BLOG @CACM

The *Communications* Web site, <http://cacm.acm.org>, features more than a dozen bloggers in the BLOG@CACM community. In each issue of *Communications*, we'll publish selected posts or excerpts.

Follow us on Twitter at <http://twitter.com/blogCACM>

DOI:10.1145/2800200

<http://cacm.acm.org/blogs/blog-cacm>

Moving Beyond the Cold War

John Arquilla assesses the need for cyber arms control.

John Arquilla
"From Russia, Without Love"
<http://bit.ly/1FuuYIX>
June 3, 2015

Though hardly as sexy-sounding as SMERSH, the Stalin-era Soviet counterintelligence organization—much puffed up by Ian Fleming in his James Bond novels—the designator “APT28” may refer to a Russian, or at least Moscow-linked, outfit with truly mass disruptive capabilities in cyberspace. SMERSH was an acronym for *smyert shpionam* (roughly, “death to spies”), while APT refers to the “advanced, persistent threat” that the Fire-Eye cyber security firm has studied so closely—in particular its activities before and during the Russo-Ukrainian conflict. And what is known thus far about APT28 is most troubling.

In Ukraine, the group—its capabilities are clearly beyond the capacity of any individual—has launched disruptive attacks on critical infrastructure, as well as on Internet connectivity. Government and military communications have also been targeted. The key tool—but hardly the only one—is Uroburos, malware that infects and takes over machines, exfiltrates sensitive data, passes false commands, and causes

shutdowns. Interestingly, the scope, scale, and specific targeting engaged in against Ukraine mirror quite closely the patterns of cyber attack witnessed during the Russo-Georgian War of 2008.

Russia is alleged to be involved in a range of other recent high-profile cyber incidents as well. Last October, the White House admitted its information systems had been hacked—with Moscow-friendly perpetrators being the prime suspects. And in January of this year, the pro-Russian group Cyber Berkut (“special police”) got into German Chancellor Angela Merkel’s and other German government sites, disrupting them and leaving messages criticizing German support for the Kiev government of Ukraine. These hacktivist incidents were in some respects like the cyber attacks on Estonia in 2007—but that earlier case was more far-ranging, mounting costly strikes against banking and other economic targets as well.

And it is in the realm of economic cyber war that the Russians have been concentrating of late, according to Kevin Mandia, founder of the cyber security firm Mandiant. Just before the opening of the G20 summit meeting in Brisbane, Australia last November, Mandia made the point explicitly that the Russian government was “actively condoning cyber

attacks on Western retail and banking businesses.” Expanding on his remarks, Mandia made clear his conclusion was based on the inference that, given strict controls over cyberspace-based activities in and from Russia, it would stretch the limits of credulity to believe Moscow was unaware of these hacks.

Circumstantial evidence abounds as well—but as yet there is nothing that would stand up in a criminal court as proving Russian culpability beyond a reasonable doubt. And so a form of covert cyber warfare, with costly economic implications, continues to unfold. Much as groups of pro-Russian insurgents—including, it seems, many actual Russian soldiers—have been fighting in eastern Ukraine, with Moscow all the while denying involvement. We live now in an age of shadow wars, real and virtual.

It is thought the Russians were engaging in covert cyber action of a very sophisticated sort as far back as the spring of 1998, when an extended series of deep intrusions into U.S. defense information systems began—and continued, the public record suggests, for quite some time. I was involved in some of the investigation into this matter, which was initially labeled “Moonlight Maze,” and so can only refer readers to what has been openly reported. But the key point here is there was a strong sense, even back then when the Russians were still reeling from the effects of the dissolution of the Soviet Union, that their cyber capabilities were quite substantial.

It is ironic that, just a few years prior to the Moonlight Maze episode, the Russians asked for a meeting to be

held between a few of their top cyber people and some from the U.S. The ostensible idea being to establish a process for avoiding hostile “incidents in cyberspace.” The Russian delegation was headed by a four-star admiral who probably had in mind the analogy with preventing “incidents at sea.” I was on the American team, and found the Russians’ ideas quite sensible—including their call to consider the possibility of crafting behavior-based forms of arms control in cyberspace. There is no way to prevent the spread of information technology that can be used for cyber warfare, but there can be agreement not to use these capabilities aggressively, or against civilian targets, etc. The Russian idea was akin to the controls that exist today over chemical and biological weapons—many nations can make them, but virtually all covenant never to use them.

I was very taken by the idea of cyber arms control, and recommended in my report on the meeting that the U.S. pursue these talks further. My recommendation was, to put it mildly, hooted down in the Pentagon, where the view was that the Russians were afraid of us and were just trying to buy time because they were so far behind. Well, that was nearly 20 years ago. If the Russians were behind then—and I sincerely doubt it—they certainly are not now. Indeed, Russia is a cyber power of the first order, like China and a few others. And, like China, its cyber security capabilities are quite robust—much more so than American cyber defenses.

Ever since that fateful first Russo-American meeting of cyber specialists, the Russians have occasionally raised the prospect of cyber arms control at the United Nations. We have routinely rebuffed such suggestions. But perhaps it is time, all these years later, to reconsider the possibility of behavior-based agreements to limit cyberwar. After all, by now we know for sure the Russians are not making such proposals out of fear.

Reader's Comments

After reading your article all I wanted is to go back to Russia and hate U.S., U.N., and others. Because they hate us (your article is proof). Your article does not increase peace in the world, does not critically analyze the situation (others do not cyber-attack?). It simply

states the now-trending “Russia is bad.” Even worse, the title implies if I am from Russia, then I am without love to you. Really sad to read this in the scientific journal.

—Ayrat K.

I am appalled to see such a propaganda piece in a reputable scientific journal like Communications. I am reading Communications to get facts and science, but here I see only speculation, hearsay, and general FUD.

The most troubling feature of the article is that it is apparently was written by a U.S. citizen—a country that is believed to be behind the most sophisticated cyber weapons code in the world, the country that is believed to be the only one that is known [so far] to cause a real-world damage to the other country via a cyber-attack without a formal declaration of war. I highly recommend everyone who is interested in facts about cyber-attacks to learn about Stuxnet: <http://en.wikipedia.org/wiki/Stuxnet>. Time will be much better spent.

I urge the editors of Communications not to keep silent about the cyber-war and cyber-crime, but to do a real and in-depth scientific study. For example, what the experts on the software ethics would say about something like the highly sophisticated code of the “Equation Group” and its nefarious intent? Is the fact that there is, undoubtedly, a huge team of highly skilled software developers who write such code, a failure of the modern education system to include ethics into the education system, or is it an unfortunate side-effect of any scientific and engineering progress? Do the people who write it understand the evil they bring onto the world or do they “just follow the orders”?

As a person who has dedicated his life to use his software engineering knowledge to make this world a better place, I am greatly disturbed by this.

—Roman Elizarov

It is hard to accept the “propaganda” charge, as the article makes the key point that Russia has long wanted to pursue cyber arms control—something the U.S. has blocked. That Moscow now has such superb cyber warfare capabilities—and is apparently using them—is in some respects a consequence of American intransigence in the area of behavior-based cyber arms control.

—John Arquilla

© 2015 ACM 0001-0782/15/09 \$15.00

Call for Nominations for ACM General Election

The ACM Nominating Committee is preparing to nominate candidates for the officers of ACM: **President, Vice-President, Secretary/Treasurer; and five Members at Large.**

Suggestions for candidates are solicited. Names should be sent by **November 5, 2015** to the Nominating Committee Chair, c/o Pat Ryan, Chief Operating Officer, ACM, 2 Penn Plaza, Suite 701, New York, NY 10121-0701, USA.

With each recommendation, please include background information and names of individuals the Nominating Committee can contact for additional information if necessary.

Vinton G. Cerf is the Chair of the Nominating Committee, and the members are Michel Beaudouin-Lafon, Jennifer Chayes, P.J. Narayanan, and Douglas Terry.

Association for
Computing Machinery