1-9-2015

North Korea's attack on Sony Pictures gets the headlines, but many countries are engaged in this new war front

Erika Simpson
Western University, simpson@uwo.ca

North Korea's attack on Sony Pictures gets the headlines, but many countries are engaged in this new war front

Erika Simpson, Special to QMI Agency

Friday, January 9, 2015 4:16:09 EST PM

North Korea's border features menacing towers that warn "American capitalist pigs" to go home. Yet during my visit as part of the International Next Generation Leaders Forum, I felt safe surrounded by American soldiers, who laughed jeeringly because the threat from North Korea's 1.2-million strong army seemed farcical. The emaciated North Korean soldiers with their old-fashioned Soviet-style uniforms who guarded the truce line were a poignant reminder of under-equipped Eastern European soldiers during the Cold War.

But what we could not readily observe was that North Korea ranks in the top eight globally in terms of its cybermilitary capabilities. It surpassed Iran in 2009, according to Maj. Steve Sin, a senior analyst in the Directorate of Intelligence for U.S. Forces Korea.

It would make sense for North Korea to plan some kind of cyber-Pearl Harbour against the U.S. because any retaliatory U.S. cybercampaign would have limited reach. A full-scale cyberwar would not significantly damage such a primitive, agrarian society. Since its starved civilians, racked by famine, are not permitted to use the Internet, watch American television shows or listen to anything other than state-sponsored radio (for fear of being shot, hung or thrown into one of North Korea's notorious prison camps), only the government's elite would be affected.

Cyberweapons are cost-effective to develop and easy to copy and steal. Banning them as part of a global arms control regime could be non-enforceable.

When the STUXNET virus destroyed one-fifth of Iran's nuclear centrifuges in 2010 by causing them to tear themselves apart, it was the most sophisticated cyberweapon ever created and the first that was able to destroy physical infrastructure. The U.S. and Israel are believed to have jointly developed the software to carry out an almost undetectable attack on Iran's nuclear bomb-making ambitions, yet its code is still worming its way elsewhere around the world.

Cyberweapons could use viruses and logic bombs to paralyze computer networks. Logic bombs contain malicious code designed to be executed should certain events occur at some pre-determined time. Encryption and software that distorts cyberfingerprints and addresses ensure attackers can remain anonymous and undetectable. Viruses and bombs can lie dormant in host devices — perhaps in machinery and equipment made in South Korea or China — until globally co-ordinated commands are given to perform tasks.

NATO carried out the first cyberattacks during the Kosovo war in 1998-99 by attacking Serbian air defence systems, telecommunications and satellite infrastructure. During the Iraq War, the U.S. dismantled Iraq's communications grid, jammed its cellphone towers and attacked its satellite technology. Once unleashed, many countries including China, Iran, Libya, Russia, Syria and North Korea raced to develop their own cyberweapons.

According to a CNN interview of a North Korean defector in December, there are about 1,800 technical wizards in North Korea's cyberwarfare Unit 121, which launched the recent attack on Sony. Another defecting Unit 121 officer claimed in 2004 that North Korea was conducting cyberwarfare operations from Chilbosan, a secluded North Korean government-operated hotel in Shenyang, China.

Then in 2009, North Korea reportedly broke into the South Korean and U.S. defence departments, tested a logic bomb and caused significant damage. This led to a UN Security Council resolution barring sales of mainframe and laptop computers to North Korea.

North Korea's only close ally, China, is often accused of aiding and abetting cyberattacks and thefts. China supposedly hacked the networks of U.S. and South Korean banks, defence

ministries and intelligence communities in 2009, using equipment located in a dozen countries on three continents.

As part of an investigation after Google was attacked in 2010, it was discovered that at least 20 large companies from a wide range of businesses — including Internet, finance, technology, media and chemical sectors — were targeted by China. According to Google's official blog on Jan. 12, 2010, a primary goal of the attackers was to access the gmail accounts of Chinese human rights activists.

But according to Prof. Ron Deibert, director of the Canada Centre for Global Security Studies and the Citizen Lab at the Munk School of Global Affairs in the University of Toronto, the world's most ambitious cyberwarfare unit — U.S. Cyber Command under the command of Gen. Keith Alexander of the National Security Agency — provides a model for similar developments in other states' armed forces, who feel the need to adapt or risk being left behind.

Russia is second only to the U.S. in its cybercapability. Russia attacked Estonia's websites, including its banks, broadcasting, media and parliamentary services, in April 2007 because of a low-level diplomatic dispute. Estonia's foreign minister accused the Kremlin of direct involvement in state-sponsored cyberwarfare.

Why hasn't Russia attacked Ukraine using cyberweapons? An all-out assault that cripples Kiev's military command and control, civilian fiscal and energy systems, even its air traffic control and broadcasting could be quite feasible.

The Russia-Ukraine conflict has so far stayed at a low-level of cyberwarfare with only denial-of-service attacks on state websites by both sides in the run-up to the March referendum on the fate of Crimea. But NATO chief Jens Stoltenberg announced in December that NATO will activate four trust funds to help pay to upgrade Ukraine's logistics, cyberwarfare, and command and control systems.

Former U.S. defence secretary Leon Panetta thinks the U.S. should work with Ukraine to prepare its cyberdefences.

"We've seen (Russia) use (cyberwarfare) in Georgia. We've seen some elements of that being used in Crimea," he said, going on to call cyberattacks the "battleground of the future."

Future cyberbattles could be very costly. South Korea says North Korea has carried out six major cyberattacks on its institutions, costing the country $780 million. One attack by North Korea on South Korea's largest bank, Nonghyup, left about 30 million account holders unable to withdraw money for days in 2011.

Unlike during the Cold War, relying on deterrence strategy to prevent perpetrators from attacking by threatening mutual assured destruction will not work. It could prove impossible to threaten credible retaliation against shadowy enemies that anonymously launch attacks from somewhere in cyberspace.

Associate professor Erika Simpson teaches about international security, terrorism and global violence in the department of political science at Western University. A former NATO fellow, she is the author of the book NATO and the Bomb, and opinion pieces available on her blog erikasimpson.wordpress.com.