Cyber Cease-Fire: US v. China

BY DON EIJNDHOVEN
(http://darkmatters.norsecorp.com/author/deijndhoven/)
http://www.argentconsulting.nl/ (http://www.argentconsulting.nl/)

Interesting times indeed, now that the outcome of Chinese president Xi Jinping's two-day visit to the White House last week has been made public (https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states). According to the White House press release, this is what was agreed:

- The United States and China agree that timely responses should be provided to requests for information and assistance concerning malicious cyber activities. Further, both sides agree to cooperate, in a manner consistent with their respective national laws and relevant international obligations, with requests to investigate

cybercrimes, collect electronic evidence, and mitigate malicious cyber activity emanating from their territory. Both sides also agree to provide updates on the status and results of those investigation to the other side, as appropriate.

- The United States and China agree that neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
- Both sides are committed to making common effort to further identify and promote appropriate norms of state behavior in cyberspace within the international community. The United States and China welcome the July 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International security, which addresses norms of behavior and other crucial issues for international security in cyberspace. The two sides also agree to create a senior experts group for further discussions on this topic.
- The United States and China agree to establish a high-level joint dialogue mechanism on fighting cybercrime and related issues. China will designate an official at the ministerial level to be the lead and the Ministry of Public Security, Ministry of State Security, Ministry of Justice, and the State Internet and Information Office will participate in the dialogue. The U.S. Secretary of Homeland Security and the U.S. Attorney General will co-chair the dialogue, with participation from representatives from the Federal Bureau of Investigation, the U.S. Intelligence Community and other agencies, for the United States. This mechanism will be used to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side. As part of this mechanism, both sides agree to establish a hotline for the escalation of issues that may arise in the course of responding to such requests. Finally, both sides agree that the first meeting of this dialogue will be held by the end of 2015, and will occur twice per year thereafter.

Second-guessing

At first glance this sounds wonderful, but it didn't take long before the second-guessing started (http://www.theguardian.com/us-news/2015/sep/25/us-china-cyber-security-obama-xi-jinping-inconclusive-summit). With Barack Obama making statements such as "What I've said to President Xi, and what I say to the American people, [is] the question now is: 'Are words followed by actions?'".

It's important to look at this meeting in the context in which it was held. As most people are aware, the US has been experiencing cyber-attacks almost non-stop for years now, on multiple fronts. The US criticizes China for attacking not only US government infrastructure, but commercial enterprises are suffering massive theft of intellectual

property in almost every industry as well. The widely publicized OPM hack (http://www.wired.com/2015/07/massive-opm-hack-actually-affected-25-million/) was only the most recent event that made the American cup 'runneth over'.

But the US is hardly the innocent victim that it portraits itself to be. Well-known whistleblower Edward Snowden revealed that the US has actively been attacking Chinese infrastructure as well (http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking), in order to 'prepare the battlefield' for any potential physical conflict. They have admitted doing so, but claim that no intelligence from the large cyber intelligence gathering 'driftnet' known mostly by its moniker PRISM is fed to American enterprises for their commercial benefit. Whether that is true, of course, remains to be seen. After all, accusations of unfair commercial advantages through government espionage have been shown to contain some substance in the past (http://www.cyber-rights.org/interception/stoa/ic2kreport.htm#Summary).

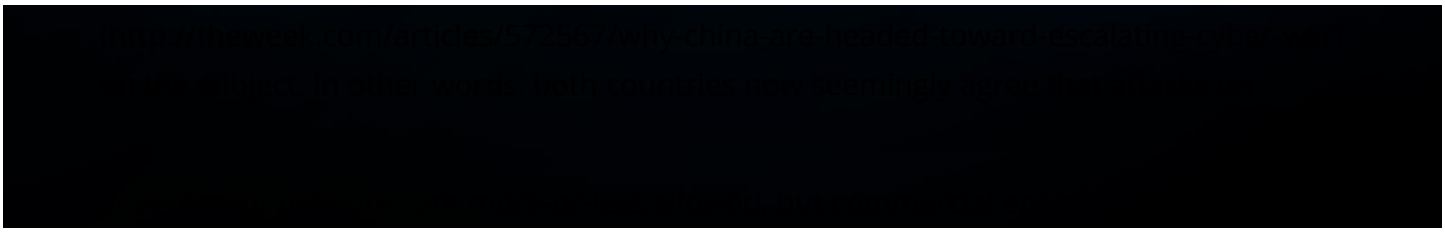
Limiting cyber-attacks

In this regard, it is not surprising that it is the US calling for an agreement on limiting the cyber-attacks between the two nations. When taking the theft of intellectual property into account, the US simply has more to lose. It should also not be forgotten that not long ago China signed a treaty with Russia (http://www.russia-direct.org/analysis/china-russia-cyber-security-pact-should-us-be-concerned) that, among other things, contained a pledge that they would not hack each other. This same treaty also further solidified their efforts to influence global internet governance, about which I commented in an earlier article (http://darkmatters.norsecorp.com/2015/01/21/gccs-2015-battlefield-for-the-internets-multi-stakeholder-coup/), giving the US all the more reason to try to calm the waters with China.

So what does this treaty mean?

Of the four points covered under Cybersecurity, only the first two are points with some meat to it. As also mentioned in my previous article, the Chinese are very unlikely to sign any treaty on internet norms of behavior that include a reference to the UN's definition on human rights. The entire bullet point might as well not have been there. It is window dressing and was probably only agreed upon because it shows a willingness to 'get along', whether real or imagined. The last point about the 'cyber hotline' doesn't actually say a whole lot at all, so let's move on to the more salient points.

It should be noted that the US is trying to stop the attacks against American businesses while trying to keep the option of 'battlefield preparation' on the table. This isn't guesswork, it's public record, just look at what American politicians are saying



considered off-limits. In the unlikely event that both parties actually honor the agreement, this would be a clear win for the US.

An unlikely agreement

And that the agreement will be honored does seem very unlikely. For one, the Chinese government has never acknowledged that it has any involvement in cyber-attacks against commercial enterprises, and it is highly unlikely that they ever will. If those attacks would now suddenly cease, it would be a tacit admission that it had such control in the first place and put the lie to every official statement the Chinese government has ever issued on this topic. Another important factor is the simple question of "Cui Bono?". Who benefits? The Chinese would lose a very effective method for national advancement in many areas, and the only cost thus far has been (relatively light) international criticism. They would gain nothing, whereas the US would gain a stopgap in the massive IP drain.

In short: The agreement seems a bit one-sided and that does not bode well. It may well be that China agreed only to stave off the sanctions that the US has been casually dropping (http://www.theguardian.com/world/2015/sep/24/obama-china-financial-sanctions-hacking-xi-jinping) to the press recently. Whether China takes these sanctions seriously is debatable, because China still remains the greatest holder of US debt (http://www.cnbc.com/2015/05/16/china-tops-list-of-us-foreign-creditors-once-more.html), which means it can give a considerable pushback. Then again, China not honoring the agreement is probably expected. Despite what some critics may say, the people involved in drafting this treaty are not fools. With this agreement on the table it makes the American case much stronger if China does violate it, as Jason Healey points out (http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0925/Opinion-Even-if-flawed-cybertheft-deal-with-China-a-win-for-Obama).

As always, time will tell.

YOU MIGHT ALSO LIKE:

THE UPSIDE OF ACCIDENTALLY HIRING A HACKER
(HTTP://DARKMATTERS.NORSECORP.COM/2014/09/26/THE-UPSIDE-OF-ACCIDENTALLY-HIRING-A-HACKER/)

ACTIVITY FROM CHINESE IP CONTINUES, HIGHLIGHTS ATTRIBUTION ISSUES
(HTTP://DARKMATTERS.NORSECORP.COM/2014/09/11/ACTIVITY-FROM-CHINESE-IP-CONTINUES-HIGHLIGHTS-ATTRIBUTION-ISSUES/)

AGGRESSIVE CHINESE IP: ACTIVITY CONTINUES, APPEARS TO BE NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
(HTTP://DARKMATTERS.NORSECORP.COM/2014/09/04/AGGRESSIVE-CHINESE-IP-ACTIVITY-CONTINUES-APPEARS-TO-BE-NATIONAL-UNIVERSITY-OF-DEFENSE-TECHNOLOGY/)

CHINESE IP ADDRESS DISCOVERED TARGETING MULTIPLE PORTS
(HTTP://DARKMATTERS.NORSECORP.COM/2014/08/28/CHINESE-IP-ADDRESS-DISCOVERED-TARGETING-MULTIPLE-PORTS/)

Don Eijndhoven

Don Eijndhoven (@ArgentConsulting), Chief Executive Officer of Argent Consulting B.V, lead cyber security architect and guest lecturer Cyber Resilience at the Nyenrode Business University. Don can be reached at d.eijndhoven@argentconsulting.nl.

▶ MORE POSTS (11)

(http://darkmatters.norsecorp.com/author/deijndhoven/)

TOPICS: CHINA, CHINESE INFRASTRUCTURE, CYBER CEASE-FIRE, CYBER INTELLIGENCE GATHERING, CYBER-ATTACKS, CYBERCRIMES, DRIFTNET, GOVERNMENT ESPIONAGE, HACK, HACKING, INTELLECTUAL PROPERTY, INTELLECTUAL PROPERTY THEFT, OBAMA, OPM HACK, PRISM, SANCTIONS, TRADE SECRETS, TREATY, UNITED STATES, US GOVERNMENT, WHISTLEBLOWER, XI JINPING,