Editor: Gary McGraw, gem@cigital.com

Silver Bullet Talks with Nate Fick

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.

Nate Fick, CEO of Endgame, discusses cybersecurity, the term *cyberwar* from a Marine's perspective, and his time at the Center for a New American Security.

Many of us in computer security have no idea what real war is like, so we blithely throw around the term cyberwar. Are we watering down reality way too much?

I see a bright red line between the kinetic and nonkinetic worlds, and philosophically, I learned my lessons in the kinetic world. In the kinetic world, if you're going to kick a hornet's nest, you better be sure you'll kill all the hornets. In the cyber domain, for a whole bunch of structural reasons, I don't think that's possible. We need to be very careful in how we talk about offensive cyber capability and cyberwar. Another bright red line for me is between the federal space and the commercial. They're wildly different conversations, and too often we conflate them.

I loved your book, *One Bullet Away*. What made you write it?

The book's dedicated to my good friend and comrade, Brent Morel. Brent was my hand-picked replacement; he was killed on April 7, 2004, leading the platoon in Anbar Province. I decided to write about the experience after Brent was killed because I felt that we had heard from generals, journalists, and politicians, but we hadn't heard much from the guys who were actually fighting the war.

It's good for people to understand the realities of what you all went through for us. It feels somewhat trite, but I want to know the answer: How's leading a start-up similar to and different from leading a combat platoon?

It isn't trite at all. The combat and start-up worlds are both characterized by euphoria and terror in rapid succession. I think I got spoiled in the Marines because people actually did what I said, and in the start-up world, that's not always true. But I think they have a lot of similarities. I had the privilege of working for some great leaders in the Marine Corps, and the best of them was a guy who, if he said, "Go up on the roof, do a swan dive, and figure out how to stick the landing on your way down," I would have saluted and said, "Aye, aye, sir," and gone and done it. I once asked him about his leadership philosophy—why we all followed him through the gates of hell and were happy to do so. He said, "I'll give it to you in three words, Nate: officers eat last." For him, leadership wasn't about privilege, it was about responsibility. What did that mean day to day? He told us what to do, but he didn't tell us how to do it. I learned a lot from him, so even though I don't set up machine gun positions or plan ambush patrols anymore, a lot of the intangible stuff I learned in the Marines I still draw on every single day.

After that, you joined the Center for a New American Security as one of its founding fellows, eventually becoming CEO of that organization. What does CNAS do, and why is it important?

It's a nonpartisan research organization. Many people would be surprised to learn how much

About Nate Fick

Nate Fick is CEO of Endgame, a security intelligence and analytics company. He has more than a decade of experience in the security community, and is an operating partner at Bessemer Venture Partners, where he focuses on defense and intelligence technologies. Before joining Endgame, Fick was CEO of the Center for a New American Security, a national security research organization. He also served as a Marine Corps infantry officer, including combat tours in Afghanistan and Iraq. His book about that experience, *One Bullet Away*, was a *New York Times* bestseller, a *Washington Post* "Best Book of the Year," and one of the *Military Times*' "Best Military Books of the Decade." Fick graduated with high honors in classics from Dartmouth College and holds an MPA from the Harvard Kennedy School and an MBA from the Harvard Business School.

cutting-edge thinking, innovation, and policy formulation is done outside the government, where people aren't living their days driven by the tyranny of the inbox, and you can challenge conventional wisdom openly without worrying about the ramifications.

CNAS was started by Michèle Flournoy and Kurt Campbell in 2007 to bring together a critical mass of national security thinkers who weren't aligned with any one political party or in the pocket of industry. Every project we ever did was signed by individual people; the organization never took an institutional position. It's a young organization filled with young people—not necessarily young in terms of age, but fresh in their thinking and willing to challenge conventional wisdom. In a field where gray beards dominate, where your credibility often moves in lockstep with your age, we wanted to break that mold and build a different kind of think tank.

The national security establishment seems enamored with cyber offense but is seriously confused about what constitutes defense. What should cybersecurity defense look like?

I think it starts with the mantra, build better software. If there were to be a silver bullet, that's as close as we would get to it, right? Beyond that, I think we have a skillset imbalance in the sense that the ability to do harm on the offensive side is becoming increasingly commoditized. The barriers to entry are coming down around the world, and you see it in the marketplace, in companies operating in that space suddenly competing with Romanian teenagers. But ultimately, I think we'd all be better served if we could make defense cool in the same way that offense has this aura about it.

Even if we scrutinize the Snowden documents, it's very clear that the attribution problem on the Internet hasn't been solved. Why does knowing exactly who's attacking you matter?

It matters if you're going to fight back. If you're only defending yourself, it doesn't matter. If we're talking about building better armor on our tanks, it doesn't really matter where the inbound shells are coming from. If we're talking about missile defense, the strategic defense initiative, and everything that flowed from it, you don't necessarily need to know where the shot came from. If you're going to retaliate, if you're going to fight back, then attribution becomes essential.

I'm always skeptical when somebody says, "This time is different," because you know what? This time is never different. On the war fighter side, as soon as you're talking about firing back, you need to abide by a couple of principles that are intrinsic to how we as Americans fight and to how, I would argue responsible, forces have fought all the way back to Thomas Aquinas, the fount from whom these two principles flow. The first of them is noncombatant immunity. If you're going to fight back as a state using sanctioned power, where the state has a monopoly on the legitimate use of force, you have to do everything possible to make sure that you're not impacting noncombatants. The second is that your response must be proportional. If somebody punches me in a crowd in Iraq, I can't reply by firing my M4 at him, right? A sense of proportionality and a sacred tenet of noncombatant immunity—let's acknowledge those and then we can have the conversation on how achievable those things are in the cyber realm and what that looks like.

We ask the NSA to spy, which it's exceptionally great at, but we also ask it to secure our cybersystems, which makes spying more difficult. We're asking these guys, our own people, to work at cross-purposes, which is basically impossible. What's a better solution?

I can agree with you on the problem statement, but I'm not sure I have a better answer. Go back 30 or 40 years, and you could actually target collection outside the US. Remember during the Cold War, when the US had submarines tapping underseas cables? We could actually access data—conversations—that could only be happening outside the US. But with the global distribution of software and the way that our global communications architecture has evolved, the world, technology, and norms have changed faster than law and policy.

Our government has to pick up the pace if it's going to work constructively with technologists and the private sector. Maybe we need a cyber-focused, federally funded research and development corporation, something like what RAND in Santa Monica, California, was for the nuclear era. Imagine something focused on cyber that doesn't require a classified staff—you can have a very diverse group of people, and you don't have to wear a dark suit to work. It could be an excellent way to try to improve the tidal ebb and flow between the two worlds, because right now it's just not good enough.

Why are liberal arts important for business and military leaders?

The basic tenets of leadership don't really change, and I think that one of the most important things you can do as a military officer or as a CEO is to explain and contextualize. Build shared contexts, set a vision, set a direction, build the context so everybody understands it, and then get the troops marching in the same direction. I spend a lot of time feeling as if I'm steering a wooden boat down a river through the rapids, and I try to swing the rudder enough to avoid the big rocks, but every now and then, we hit one, and a couple people fall out of the boat, and you've got to pull them back in and patch the hole, and keep everybody aboard until you hit the next rock, and you do it all over again. War feels a little bit like that. I think growing a business feels a little bit like that. That's a fundamentally human thing, right? It requires connecting with, understanding, and communicating with people in speaking and in writing. These aren't technical skills. Do I wish I could layer an engineering degree in there for myself? Absolutely. I spend a lot of time with our guys trying to better learn the intricacies of what they do, but the reality is it's not how I spend my time, and I don't think it should be. I think we need leaders who are building context and helping their subject matter experts have the direction, the resources, and the support they need to do their jobs well.

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.*