

# North Korea (DPRK) Cyber Operations Groups

[xorl.wordpress.com/2021/04/24/north-korea-dprk-cyber-operations-groups/](https://xorl.wordpress.com/2021/04/24/north-korea-dprk-cyber-operations-groups/)

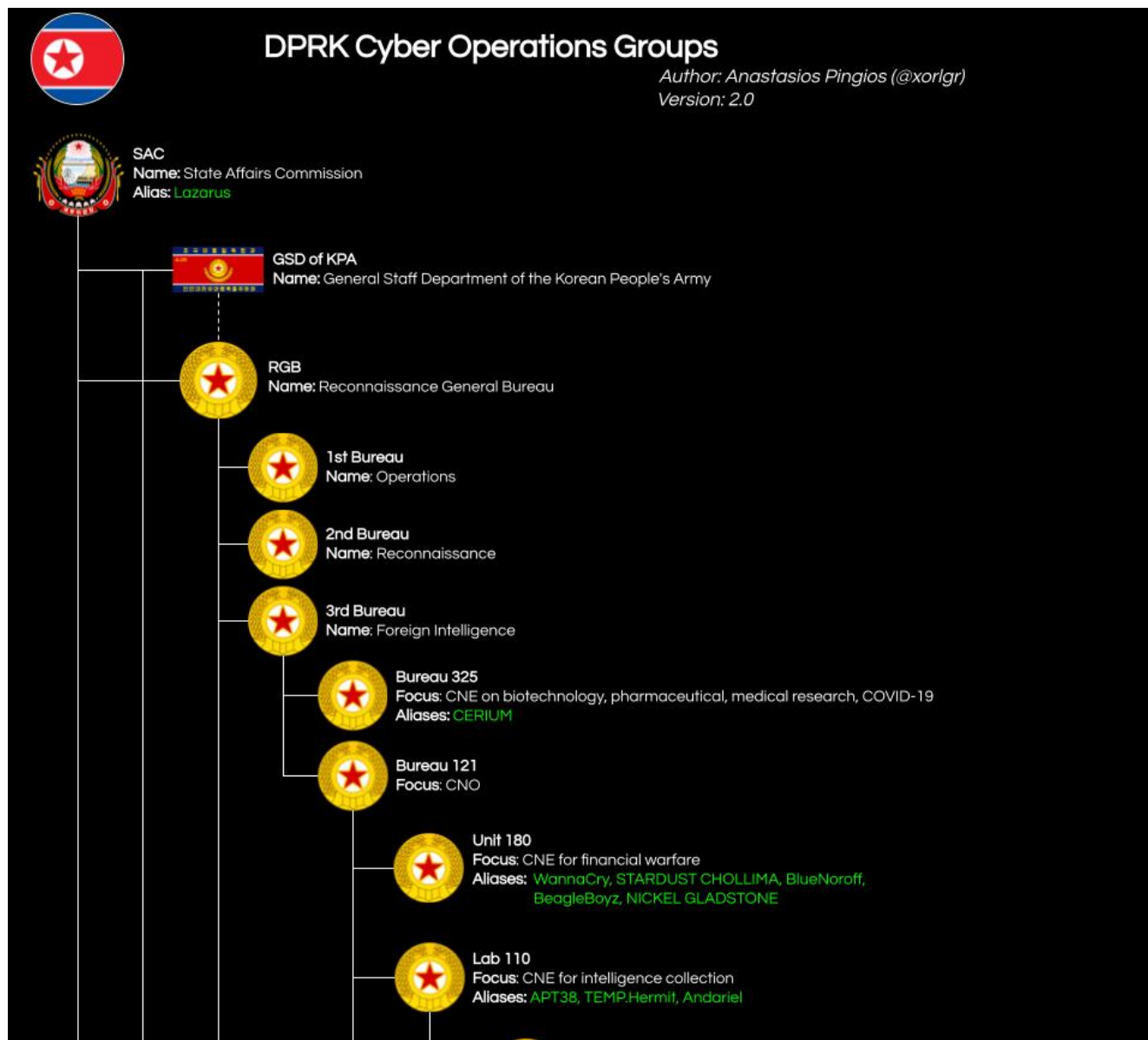
April 24, 2021

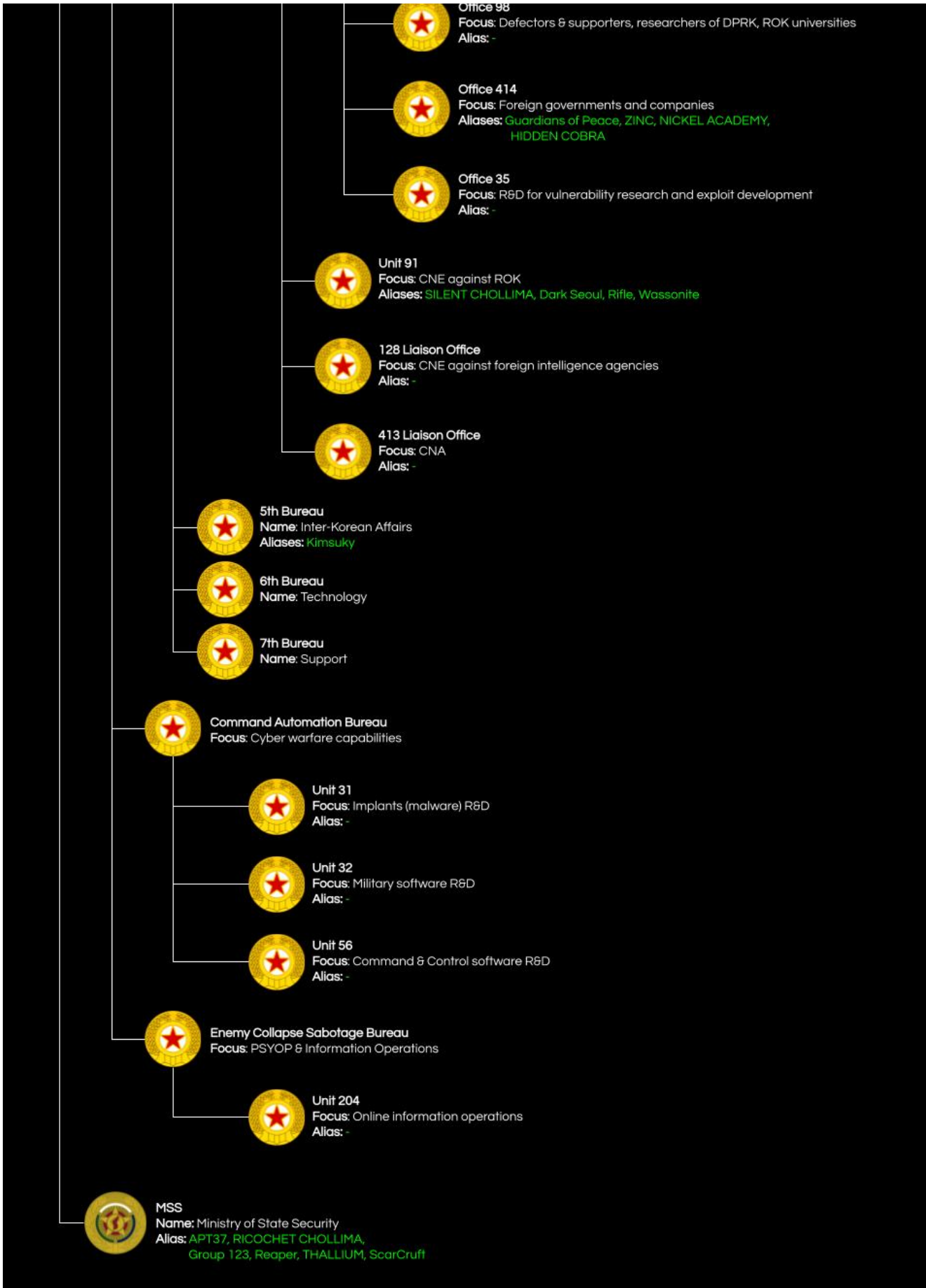
[leave a comment »](#)

After [Russia](#), [US](#) and [China](#), here is my mapping of known APT groups with (offensive) cyber operations capabilities from DPRK (commonly referred to as North Korea). As always, please let me know if you notice any mistakes, errors, or missing information since this is supposed to be a live document, updated as soon as new information becomes available.

The sources used are listed below the diagram, similarly to the other cases.

*Last update: 28 March 2022*





## Sources

---

### ChangeLog

---

- Version 2.0 (28 March 2022): Updated based on Mandiant's research.
- Version 1.5 (28 April 2021): Added Bureau 325. (credits: [@SwitHak](#))
- Version 1.0 (24 April 2021): First publication.

Written by xori

April 24, 2021 at 13:39

Posted in [threat intelligence](#)

### Leave a Reply

---

Fill in your details below or click an icon to log in:

You are commenting using your WordPress.com account. ( [Log Out](#) / [Change](#) )

You are commenting using your Twitter account. ( [Log Out](#) / [Change](#) )



You are commenting using your Facebook account. ( [Log Out](#) / [Change](#) )

[Cancel](#)

Connecting to %s