Essentials of GeoSpatial Intelligence (CyberGeomatics)

POC:

Dr. Michael L. Thomas

Assessment Plan:

DUE DATES

1,000 to 1,200 word mid-term paper (40%) after Lesson 4 COB

1,600 to 2,000 word final paper (40%) after Lesson 8 COB

Participation (20%) All periods

The 2018 National Cyberspace Strategy calls out by name nation-states that are deemed to be hostile to US national interests. From this strategy as a "Point of Beginning", this course examines various GEOCYBER themes and issues and focuses on the challenges presented by the Nation States named in the strategy. Aspects to be evaluated include the geographies of cyberspace, the geopolitics of cyberwar, techniques that might be employed in such a cyber domain conflict and how they are related to censorship on the Internet, ideas on regulation and network architecture, the geopolitics of censorship and hacking, cyberwar and information operations capabilities of allies and competitors, and the politics of "grassroots" activism enabled by (Cyber) Internet Communication Technologies (ICT).

Course Classification: UNCLASSIFIED

Course Objective: This course educates students on the fundamentals of why CyberGeomatics (Geographic data aspects in the Cyber Domain) is important, how data and observables are used, what products can be produced for decision making, and a look at emerging forces of change in the field in different Areas of Interest (AOIs).

This course will teach students the following concepts:

- the cyber characteristics of the 4 nation states named in the 2018 Cyber Strategy.
- the impacts of increased flow of information across the world and the risks associated with those increases
- information-related practices or capabilities U.S. allies have employed effectively, and which could the U.S. military adopt

- information-related practices or capabilities adversaries or potential adversaries have used effectively, and which of these could the US military adopt.
- adversaries practices in the information environment that the US military cannot consider doing because of ethical or legal constraints, and which of these should it be most prepared to counter

Desired Learning Outcomes:

At the end of this course, students will be able to:

1. Apply the fundamentals and principles of CyberGeomatics and classify the spatial aspects of information;
2. Interpret/uncover information operations of various nations, identifying the strengths and weaknesses of different nation's approaches to cyber and information operations. The main focus are the cyber capabilities of the named nation threats in the National Cyber Strategy;
3. Compare expectations and rights of individuals and governments related to the use of geolocation technologies, data, and privacy from various perspectives;
4. Describe ways different nations model and conduct information operations;
5. Discuss ways the DoD collects and analyzes cyber information;
6. Demonstrate the application of CyberGeomatics to cyber operations;
7. Evaluate potential GeoInt technology paths to mitigate Information blind spots;

Class Participation:

Students are expected to actively participate in class discussions and engage with other students and the lesson instructor. Students are encouraged to actively participate in class discussions. Preparation for the class discussions will be done by analyzing the listed class readings.

BOOKS: texts are available for download at the link provided.

1. Paul, Christopher, Clarke, Colin P., Schwille, Michael, Hlavka, Jakub P., Brown, Michael A., Davenport, Steven S., Porche III, Isaac R., and Harding, Joel, Lessons from Others for Future U.S. Army Operations in and Through the Information Environment. Santa Monica, CA: RAND Corporation,
2018. https://www.rand.org/pubs/research_reports/RR1925z1.html.
2. Paul, Christopher, Colin P. Clarke, Michael Schwille, Jakub P. Hlavka, Michael A. Brown, Steven S. Davenport, Isaac R. Porche III, and Joel Harding, Lessons from Others for Future U.S. Army Operations in and Through the Information Environment: Case

Studies. Santa Monica, CA: RAND Corporation, 2018. https://www.rand.org/pubs/research_reports/RR1925z2.html.

Lessons:

IP01: Explain and analyze why this topic is important, the impact of Geospatial Intelligence (GeoInt) on Cyberspace, and censorship of the Internet from the 1990s to the present.

Desired Learning Objective:

Describe the impacts of increased flow of information across the world and the risks associated with that increase. Define the role and use of Geospatial Intelligence in the Cyber domain ranging from cyberwarfare and cyberterrorism and explain the degree and impacts of Internet censorship in various parts of the world and how it is commonly measured.

IP02: Chinese Cyber/Information Warfare and Its Regional Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations in China and the impacts of such operations on its neighbors in Asia.

IP03: Russian Cyber/Information Warfare and Its Regional Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations in Russia and the impacts of such operations on its neighbors in Europe.

IP04: DPRK Cyber/Information Warfare and Its Regional Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations of the DPRK and the impacts of such operations on its neighbors in East Asia.

IP05: Iranian Cyber/Information Warfare and Its Regional Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations of Iran and the impacts of such operations on its neighbors in Middle East.

IP06: Al Qaeda's Cyber/Information Warfare Techniques and Its Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations of Al Qaeda and AQIM and the impacts of such operations globally.

IP07: ISIS Cyber/Information Warfare Techniques and Its Impacts

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations of ISIS and the impacts of such operations in the Syria AOI.

IP08: Hezbollah Cyber Capabilities

Desired Learning Objective:

Explain and analyze the policies and impacts of cyberwar/information operations of Hezbollah.