

Interview

Silver Bullet Talks with Richard Clarke

GARY MCGRAW
Cigital

Richard A. Clarke is an internationally recognized expert on national security, counter terrorism, and cybersecurity. He's an on-air consultant for ABC news and teaches at the Kennedy School of Government. Clarke served for 11 consecutive years in the White House for three different presidents, including a stint as special advisor to the president for cybersecurity. Before his work in the White House, he worked in the Pentagon, the intelligence community, and the State Department. He's the author of a number of books, including *Against All Enemies* and his new book *Cyber War* (which is orange).

Hear the full podcast or watch the videocast of the interview at www.computer.org/security/podcasts/ or www.cigital.com/silverbullet/.

Gary McGraw: Thanks for joining us.

Richard Clarke: Thank you.

McGraw: I really appreciate it. One of the points you hammer home in your new book, *Cyber War*, is that the US is more dependent on cyber infrastructure than potential enemies, say North Korea or Iran. When you factor

in defense, as well as offense, it seems that we're not in such great shape from a cyberwar perspective. What's to be done to change the focus of the emerging cyber command from offense to defense?

Clarke: Well, several things, here—that's a rich question. First of all, we are very dependent on cyber systems, and when you think about one's cyber strength as a nation, I think you need to take into account the level of your dependence on cyber, and your ability to defend that, and your offensive capability. All three are factors.

US cyber command actually says it has a predominately defensive mission.

McGraw: Do they?

Clarke: Yeah, but the only thing they are defending is themselves and the Pentagon—the rest of the military. They're not defending even the civilian agencies of government; that's [the US Department of Homeland Security's] job, and someday they may be able to

do that. Homeland can't do it today.

Cyber command is certainly not defending things in our own private companies, like banks or the power grid or railroads or anything else. So, I think in answer to your question [about] what's to be done, there has to be a big policy decision at the highest levels to say that somebody, whether it's cyber command or DHS, should be given the responsibility to defend the nation as a whole against cyber espionage, cybercrime, and, heaven forbid, someday a cyberwar.

McGraw: Asymmetry and asymmetric warfare are also parts of the situation that you have to consider. It's fairly straightforward for one person to cause a really big impact in a cyberattack, and it's really hard to assign blame. Can we alleviate that problem, or are we really stuck with it? I guess this is related to the guy who tried hard to blow up Times Square (very poorly).

Clarke: I think one person can do a lot of damage, but not a catastrophe. I think, at the moment, we're talk-

The Silver
Bullet
Security
Podcast
with Gary McGraw



This is the landmark 50th episode in a series of interviews with security gurus.

Check out video of Richard Clarke's interview!

www.computer.org/security/podcasts

About Richard Clarke



Richard A. Clarke is an internationally recognized expert on security, including homeland security, national security, cyber security, and counterterrorism. He's currently an on-air consultant for ABC News and teaches at Harvard's Kennedy School of Government.

Clarke served the last three presidents as a senior White House advisor. Over the course of an unprecedented 11 consecutive years of White House service, he held the titles of Special Assistant to the President for Global Affairs, National Coordinator for Security and Counterterrorism, and Special Advisor to the President for Cyber Security.

Prior to his White House years, Clarke served for 19 years in the Pentagon, the Intelligence Community, and the State Department. During the Reagan Administration, he was Deputy Assistant Secretary of State for Intelligence. During the Bush (41st) Administration, he was Assistant Secretary of State for Political-Military Affairs and coordinated diplomatic efforts to support the 1990–1991 Gulf War and the subsequent security arrangements.

He's currently a partner at Good Harbor Consulting.

ing about nation states, and maybe criminal cartels to do things like take down a power grid. I think one individual probably won't have all the skill sets and all the abilities and all the simultaneous activity that has to go on to make that happen.

So, we're talking right now about other nations, and there is an asymmetry. You have North Korea, for example, which virtually has no cyberspace of its own, which has to go outside of its country to attack.

They go to China, and they rent hotel suites and set up in Chinese hotels. They go to South Korea, where they blend in and probably operate out of safe houses.

Here's this nation with no cyberspace and with very little else going for it, and yet it has an ability to launch cyberattacks against the US.

There is a threshold that you have to get over, but it's a pretty low threshold, and then any nation, no matter how small, no matter how poor, if they get above that little threshold, then they can do real damage, even to a big country.

McGraw: I've written a bunch of very geeky books on software security. Some are "good guy"

books, like *Software Security*, and some are "bad guy" books, like *Exploiting Software*. The bad guy books outsell the good guy books about four to one, so it seems that people suffer from what I call the "NASCAR effect" when it comes to computer security—watching the crashes is way sexier than preventing them.

How can we get people to realize the importance of cyberwar and the problem that we're facing without resorting to FUD [fear, uncertainty, and doubt]?

Clarke: I'm trying to do that in the book. I tried not to overstate the thing. And one of the things I say is, look, we're not going to have a cyberwar just because nations got out and got cyber-wise. The analogy I make is that there are nine nations that have nuclear weapons that we know of, and they don't go around using nuclear weapons just because they have them.

In fact, nobody's ever used a nuclear weapon in anger, except the US, and we did that in 1945. So just because nations are acquiring cyber commands does not mean they are going to go to war. It works the other way around. If a nation makes a deci-

sion to go to war, for the reasons that they normally do—economic, political, ideological—then they look for what their weapons are. No one is going to attack us in a big way—cyberwar, just for the heck of it.

McGraw: I'm thinking about how you engage the policy makers and the public in understanding this without exaggerating some of the things that can happen. You and I both know, and the people who listen to this podcast know, impacts are serious and really can happen. But when you say it to the general public, they think you are Chicken Little.

Clarke: Right, so you have to be very careful and, therefore, I talk about cyber espionage as a motivator, because people can't get motivated about cyberwar. It's never happened in any big way, certainly not to us. Perhaps it did to Estonia and Georgia and other countries, but it hasn't happened to us in a big way, and, until it does, people are not going to take it seriously.

So, let's talk about cyber espionage as a thing that happens every day and is costing the US a lot of its competitive advantage in the world because we're spending stock holders' money and taxpayers' money on R&D, and then that R&D is acquired on pennies on the billions by people who hack in and steal it.

McGraw: Like the Google attack, for example.

Clarke: The Google attack is one example, [as is] the attack on the F-35, an airplane that hasn't even flown in service yet, but vast amounts of data about it have been stolen. Three hundred British companies got a letter from the head of the British security service saying, you have to assume your company has been successfully hacked by China. It doesn't just

happen in Britain.

It's happened in the US, and we just haven't sent that letter out yet.

McGraw: Well, do you think the people, when they get the letter, are going to believe it?

Clarke: I do, I do. The first thing a CEO is going to do is call his CIO or CISO and say, "Why didn't you tell me this?" In part, that's because some of these people don't know they've been attacked, and some of these attacks are really quite subtle. Attackers can exfiltrate large amounts of data—in some cases, terabytes of data—without people noticing.

McGraw: The best attacks these days are that way.

Clarke: Yeah.

McGraw: Lots of stealth in this group.

Clarke: Exactly. So the CEO is going to say, look, I gave you a lot of money. You bought anti-virus stuff. You bought intrusion prevention stuff. You bought firewalls. What was up—you mean that stuff doesn't work?

And the answer is, it doesn't.

McGraw: We know that, us geeks. We're with you on that one.

Your book has some really fascinating stories in it. I particularly like the description of how information warfare played a role in Israel's attack on the Syrian nuclear facility. It was fun to read. But the book also describes some scenarios that are kind of basic—like the thing that you invoked a minute ago, the DDOS [distributed denial-of-service] attack on Estonia. You know, that would not work against Amazon.

Or worse yet, the North Korean script kiddie stuff that happened recently. So, isn't it dangerous to mix the very serious cyberattack possibility and these stories of in-

tense command-and-control radar system rooting versus the script kiddie stuff?

Clarke: I think we have to tell people what actually has actually happened, give them the complete inventory.

What is everything we know that has happened in the way of cyberwar as opposed to espionage and crime? True, pretty basic tools [were] used against Estonia and against the nation of Georgia, but they worked.

McGraw: You know your target, I suppose.

Clarke: Yeah, the banking system in both countries was disrupted badly. Communications in and out of the countries were disrupted badly, mobile telephones, the Internet, all very severely affected. Now, you're right, if that happened here—

McGraw: We've got Akamai and edge routing and all sorts of other stuff here.

Clarke: Oh, and Arbor and all sorts of companies that specialize in DDOS attacks. And we probably could do a better job, but the largest DDOS attack anyone has ever seen by volume was July 4th of 2009, and that was the North Korean attack on some things in South Korea, but mainly on things in Washington, D.C. That worked in taking some of those things offline. Frankly, it didn't make a big deal of difference whether those things were online or not because they are just public webpages. But for all of our skill at DDOS mitigation, sites did go down.

McGraw: Right, so putting out the whole range is the important part. But one of the problems that we're sensitive to in the security industry is the overuse of FUD. People tend to overemphasize, and

they are banging the drums all the time, but the question is whether the public would be able to discriminate between something like Israel taking down the Syrian air defense versus just a DDOS.

Clarke: Well, we try in the book both to tell the readers everything we know that has actually happened and to say what was significant and what wasn't, so obviously the ability to take down an air defense network just before they were bombed is—I think that goes without saying—important. Disruptions that the North Koreans did on July 4th were largely attention grabbing and didn't have any significant disruption.

McGraw: Okay. I think you got the balance right in there, by the way. The doomsday stuff that some reviewers have been harping about, I think it's because they don't really understand what can happen.

On page 86 of the book, you say, "Of the three things that make cyberwar possible, the most important may be the flaws in software and hardware." I couldn't agree more. I think we've made tangible progress in software security over the last decade, especially in the last five years on the commercial side—all without regulation.

What's your view on the importance of software security and whether we're making progress? From your seat, how do things look?

Clarke: I think if you somehow wave a magic wand and solve the software security issue, 90 percent of the problem of cyber penetration would go away. Because what's left after that is human engineering and misconfiguration. Software assurance is key to [solving] this problem and to the elimination of the threat of cybercrime, and cyber espionage, and cyberwar.

That having been said, yeah,

we've made progress, but we've made a progress from a really low beginning.

McGraw: That's right, it's easy to double.

Clarke: There's a lot more that has to be done. You've written about how it can be done. It is possible. It just takes longer, and you have to have higher standards, and people have to insist on those higher standards.

NASA, when it had human beings in space, back when the US was a space-faring nation, used to insist on very high standards of software quality and software assurance. It would never have gone to a commercial off-the-shelf acquisition for a key program. Other people aren't like that.

McGraw: NASA was also spending the government's money, and they spent something like \$25,000 a line, an estimate I got from John Knight from UVa [University of Virginia]. So, yeah we can do it—whether we can spend that much is a question, too. The balance is a tricky part of the whole thing.

Clarke: I think we have to ask ourselves, what is the balance? How much could you lose versus what's the cost of having a secure piece of software? We don't need secure software on everything, but maybe you do need it in the Defense Department for command and control. Maybe we shouldn't have US Cruisers running Windows.

Almost every locomotive running on US rails today is still using Windows XP and downloads and updates twice a day.

I don't like that idea, trains—big trains—running around, I don't like that idea.

McGraw: Well, yeah, but we can also compare Windows 98, which didn't even have kernel, to Windows 7, which actually seems to kind of work from a security per-

spective. And that demonstrates the progress too.

Clarke: There's been progress, there absolutely has. But I think we have to [remind] ourselves, it's not over by any means.

McGraw: Oh, no.

Clarke: What can we do to improve it? One thing we can do is insist on certain functions being performed by high-performance software, and I don't want to regulate how you do it, but I think we might regulate that these are functions that require high-assurance software.

McGraw: You seem to put a fair amount of credence in the idea of scanning and possibly blocking network traffic as part of the solution to defending ourselves. I think that is one part of your “defensive triad” even. And I think you've been unduly influenced by Ed Amoroso, by the way.

In some sense, describing software exploit at the level of packets is kind of like describing the brain at the level of neurons. We can only really solve this problem, in my view, by building systems that aren't broken. Trying to protect the broken stuff from attacks aimed at it over the network seems to me to be futile. I'm not sure I buy into the whole network monitoring thing, plus it brings up personal liberty issues.

Clarke: It only brings up personal liberty issues if (a) the government is doing it, and (b) the companies that are doing it are not regulated with regard to privacy.

So, Google is reading your email or your Gmail.

McGraw: Not mine.

Clarke: I don't have Gmail either, that's why. But Google is the price of getting Gmail for free. Google

actually reads the words of your email and then allegedly stores that information so they can tell advertisers about you. That bothers me.

In any event, if we had AT&T scanning software, that scanned things moving on its backbone, we'd have to have a regulator, and I would want that regulator to be a private company, a third-party auditor that would go in and assure that they were not saving that information for any advertising purposes or anything else; that they really didn't know the content, they were only looking at the 1's and 0's for known malware and known attacks.

McGraw: It's just so easy to manipulate the bits and change the patterns.

Clarke: It is.

McGraw: In my view, there is something that Ed and the guys could do—we could just watch for big patterns over the network.

Clarke: Yep, and they do.

McGraw: Like when everybody gets up and flushes the toilet after M.A.S.H.

Clarke: The question is, what do they do about it? Some backbones don't particularly look for these things. I think AT&T probably does, but the question is what do they do when they see them? Do they have the legal top cover so that they can step in and do something? I think all these tier-one ISPs are afraid that if they step in and stop a certain packet or a certain trend going on, that they could be sued because your email didn't get through.

We need to give them more. I think they have legal top cover now, by the way. I think their lawyers are just overly cautious about this, but I'm not a lawyer. So, if they think they need more legal top cover, let's give it to them.

McGraw: Interesting. I absolutely agree with you that the rush toward a smart grid, electrical infrastructure is rife with security risks, and, that from a cyberwar perspective, attacking the power system makes all kinds of sense. It's target one. So, why is it that the electric regulators, including the FERC [Federal Regulatory Energy Commission], don't really seem to understand cyber risk at all?

Clarke: We have been working on the FERC for over a decade, and it's been Chinese water torture. Slowly, we've been dripping and dripping, and, slowly, they've gotten the general understanding that they have to do something. They issued regulations on it that are not great, but they are a beginning.

McGraw: It's a start.

Clarke: They're a start, and they have one gaping hole in these regulations. The FERC has no ability to know if anybody's following them or not.

They issued Con-Ed [Con Edison in New York] this regulation, and Con-Ed says, okay, I'm certified, I'm doing it. FERC wouldn't know whether they were doing it if the lights went out. I mean, FERC has no cyber ability, no audits, and there is no requirement in the regulations that Con-Ed gets audited by a third party, so FERC is not auditing them, and there is no third-party audit. So how the hell do we know whether these regulations are being violated or not?

McGraw: Exactly. That's a case where maybe regulation makes sense, because we are always talking about public-private partnership and no regulation, and I know the politics behind all that, but there are certain things we've got to protect.

Clarke: The word "regulation" sends most people running out of the room screaming.

McGraw: It's like "liberal."

Clarke: It depends on your hot button, but people don't want regulation until you ask them, now the toy that you give your grandson for Christmas, what if it's from China, and it's got a lead paint on it, and he licks that lead paint off? Do you want the Food and Drug Administration or the Federal Trade Commission issuing regulations about lead paint on toys?

You can go through a whole long list of things where you ask people, do you want this to happen? No. Do you want regulation to stop it? Yes. They like regulation, but they think they don't like regulation, and somehow when you say, we need new cyber regulations, they'll go, oh, big government stealing my emails.

Like the government wants your emails. What would it do with your email? I think there are some smart regulations that can be done. Now, what do I mean by smart? Where you give me the end state, don't give me five volumes written by a government lawyer. Give me an end state, what do you want me to do?

McGraw: What. Not how.

Clarke: Exactly. Then you don't have a bunch of government inspectors, like the guys who were supposed to check on the mine in West Virginia and the guys who were supposed to check on the oil well off Louisiana. You have what we have under some other laws, which is a requirement for third-party audit.

Under the Sarbanes-Oxley financial thing, if you are a publicly traded company, you have to have an audit firm come in every year, and it audits you.

McGraw: Can you imagine telling the CEOs of the power companies that they could go to jail? I guess they can already under Sarbanes-Oxley, if their books are a mess.

Clarke: Yeah, if they are publicly traded now, they have to be inspected by auditors. Under Sarbanes-Oxley, one of the things that the auditors have to certify on every publicly traded company every year is that their cybersecurity is adequate.

McGraw: I've been involved in those battles in New York.

Clarke: For some companies, including the banks, getting audited for cybersecurity is a real phenomenon. If the banks have to be audited for cybersecurity, why not the electric power companies?

McGraw: Point taken.

Personal freedom and liberty are clearly important to you. How do you balance cybersecurity and individual liberty, avoiding kind of a cyber-nanny state or Big Brother while also actually addressing cyber risk?

Clarke: I think it's vitally important that we build up trust between the government and the people; we don't have trust right now. We have to build up trust. We had warrantless wiretapping by the NSA [National Security Agency] in the US—let's just say it, we had warrantless wiretapping in the United States by the NSA. I love the guys at NSA, but—

McGraw: They shouldn't have done it.

Clarke: They shouldn't have done that, and that's a blot on their record, and they lost a lot of trust by doing that, so how do we handle this? I think we need a very robust commission, an ongoing commission of trustworthy people. People who, when you see that name, that a particular woman's on that commission, [you can say] well, I trust her, automatically—people with that kind of reputation. That has subpoena power, has a staff of experts,

is independent, and issues public reports, and goes around checking on whether the government is getting into things it shouldn't be getting into in terms of privacy.

McGraw: Kind of a personal liberty or civil liberties commission.

Clarke: Right. Now, there is one.

McGraw: I know, I've met the guys. I did a panel at RSA, and it was a lot of talk.

Clarke: They're pathetic. They've never done anything that I'm aware of, and nobody even knows they exist let alone the people who are on it. So, let's get rid of that one, and let's create one with a lot of power, and let's have a law that creates and gives it subpoena power and gives it independence. Let's have it issue annual reports and special reports when necessary, and let's have it go around and protect our privacy rights and our civil liberties.

McGraw: On the NSA front, I worry a lot about putting the NSA or the rest of the intelligence committee in charge of cybersecurity.

Clarke: Oh, I do too.

McGraw: My main concern has to do with separation of duties and de-conflicting offense and defense. If you imagine spying on your adversaries, spycraft is made way easier if there are problems in software that can be exploited. If you are in charge of spycraft and in charge of making sure the advance systems are secure—

Clarke: It's a conflict of interest.

McGraw: Exactly. So it reminds me about the balance we struck during the Cold War, when we decided to pull the guys who build weapons and put them in the Department of Energy and the guys who use nuclear weapons and put them into

the Department of Defense, and that separation of concerns seemed like a really good idea—so you're with me on that one?

Clarke: Yeah, one of the things that we say in the book is that we'd like to see a cyberdefense administration and, for lack of a better place, we suggest it be in the Homeland Security Department.

There are a lot of good people in Homeland Security, there are. I mean the Secret Service does a great job, Coast Guard, I think, does a great job. They are good people—there are 140,000 of them.

McGraw: It's big. It's a very big thing.

Clarke: They are hard working, they are good people. They just don't have the cyber capability right now, maybe a little. But they don't worry about it. They want to build the cyber capability, and they want to consolidate the things they have and get additional powers and additional resources, and calling it a cyberdefense administration would make sense.

They have got all these entities, Secret Service, Coast Guard, Customs and Border Patrol. Add to one of them at that level a major agency, Cyberdefense Administration, so we don't have to use the NSA to do defense.

McGraw: That's going to be a heck of a political battle. Even if you think about the Obama administration and the trouble they had sorting out the National Security Council versus the Treasury. That never really got resolved properly, so then you end up with somebody with multiple line reports. I was talking to Howard [Schmidt, US Cybersecurity Coordinator] on Thursday, and I'm glad he's doing it, but I still think he's crazy.

Clarke: It's a tough job. There's no doubt about that, because Howard

was not given a clear mandate and clear authority and responsibility.

McGraw: Right. It's more cheerleader and consolidator. But the good thing is that Howard really understands the technical issues behind the thing and has been in the wars seeing how us geeks try to resolve these things.

Clarke: Howard has got all the background necessary to do the job. We'll find out when he tries to propose something serious whether he's got the clout.

McGraw: Right.

For years you worked on nuclear nonproliferation together with the Russians back in the SALT [Strategic Arms Limitation Talks] and the START [Strategic Arms Reduction Treaty] days, I guess. And we're all very grateful for that important work, so thanks for that. In nuclear arms control, it seems that verification is at least possible. This may not be the case when it comes to cyber weaponry, so how can you make progress in an arms control sense so that we can control and limit cyberwar capabilities?

Clarke: Arms control verification, whether you are verifying nuclear weapons or, the hardest one, biological weapons, or chemical weapons, which turned out to be really hard to do, or even conventional weapons, counting tanks—every time we started down one of these roads—and I was present for each of them; I was present for conventional, for nuclear, for bio, and for chemical—every time we started down one of these roads in arms control, we were told, oh, you can't do it.

You can't do it. It's so hard. Verification is going to be so hard. And it was. It absolutely was, and we spent an awful lot of time trying to figure out a lot with creativity and trying to figure out how to verify arms control in those areas, and one

of the things that we discovered is arms control is not a 1 or a 0 function. It's spectrum: you are never going to have 100 percent verification ability on damn near anything, so how much is enough depends on a couple of things. One, what's the risk if you're wrong? If you think that the other guy is playing by the rules and he's not—

McGraw: Then what?

Clarke: What's the risk to you?

You have to take that into account when figuring if these verification systems are acceptable or not. So, can you verify? It depends on the proposal. There are certainly things about arms control of cyber that you could never verify, but there are also probably some things you could. And I think what we are suggesting in the book is, let's take some baby steps, just as we did with nuclear and bio and chemical.

Let's take some baby steps. Let's have some proposals, build up some trust, build up some expertise, begin the international dialogue. You know, in all of these other forms of arms control, it took years of talking to each other just so we understood what we were talking about. We would be saying the words back and forth to each other, but they would have different meanings and different understandings. It took a long time to establish negotiators on both sides of the table.

Or, sometimes, multiple sides to a table, negotiators that were sufficiently expert in the subject matter that we could actually have a negotiation, so what we are saying is, let's begin, and we have some ideas of things that we think are fairly unobjectionable, like having a cyber risk reduction center modeled on the nuclear risk reduction center, which could have an international staff, and you could call it when you were in trouble.

You could say, that bad guy is attacking me, help me. Come ver-

ify that it is him that is attacking, and help me stop the attack and share information. Something like that would be a good first step.

McGraw: Last question—how does being a guest on Silver Bullet compare to being on the Colbert Report?

Clarke: The thing with the Colbert Report, you know after one or two serious questions, you're going to get something right off the left-field wall.

McGraw: You don't know what it is.

Clarke: Right off the green monster, and it's live, and you have to respond in an instant because they can't have dead air while you are thinking about it.

McGraw: Right.

Clarke: The rule on the Colbert Report and, for that matter, on the Daily Show, is that the host is the comedian, not you. So don't think you have to say something funny. It's a tough gig to be a guest.

McGraw: So, [Silver Bullet is] a little easier.

Clarke: This is a little easier

McGraw: Glad to hear it. Great, thanks a lot.

Clarke: Thank you.

See the full text of this interview at www.computer.org/cms/Computer.org/dl/mags/sp/2010/04/extras/msp2010040005s.pdf. To celebrate this 50th episode, visit the videocast of this interview at www.computer.org/podcasts. □



We have an immediate need for a skilled and qualified professional to fill the following position: **Assistant/Associate Professor, MS in Cybersecurity -Intelligence and Computer Forensics Program – Tenure Track (Spring 2011):**

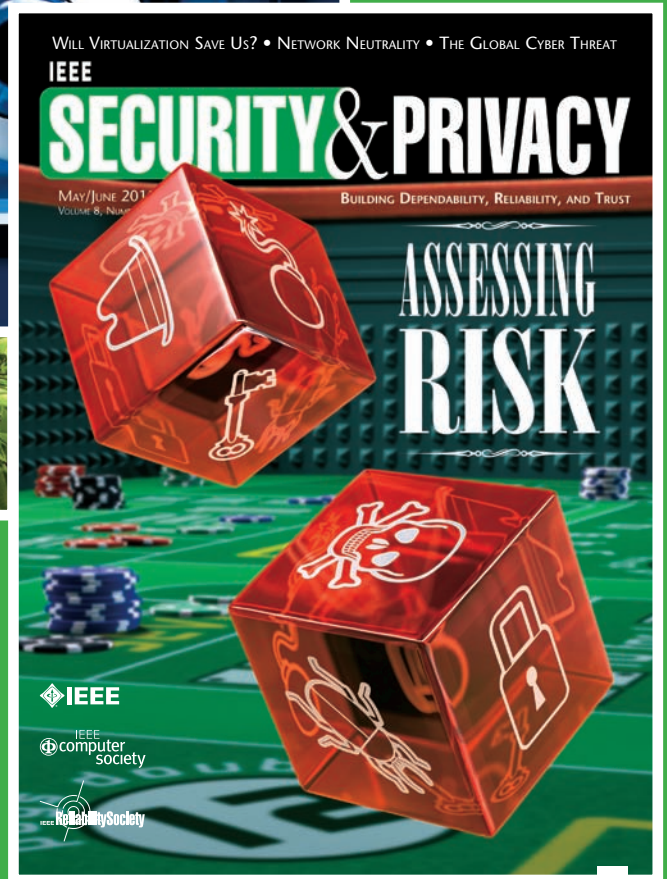
Responsibilities: include primarily graduate online instruction (some traditional undergraduate level instruction when needed), course development, student advising, industry outreach, and graduate student recruitment in collaboration with our admissions team. We are interested in a candidate who can work within a team-oriented faculty and with strong project-based curricula in either the Cybersecurity – Intelligence or Computer Forensics concentrations. Please visit www.onlineutica.com/programs/masters-cybersecurity.asp for the courses offered in each concentration.

Qualifications: The ideal candidate will have significant industry experience and a PhD (preferred) in Cybersecurity -Intelligence or Computer Forensics or related field and an understanding of adult learning principles. The candidates should be able to teach online graduate courses and on-campus undergraduate courses, if needed. Experience with graduate program accreditation process is desirable. Rank will be determined based on qualifications of the successful candidate. Review of applications will begin immediately and will continue until a candidate is selected.

To apply: Please submit a letter of application, curriculum vitae, and list of three references to: Ms. Patricia Swann, Dean, School of Business and Justice Studies, Utica College, 1600 Burrstone Road, Utica, NY 13502.

For more information on position(s), visit: www.utica.edu/finance/hr and click on Employment Opportunities.

EOE



■ Subscribe Now!

IEEE Security & Privacy magazine is the premier magazine for security professionals. Each issue is packed with information about cybercrime, security & policy, privacy and legal issues, and intellectual property protection.

Watch for these special issues! ■

Mobile Device Security ■ Sharing Sensitive Information ■ S&P of Cloud Computing
Reliability of Embedded and Cyberphysical Systems ■ Engineering Secure Systems

www.computer.org/security