http://ezli007.blogspot.com/2011/06/china-and-us-sizing-up-for-cyber-war.html

China and the US: Sizing up for cyber war?

6/9/2011

Although there were strong reactions after Google's Gmail accounts were phished, some analysts say that similar occurrences happen all the time, and US government chest-thumping is code for internet censorship.

As senior US officials warn that cyber attacks on vital systems would be considered "acts of war" eliciting a real world military response, one professor at the National Defence University surmises that battles of the future might be fought by guys hunched over keyboards in dark basements, rather than strapping lads toting M-16s.

In light of recent cyber attacks on Google apparently launched from China, online tensions - the possible precursors to outright conflict - have been spreading from chat rooms, to Gmail accounts and into the meeting rooms of military decision makers in recent weeks.

"We operate in five domains: air, land, sea, outer space and cyberspace," says Dan Kuehl, a professor of information operations at the National Defence University in Washington. "An ever increasing amount of what we do has dependencies on cyberspace; a guy typing on a computer is one of the new faces of war," Kuehl told Al Jazeera, stressing that he is not speaking for the US government or his elite military university.

"A response to a cyber-incident or attack on the US would not necessarily be a cyber-response. All appropriate options would be on the table," Pentagon spokesman Colonel Dave Lapan said recently.

Tough talk and phishing trips

One US defence official told The Wall Street Journal newspaper: "If you shut down our power grid, maybe we will put a missile down one of your smokestacks," in rhetoric likely aimed at China. For its part, the Chinese government categorically denied any involvement in the cyber attacks, which Google reported to the US state department and media outlets last week.

The reason for this sort of digital tough-talk is related to basic military strategy. "There is value in ambiguity," Kuehl said. "You don't want your adversary to think 'I can go up to that red line but I can't cross it'. You want them to think 'I won't do anything in the first place'," for fear of old fashioned physical reprisal.

Phishing attacks recently launched against Google's mail service targeted the personal e-mail accounts of some senior US officials, along with Chinese journalists, human rights activists and South Korea's government.

These attacks are similar in form to the scam e-mails most people receive from, say, the widow of a Nigerian millionaire who asks the user to open a message so they can claim their $14m reward for being a nice person. Once the message is opened, the victim's computer is compromised.

"This was a pretty straight forward phishing attack, other than the more sophisticated social engineering where the e-mail seems to come from someone who you know," says Richard Stiennon, the chief research analyst at IT-Harvest and author of Surviving Cyberwar, referring to recent actions against Gmail.

"The Chinese have the early advantage in executing cyber warfare. If you have a large information gathering operation, knowing even the personal data of officials can be valuable," he told Al Jazeera. If data is stolen from personal accounts it is likely dumped into massive data banks for processing, crossing referencing and analysis.

WikiLeaks documents indicate that US diplomats are concerned about China's government recruiting top hackers to launch cyber war campaigns.

"There is a strong possibility the PRC [People's Republic of China] is harvesting the talents of its private sector in order to bolster offensive and defensive computer network operations capabilities," said a secret state department cable from June 2009.

Tampering with logistics

Since 2002, cyber intruders, apparently from China, have exploited vulnerabilities in the Window's operating system to steal login credentials in order to gain access to hundreds of US government and defence contractor systems, according to a 2008 cable.

China, for its part, says it is ready for online conflict should it arise. "Of late, an internet tornado has swept across the world... massively impacting and shocking the globe. Behind all this lies the

shadow of America," said a recent article published in the Communist-Party controlled China Youth Daily newspaper, signed by Ye Zheng and Zhao Baoxian, who are scholars with the Academy of Military Sciences, a government linked think-tank.

"Faced with this warm-up for an internet war, every nation and military can't be passive but is making preparations to fight the internet war," the article said.

That attacks apparently came from China does not, onto itself, implicate the Chinese government. Internet or IP addresses which delineate where a computer is physically located can be compromised, allowing users in one country to take over a computer somewhere else to launch attacks.

"How do you know where to strike back? You don't," says Bruce Schneier, a technology expert and author of several books who The Economist magazine describes as a "security guru".

"You don't have nationality for cyber attacks, making retaliation hard," he told Al Jazeera.

But the nature of the Chinese state, where information is closely controlled, most corporations are linked to the Communist Party apparatus and dissidents are crushed, means the government likely had some knowledge of what was happening, Stiennon says.

And, even if the Google attack was carried out by rogue hackers, American defence planners haven't been taking any chances. One possible scenario involves a Chinese move to re-take Taiwan - an island which China views as a renegade - despite the US and UN considering it a sovereign country.

"The Chinese have looked at their biggest potential military adversary, the US, and decided that their biggest weaknesses are that they are far away and dependent on computers," says Kuehl from the defence university. He thinks likely Chinese strategies are twofold: The obvious "degrading enemy military apparatuses in the theatre of war" and "preventing the enemy from getting there". Cyber attacks, targeting battle ship deployments and logistics, would play decisively in the latter.

"The threat, from a military perspective, isn't data denial, it is data manipulation," Kuehl says. "What do you do when the data on your screen is wrong and air traffic controls, money, deployment orders and personnel have all been tampered with?"

Misdirection and censorship

Regardless of China's broader aims or involvement from the Chinese government in recent cyber mischief against Google, there is nothing new or impressive about recent cyber attacks, even though the international media has focused on them, Schneier says. "Millions of these kinds of attacks happen all the time," he says. To him, recent phishing operations against Google are not even worthy of a blog post, as such events happen so frequently.

Chris Palmer, the technology director with the Electronic Freedom Foundation advocacy group, thinks recent rhetoric about cyber war is a "smokescreen to limit freedom of speech on the internet".

"If I was being cynical, this campaign [about cyber security] is being launched by defence contractors to drum up a threat and get money from it," Palmer told Al Jazeera.

The US state department's tough talk about physical reprisals is not the way to defend American infrastructure from attacks, he says. The solution is much simpler: Taking sensitive data off the internet entirely.

Gaining access to military documents or networks controlling physical infrastructure like water treatment plants and nuclear facilities "should be like Mission Impossible, requiring a physical presence". In the film, Tom Cruise has to sneak into a heavily guarded room to physically access a computer with secret information.

In the 1980s and early 1990s, power plants, for example, ran on private networks where the censors would talk to the controllers, Palmer says. "Now things that are supposed to be private have become virtually private, going over the same lines as internet traffic." As getting online became cheaper, and operating private networks became more costly and cumbersome compared to using the standard internet, companies began using the regular net.

"Not being on the internet costs more for dollars and opportunity cost," he says. "The design and the reality don't match anymore, but the design was supposed to be private." And this semi-public link to the broader net leaves vital systems potentially open to attack.

While military contractors propose new products to defend against online threats, commercial cyber crime - where companies seek data on competitors and rivals try to steal industrial secrets - may be a bigger issue than fears of nation to nation conflicts spilling onto the internet.

"The [US] defence department, just like everyone else, is struggling with the rapid rise of cyber threats," says Richard Stiennon, the security analyst. "It is all new. They don't have a basis in international law or jurisdictional avenues from which to build a cyber response."

And, the need for better international norms for governing cyber conflict is one of the few points of agreement between analysts. "The big thing here is that there is nothing magic about cyberspace," Schneider says."Everything that is true is still true when you put the word 'cyber' in front of it."

Some may say that international laws are often worth little more than the paper on which they are printed. And, sadly, the ability to exert force still determines the international pecking order. But, it may still be better to have an unenforceable framework for online conflict than none at all.

As Bruce Schneier puts it, "I think a UN conference on cyber war would be a great thing to do".