South Korea's cyber-war ambitions could backfire badly

February 25 2014, by Alan Woodward

What's worse than an enemy with a gun? An enemy with malicious code. Credit: Niall Carson/PA Archive/Press Association Images

South Korea has made a suprisingly public announcement that it plans to develop cyber-weapons for potential use against North Korea. The decision to make its plans known is baffling and the potential consequences of taking hostilities online are deeply troubling.

When the Iranian nuclear processing plant at Natanz was hit with Stuxnet it marked a new stage in modern warfare. Stuxnet was the first code-based weapon ever used and by the time it was discovered in 2010, it had ruined almost a fifth of the Natanz centrifuges and caused so much disruption that the Iranian nuclear programme is yet to fully recover.

For those with a vested interest in seeing the Iran's nuclear ambitions fail, Stuxnet appeared to be a major success. But the law of unintended consequences has resulted in some very troubling repercussions from the attack on Natanz, which makes it all the more surprising that South Korea wants to take a similar path.

From a purely technical perspective, Stuxnet was truly impressive. It targeted a particular class of computer called a Supervisory Control And Data Acquisition (SCADA) system. The virus was able not only to disrupt Iran's centrifuges so that they ran at incorrect speeds, but also report back to the power plant controllers that everything was fine. While it caused havoc by making highly sensitive systems operate erratically, those in charge had no idea anything was wrong.

The SCADA systems attacked by Stuxnet were a particular range made by Siemens, which were known to be used in the Natanz facility. That means the attack was probably highly targeted. It appeared to be the code equivalent of the type of smart bomb you see on the TV. It was able to take out the bad guys without any messy collateral damage.

But that's fiction. The reality is that "surgical strikes" often do have collateral impact and so did Stuxnet. In fact, Stuxnet's collateral impact continues to be felt today, years after the original attack. The reason is simple: SCADA systems are used in just about every form of critical infrastructure we need in modern life, from our power stations to water processing plants to transportation control systems. And the versions produced by Siemens are among the most commonly used SCADA systems.

By releasing a code-based weapon like Stuxnet, the still unidentified attackers did something quite different to launching a missile in Iran. Rather than exploding on impact, the weapon stayed intact.

When you use a weapon against an adversary and it is not destroyed, you have effectively given it the weapon to re-use elsewhere. So it was no great surprise when copies of Stuxnet became available around the world and it soon became possible to watch a YouTube video showing how to modify the code to attack your chosen SCADA system. It took only slightly longer for derivatives of Stuxnet to appear and the sons of Stuxnet were easier to use and faster to deploy. Weaponry has a horrible habit of evolving quickly and code-based weapons are even easier to improve than most.

Hi, we're the enemy

One thing that Stuxnet did have was plausible deniability. It was impossible to determine who had developed it. Fingers have been pointed at the US and Israel for many years but, even to this day, accusations about who attacked Irean are based on little more than hearsay and speculation.

Code-based weapons are not like nuclear weapons in that they do not require vast, expensive facilities to develop the raw materials. All you need is a group of clever people and relatively modest computing facilities. Unlike nuclear weapons, they are within the reach of most industrialised countries, and quite a few developing nations. A small rogue state could launch an attack against a militarily powerful nation, cause significant damage and no one need ever know it was behind the attack.

So it is particularly strange that South Korea has made its intentions public. Any attack on the North will now automatically be blamed on the South, thereby ratcheting up tension and possibly leading to armed confrontation. It's the one move I really can't understand.

The US believes a cyber-attack should be treated as an act of war and would like to reserve the right to retaliate using good old-fashioned bombs and bullets if the time comes. This is quite reasonable in many ways, given how serious a code-based weapon could be. An enemy need not bomb a country into submission anymore, it could simply turn off the power and water. No country – the US included – could survive that for long. Unless you threaten real physical retribution against an aggressor, there is a danger that someone will try their luck. Although, all this of course assumes you know who to launch reprisals against. Iran still doesn't.

Why then would South Korea threaten such action against North Korea so openly? Obviously it doesn't want the North to develop nuclear weapons as it has no such weaponry itself. What's more, a Stuxnet-like attack could be seen as justified because it will supposedly affect only the nuclear facilities engaged in developing nuclear weapons.

But South Korea has a far more advanced critical national infrastructure than North Korea. If the North picks up the code-based weapon used to attack it and uses it to retaliate, very serious damage could be caused in the South, not least in financial terms.

The threat of North Korea developing nuclear weapons is certainly frightening but it is still not even clear if it has the resources needed to do it. And even then, it knows that using a nuclear weapon against the South or anyone else would be national suicide. It is more likely to have the resources needed to re-use a cyber-weapon. South Korea could knock out a half-baked nuclear programme but what it can expect in retaliation could be far worse.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation

Citation: South Korea's cyber-war ambitions could backfire badly (2014, February 25) retrieved 3 May 2024 from https://phys.org/news/2014-02-south-korea-cyber-war-ambitions-backfire.html