# US Cyber Operations Groups

xorl.wordpress.com/2021/04/18/us-cyber-operations-groups/

April 18, 2021

leave a comment »

My previous post on the Russian (offensive) Cyber Operations Groups became more popular than what I expected, so I decided to do something similar for other nation-state actors with multiple intelligence organizations performing offensive cyber operations. So, I picked the United States as the second one, and hopefully will continue with more of these in the future.

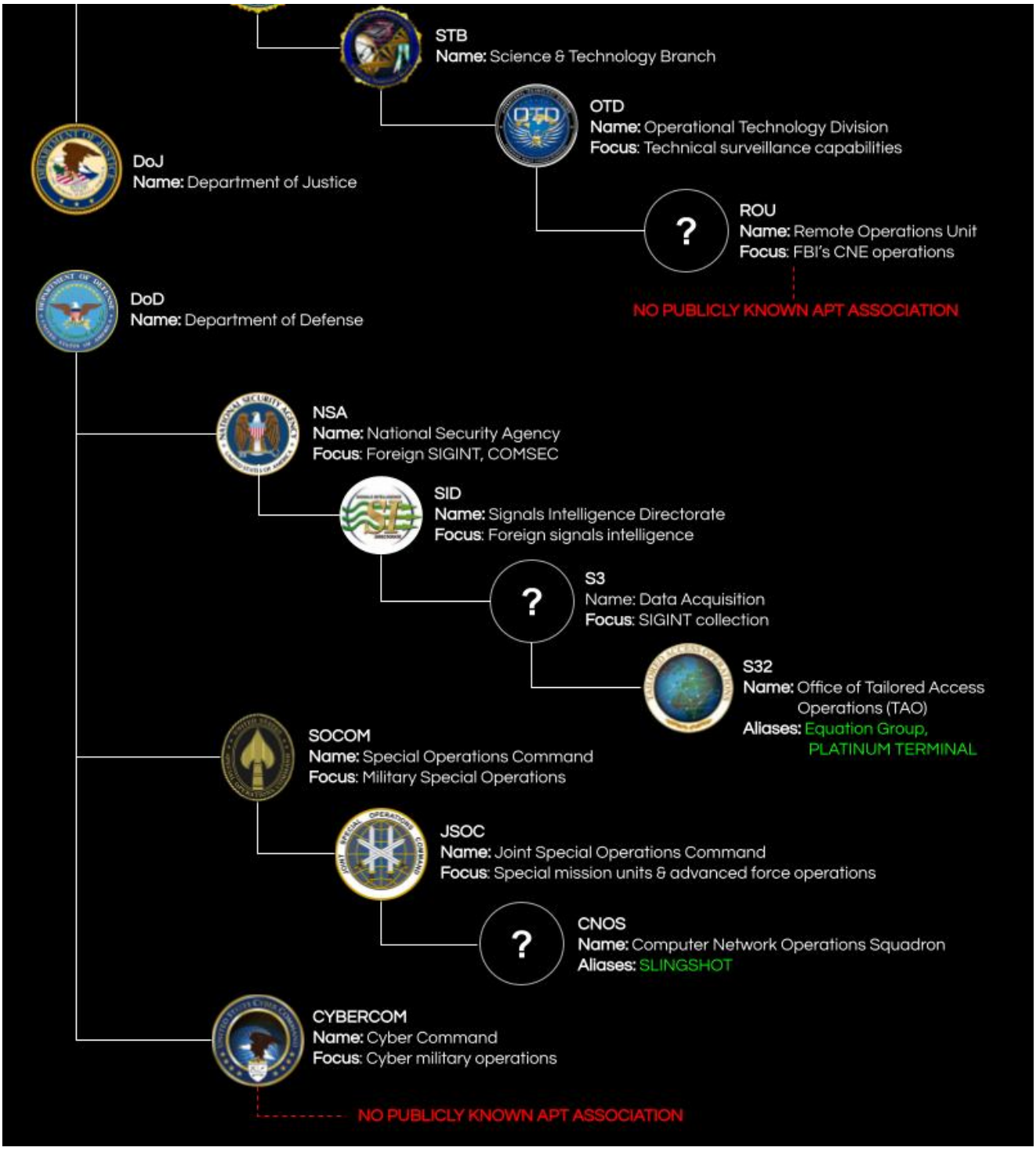
In the case of the US it was harder since there are very limited details publicly available. The main sources that I used for this one were (full list of sources used below the diagram):

- Government leaks (E. Snowden, Wikileaks, Shadow Brokers, etc.)
- Statements from government officials in reputable news outlets

You might notice that I didn't expand the CYBERCOM (which is massive) and the reason is that although it's publicly known that it now performs offensive cyber operations, there is no publicly known APT association. So, I decided to avoid making this a huge diagram for no reason. Same with the NSA that has multiple other divisions/offices performing cyber operations but there is no publicly known APT associated with them either.

I hope I got it right, but if you notice any mistakes, missing details or incorrect information please let me know to update it accordingly.

*Last update: 29 APRIL 2021*




## Sources

## ChangeLog

- Version 2.5 (29 April 2021): Kaspersky Labs correlated Lamberts with Longhorn APT group. Added it.
- Version 2.2 (23 April 2021): Add APT-C-39 to CCI and remove Vault 7 from TAO
- Version 2.0 (18 April 2021): Update SLINGSHOT attribution (thanks to Midwest and @slaeryan)

- Version 1.0 (18 April 2021): First publication.

Written by xorl

April 18, 2021 at 11:53

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