Delegate Name: Tanvi Rawat

Country: Democratic People’s Republic of Korea

Institution: United Nations Security Council

Topic: Mitigating and assessing the dangers of cyber attacks

“One of the internet’s strength is its ability to help consumers find the right needle in a digital haystack of data.” — Jared Sandberg

The internet, despite being a platform created in the late 20th century has spiked into a much bigger ordeal with an unimaginable number of users and an incredibly vast array of services and applications. However, as users increase, so do malicious intents. Cyberattacks have grown to such an intimidating level that the identification and abolition of this issue requires international attention. Previous steps have already been taken by the UNSC, which encouraged negotiations between states to raise awareness of emerging threats posed by new technologies and highlighted the importance of counter-strategies against the malicious use of Information Technologies[[1]](https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php). In addition to this, the UN has passed numerous resolutions, such as: Resolution 55/63 (the very first one to exist!) and Resolution 64/211[[2]](https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx), which combat the criminal misuse of information technology and protect critical information infrastructures.

The Democratic People’s Republic of Korea (DPRK) is a nation with one of the world’s lowest percentages of internet penetration rates, thus giving it the advantage of fewer vulnerabilities to cybercrimes as compared to its internet-reliant adversaries[[3]](https://thesoufancenter.org/intelbrief-2024-february-22/#:~:text=With%20a%20minimal%20online%20presence,fear%20of%20equivalent%20online%20retribution.).

Out of its population of 26.07 million, fewer than 10,000 people have been able to access the international websites, with a majority of this small group belonging to foreign expats, government officials, and the country’s political elite[[4]](https://datareportal.com/reports/digital-2024-north-korea#:~:text=Internet%20use%20in%20North%20Korea%20in%202024&text=Our%20analysis%20of%20the%20available,and%20the%20country's%20political%20elite.).What the country does have is an intranet, with websites of North Korean news, cookery and innocuous topics[[5]](https://www.bbc.com/news/world-asia-30586940), which the common people can access, though they are cut off from the world wide web.

Due to this isolation from the WWW, the complete shutting down of the internet in DPRK (December 22, 2014)[[6]](https://en.wikipedia.org/wiki/Internet_in_North_Korea) went unnoticed by the common folk. The United States of America served as the prime suspect for this attack, as Mr. Obama had said that the US would respond to the attack by the DPRK on Sony "in a place and time and manner that we (the USA) choose."[[7]](https://www.bbc.com/news/world-asia-30584093). Despite the ever increasing number of cybercrimes attributed to the Democratic People’s Republic Of Korea (by the west), the regime does not publish an official cyber-strategy doctrine. The cyber strategy of DPRK is focused on the aggressive collection of information and financial data to help maintain the reputed Kim family dynasty and unify the Korean peninsula under the leadership of the supreme[[8]](https://www.recordedfuture.com/north-koreas-cyber-strategy). The state gathers information in order to better understand its adversaries perspectives and acquire technology to help in times of conflict. Financial resources are sometimes diverted to fund various activities, such as nuclear and missile programs.

The delegate of DPRK believes that in order to resolve the problem of frequently occurring cyberattacks in the world, various nations should strengthen their bonds with each other. Aiming for a goal together will only lead to more creative innovations, which can be used to protect mankind from any threat involving their much-needed technology. Information on the latest technological developments should be shared with every nation, regardless of whether it is developed, developing, or underdeveloped, so that its risks can be discussed and debated in order to ensure its security. The government should raise awareness and spread knowledge to youngsters, who have just come to learn about the internet, and also to the elderly, who may be unfamiliar with it, informing them about ongoing scams and the dangers of the cyberworld. Antivirus programmes, ad-blockers, Pop-Up blockers, etcetera, should be encouraged and provided for free. The idea of a hardware-based digital wallet[[9]](https://www.kaspersky.com/resource-center/definitions/what-is-a-hardware-wallet#:~:text=The%20most%20important%20aspect%20of,stealing%20the%20hardware%20wallet%20itself%20.) should be promoted, as they do not connect to the internet on their own, which makes them an impossible target for hackers.

**BIBLIOGRAPHY**

Link 1:

<https://www.securitycouncilreport.org/monthly-forecast/2022-02/in-hindsight-the-security-council-and-cyber-threats-an-update.php>

Link 2:

<https://www.itu.int/en/action/cybersecurity/Pages/un-resolutions.aspx>

Link 3:

<https://thesoufancenter.org/intelbrief-2024-february-22/#:~:text=With%20a%20minimal%20online%20presence,fear%20of%20equivalent%20online%20retribution>.

Link 4:

<https://datareportal.com/reports/digital-2024-north-korea#:~:text=Internet%20use%20in%20North%20Korea%20in%202024&text=Our%20analysis%20of%20the%20available,and%20the%20country's%20political%20elite>.

Link 5:

<https://www.bbc.com/news/world-asia-30586940>

Link 6:

<https://en.wikipedia.org/wiki/Internet_in_North_Korea>

Link 7:

<https://www.bbc.com/news/world-asia-30584093>

Link 8:

<https://www.recordedfuture.com/north-koreas-cyber-strategy>

Link 9:

<https://www.kaspersky.com/resource-center/definitions/what-is-a-hardware-wallet#:~:text=The%20most%20important%20aspect%20of,stealing%20the%20hardware%20wallet%20itself%20>.