ZULU TIME
INOSC EAST
INOSC WEST
AFNETOPS/CC Vision
AFNOC Mission
Execute AFNETOPS/CC authority to command and control the operation and defense of the AF Network
AFNetOps C2 Relationship
SIPRNET

CyberSecurity

It Isn't Just for Signal Officers Anymore

(PHOTO: U.S. Air Force)

Lt. Col. D. Bruce Roeder, U.S. Army, Retired

"SIGO!" WAS THE CRY that went up at the dining-in when the cantankerous public address microphone on the dais at the officers' club ballroom failed to work. The meat eaters in the unit would laugh or smile in relief as the poor SIGO (signal officer) valiantly struggled to get the malfunctioning feature of the podium to work as it should have. That is how some of us have approached the subject of cybersecurity: it is that wire-head guy's bailiwick, and thank goodness!

Well, if it ever was so, then it is no more. When Director of National Intelligence James R. Clapper issued the 2013 *Worldwide Threat Assessment of the US Intelligence Community* to the Senate Select Committee on Intelligence, cyberthreats appeared ahead of terrorism and weapons of mass destruction in its list of global threats to U.S. national security.[1] Indeed, cyberattacks are constantly in the news. Cybersecurity expert and Finnish reserve officer Mikko H. Hyppönen posits that in developed countries, people are more likely to be victims of crime online than crime "in real life."[2] With the ubiquitous nature of online interactions in modern life, the cyberthreat is a top security threat to individuals and the nation. So, how is that frantic SIGO doing anyway, with his efforts to make the funky thing work properly?

Lt. Col. D. Bruce Roeder, U.S. Army, Retired, is an instructor at the Department of Distance Education at the U.S. Army Command and General Staff College at Fort Leavenworth, Kan. He is a graduate of the United States Military Academy and has an M.A. from Webster University. Lt. Col. Roeder previously served in a variety of provost marshal, security, and operations assignments.

Well, let's take a look at the difficult situation our SIGO faces. First, in simple terms, three typical kinds of cyberattackers pose a threat: criminals, ideologues, and nation states. Usually, professional criminals are motivated by greed. They fall under the jurisdiction of law enforcement although the technology they use tends to be beyond the capabilities of ordinary police agencies. Next are the ideologues and so-called "hacktivists," such as WikiLeaks or Anonymous, who generally are motivated by their political or philosophical worldview, or perhaps by cynicism. They often announce their targets and, sometimes, conduct attacks merely to gain attention or to get a laugh. The law treats them as criminals, too. The third type is nation states, which usually are motivated by security, economic, or other interests. They can plan and execute coordinated cyberattacks against their enemies. Normally, they have access to more resources than criminals and ideologues. It is not always easy to assign cyberattackers to neat categories, however. Further muddying the water is the open question of whether a cyberattack is a use of force.

Moreover, determining which specific cyberthreats are most dangerous to U.S. national security and which are most likely to do damage is difficult. Specific cyberthreats arise in unexpected ways. For example, Stuxnet, the fiendishly destructive malware that targeted centrifuges at the uranium enrichment facility in Natanz, Iran, now poses a threat well beyond its original purpose. This is because code used to build Stuxnet (discovered in 2010 and widely considered a state-sponsored cyberattack) was leaked inadvertently onto the Internet. Some analysts believe its descendants (such as Duqu and Flame) or their progeny could already be residing in the databases of critical infrastructure worldwide.[3] The bad things going on are beyond any SIGO's skill set or resources. How should we respond at this point?

More Bureaucracy?

The typical, and even mandatory, response of government is to give an office or agency the responsibility and resources to fix a problem. This predictable, slow, and top-down approach to problem solving at the national level is ineffective against an uncertain, fast-changing, and bottom-up problem. For example, the Department of Defense established United States Cyber Command (USCYBERCOM), a subunified command subordinate to United States Strategic Command. The service components are duly organized to provide support. The Army has the U.S. Army Cyber Command, the Navy has the U.S. Fleet Cyber Command, the Air Force has the Twenty-Fourth Air Force (Air Forces Cyber), and the Marine Corps has the Marine Forces Cyber Command. However, as capable as these units are, they focus mainly on the cybersecurity threats to U.S. defense information networks. On the other hand, "the government is often unaware of malicious activity targeting our critical infrastructure," said Gen. Keith Alexander, former head of the National Security Agency and USCYBERCOM.[4]

When it comes to the civil sector, U.S. Congressman Mike Rogers of Michigan says that "today, we are in a stealthy cyberwar … and we're losing."[5] However, there is no doubt U.S. business leaders realize the cyberthreat is real and that it would behoove them to work closely with the government to prevent a big attack or be ready to respond to one effectively. To them, if something affects their profits, it is important. Even so, companies currently have little incentive to alert federal officials after being hacked because the feds will then turn around and share that information with their competitors. Moreover, if businesses share certain information with some of their competitors, they risk prosecution from the government under antitrust laws. Therefore, unless corporations have some protection from liability or losing their competitive edge, they are unlikely to work together voluntarily. Legal protections need to be codified by Congress, but Congress has not passed any cybersecurity legislation since 2002. On 12 February 2013, President Obama issued an executive order named "Improving Critical Infrastructure Cybersecurity" as a stopgap measure to shield businesses from antitrust litigation if they voluntarily share data with their competitors.[6] Even when Congress does act, participation will almost certainly remain voluntary on the part of the civilian-owned economic infrastructure.

The care and feeding of the government cybersecurity apparatus (including affiliated contractors) will almost certainly enable us to gain and maintain contact with the cyberthreat, but that apparatus will unlikely be able to seize the initiative from the enemy. It appears that we are coming at the problem like a bull in a china shop. Solving the problem will require something more.

The defining characteristic of the World Wide Web is that it is worldwide; the very strength of the Internet is its international character. That is precisely the feature that allows hacktivists, cybercriminals, and their money to flit quickly and easily from country to country as their websites are painstakingly identified and shut down. It is crucial for an effective cybersecurity effort to have the same ability to cross international jurisdictions. Agencies must be able to coordinate with similar agencies across the globe just as nimbly as the criminals can. The United Nations Interregional Crime and Justice Research Institute (UNICRI) website offers insights about how such an operational approach might be able to work.[7] Although UNICRI is a small and underfunded agency within the United Nations, this organization is, at least, looking in the right direction.

Hire the Hackers?

Journalist Misha Glenny has interviewed several cybercriminals. He has not only found that the institutions tasked with keeping us safe from cybercrime do a poor job of deterring, finding, and investigating cases, but also that they might

Cadet 4th Class Anthony Canino, left, and Cadet 2nd Class Matthew Toussain discuss network defenses during a National Collegiate Cyber Defense "At Large" regional competition at the Air Force Academy, 6 March 2011. (courtesy photo/Jeff Scaparra) be driving back the key to a solution.[8] Glenny's assessment is that we have a surplus of technology being thrown at the problem but a shortage of human intelligence. While we continue to pour billions of dollars into ubertechnological solutions to cybersecurity, he proposes instead that we look at the characteristics and abilities of the hackers at the center of the problem. While the hacker is only one piece of the overall cybersecurity threat, this piece may be the most vulnerable. Many figures in the business of hacking are not Mafiosi craving the high life, but shy, socially awkward math geniuses who, in his view, are prone to being swayed by sponsors more sophisticated than they are. Glenny presents some facts regarding several recent well-known cybercriminals, including Scotsman Gary McKinnon, Ukrainian Dimitry Golubov, Sri Lankan Renukanth Subramaniam, American Max Vision, Nigerian Adewale Taiwo, and Turk Cagatay Evyapan. He describes some common qualities they and many other hackers share. These include advanced math and science abilities along with advanced computer hacking skills developed during their childhood and early teen years, before their moral compasses were formed. He also, interestingly, points out characteristics consistent with Asperger's Syndrome, a mild form of autism, as well as its attendant depression. These disabilities in the real world often seem to accompany amazing skills in the virtual world of computer hacking. By choosing to prosecute and punish rather than attract and hire these savants, the United States is punishing and alienating its best chance of finding and fixing the problems that vex it, or so the argument goes. Glenny makes a compelling case that, sometimes, we should consider hiring them instead—as our adversaries do. China, Russia, and other countries, he asserts, recruit and employ these gifted people before and after their involvement in cybercrimes. These countries mobilize them to work for the state, while we continue to rely on our criminal justice system to investigate and punish them.[9]

Have a Back-up Plan?

Long-time computer engineer Danny Hillis warned early in 2013 that while we spend a great deal of energy and attention focused on protecting the computers on the Internet, we give little thought to the security of the Internet itself as a medium.[10] Hillis considers the Internet an emergent system. He says we do not fully understand it, like the weather and the economy: "it's changing so quickly that even the experts don't know exactly what's going on."[11] He says that because of how the Internet has expanded, we do not even know how an effective denial-of-service attack would affect us, so we need "a plan B."[12]

Staff Sgt. Kenneth Tecala, an aviation operations sergeant, and Chief Warrant Officer 2 Ben Carmichael, command and control system integrator, both with Air Defense Artillery Management, Brigade Aviation Element, Headquarters and Headquarters Company, 2nd Brigade Combat Team, 1st Armored Division, troubleshoot the Rocket, Artillery and Mortar Warning system during Network Integration Evaluation 13.1 at McGregor Range, N.M., 13 November 2012. (U.S. Army, Sgt. Candice Harrison)

The good news is that a backup system consisting of a basic plan for alternate ways essential services can continue communicating and functioning should be relatively easy to design, according to Hillis.[13] Although he does not offer details on how it might work, cybersecurity planners who were around during the Y2K scare (referring to the anticipated damaging effects of the millennium bug) could dust off their old plan. That would provide a decent start. The backup plans would vary according to the sector of infrastructure involved. Having continuity plans independent of computer-based operations, and exercised and updated regularly, can provide a safeguard should the worst happen. The plans can also be vehicles for creative problem solving in an organization. The resiliency mindset at the core of the Army's recent efforts to improve comprehensive soldier fitness can be applied to our national critical infrastructure as well as to our personal mental health. Developing well-balanced, robust, and confident key infrastructure sectors whose resilience and total well-being enable them to thrive in an era of high information exchange and persistent threat is not too hard to do. In fact, it is a worthy goal within our reach.

Late to the Party Indeed

Whether we can avoid a catastrophic cyberattack, or for how long, remains uncertain. Given the nature of the threat, the omnipresence and vulnerability of the Internet and our computers, and the limited resources of the "good guys," our chance of success may seem slim. Yet, those of us in the government and the military have been aware of cybersecurity issues for a long time. We conduct mandatory online annual training to demonstrate our knowledge of computer and information security. In fact, to military people, those sessions sometimes feel like the old SIGO is getting revenge for all those dinings-in from days gone by. Therefore, we can approach cybersecurity expecting that military personnel will be receptive to anticipating and overcoming the challenges of readiness, if not well prepared to respond to a cybersecurity crisis. The 2013 report from the director of national intelligence was an important milestone and clarion call (the 2014 update still lists cyberthreats first). Just as physical security is an inherent responsibility and not solely the job of the provost marshal, so too cybersecurity is not the wire-head's lane; it is all of ours. For anyone who has mistakenly filed cybersecurity into the SIGO's inbox, you should call your office. The podium is ours, and the SIGO is each of us. ***MR***

NOTES

[1] Director of National Intelligence James R. Clapper, statement for the record to the Senate Select Committee on Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* (12 March 2013), <https://www.hsdl.org/?view&did=732599>.

[2] Mikko H. Hypponen, *Three Types of Online Attack* (November 2011), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/mikko_hypponen_three_types_of_online_attack.html>.

[3] Ralph Langner, *Cracking Stuxnet, a 21st-century Cyber Weapon* (February 2011), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon>; Kaspersky Lab website, Resource 207: *Kaspersky Lab Research Proves that Stuxnet and Flame Developers are Connected* (11 June 2012), <http://www.kaspersky.com/about/news/virus/2012/Resource_207_Kaspersky_Lab_Research_Proves_that_Stuxnet_and_Flame_Developers_are_Connected>.

[4] Ann Flaherty, "Feds Roll Out Cyber Plan as Hill Vows Legislation," Associated Press, *The Big Story* (13 February 2013), <http://bigstory.ap.org/article/white-house-revealing-obamas-cybersecurity-plan>.

[5] Mike Rogers, "America is Losing the Cyber War vs. China," originally in *Detroit News*, 8 February 2013, reproduced online by Congressman Mike Rogers, <http://mikerogers.house.gov/news/documentsingle.aspx?DocumentID=319502>.

[6] President, Executive Order no. 13636, "Improving Critical Infrastructure Cybersecurity," *Federal Register* (12 February 2013), <https://www.federalregister.gov/articles/2013/02/19/2013-03915/improving-critical-infrastructure-cybersecurity>.

[7] United Nations Interregional Crime and Justice Research Institute website, About UNICRI, <http://web2012.unicri.it/institute/>.

[8] Misha Glenny, *Darkmarket: How Hackers Became the New Mafia* (New York: Vintage Books, 2012), 271.

[9] Ibid., 269.

[10] Danny Hillis, *The Internet Could Crash. We need a Plan B* (February 2013), video online at Technology, Entertainment, and Design (TED) website, <http://www.ted.com/talks/danny_hillis_the_Internet_could_crash_we_need_a_plan_b.html>.

[11] Ibid.

[12] Ibid.

[13] Ibid.