Bryan Neill
4/3/22
COM 323-1
CRW #10

How does the "surface web" compare with the "dark web" in terms of terrorism?
What is the conceptual difference between physical territory and digital territory in terms of contemporary terrorism and combatting it?

As the internet's popularity started to rise in the early 90s, so did the uses for it. Online shopping, reading information from encyclopedias, receiving email, and reading the news are the tasks that most people used the internet for in its early days. However, as it grew, criminals realized that the internet was the perfect place to conduct business anonymously.

As we know the "surface web", or the internet that is indexed by search engines and largely what we use on a daily basis, is almost impossible to stay anonymous on. With the internet so heavily policed by government agencies now, it's nearly impossible to purchase illegal goods or have the surface web help facilitate crimes in the physical world without getting caught. Therefore, many who participate in illegal activates started using the "dark web." Ironically, this is based on a technology called TOR, that was developed by the US Government. Through a network of VPNs users can browse websites that are inaccessible by a normal web browser and remain anonymous. This has made the dark web a hotbed for illegal activity such as drug and weapon sales, contracted killing, and child pornography.

Terrorist groups are also another that thrive in the dark web. With many groups such as ISIS and ISIL getting shut out of major social media platforms, the dark web allows them a place to post their manifestos and propaganda to not only radicalize others, but also to organize.

Traditional warfare has been fought over and on physical territory. Countries fighting for land, over disputes with other countries etc. But in today's digital age war is being fought online. We see a few different examples of this in the articles, one being the ability terrorist groups have had to make viral content and take over hashtags. They have even created new hashtags to help push their narratives, such as #AllEyeOnISIS. While they aren't doing anything

new, they're employing some of the same tactics that PR firms would use to push content from celebrities out to the masses.

Another type of digital warfare is information warfare, this has been mostly seen as a more nuanced effort led by powerhouses such as Russia and China. The governments of these countries have spent large amounts of money studying the internet which resulted in the creation of "troll farms." This is a job in which people maintain multiple fake online personas to push out misinformation and stir controversy. The comment on other people's posts, start discourse and post fake news to try and increase the political divide in other countries, and push whatever message their country's government wants out there. Russia has even gone so far as to create a state controlled media network, Russia Today. This network pushes out content that tends to be on the far right and is translated in many languages. By doing this Russia's intent is to have their narrative get widespread attention and be a player amongst the major world media networks.