CyberPro

June 2010

Keeping Cyberspace Professionals Informed

SENIOR LEADER PERSPECTIVE: SCOTT BORG

NSCI's Lindsay Trimble recently had the opportunity to interview Scott Borg, director of the U.S. Cyber Consequences Unit – an independent, non-profit institute that investigates the strategic and economic consequences of cyber attacks for the U.S. government. He is regarded as one of the leading authorities on the economics of cyber security and is responsible for many of the concepts that are currently used to analyze the implications of cyber attacks in business contexts. Borg has commented on cybersecurity issues for CBS, CNN and NPR and been a guest lecturer at Harvard, Yale, MIT, Columbia and other leading universities. He is currently a member of the Commission on Cybersecurity for the 44th President and a Senior Research Fellow in International Security Studies at the Fletcher School of Law and Diplomacy of Tufts University.

NSCI: Since the U.S. Cyber Consequences Unit was created, what changes have you seen in the types of cyber threats our nation faces?

BORG: The changes in cyber attacks we've seen over the seven years that the US-CCU has been operating have been enormous. When we began our work as a government-sponsored, non-profit research institute, cyber security was a specialist interest, narrow in scope, compared with physical security. Cyber attackers were still largely isolated, adolescent amateurs. The leading attack tools were general-purpose viruses that would do only two or three simple things. The attacks were nearly all aimed at causing denials of service that would be immediately apparent.

Nowadays, cyber security is a field of general interest, so broad in scope that it is increasingly absorbing physical security. Cyber attackers are highly-organized, adult professionals. The leading attack tools are customized programs that can carry out many different complex procedures, depending on the contexts in which they find themselves. The more serious attacks are nearly all aimed at hijacking systems to carry out operations that the owners won't immediately spot. This has been a huge transformation.

NSCI: Should we be more focused on defending against potential attacks by terrorists and other criminal organizations or do you see a different type of attack in the near future?

BORG: Terrorists have never been a serious cybersecurity problem, although they could become one in the future if they acquire the necessary cyber attack expertise. In the case of al-Qaeda, the main reason they haven't been a problem is that the half-dozen terrorist leaders who knew something about cyber attacks and were proposing to employ them were all killed or captured.

Financially-motivated criminals have been a big security problem and are likely to become a much bigger one. This is because they have impressive, rapidly-growing capabilities. In the future, they will

increasingly employ those capabilities to manipulate markets, so that they can collect bigger profits without a payment trail.

The biggest future danger is that ideological fanatics or irresponsible political regimes will acquire the sort of attack capabilities that are now only possessed by high-tech nation states. If those groups or governments were then to attack our critical infrastructures, they could cause catastrophic damage.

NSCI: From your research, what would be the most destructive strategic or economic consequence of a large-scale cyber attack?

BORG: The most destructive cyber attacks would be those that caused massive physical damage to the equipment we depend on for electricity, oil and gas, transportation, and other critical supplies and services. A long-term interruption of telecommunications and the Internet, while harder to achieve with pure cyber-attacks, would cause a similar level of destruction. Almost as bad would be cyber attacks that caused a loss of confidence in banks, financial services and other economic institutions.

All the targets that could hurt us most and that we most need to defend are critical infrastructure industries. This is because all of the business activities that supply us with essential goods and services are dependent on those industries. Without them, most of us would soon be thirsty, hungry and, during much of the year, dangerously hot or cold.

NSCI: What defensive tactics does your team recommend for government and private organizations to use in preparing against cyber attacks?

BORG: My colleague, John Bumgarner, and I wrote the "2007 US-CCU Cyber-Security Check List," which enumerates all of the things a corporation or other large organization needs to do to protect itself against cyber attacks. We will produce a new edition as soon as we have the necessary corporate sponsorship, but our 2007 checklist is still the most up-to-date and comprehensive document of its kind.

No list of cybersecurity measures, however, can solve our cybersecurity problems! This is because the security problems produced by information technology are too deep and pervasive to be dealt with adequately by a bunch of cybersecurity professionals running around trying to plug the massive vulnerabilities we are currently building into everything. Cybersecurity professionals don't have the necessary budgets or authority. Even if they did, cybersecurity measures are not a cost-effective way of dealing with the problem. What we really need to do is design more resilient processes and industries. A large portion of the best and most cost-effective solutions to cybersecurity problems are not cybersecurity solutions. They are operational process solutions.

NSCI: Does your team's research focus mainly on preemptive counter-measures or does it also analyze ways to respond to attacks?

BORG: The central focus of our research is actually consequences. We research attack scenarios in order to find out what cyber attacks are actually possible, how difficult they are, who could profit by them,

and, thus, how likely they are. We research vulnerabilities in order to find out how the various attacks could be stopped, how costly it would be to stop them, and, thus, how likely they are to be stopped under various conditions. But the real core of our research is investigating what the consequences of various cyber attacks would be. I have figured out how to quantify even things like damage to business relationships, loss of confidence in systems or institutions, and loss of competitive information. I have also found ways to trace the knock-on effects throughout the economy. Thus, with sufficient cooperation from the corporations involved, my colleagues and I are able to work out what the costs of any given cyber attack would be – both for the individual business and for the economy as a whole. By quantifying these consequences, we can then make objective judgments about what policies would be cost-effective in dealing with the prospective losses.

NSCI: How about things like the issue of attribution?

BORG: The US-CCU tries to investigate the consequences of cyber attacks under all likely conditions. Being able to attribute cyber attacks to people who want to remain anonymous is not a condition likely to occur. At the end of the last RSA convention, I led a discussion at the bar in which we tried to pick the 10 stupidest things anyone had said at the convention. Our No. 1 pick for the single stupidest thing anyone said at the RSA convention was "as soon as we solve the attribution problem."

However painful it might be to admit, we have to accept that anonymous cyber attacks are a fact of life and likely to remain so. Under all foreseeable conditions, people will be able to acquire laptops or smart phones without revealing their true identities, and they will be able to get online wirelessly without revealing their true identities. That's all that's needed to launch an anonymous cyber attack. Even if biometric identifiers were required to get Internet access – which for economic reasons is virtually inconceivable – those biometric identifiers would be electronically spoofable. Where cyber attacks are concerned, attribution isn't an issue; it's sheer fantasy.

NSCI: How does your team disseminate information to the public sector and government leaders?

BORG: We provide reports and briefings to many different government, business and public groups, but always, to some degree, on a need-to-know basis. This is because of the sensitivity of the subject matter.

Some documents, such as our cybersecurity check list, our laptop travel guidelines, our overview report on the cyber campaign against Georgia, or our analytic comments on most news developments are provided to virtually everyone. The last time I did a Google search on "cyber consequences unit," their search engine turned up about 350,000 Web sites where our work was cited or posted.

Other documents, such as the complete, hundred-page version of our report on the cyber campaign against Georgia, are classified by the government and only available to people with the appropriate security clearances. In fact, some reports we produce are too sensitive to be entrusted to any sizeable group of people, even if they have high level clearances. These reports are supplied, usually in person, to the few people in government and industry who genuinely have a need to know.

Fortunately, most of our research is not that sensitive. The bulk of it, especially my economic research, is work that we are eager to make public in as many speeches and publications as we have the time and money to produce.

NSCI: What positive changes have you seen leaders take as a result of US-CCU research and analysis?

BORG: There has been a huge shift in public understanding toward the positions and principles that the US-CCU has been advocating. How much this has been due to the US-CCU's influence and how much it is due to the fact that we were simply ahead of the curve would be hard to say. There are certainly many categories and terms that my colleagues and I introduced which are now taken as standard. I often see PowerPoint presentations, for example, where people are applying frameworks that were my work without out any awareness that these frameworks had to be created by someone, let alone an awareness of who was responsible. So, as far as public understanding is concerned, we could probably claim to be responsible for some considerable changes.

As far as practical measures are concerned, we have not yet been as successful. There are a lot of little changes we have successfully promoted, in some cases simply because they were items in our check list. There are also cases where our warnings have probably helped critical infrastructure industries to escape from some emerging dangers. But the big changes we have been working to bring about in the cyber defenses of America and its allies mostly haven't happened yet.

NSCI: Shortly after naming Howard Schmidt as the first Cybersecurity Coordinator, he appeared to dismiss much of the cyberwar threat[1]. What is your reaction to this?

BORG: "Cyberwar," as a term, has done a lot of damage, because cyber attacks and even sustained cyber conflicts do not correspond to what people would ordinarily describe as "war." Indeed, one of the key characteristics of cyber conflicts is that they will elude most of the existing definitions of warfare. Sometimes this has caused people to overstate wildly what is already going on, misleadingly claiming that it has the features of war. Other times, it has caused people to underestimate what is already happening, because some of the most destructive recent cyber attacks, such as the massive thefts of military and business information, don't look enough like warfare. Although some news stories have made it sound as though Howard Schmidt and I are on opposite sides of this issue, we are actually in complete agreement about the need to stop using the term "cyberwar," except, perhaps, in a few specific military contexts.

Howard and I are also in agreement that exaggerated claims about the losses due to cyber attacks threaten to undermine the credibility of the entire field. One of the current exaggerated claims is that the cost of cyber espionage to the American economy is a trillion dollars a year. My research and that of my colleagues suggests that the real number is probably around 2% of that figure. This is still a huge number – about $20 billion annually – and that number could get a lot larger in the future. But this is a

[1] http://www.govinfosecurity.com/articles.php?art_id=2267&rf=030810eg

long way from the sort of number that is currently being thrown about. When Howard Schmidt criticizes exaggerated claims about cyberwar and the economic losses due to cyber attacks, he isn't belittling those things. He is just being sensible.

NSCI: Is there anything else you'd like to add?

BORG: Watch for my long-promised book, *Cyber Attacks: A Handbook for Understanding the Economic and Strategic Risks*. It covers the entire field of cyber security from an economic standpoint, showing how to quantify almost everything relevant to cyber risk, but hiding the math in words and pictures to keep the text readable. It should be out later this year.

Illustration by www.callicuttart.com – NSCI Copyright 2009