and --

[applause]

Bruce Schneier:
-- it's one we see again and again. This is not a few things, cyber war, cyber 9/11, cyber Pearl Harbor, cyber Katrina, cyber Armageddon -- every one of these words gets to be the millions or 100,000s of hits on Google. This is not just a few headline writers making a big deal. I mean, yes, the word "war" has flipped. We don't want to use it when we're actually at war, and we use it all the time when we're at rhetorical war. And this might seem like a petty semantic argument, but actually this matters a lot. All right, words matter a lot. Words have power. Words frame debate. Words suggest solutions. And words cause policy to be implemented. We are not just discussing whether the threat of cyber war has been grossly exaggerated, we are discussing how we are going to deal with Internet threats. This debate has ranged all around. We've heard about espionage. We've heard about terrorism. We've heard about crime. We've heard about kids playing politics, and it's all here on a panel on cyber war. So when you think about this I urge you to vote that the threat of cyber war has been grossly exaggerated, it's been grossly exaggerated by government and industry intent on grabbing power and money.

John Donvan:
Thank you, Bruce Schneier, and that concludes our closing statements.

[applause]

John Donvan:
And it's now time to learn which side has argued best in the judgment of our live audience. We are asking you again to go to the keypads at your seat to register your vote on this motion, "The Cyber War Threat Has Been Grossly Exaggerated." If you agree with this motion, if you are with the "for" side, press number one, if you disagree, push number two, and if you remain undecided or became undecided, push number three.

And we'll have -- looks like everybody's done -- we will have the results in just a couple of minutes. I want to -- first of all, what I really want to do is thank this panel that has been just spectacular, informative, as well as entertaining.

[applause]

John Donvan:
Really.

[applause]

John Donvan:
And I think -- Robert Rozenkranz, I think Washington, D.C. was a good idea, this audience has been terrific and we want you to really applaud yourself, you were very lively, terrific questions, so thank you for that.

[applause]

John Donvan:
So I'd like to also thank our venue, the Newseum, and our partners, NPR, WAMU, Bloomberg Television and Newsweek and, of course, a very special thanks go to CEO, Jeff Ganek from tonight's corporate underwriter, Neustar. Thank you, Jeff, very much for doing this.

[applause]

As was already said a number of times, this is the first time we've taken the program outside of New York City and without Neustar's support, it just wouldn't have happened so we hope this is not the last time that happens. We'll be back, Jeff. [laughs]

Male Speaker:
Thanks to our moderator.

[applause]

John Donvan:
Well, thank you so much. We're going to be back in New York City beginning our next season on September 14th and the season will kick off with Michael Hayden arguing for the motion which is "Treat terrorists like enemy combatants not criminals." This fall will also include debates on same-sex marriage, banking reform, atheism and airport profiling. To receive updates and ticket information, make sure to visit the Intelligence Squared U.S. website and sign up for our mailing list and you can also join our Facebook page.

Bruce Schneier:
Can we be on those panels?

John Donvan:
It's all booked. You're on.

[laughter]

John Donvan:
All of our debates can be heard on more than 220 NPR stations across the nation and you can also watch the debates on Bloomberg's television network, check Bloomberg.com for air dates and times and don't forget to read about tonight's debate in next week's edition of Newsweek and to pick up a current issue on your way out.

I want to thank all the people who asked the questions. I also want to thank the gentleman whose question I did not take for being gracious in giving up the microphone, and for you up in the balcony for making your presence known and coming down here. So I think I heard a door opening in the back and there's supposed to be somebody running forward in an excited manner with a piece of paper that I will unfold but Dana, do you have information on how close this is? Here she comes now.

Bruce Schneier:
If you have to stall I think Mike and I can switch sides for 10 minutes.

John Donvan:
Yeah. I think that happened already. So we have the final results in. Our motion is the cyber war threat has been grossly exaggerated. Remember, the team that changes the most minds is our winner. Before the debate, 24 percent were for the motion, 54 percent against, 22 percent undecided. After the debate, 23 percent are for the motion, 71 percent are against and six percent undecided. Against the motion wins. Congratulations to them. Thank you from me, John Donvan and Intelligence Squared U.S.

[applause]