CHAIRE DE CYBERDÉFENSE ET CYBERSÉCURITÉ

SAINT-CYR THALES SOGETI

Interview with Ellen Nakashima (The Washington Post - USA)

by Daniel Ventre1 (CNRS ; Chair in Cyber Security and Cyber Defense)

May 2013 – Article n°III.5

Ellen Nakashima is a national security reporter for The Washington Post[2]*. She co-authored the book « The Prince of Tennessee: Al Gore Meets His Fate »*[3].

Daniel Vente (D.V) - Mandiant cyber security company recently published a report on Chinese cyber espionage activities. The report has received substantial criticism from Chinese media, and government but also from cyber security experts in the U.S. (for instance due to its methodology of investigation). But, whatever their quality, do you think that such reports may change the perceptions among politicians and have an impact on cybersecurity and cyberdefense policies?

Ellen Nakashima (E.N) - The Mandiant report is widely seen as the first public confirmation of what has long been asserted by analysts and privately by U.S. officials: that the Chinese government is behind a widespread and persistent campaign of cyber economic espionage. The Mandiant report's value lay in pointing to a specific unit of the PLA as the perpetrator of a large number of intrusions. After it came out, government officials cited it in describing the cyber economic espionage threat, so it gave them cover to say publicly--attributing to a commercial report--what they have long known, but could never say. In that sense it has become a touchstone. Government officials are just more constrained in what they can say publicly for a combination of diplomatic, intelligence and operational reasons. In any case, I think the report was a significant development in that it made the public and politicians take notice of the problem. It gave specificity and concreteness to what has largely been a debate of charge, countercharge and denial. The challenge now is to figure out how best to encourage/force/persuade China to stop its cyber economic espionage. That is a complex issue that requires understanding their motivations, their cost-benefit calculus and the levers that will alter their behavior. The Mandiant report was important in creating a public awareness and possibly support for more aggressive government policies vis-a-vis China.

[1] *Copyright : this article may not be reproduced in any form or by any means without written permission from the copyright owner*

[2] http://www.washingtonpost.com/ellen-nakashima/2011/03/02/ABdt4sM_page.html

[3] David Maraniss, Ellen Nakashima, *The Prince of Tennessee: Al Gore Meets His Fate*, Simon & Schuster, 2001, 320 pages, http://www.amazon.com/Prince-Tennessee-Gore-Meets-Fate/dp/0743210506

D.V - Cyber Security and Cyber Defense policies: could you please explain us what the main differences are between Republicans and Democrats' approaches of such issues?

E.N - National security issues do not generally break down along party lines. In fact, there is remarkable continuity between GOP and Democrat administrations when it comes to national security. Cyber is no different. Information-sharing is a good example. The CISPA bill in the House is co-sponsored by the Republican chairman of the Intel Committee and his Democratic co-chair, and it passed the house with a fair number of Democratic votes. That said, the Democrats in the Senate and the Democratic Obama administration are insisting on greater privacy protections in any information-sharing legislation. But that can probably be worked out.

In broad-brush strokes and at the risk of over-generalizing, most Democrats are more comfortable with the idea of regulating cyber standards than most Republicans. But there are centrist Democrats who are sympathetic to industry's argument that regulation will stifle innovation. The positions depend on the political winds and make-up of the Congress. So for instance, the Obama administration, which last year was firm on mandating cybersecurity standards, has this year pretty much abandoned that approach. They have backed off the mandatory approach in favor of legislating incentives to comply with voluntary standards[4].

D.V - Among politicians, but also among the industry, the media and citizens did the perception and consciousness of cybersecurity and cyberdefense issues really change during the last 20 years in the United States? What have been the main steps of this evolution?

E.N - Cybersecurity has only really hit the public consciousness in the last few years. Up till then, to the extent that citizens thought of it at all, they thought of it as preventing identity theft. But with people hearing senior administration officials warning about a Cyber Pearl Harbor, and with the news of Stuxnet in 2010, the average person has become more aware that computers can be used as weapons, too, to destroy or damage machines that control our electric power supply, transportation networks, financial transactions, etc[5].

D.V - Efforts to conceptualize cyberconflict mainly refer to 'Cold War' and 'War on Terror' strategies, policies and concepts: Cyber Cold War; Cyber deterrence; Cyber Terrorism, invisible threat; insider threat … Are they the most appropriate analogies that we might use to talk about cyber security issues?

E.N - Cyber security is such an amorphous term. The most useful analogy depends on what you mean by cyber security. Do you mean protecting your company's data against theft from China? Or protecting your Scada system against an Iranian agent who manages to sneak a thumb drive in? Or against a terrorist who has now acquired the capability to launch a destructive cyber attack on an industrial control system? You get the point. The problems are diverse. Deterring a nation state that is conducting massive cyber economic espionage is different than deterring Hezbollah from sabotaging a power plant or a hactivist group from

[4] http://tinyurl.com/clfsjyf

[5] http://articles.washingtonpost.com/2012-06-06/world/35461160_1_cybersecurity-cyberattack-cyberthreat

disclosing embarrassing emails from a company or an eastern European crime syndicate from stealing credentials to get into bank accounts.

Then there are the analogies to the public health model of cybersecurity-- detecting, monitoring and preventing threats through surveillance of indicators of risk; and to biological systems that self-heal.

To me the more important point is that government officials, academics, and industry experts who speak about cyber issues would do us all a favor if they would be more precise in their language. By indiscriminately calling all actions an "attack" -- from a probe to try to get into a computer, to an intrusion that results in no data exfiltration, to a hack that results in terabytes of stolen data, to a denial of service that is not an intrusion at all, to a compromise that results in disruption of a power grid, to a penetration that leads to a pipeline explosion -- commentators confuse the public about what the stakes are, and where the thresholds for response actions might be. Imprecise language makes for a muddy debate and bad policy. Clarity, candor and precision are key.