

**39th IFPA-Fletcher Conference on National Security Strategy and Policy:
The Marine Corps: America's Expeditionary Force in Readiness**

April 14 – 15, 2011

Mr. Matthew Devost, President and CEO, FusionX

Panelist, Session 1, "The 21st-Century Security Setting: Identifying the Demand"

MATTHEW DEVOST: I would be remiss if I didn't mention I'm also a graduate of St. Michael's College, as is the speaker this morning. And it was at St. Michael's College, actually, in the early 1990s, that I had these two interesting passions. I was a political scientist focusing on national security issues, and a computer scientist. There were two disciplines that hadn't been intermingled. And as part of that, I was looking at a lot of issues, asymmetrical threats, emergence of terrorism issues, was a key thing I was looking at.

And then I also befriended a group of hackers. And those hackers were part of what I'll call the white hat hacker community today, but they were illicitly breaking into networks back then for the intent of exploring. And they were breaking into the Department of Defense and into AT&T, into NASA. And I had this come-to-Jesus moment where I said, Wait a minute, there's a huge issue here. I keep looking at these emerging national security threats, we have this increasing dependence on technology, and now we have people that are demonstrating that there's vulnerabilities associated with those technologies.

So that was the start of my career looking at all of these issues, not only looking at the national strategic aspect, but looking at it from a tactical, computer science perspective.

I want to acknowledge my own bias up front. A majority of what I do in the cyber field is helping people manage risk, where cyber is viewed as a huge risk to operations. So a lot of my perspective, and I'll acknowledge that up front, is based on looking at cyber as risk. But we'd be remiss if we didn't think of cyber as opportunity as well. So I want to put that point across in the context of this presentation. When you hear me talking about risk, risk to our networks. It's also opportunities that are available for us to exploit and use these technologies as enablers.

I also want to thank the conference organizers. A few days ago I got an email that said, "We can't support your requirement to give your presentation on your Mac in Keynote." So I counted up last night, just out of curiosity. I've given a little over 500 presentations on cyber issues over the past 18 years. And you get caught in this rut and routine of what you're going to talk about. And not being able to use my clutch Keynote presentations caused me to sit down and think, What do I want to tell this audience in the course of 10 to 15 minutes that I think is most important?

And there's probably five other conferences taking place this week that are going to have cyber components, and people are going to talk about what an enabler it is, what a vulnerability it is, the need for public/private partnership. So my perspective's going to be a little different. I'm going to give you ten concepts, ten things that either challenge current perceptions, or actually reinforce perceptions that I want you to think about in the context of cyber. Hopefully that will lead to some lively discussion.

So the analogy for that – I don't know if anybody's seen *The Matrix*, the movie *The Matrix* – we're going to take the red pill for today, which is going to be a little bit of a unique perspective.

So I start the red pill with an old slide. It's the only actual slide that I carried forth from my other presentations. This is a chart I put together with two colleagues back in 1995 that operated on a simple premise. And that was, in the cyber domain we're not just talking about cyber, we're talking about cyber and physical, and that those lines are going to be continuing to blur.

Everything up until that point, where you'd put in that Quadrant A up there, where we thought about, okay, we have physical weapons that can be used against physical targets. And then we had this concept of cyber thrown out there that said, well, hackers can break into computer systems and they can cause consequence against data that we care about or communication lines that we care about.

We wanted to extend it even further and say, we need to think about cyber in the context of people using physical means to go after cyber. If I'm an adversary that wants to impact network operations in a particular geographic region, I'm probably going to have better odds, unless I'm

highly sophisticated, going in and using conventional weapons to blow up some of those interconnection points. Adversaries would think in that same way.

The correlation to that though is also that I can use cyber to cause physical consequence. And that's kind of the Hollywood sexy scenario; we see that in a lot of movies. And there's some real fundamental realities there, that you can have an impact, a pretty significant impact and a growing impact on physical infrastructure, on physical safety, personnel safety through the use of cyber means. And those lines are blurring more and more every day. People might engage in attacks that they think are physical attacks that have huge cyber consequences.

One example I always like to look at is the first World Trade Center attack in the '90s. One of the things that they've looked at in the World Trade Center attacks was using a radiological device at surface level outside the towers. How many people does that kill? Maybe a handful in close proximity to the weapon as it explodes. What would have been the true impact of that?

It would have been much more devastating from an economic perspective, because you would have had, from the radioactive contamination, the inability to inhabit those buildings and engage in the commerce that was required, the stuff that was happening in those buildings. And back then, we didn't have hot sites and resiliency and backup. That actually served as a catalyst for people, especially in the financial services industry, to think about, Wait a minute, what about if my primary site goes down? What if I still have the workers, but I don't have the computers?

And we weren't in a position to deal with that consequence back then. We're in a better position to deal with it now. But the intent of the adversary wouldn't have been to deny us access to our computers. But that would have actually been more devastating than the physical consequences of the attack itself.

Another concept: **The network will be everywhere.** That diagram that I showed you came from a paper that I wrote with two colleagues in 1995. The title of the paper was, "Information, Terrorism: Can You Trust Your Toaster?" It was a great title. People come up to me now, still, 15 years later, and say, "You're the toaster guy, right?" I'll say, "Yeah, I am."

But the point we wanted to get across was that we're moving towards this environment where the network is going to be everywhere. I have multiple networks in my pocket right now, a couple more in my bag. Everything is becoming network-enabled. You hear about smart grids, you hear about mesh networks. That has pretty interesting connotations, right? Because we think about cyberspace, as we define it right now, it's going to be completely different in five years.

Just by way of example, everyone hears about moving from IPv4 to IPv6? Well, let's just conceptualize the difference in the IP address base. So IPv4 there in that center square, let's look at IPv6 in the outer square, to put those in context, extend that outer square to be the size of the solar system. So we're talking about everything is going to be enabled and is going to be on the network at some point. That provides a lot of great opportunity, but also a lot of great risk as well.

Another concept: **The network will always be compromised.** That's something that we're going to have to get comfortable with as we move forward and we talk about these huge networks and everything being interconnected, is that the adversary is going to be in the network at all times. That's just going to be the fundamental reality of how things happen. Sometimes it's going to be the adversary that you're fighting. Sometimes it's going to be an adversary that you're not fighting. That is the ultimate reality, is that the bad guys are going to be in the network.

That means we have to put emphasis on different areas. We have to think about issues like mission resiliency, and how do you accomplish your mission when you don't have a secure network, when you have a compromised network? What components become important in order to be able to still get the benefits of using those networks when you operate in a consistently compromised state?

Kill with a borrowed sword. This is an ancient Chinese stratagem that I've adopted as one of my pet phrases. This is how adversaries look at our networks today. You can use the capability in infrastructure that we've built as a tool against a society. You can look at September 11th as a similar concept. Al Qaeda could never build missiles that could be delivered with the level of

precision and explosive and incendiary impact as it could achieve by hijacking commercial airlines. So they utilized that infrastructure as a weapon.

The Postal Service, as a mechanism for delivering anthrax, a near anonymous, or anonymous capability for disseminating anthrax. And the ability— I forget what stamps cost back then, say 43-cent stamps, to shut down entire government buildings. And we were lucky with some of the anthrax attacks, with the response model, because we could afford to shut down those buildings. What would happen if those envelopes had arrived at buildings that you couldn't afford to shut down? Changes the operating model and the things that you need to think about.

The other piece of this is, how do we use this to our advantage? How do we think about other people's networks as enablers for us? The equivalent right now, I always like to point out, in cyberspace, on the security side, is that the adversary views our cyber networks and the ability to pre-deploy in them, pre-position in them as the equivalent of being able to pre-position explosives in the ball bearing plants; you can dig in, root in. And we're not engaged in conflict with some of these adversaries that are compromising some of these nodes, networks, critical infrastructure, et cetera. It's just on the potential that there could be conflict, and that could be something that's of value.

So if you think about potential conflict, and you think about strategic consequence or strategic advantage, how do you put it in the context of being able to kill with a borrowed sword or use some of these networks to our advantage.

This is another: **(We don't know what a needle looks like)** I hear a lot about finding the needle in the haystack on the cyber issues. We capture all these logs, and our networks are getting bigger, and we have all this data, and we say, the adversary's in there; we need to just find the needle, the problem is finding the needle in a haystack. I think the problem is more fundamental in that we don't know what the needle looks like right now. We really don't when it comes to sophisticated cyber operations.

I know there's some programs at DARPA that are looking at this. There are smart people that are looking at it. But it's not a matter of being able to capture more data or write more signatures. It's about being able to define an adversary, define intent, being able to determine what are the attack trees. And until we solve those issues, you're going to be able to capture as much data as you want; you're not going to have improvement in how you're able to secure these networks.

We hear a lot about the CIA – the confidentiality, integrity and availability of information – as being a fundamental concept. And those are all important, they've been around for a long time. But I want to throw three others out there that I think are equally important – **identity, authentication and authority**, those kind of key enablers for future network operations.

We need to know who's on the network. We need to know the health of the entity on the network. And we need to know what they're authorized to do. If you think about this in the context of the adversary constantly compromising the network, if you think about this in the context of the needle in the haystack, maybe we don't need to be able to define the needle if we can define the hay. If you think about it in that context. And these are going to be the three principal issues associated with being able to do that, being able to operate in these new network environments.

Another concept: **Cyberspace has borders**. You hear all sorts of experts talk about cyberspace is borderless, there's no national boundaries. There are boundaries; they're called routers. So we need to think in that context and appreciate that, because that also serves to facilitate our current view of what our security posture is.

Our security posture is based on something that has definable borders. And that's another thing that is going to change. As we move towards these mesh networks, as we move towards everything being network-enabled, we're going to lose some of that concept of borders. So if we think right now that we're operating in a cyberspace that is borderless, we're going to be completely unprepared for when the borders actually do go away.

On places like battlefields, they're going to be some of the first places that those borders do go away, where you have these mesh networks, things coming together in real time to formulate new networks.

It's also important in the context of understanding how networks communicate. I was in Central America last week – it's an interesting story – working with a group of businesses. There were five companies; they were all owned by one parent company. And they wanted to take advantage of putting a new data center in place, and they wanted to do that securely. They had a lot of regional risk issues for a lot of the issues that some of the panelists talked about earlier, the concerns about their operations in Central America.

And there was this one guy who had been with one of the companies for 35 years, and he was the dissenter amongst the other four leaders of the other companies in placing that data center in Miami. He wanted to put it in Guatemala. Now, I don't know enough about Tier 4 data centers in Guatemala to be able to comment as to whether that's even available, but his issue for wanting to put it in Guatemala was that they have operations in Panama that have a huge latency requirement; they need very low latency in order for that business to survive. So the need for the person at the terminal to be able to communicate very rapidly with the server at the other end.

And I finally had to pull him aside and said, "You don't understand. To get from Panama to Guatemala, you go through Miami." He couldn't think in terms of the geographical context of, in Central America, the pathway, the most efficient pathway for communication was going to actually be through a node in the United States.

So we need to think about that and remember that kind of context as well.

There's no Moscow Rules for cyberspace. That's a phrase I stole from my friend, Bob Gourley, who's a former CTO over at DIA. There are no norms with regards to cyber operations, especially as it relates to espionage, as it relates to this kill with a borrowed sword and pre-positioning. And we need to think about the impact, the consequence of that.

We are a society that likes to think about operating within norms and rules and procedures. And we have adversaries that are acknowledging this completely new domain of cyberspace and acknowledging that there are no social norms that are governing it. I think that's part of the issue with some of the current rub-up with the Chinese, and the Chinese breaking into the networks in the United States, whether it's government sponsored or not. They're kind of just, Who cares? Of course, we're breaking into networks. Of course we're looking at these particular issues. It's to be expected. This is kind of the new domain. This is a new place, and we're going to be fully exploring it to the extent it's possible.

That's tough for us to get our arms around, and it's maybe an artificial constraint a lot of times in the way that we think about cyber, is that we want it to be rule-based when everybody else is thinking, Perhaps there are no rules.

I don't know if you followed the Adobe Flash vulnerabilities that have come out over the past couple of days. It was interesting, I actually was ground zero for the first Flash vulnerability.

But what was interesting is when you go and do the analysis and figure out, those zero-days were being announced on Twitter by someone in China. When you go down and do the attribution, the data that was being released and people were being targeted, it was being announced on Twitter as this kind of like, "Hey, this is great, there's a new zero-day. I'm submitting it in right now. You'll see it operationalized soon."

It was very open, not a restricted Twitter. It was on an open Twitter feed. And then a few days later he said, "Get ready, Adobe zero-day number two is getting ready to hit the channel." What happened? Three days later we had the emergence of a brand new Adobe zero-day vulnerability.

So they're operating in the open, something that has pretty significant consequence. That Adobe zero-day is the same one that targeted RSA, that has taken into account the potential integrity of the secure ID tokens, which are used to secure a lot of networks and information. And for somebody to just be blatantly operating and saying, "Hey, yeah, I've released the vulnerability

that's going to be used in those types of attacks" is pretty interesting. It shows the no-Moscow-Rules aspect.

No silver bullets. And this is kind of a no-brainer as well. I've seen a lot of technologies and approaches to cyber that propose to be the silver bullet. It doesn't exist. It's like believing in unicorns. My daughter would love to see a real life unicorn, but she's not going to see a unicorn, unless it's in the movies. We're not going to see a silver bullet, maybe unless it's on TV.

So we need to be thinking about the higher level issues. We still don't even have a national strategy for cyber issues. We're looking for all these technical solutions, but we haven't even defined what our strategy and objectives are within this new domain at the national level. So we need to be thinking, not in the context of technologies that we deploy, but, I would argue, move the debate up a level.

In my bio, they talk about the Cyberconflict Studies Association. That's one of our key focuses, is defining, What are the strategic issues? What are the correlating issues to the debate and the academic thought that went into looking at nuclear issues? Where is that and how does that happen in cyberspace? What are those issues?

This is my final concept: **(OBSERVE ---ACT) What if this was your new ODAA Loop** - That's kind of the preposition that we have when we start thinking about network operations. And it kind of carries over. I wrote just a little essay a couple years ago, called, "We All Live in the Future Now." And I'm not one to posit Devost's rules, but I have two.

The first one deals with artificial intelligence and it says that, as opposed to artificial intelligence being proven when it can interact with a human and the human can't tell the difference, my Devost's rule on AI says that artificial intelligence has proved that it's sufficiently intelligent when it has the ability to interpret vanity license plates. So that's my number one.

My rule number two is something I call Devost's Law of Exponential Change, and that was that massive change becomes twice as easy every 36 months. I think these networks are a key driver

in that. Think of some of the issues that the other panelists looked at and you see the massive turmoil and change happening at a much rapider pace. What's the difference between a protest and a revolution? Is it Twitter? Or Facebook? There's some interesting aspects to how these things play and the consequence that networks have in how it happens.

This might be the new operational norm. It's certainly going to be part of the operational norm for cyberspace-related issues. That also causes you to think about what does the pointy end of the spear look like in cyberspace.

DoJ yesterday was all over the news. It had this huge success in that they got the legal authority to go and take down the Coreflood botnet that had infected million of hosts worldwide. Coreflood has been around for four years now, maybe five years in the wild. That is a long duration and a lot of consequence to suffer over one single botnet.

If there were a Mail Boxes Etc. in Toronto that had 20 tractor-trailer trucks a day pulling up and delivering documents that were internal DoD documents, sensitive, maybe some classified material, would we feel required to take some sort of action to stop that from happening? You see the equivalent happening right now in cyberspace all the time. Yet we don't have a very proactive approach to dealing with some of these issues.

And I think that's one of the key things we're going to have to look at operating in this new domain, is what is that proactive approach? What does the pointy end of the spear look like? Not just in conventional military operations, but in those things that impact the US military on a day-to-day basis just by nature of the participation in the network.

I'll just close talking about the world that we live in right now as it relates to, I'll call it the ability to have a sustainable impact on critical infrastructure in the United States through cyber attack. And I've got two approaches to that.

The first is that those with the intent lack the capability. So would an organization like Al Qaeda love to come and take down power on the East Coast of the United States using cyber-only

means? Absolutely. I think they would view it was a requirement to use that capability if they had it. That doesn't mean that they have the capability. It's a lot more complex and more difficult.

And trust me, I've looked at all these networks. One of the things I did for the greatest part of my career, and still do, is engage in basically white hat assessments of networks. There was a point in time where I touched every single machine on DoD networks worldwide. It was a great gig when you're young and single to travel around the world. But the vulnerability was so dismaying that I went on and started doing it in the private sector. So we worked with large banks and telecommunication providers, et cetera. It is hard to have mass consequence in cyberspace. It takes significant capability, planning, et cetera.

So an adversary like Al Qaeda is not necessarily going to have the capability.

And then those with the capability lack the intent. It is possible. I know I could do it with my team. We could have significant consequence against major critical infrastructure, even domestic military systems in the US. But there's no intent there. Fear of escalation, economic interdependence, there's all these kind of classic deterrents that come into place that keep some of those more drastic, non-espionage-type attacks in check.

But we need to think in cyber in the context of both of those assumptions changing. That's the reality. We need to think about it, and those that have the capability might have the intent. What does that mean? And those that have the intent might develop the capability.

And thinking about that, what does it mean to be forward-deployed in cyberspace? What does it mean for issues of convergence? That's one thing that I've tracked very closely in these issues, is the convergence between nation states, organized crime, cyber crime, terrorist organizations, et cetera. You're starting to see massive levels of convergence. How does that impact these issues as well?

So that's it for my ten ideas. I think now we transition to the Q&A period. [Applause]