National Security Cyberspace Institute

NSCI

CyberPro

February 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: JIM CHRISTY

NSCI's Lindsay Trimble recently interviewed Jim Christy, director of Futures Exploration for the Defense Cyber Crime Center. Christy is a retired computer crime investigator with the Air Force Office of Special Investigations that specialized in cyber crime investigations and digital evidence for more than 23 years and 38 years of federal service. Every year, Christy plans and organizes the "Meet the Fed" panel at Black Hat and Defcon, the world's largest hacker convention with more than 9,500 attendees. He also teaches two graduate courses at George Washington University, Elliott School of International Affairs – "The Cyber Threat to American National Security" and "National Cyber Policy." Christy won the 2003 Distinguished Information Service Award from the Association of Information Technology Professionals for his contributions in the field of information management.

Can you give us an overview of the work done at the DoD's Cyber Crime Center?

The Department of Defense Cyber Crime Center is one of six national cyber centers designated by President Bush about two years ago. It's a Cyber Center of Excellence specializing in digital forensics and cyber crime investigation.

We have five major units within what we call the DC3. We have the world's largest accredited Digital Forensics Lab. It works on criminal and counterintelligence and fraud investigations. Investigations ranging from white collar crime, child pornography, espionage, terrorism, and perform the digital forensics on them to be used in the legal process or operations.

We have the Defense Cyber Investigations Training Academy, where we train criminal and counterintelligence investigators in the Department of Defense on how to perform digital forensics exams and how to run cyber crime investigations. We also train information assurance folks who use the same tools and processes for their jobs.

Then we have the Defense Cyber Crime Institute. They do our research and develop tools used by all of our other organizations. They also do testing and validation of those tools. Before you can use a tool in an accredited lab, it has to be independently tested first.

We also have the Defense Industrial Base Collaborative Information Sharing Environment organization (DCISE). DCISE is basically an organization that is the focal point and clearing house for referrals of intrusions from the defense industrial base. The big defense contractors can voluntarily refer intrusions to us. We'll process them in our laboratory and share sanitized results with the rest of our partners of the DCISE. These contractors voluntarily sign up for this program and we share information with them – at the classified and unclassified levels. A true public, private partnership.

That's what we do. It runs the cyber gamut.

You are now the director of Futures Exploration for DC3. What role does information sharing play in partnerships with federal agencies, state and local law enforcement, private industry and academic institutions? How do you balance information sharing with maintaining effective security?

Unlike some other organizations, we think *defense* comes first. To play good defense, you have to share information. We have multiple vehicles we use to share information. The DCISE organization's whole job is to collect information and share it with the partners and the rest of government to protect their systems. It's key for someone seeing new information to share it, so it can get analyzed and a countermeasure can be applied by the whole community.

We just finished our ninth annual DoD Cyber Crime Conference attended by over 1,100. We opened the conference up to all federal, state and local law enforcement and all contractors working for those organizations. We include federally funded academic institutions specializing in cyber security and digital forensics as well as practitioners all of the federal agencies. We run the conferences at the FOUO (For Official Use Only) level as well as a couple of off-site classified sections to share information. We had 175 speakers this year and many hands-on training courses attended by over 500 students – all of this to share information with all the partners who need this information.

For the past three or four years, we've been running annual DC3 Digital Forensics Challenges. We run these contests that have aspects of digital forensics exams that we see in the cases we process every day – and last year, we had over 1,100 teams from 61 countries that participated. Then we share the results with the community.

Information sharing is absolutely critical to success. A lot of organizations don't want to share information because it might compromise investigations or operations. I think defense has to come first! You've got to be able to defend yourself. Our national and economic security is so dependent on technology today. Our job is defense and, to be good at defense, you've got to be able to share.

Since your time as a computer crime investigator with the Air Force, what changes have you seen in cyber crime?

In the '80s, we'd be running cases on ankle biters and script-kiddies. My guys would ask me "Why are we running a case on a 16-year-old?" I would tell them we were exercising the system. I knew it was only a matter of time before organized crime, nation states and terrorists would adopt the same tools and techniques to use against us. We had to exercise the system so we could collect the evidence, get attribution for an attack and be able to respond quickly enough – almost in a real-time sense.

What we've seen over the past several years is that law enforcement doesn't care about those ankle biters anymore. They focus on those nation states, terrorist organizations leveraging technology and the organized crime going after your personal privacy and your personal resources. The traditional adversaries now apply these tools and techniques for their advantage.

How would you define "cyber crime" vs. "cyber warfare"? Where is the line? How do thresholds between criminal activity and warfare help in determining appropriate response?

You can divide cyber warfare down into computer network defense, computer network attack and computer network exploitation. It's a real fine line and there's some overlap in all of those. What's constant in all of them is that an intrusion is against the law. It's always going to be a crime, whether it's espionage, terrorism, etc. If someone is attacking or exploiting us, those are crimes.

There are tools and mechanisms to collect information that only the law enforcement community has domestically – search warrants, subpoenas, wire taps, etc. The intelligence community doesn't operate inside our borders. To get attribution for an attack, it's key that law enforcement is involved quickly, using those tools to track down and analyze what's happening and who's doing it to us. Then, a decision can be made on what kind of course of action is appropriate – To determine a course of action you need to know who is attacking and why. Whether that's military action, economic sanctions, diplomatic sanctions, increased security or if we'll run a criminal case against an individual for prosecution, etc.

With computer crime investigations and cyber crime, the legal system gives you the tools to legally get the information domestically, but the intelligence community doesn't have those rules outside our borders.

Cyber warfare is a crime because you have to commit crimes to carry it out. Military, Intel and law enforcement have to be joined at the hip to be successful. Like my boss says, "Electrons don't wear jerseys." You don't know whether it's an attack by an ankle biter, or whether it's espionage or fraud, until you track it back to the origin and have attribution for the attack. You don't know what the motive is until you find out *who* is attacking you. The law enforcement community gives you the tools to gain attribution and they have to work closely with the intelligence community and the military, which are also gathering and sharing information for that common operating picture. Sharing information is the key to success.

Many believe cyber crime serves as a proving ground for the tools, skills and tactics for cyber warfare. They argue any distinction between the two is not real useful. What do you think?

I think the hacker community were the leaders and the organized crime groups, terrorists and nation-states were slow to recognize the potential benefit of the hacker tools – that applies to our government as well as our adversaries. But they have now. I would think that almost every country and major crime organization today has some kind of information operation capability. Certainly, in the old days, the hacker community were the leaders. Today, the nation states have well organized, well funded programs to do the development of tools and skills.

Are the technical complexities of cyberspace becoming better understood by prosecutors and high-level officials? When will we get to a point where this information can be effectively communicated to a judge and jury?

I think we're there. I don't know many households that don't have a computer, or a workplace that doesn't have a computer. They are part of day-to-day life today. People may not understand how they work and all of the complexities that go along with a network, but people understand the general concepts. We've been very successful in prosecuting computer-related crimes. I don't think it's a communication issue anymore.

Having the resources to defend our critical infrastructure against cyber attack is a different story. That's a really hard problem, and a really expensive problem. I'm not sure there's a lot of public support for that because people don't understand that yet.

What do you think it will take for the public support for those defenses to grow?

Unfortunately, it will probably take an electronic Pearl Harbor or an electronic 9/11. That's the way we react. We react to emergency situations. There are so many different (and competing) priorities that the administration has to deal with now: the economy, two wars, unemployment, etc. The squeaky wheel gets the grease. It's hard to prepare for things that have never happened.

Is there anything else you'd like to add?

For the law enforcement community, we also have a sharing environment – a secure portal, the National Repository of Digital Forensic Intelligence (NRDFI) – run by Oklahoma State University and DC3. If you're a sworn law enforcer at the federal, state or local level, you get access for free to tools, techniques and a forum for discussion of cases, tools and techniques. Oklahoma State University does a terrific job. We have about 1,300 investigators from about 300 different law enforcement agencies that are currently participating in sharing information.