Most appealing areas would surround Investigation, Protection and Defense, and Cyberspace Intelligence.

Investigation

 -Cybercrime Investigation

 -Digital Evidence Analysis

After two years into my degree program. I’m finding Investigation job areas to be the most interesting. Specializing in Cybercrime investigations and evidence analysis is going to be my goal and focus while completing this degree. I’m a natural investigator and always believed I have a detective’s brain. This would be the perfect implementation of my natural abilities and to build on with technical skills the job requires.

Cyberspace Intelligence

-All-Source analysis

-All-Source Collection Management

My second largest interest would be in the Cyberspace Intelligence field. Working in All source collections management sounds the most appealing as it would be real life collection with the technical knowledge for attacking/targeting networks.

Protection and Defense

 -Digital Forensics

 - Incident Response

Cyberspace Effects

 -Target Network Analysis

Least appealing area would be Oversight and Governance. I see myself as more of a hands-on problem solver, I want to be the boots on the ground or in the computer Lab. Having taken some previous courses on Cybersecurity policies, it seems too much like law work or writing a law book to be honest. I find it very unappealing to just apply laws, rules and regulations to work in the Cybersecurity space.

I’ve also included some of the Task statements and Knowledge statements I found the most appealing within these fields. (On page 2).

T0193 Process Crime scene

T1090 Best methods to determine network intrusion

T1137 Investigate suspicious activity

T1192 Conduct analysis of network attacks

T1198 Identify data or intel of value

T1324 Process digital evidence

T1505 Analyze threats for counter intel

T1526 Identify parties for intrusion/crime

K0674 Network protocols

K0682 Cyber threats

K0684 threat characteristics

K0744 OS and Software

K0969 Cyber attack tools/techniques

K1139 Cyber threats/vulnerabilities

K1152 Digital evidence extraction tools/techniques