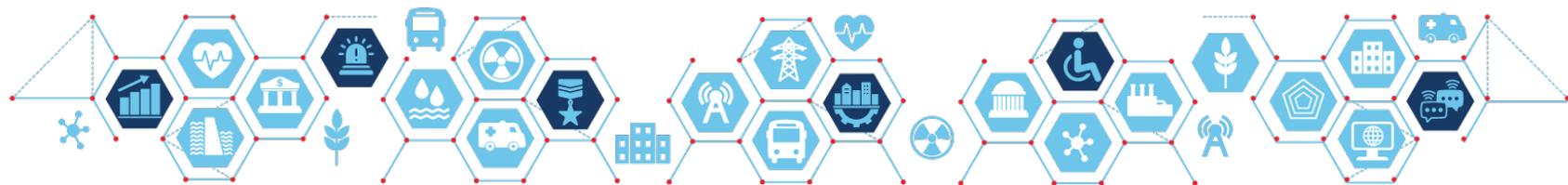


This briefing was developed for **The Blue Book Project**, lead by the Commonwealth of Virginia, support by CNA, and funded through a FEMA regional catastrophic planning grant.

Blue Book Project Goal: Develop a coordinated operational process to support local, state, federal, and private sector priorities; support Virginia residents; and ensure continuity of government while managing consequences from a coordinated nation-state cyberattack on critical lifeline services.





# The Blue Book Project

## North Korea Threat Briefing



# North Korea: A Formidable Threat



CNA

## North Korea is still at war.

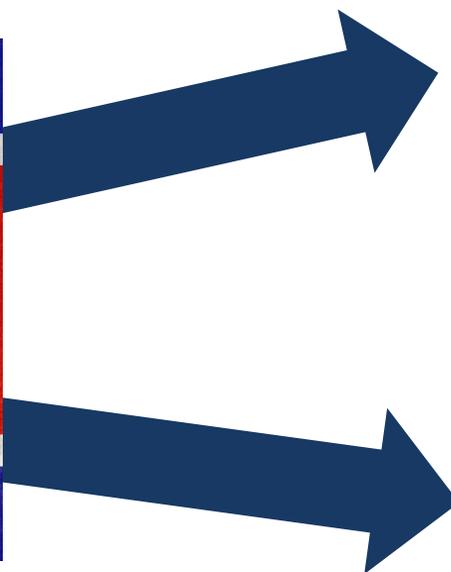
- 1.1 million soldiers
- 1000+ tanks
- 8,000+ heavy artillery
- Nuclear weapons
- 200+ ballistic missiles
- Active cyber capabilities
- Horrible human rights record



71 years after the Korean War, North Korea remains hostile to the US. It has a long history of violent behavior and maintains a massive military that includes nuclear weapons.

# North Korea Cyber: 2 Tiers of Threat

**Very Capable**



**Steady State**

**Operates from China,  
Europe, & Africa**



**Crisis**



# North Korea Steady State Threat



CNA

<b>Known threat groups</b>	<b>Andariel</b> <b>Lazurus</b> <b>Kimsuky</b> <b>Bluenoroff</b>	<b>Legitimate IT business, hacking, cyber crime</b>
<b>Likely targets</b>		<b>Generate revenue, gather intelligence, &amp; penetrate critical infrastructure</b>
<b>Known examples</b>	<b>Sony 2014</b> <b>Seoul Subway 2014</b>	<b>\$1B+ cyber theft 2022</b> <b>WannaCry ransomware</b>

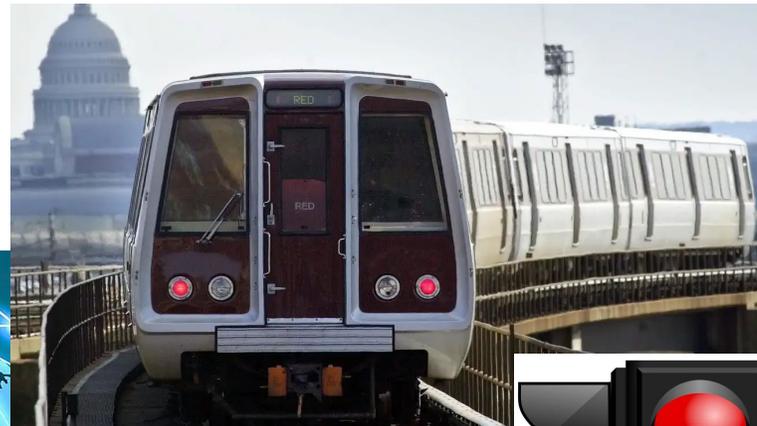
**Under “normal” circumstances, North Korea is unlikely to conduct large scale cyber attacks against critical Infrastructure**

# North Korea Crisis Threat



CNA

**In the event of a war on the Korean Peninsula, North Korea will likely employ cyber capabilities to cause confusion & damage in US**



**Virginia has numerous critical infrastructure assets that are potential targets for North Korean cyber attacks**

# North Korea use of MDM



## Miscellaneous Efforts

Primary targets are South Korea and the US

- Clear professionalization since 2020
- Targets journalists in order to influence narratives
- Social engineering, rapport-building, etc.
- State-sponsored media, multi-lingual elites, US and Chinese social media platforms
- Unexpected success on TikTok

The New York Times

**North Korean Propaganda Gets a YouTube Makeover: Fewer Parades, More Pizza**

You Tube and other social media platforms give the country an easy way to spread propaganda and push a more modern, upbeat message



# Let's Connect



CNA

**Feel Free to email us with questions**  
**[bluebookproject@vdem.virginia.gov](mailto:bluebookproject@vdem.virginia.gov)**

**Check out the Blue Book TV Reading Corner for more information and resources**

**[Reading Corner - The Blue Book Project | VDEM](#)**

