Editor: Gary McGraw, gem@cigital.com

Silver Bullet Talks with Thomas Rid

Gary McGraw | Cigital

Hear the full podcast at www.computer.org/silverbullet. Show links, notes, and an online discussion can be found at www.cigital.com/silverbullet.

Thomas Rid, Reader in War Studies at King's College London, discusses how his life as a "wandering academic" influences his work, cyberwar, military dictionaries, and the problem of jargon.

You wrote a book called *Cyber War Will Not Take Place*. I think cyberwar is inevitable because of the highly vulnerable systems that we've surrounded ourselves with and that we depend on every day. What's up with that orthogonal view?

If we look at the substance here, we might not actually have that much disagreement. I agree that systems are highly insecure, especially control systems. Industrial control systems are shockingly insecure. So our disagreement perhaps is a conceptual one. We've never seen a casualty or a fatality—nobody has ever died as a result of a cyberattack. I'm not saying it's impossible in the future, but to date, we haven't seen that. I'm hesitant to use the metaphor of war in a lighthearted fashion. I have colleagues, historians, who work on the First World War. That conflict caused something on the order of 36 million casualties. They wouldn't take me seriously if I was talking cyberwar all day.

But you're raising one of the trickiest questions for cybersecurity today: with the state of system security—especially critical infrastructure security—being as low as it is, why haven't we seen a lethal attack yet, given that a lot of people would like to cause havoc?

How did deterrence work during the Cold War, and could it work in cyberwar?

During the Cold War, deterrence was very simple: you had two main adversaries, the US and the Soviet Union. They both had nuclear weapons, and they threatened nuclear retaliation if the other side deployed a weapon first.

In some ways, that's too simple a characterization. If we look at deterrence in a domestic context when we talk about crime, we have a very different picture. Deterring crime means keeping crime levels on a manageable scale—fewer offenses, fewer attacks; you have a certain statistic that you're trying to keep flat, such as murder rates in a certain jurisdiction. You might do that through law enforcement. Not by just threatening to use force but by actually using it. In other words, using force in the domestic context means maintaining deterrence. In the Cold War context, using force meant deterrence was breaking down. Deterrence in the context of cybersecurity has more in common with crime than with nuclear weapons.

Some people claim that getting rid of graffiti, fixing broken windows, and stopping petty crime has a deterrent effect against bigger crimes such as murder. In the cybersecurity context, has anyone used a really good cyberdefense as deterrence?

The question of defense is very pertinent to deterrence, but in some ways, it's an offshoot. If you don't punish people, there's no deterrence. You have to use force. So what does that mean in the context of cybersecurity? First, we have to

 Copublished by the IEEE Computer and Reliability Societies 1540-7993/13/$31.00 © 2013 IEEE

be able to identify attacks and then punish their perpetrators. If you're able to trace back a certain attack to, say, two schools in China, at some point you need the log files to trace the attack to specific individuals. That's not a technical problem; it's a political problem. You need the support of a specific government to twist the arms of ISPs to provide that data. That was the situation in the Aurora attacks against Google.

About Thomas Rid

Thomas Rid is a Reader in War Studies at King's College London. Rid has worked as a visiting scholar in Jerusalem, at the Wilson Center, at RAND, and at the Institut Français de Relation International in Paris. He received a PhD in political science from Humboldt University of Berlin; his books include *Understanding Counterinsurgency*, *War 2.0*, and *War and Media Operations*. His new book, *Cyber War Will Not Take Place*, is out in the US with Oxford University Press in September 2013. He lives in London with his wife. Contact him at thomasrid.org/contact.

Switzerland is able to remain neutral even during major global conflagrations, and in some sense, that might be due to its defense-related geography.
So you're suggesting we should build the security equivalent of the Alps around computer systems?

No, I'm trying to figure out a way to focus attention on building systems correctly as a deterrent, instead of trying to figure out how to destroy something more efficiently.
In the context of computer attacks, offense and defense are very different from those in military confrontations. Do offensive capabilities translate into better defense? In some military contexts, yes, but that's certainly not the case in the cybersecurity context. Let's put it this way: the situations in which you can actually achieve something productive, get a positive outcome, by doing active defense are quite limited. I'm totally with you when you say let's focus on getting the defense right, especially because the attribution problem in some of the most complex international cases is actually quite hard to crack.

I'm doing a project on the attribution problem right now, and the more work I do on it, the clearer it becomes that it isn't just a technical problem. You get the log files, maybe use some forensic methods, and then you can point the fingers at the culprit and retaliate—it's really not that simple.

But you still have to figure out who was touching the keyboard or who made the program. You can easily have a third party (mis)lead two other entities into a cyberwar.
Absolutely—that's one possible scenario. But the problems we're having in the context of the attribution problem are much more basic. Oftentimes, it's hard to tell if you're dealing with a case of international computer crime or some sort of political espionage attack. At its most basic, is this a crime, or is it espionage? What was the motivation? These are very hard questions of attribution. Forensics doesn't solve the entire problem. Think of a crime scene: with the bullet, you can determine the gun and the angle of the shot, but that tells you very little about the attacker's intention.

Another problem related to this offense-as-defense idea is that it's relatively cheap to develop a cyber-offense. Won't we end up with a pile of cyberrocks in the hands of hacker collectives, religious nuts, or maybe even terrorists?
I think it's a tricky assumption to make that it's relatively cheap to build offensive cyberweapons. I mean, yes—it depends on what you want to attack. But let's put it this way: if you're after the most hardened, well-protected, and complicated target—say, a nuclear power plant—and you want to attack it, you have to do more than crash it. You have to modify a specific control system's output values to prevent fail-safe mechanisms from taking over and essentially neutralizing the attack. Maybe if you have good developers and some creative people working for you, it's quite cheap to do in theory. But in practice, you need target intelligence. You need to know exactly what you're going after. That's hard to get.

Another issue is buried in this discussion about the cost of offense versus defense. If you look at the US government, you see several high-profile offensive operations: Stuxnet, Flame, Gauss, which could be a US-authored intelligence operation against financial institutions in Lebanon. What is it that the US government wants? Securing systems in order to be safe at home or exploiting vulnerabilities abroad?

I think that's a great question and one of the reasons why it's a bad idea to have the US Department of Defense and especially the NSA [National Security Agency] guiding our cyber defense and offense operations simultaneously. They're working at cross-purposes.
I'm not sure what the solution to that problem is. We should, I think, have a better discussion about what kinds of precedents are being set in the arena of offensive cyber-operations. For instance, imagine

you're a senior Chinese diplomat and you have a meeting with your American counterpart who says to you, "China, you're doing all this cyberespionage on American companies, stealing intellectual property," which is probably correct and probably actually a significant problem, right? You can just turn around and say, "How dare you—who claimed credit for Stuxnet in *The New York Times*? Who's pushing the envelope on offensive operations?"

"You guys are blowing up centrifuges in Iran. Which is worse?"

In a way, you're undermining your credibility. It's not just that you're raising a technical issue, but also, politically speaking, it's more counterproductive than probably recognized.

When you gave your talk here in London [www.kcl.ac.uk/sspp/departments/warstudies/newsevents/eventsrecords/mcgraw.aspx], I really liked that it was much more self-confident than what I usually hear from people with a technical background. We need more computer scientists; we need more people with a computer security background to essentially speak up and say, "Listen, if you talk about the attribution problem here, Secretary of Defense, you might want to reconsider some of your facts because I don't think you're really on target."

So what's the best way to influence policymakers when it comes to things like cyberwar? How do geeks like me get engaged in this process?

There are people out there like me—I don't have a technical background, but I'm trying to understand. There are other people who try to do that as well. We have a long attention span when it comes to technical jargon. So, I would encourage computer scientists who have an interest in security to team up with others and to be open to speaking and spending time with, say, political scientists—this is the way we do it at King's College. Bridging that gap across the disciplines into law, into political science and sociology, is really hard. We speak different languages. But I think it's very important to be able to then turn around and talk in a more educated way to those people who make decisions.

What lessons can scholars of international security teach computer security people?

Whenever computer scientists in general—I'm thinking of technicians, not just computer scientists—develop new technologies, tools, or methods, they often use metaphors. Think of the firewall; many of the basic expressions that we use, like packets, are actually metaphors. So if we talk about cyberweapons, for instance, we're in this gray area between "Is it a metaphor that we're talking about or actual, real cyberweapons?" I think there are many other examples in which political scientists, people with my background, can come in and provide some conceptual clarity in a debate that oftentimes lacks conceptual clarity.

What lessons can computer security people teach war scholars?

Everyone—not just computer security people—but all of us tend to be lazy and more comfortable in our own environment. It's good to push people outside their comfort zones and to ask tough questions about the technical understanding that people have, to explain in very simple terms things that you would find utterly boring but that many people in our field won't understand. In the same way, we also have to explain some of the political background to computer scientists, for instance, how lobbying works if you want to affect a political debate.

Do think tanks work?

Think tanks work in multiple ways and in many dimensions. It's not just what they write that might or might not matter, but let's be realistic: if RAND puts out a 300-page report, almost no politician is going to read those 300 pages. They might read the executive summary, and they would certainly have a conversation with people from RAND. I worked for RAND for a while, and we were at the Pentagon on a regular basis to brief people and have interactions in person. Even better is if you start working in the policy environment after a while and then go back to your think tank—you create this link between people, and that's what matters at the end of the day.

So, to get back to your question about how people with a technical background and computer security people can influence what politicians think, the simple answer is to not be shy. Talk to them if you get the chance, and engage. Give talks, go to talks, get outside your comfort zone, and don't just talk to other computer security people in jargon but actually transcend the jargon and talk to policy people.

The Silver Bullet Podcast with Gary McGraw is cosponsored by Cigital and this magazine and is syndicated by SearchSecurity. ■

Gary McGraw is Cigital's chief technology officer. He's the author of *Software Security: Building Security In* (Addison-Wesley 2006) and eight other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*