Cyberattack against the DPRK: Reasons for the January 2022 Escalation?

When talking about the reasons for the end of the North Korean moratorium, global media and most pundits have disregarded one factor that could have played a key role in the DPRK leadership’s decision.

On January 14, 2022, NK News reported about North Korea’s disappearance from the Internet that lasted several hours as crucial servers inside the country were unavailable. The reasons for this failure were unclear. It could well be caused by a technical malfunction or an unexpected power outage. However, a more likely scenario, as experts think, is the North Korean servers becoming a target for an outside attack.

According to Junade Ali, a cybersecurity researcher, North Korean IT-infrastructure was possibly targeted by a DDOS-attack that caused a complete Internet shutdown. In particular, the servers of North Korean KCNA news agency and North Korean airline Air Koryo were unavailable.

According to log files collected by Ali and reviewed by NK News, North Korea’s servers and the websites hosted on them disappeared from the Internet and remained inaccessible for about four hours.

On January 26, another major DDOS-attack on North Korea’s servers led to the country going offline for more than six hours, as log files and network records reviewed by NK Pro show. All this came one day after North Korea conducted its fifth missile test.

Access to North Korean Internet resources, such as websites of KCNA, Rodong Sinmun, the Ministry of Foreign Affairs and other bodies was again effectively blocked. Websites hosted on DPRK-controlled domains are mostly unreachable because the North Korean Domain Name System (DNS) stopped reporting the routes which data
packages addressed to .kp domain are supposed to go through. Those so-called Border Gateway Protocol routes (BGP) play the decisive role.

On January 27, 2022, the third attack occurred, but it seems it did not come as a surprise; for that reason it led only to network delays. North Korean Internet server response time decreased but it did not entail the collapse of the nation’s Border Gateway Protocol (BGP) routes which direct global internet traffic.

The fourth DDoS-attack took place on January 31. Access to the websites of Rodong Sinmun and Foreign Ministry was disturbed but not completely blocked.

Of course, the author would refrain from embracing double standards claiming that those attacks against the DPRK were definitely unleashed by the US government. Just like in the case with the North Korean hackers, there is no direct evidence. However, similar attacks have taken place before, while the US leadership from time to time comes out with statements that could be read into as indirect evidence.

For one, The New York Times, a US-based newspaper, reported that in 2010 the US National Security Agency (NSA), engaged in electronic intelligence, got inside the DPRK computer networks and allegedly planted there spyware which turned out to be handy in monitoring the work of computers that the US intelligence community took interest in.

In March 2013, the North faced a full-scale electronic warfare. As a result, the Internet connection was blocked on the nation’s territory. In May 2013, International hackers’ collective Anonymous broke into a North Korean propaganda website and pledged to launch another massive cyber attack on anniversary of the beginning of the Korean War (June 25).

According to The New York Times, since 2014, the US has been conducting cyberattacks against the DPRK to undermine its nuclear and missile programs. The newspaper says that Americans gained control over some parts of the DPRK computer networks and carried out remote sabotage attacks against the adversary’s defense facilities.

In January 2015, The New York Times, citing declassified documents, reported that NSA employees, with the help from Malaysia and South Korea, broke into North Korean computer networks via the Chinese segment of the Internet and planted spyware. It is understood that due to this spyware Washington was able to accuse Pyongyang of a cyberattack against Sony Pictures.

On June 3, 2016, Russian news agency TASS reported that the DPRK is experiencing disruptions in the Internet connection, as the nation’s Internet resources were “affected by a powerful cyberattack from abroad.”

In February 2018, Russian newspaper Rossiyskaya Gazeta, citing the New York Times and Edward Snowden’s research, said that the US and South Korea tried cyberspying against the DPRK and used software to knock out of service North Korean missiles. It was alleged that the US was funneling billions of dollars in recruiting professionals and preparing an attack against North Korea while in May 2017 the CIA established a new division called Korea Mission Center, a move that some pundits saw as a solid proof pointing out that Washington was gearing up for military activities against the DPRK.

The same year, Foreign Policy, citing sources familiar with the matter, reported that the first strike against the DPRK would be digital rather than physical. The preparation included installation on the Japanese and South Korean territory of fiber cables as bridges, setting up remote bases and listening posts, where hackers may attempt to gain access to North Korean content that’s largely walled off from external connections. At the same time, Foreign Policy sources described the scope of resources aimed at cyber-counteraction of Pyongyang as unprecedented.

On August 16, 2018, The Wall Street Journal reported that US president Donald Trump signed an order reversing Obama-era policy regulating Washington’s right to deploy cyberweapons. The order was described as an “offensive step forward” by an administration official, one intended to help support US military operations.

Against such a backdrop it does not really matter who is behind the attacks — the US, allied NGOs or, let’s say, South Korean protestant sects. What matters here is the North’s response since the it has most likely clearly identified the culprit. "The first shot will be in cyberspace," cited Foreign Policy the former head of a US intelligence agency, and this quote pretty much went viral online.

And the DPRK responded to this shot.

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”.