Two Fake Stories about the DPRK in November 2021

Anti-Pyongyang propaganda periodically delights the world with horror stories in the DPRK, which circulate well in the media and which now must be clarified. It happened twice in the second half of November.

On November 16, Radio Free Asia, a private non-profit news service funded by the US government, told the world the heartbreaking story that a smuggler who had smuggled copies of the Netflix series Squid Games into the country had been executed by shooting in North Korea. According to a (naturally) anonymous source, the man was traced thanks to the capture of seven high school students. The schoolboy who had bought the flash drive was sentenced to life imprisonment. The others were sentenced to five years of hard labor. Radio Free Asia's law enforcement source said that the sentencing for the series is the first case of juvenile execution since North Korea passed the “Elimination of Reactionary Thought and Culture” act in January 2021. According to the same anonymous sources and the evidence they presented in the form of a sheet of unknown text typed on a typewriter without any attribution, distributing, watching, or storing films or books from the capitalist countries of South Korea and the USA is now punishable by death.

With added drama to the original data, The Daily Mail published this fake news. A smuggler who simply imported USB sticks and memory cards with a South Korean TV series turned into a high school or college student who sold
copies to just a few people, including fellow students or simply arranged to watch together. However, "it was reported to the authorities," and searches were conducted throughout the school and nearby markets. The school principal, youth secretary, and the class teacher were dismissed. "They will certainly be sent to toil in coal mines or exiled to rural parts of the country, so other school teachers are all worrying that it could happen to them too if one of their students is also caught up in the investigation." "The residents are all trembling in fear because they will be mercilessly punished for buying or selling memory storage devices, no matter how small," said the anonymous witnesses smearing virtual tears, because "soon will blow the bloody winds of investigation and punishment."

However, since the world must be unfair, it was immediately revealed that there has been speculation that one with wealthy parents avoided punishment among the seven students arrested because his parents had bribed the authorities with $3,000. It wasn't without a philosophical debate: it turns out that the dystopian world of the game, "where losers are put to death, was clearly echoed by North Koreans living under a dictatorship." One of the characters played by actress Jung Ho-yeon, a defector from North Korea, is allegedly especially liked by the residents of the North.

Attached to the story was a survey of 200 defectors living in South Korea, in which 90% said they had used foreign media while living in the North, and 75% said they knew someone who had been punished for it.

But is it all like that? First, the border is tightly closed. If there is any movement at all, it is minimal with a quarantined infrastructure. In a situation like this, it's hard to believe a high school kid who simply went to China to get a flash drive.

Secondly, the DPRK Criminal Code is available on the Web in many languages: Articles 183 and 185 of the Code punish for viewing or selling decadent culture, but the terms are much more lenient. As for the law, so far, its text is available only on anti-Pyongyang websites in South Korea and in the "believe us, we didn't print this leaflet ourselves" mode.

Third, if the smuggler was indeed caught and executed, it was not for the flash drive but for violating "emergency anti-epidemic measures." Here, the facts of repression are confirmed by anonymous sources and articles in the DPRK media. The regular cross-border movement and sale of any items through which the virus may be transmitted could indeed be punished by death for condoning a biological attack on the country.

Fourth, and this is the most important point, since Radio Free Asia does not read North Korean content, they are unaware that the DPRK media has given the film a relatively positive review. For example, the article "About a popular television series revealing the realities of South Korean society" noted: "Through the image of a rich man, a game organizer who takes pleasure in a horrific massacre, the series presents a society in which tyranny and arbitrariness of the powerful are rampant. <...> Many South Koreans who watched the TV drama reflected on the severe economic inequality that pervades South Korea: the number of dropouts due to fierce competition for jobs, real estate, and stocks is increasing significantly in today's South Korean society.

However, this radio channel has come up with as much fake news as the famous Daily NK. Already after the squid story, it gave birth to a remarkable story together with the Daily Mail about the leather trench coat Kim was seen wearing during a recent "leadership on the ground": it turns out that this way Kim is "channeling his inner Hitler", which clearly indicates the alleged Nazi sympathies of the DPRK leader. Although Hitler did not often wear such a trench coat, Joseph Goebbels and Heinrich Himmler wore it instead, as did Joseph Stalin. It seems that no comment is needed. Moreover, although Kim was first shown on TV wearing a leather trench coat in 2019, it suddenly emerged that such trench coats were banned in the DPRK, "stating that it was disrespectful to imitate the fashion choices of the country's leader".

The second piece of trash began with a statement by Proofpoint Inc., an American enterprise security company that the Kimsuky hacker group, presumably from North Korea, has been attacking Russian scientists, foreign policy experts, and non-governmental organizations involved in various issues of engagement with North Korea. And it also sends phishing emails written on behalf of well-known experts in the Russian Federation to Korean experts.

A number of the author's colleagues confirmed the fact of the mailing, and it is a classic phishing scam: you are invited to open a document and enter your username and password from your mailbox to do so. This form is similar to the Windows popup for password-protected network resources, after which hackers retrieve the disclosed credentials.

But very recently, the author already explained to the NEO audience why Kimsuky seems suspicious to the ear: this
name might not seem unusual in English, but any Russian speaker will hear it as "Kims Bitches." The same goes for the names of other hacker groups such as Lazarus or Andariel, after which the reader should conclude that the average DPRK hacker has read not only the Bible but also the works of Tolkien. This is why there are reasonable doubts about the Korean origin of the groups.

Now let's take apart the phishing emails that "come to Russian DPRK specialists" or on behalf of Russian DPRK specialists to other recipients. If we think that we are talking about North Korean hackers in the civil service who collect some kind of data at the state's request, then attacks on Russian specialists do not make much sense. Most of them are neutral or friendly to the North, and besides, since they are few, each is widely known in Pyongyang. In addition, North Korean diplomats and officials from the Social Science Association also know the positions they hold.

Meanwhile, most phishing emails are either from addresses that don't look real or from the workplace, which is three to four years old. Representatives of other countries with no direct contact with North Korea are much more interested in knowing what Russian experts think and what information is exchanged. In addition, Russian experts on China who are not directly involved in North Korean affairs often receive such correspondence (including from "Korean experts"). For the author, this choice of goals speaks volumes.

Another curious thing. Most of all, experts from a cybersecurity company called Group-IB talked about malicious hackers from the DPRK. Its founder was recently charged with high treason.

In conclusion, the question of how a hacker attack is proved to be connected to the notorious Kimsuky is repeated. The "investigations" take this fact for granted, but the author recalls his analysis of the most frequent "evidence."

This attack uses exploits or elements of code used by hackers from the DPRK. Unique hacking software is scarce, and most use a limited set of tools. Furthermore, if such code is in the public domain, its elements could be further developed: borrowing is a common practice to save time and falsely accuse a non-participating party. In addition, the hacker market has long been industrialized. The authors of viruses and their distributors are often quite different people.

Similar software has been used in previous attacks by North Korean hackers. The programming style or chosen tactic is not a bad circumstantial clue. But it requires high volumes that allow you to guarantee that it's not a coincidence. Given that the DPRK's involvement in previous attacks might be questionable, the evidence based on "recurrence" is actually replaced by extrapolation skill. It creates a vicious circle when one "highly likely" occurrence piles upon another, but this "assumption" reservation disappears from the conclusions. And the involvement of the DPRK is cited as evidence.

"It was an IP from the DPRK." IP masquerade programs are even more widespread than hacking ones: in fact, any browser with a VPN function allows the user to pretend to be a user from another country. Yes, domestic anonymizers are easy enough to bypass and track the real IP, but there are more complicated ways.

"We have secret evidence" ("but we will not show it to you, because it is secret"). Sometimes it can mean that instead of evidence consistent with court procedures, there is evidence that seems reliable to analysts but is insufficient for the court. Or the source of the evidence or the methods of obtaining it are concealed for some reason, but the same phrase can mean statements invented from whole cloth.

"Let's put this case in a political context. The DPRK has been involved in various dirty deeds, so what stops it from committing this?" Here it is not so much about taking into account "previous crimes and bad reputation," but about forming a presupposition: if the terrible bloodthirsty Pyongyang regime can engage in cybercrime, then why not practice it? Because of this thesis, any cyber attack in the ROK is commonly attributed to North Korea if it can be considered a national security threat, and traces of other origins are not too prominent. Statements, such as ‘groups with ties to Pyongyang,’ also fall into the same category, as it is crucial to prove such a relationship. After all, simply saying ‘hackers target enemies of the DPRK’ is not evidence.

More tangible, but still circumstantial evidence includes the results of a linguistic examination. When mistakes point to the hacker’s native language or code analysis makes it possible to decide on their mode of operation, time zone, or default language choice. However, even then, there remains the possibility that ‘Russian in code’ belongs to an emigrant who has been living in the USA for ten years. In the system of political intrigue, even the logic of who benefits must be applied with caution because of the possibility of provocation.

As a result, serious evidence only emerges where the digital world meets the real world. For example, the hacker was caught right in the act, or the sources of the virus were found on his computer together with other evidence that
the attack came from there. It is often proven that the hacker received the stolen money (by tracing the transfer to an affiliated account in the payment chain, filming an ATM withdrawal, revealing the use of stolen credit card numbers, etc.), and this is how Galeb Alaumary was trapped, who claimed to have laundered money for the DPRK hackers.

In general, we would like to remind you once again that Radio Free Asia is a foreign agent. It was created as a propaganda radio to fight against communism and remains such, which is why fake news makes up a significant percentage of its content.

Konstantin Asmolov, PhD in History, leading research fellow at the Center for Korean Studies of the Institute of the Far East at the Russian Academy of Sciences, exclusively for the online magazine “New Eastern Outlook”.