CYBER SECRET SOURCES FINALLY MET A SNOWDEN LEAK TO LOVE!

The NYT has a story describing the rise of the North Korean 6,000-strong hacking unit, which (the story explains) the NSA has been watching closely since 2010.

> Spurred by growing concern about North Korea's maturing capabilities, the American spy agency drilled into the Chinese networks that connect North Korea to the outside world, picked through connections in Malaysia favored by North Korean hackers and penetrated directly into the North with the help of South Korea and other American allies, according to former United States and foreign officials, computer experts later briefed on the operations and a newly disclosed N.S.A. document.
>
> A classified security agency program expanded into an ambitious effort, officials said, to place malware that could track the internal workings of many of the computers and networks used by the North's hackers, a force that South Korea's military recently said numbers roughly 6,000 people. Most are commanded by the country's main intelligence service, called the Reconnaissance General Bureau, and Bureau 121, its secretive hacking unit, with a large outpost in China.

It goes on to explain why, in spite of having beacons throughout North Korea's network, it didn't warn Sony.

> The N.S.A.'s success in getting into North Korea's systems in recent years

> should have allowed the agency to see the first “spear phishing” attacks on Sony — the use of emails that put malicious code into a computer system if an unknowing user clicks on a link — when the attacks began in early September, according to two American officials.
>
> But those attacks did not look unusual. Only in retrospect did investigators determine that the North had stolen the “credentials” of a Sony systems administrator, which allowed the hackers to roam freely inside Sony’s systems.

It even suggests that Clapper knew about North Korea’s “capabilities” even as he was having dinner with the guy in charge of it (though it does not say whether he knew about this hack).

> “Because of the sensitivities surrounding the effort” to win the Americans’ release, Mr. Hale said, “the D.N.I. was focused on the task and did not want to derail any progress by discussing other matters.” But he said General Clapper was acutely aware of the North’s growing capabilities.

For the moment, I’ll set aside whether this is convincing (parts of the story — such as that North Korea’s hackers trained in China and now target China) don’t add up.

But I did want to point out two things. First, NYT relies on a document liberated by Snowden to bolster its case. It’s not clear how well it actually does bolster the case: it shows the NSA piggybacking on South Korean efforts in 2007, and then setting its own beacons. It provides a different timeline and doesn’t say how extensively the US has infiltrated North Korea. In any case, though, it is a Snowden document the secret cyber sources finally love, one that backs their immediate claims.

Finally, note what else this says: this is another example where we have intelligence but aren’t using it not because of information sharing rules, but because we’re too inattentive to make use of it. This will be useful when Congress tries to pass CISPA because of Sony.