



Virtual Nations

**Marie Murphy
Mad Scientist Initiative
09 Aug 2018
Learning in 2050
Georgetown, Washington, D.C.**





Current OE



- Virtual Nations are:
 - Cyber communities which have succeeded in gaining power, influence, or capital comparable to that of nation-states, posing a unique security threat which does not respond to traditional Army methodology and technology.
- Status today:
 - Digitalized nation-states
 - Estonia
 - Online-only organizations
 - Asgardia





Future OE



- Outlook
 - Short term
 - Long term
- Recognition
- Structure



- The current nation-state structure, elevated into the cyber domain
- Organized by personal affiliation, not geography
 - Not all are threats
- Appeal and Benefits
 - “Buyer’s Market” benefiting people and creating competition between Virtual Nations
 - Data security



Potential Threat Vectors

- Dispersion
 - Difficult to conduct physical operations in multiple, specific localities
 - Cyber power is also distributed
- Anonymity
 - Time lag in identifying an adversary
 - Find and prove who is sitting behind a screen
- Data Security
 - Use of blockchain to counter hacking
- Crowdsourcing
- Cyber Attacks and Cyber War



i-hls.com



Army Implications



- Fighting a different kind of battle
 - Dispersed, anonymous, civilian (unlawful) adversaries
 - Adversaries are part of a larger and even more dispersed group without state affiliation
 - No territory to defend
- How to manage allies
 - Some members of Virtual Nations may live in allied host countries
- Protocol for cyber war extending to the physical domain
- Doctrinal shift away from COIN





Going Forward



- How can we maintain dominance in an era of contested equality?
- Is diplomacy off the table?
- How can we track Virtual Nations, their “citizens”, and their activities?

