Cybersecurity and Challenges to Democracy

Joshua I. James
Joshua@cybercrimetech.com

South Korea's democracy can only be described as... developing. In the late 1970s, after the assassination of Military Dictator Park Chung-hee (who Koreans often refer to as 'President Park'), slow but relatively steady progress in terms of democracy was made in South Korea. This despite the fact that the North Korean threat, and communism in general, was a topic constantly abused to allow the government to gain more power.

Recent incidents, however, have prompted a vie for power within the South Korean government that will have serious consequences for South Korea's democracy going forward. In the recent weeks North Korea has been saber rattling per usual, to which South Koreans are generally unaffected. One issue with this situation, however, is that the recent cyber attacks on South Korean banking and broadcasting systems are also being attributed to North Korea without, at the time of this writing, any verifiable proof that North Korea carried out the attacks. South Korea currently has IP addresses tracing back to various countries, and attack patterns that are "similar" to those used by North Korea in the past. At best, the evidence is unsubstantial. However, the South Korean National Intelligence Service (NIS) (think C.I.A. on steroids) has formally released a statement claiming North Korean involvement, which, of course, no one can confirm or deny.

This statement comes days after the exceedingly toned-down proposal of the South Korean "National Cyber Terror Prevention Act". This act, in essence, gives the NIS, or NIS-controlled groups, full power to create, vote on and *enforce* anti-cyber terror policies through the creation of an NIS-lead "cyber control tower". Ironically, the act itself was proposed by the very members of Congress who are responsible for keeping the NIS in check. The most interesting aspect of the act, however, is the definition of cyber terror. Cyber terror, according to the act, can potentially be almost *anything*.

Consider that the NIS was created during the time of a military dictatorship with the express intention of fighting communism. Because of that, the NIS effectively reports to no authority save for the president. The NIS has, in the past, attempted to push anti-terrorism acts that would allow them even more power with little checks on how that power is used and abused. However, when discussing physical terrorism, many experts can, and have, resisted such a push. Cyber terrorism, however, is extremely vague. So much so that even experts in the field do not agree on its definition and how it should be handled. This is a problem most countries are currently facing that is related to the lack definition of terms like cyber crime, cyber war and cyber terrorism. Because of the lack of definition, government agencies all over the world are attempting to create jurisdiction around whatever term they choose, generally focusing on which term will bring the most power and budget benefits rather than which term correctly describes the situation.

South Korea is an extreme example of how agencies can combine fear with vague terms to expand their power. Of course, this is all made possible because the South Korean people allow it to happen, normally through complacency and cultural restrictions. However, regardless of culture, similar situations are happening in most countries right now. While a centralized all-knowing government 'cyber control tower' may have some benefits, it simply won't stop cyber crime/terror/war. Further, what benefit such an over-powered group could contribute to a democratic society is completely undermined that group's ability to abuse such power.

The reality is, cyber crime/terrorism/war is largely made possible by the public, and just like 'traditional crime' will never be completely stopped. The general public (globally) appear to have little interest in securing themselves, and they are about to give up what little freedom they have so their governments can *ineffectively* protect the people from themselves. Anyone who chooses to use technology should take responsibility for themselves, get informed and start implementing basic cyber security practices. If the people start securing themselves, the majority of digital crimes can be drastically reduced, and it won't cost anyone hard-earned freedoms to do it.

Bibliography

1. (2013) "Korean National Cyber Terror Prevention Act (English Language)". Retrieved from www.cybercrimetech.com/2013/04/south-korean-national-cyber-terrorism_13.html.

2. (2013) "Korean National Cyber Terror Prevention Act (Korean Language)". Retrieved from www.cybercrimetech.com/2013/04/south-korean-national-cyber-terrorism.html.