Intelligence and the Defense of Cyberspace

Intelligence and personnel requirements for intelligence support to network defense

by Capt Jessica J. Connatser

The Marine Corps is not adequately manning, training, and equipping intelligence sections charged with providing intelligence support to defensive cyberspace operations. This is because of a misapplication of human talent wherein the section is entirely comprised of 0231 Intelligence Specialists, who are ill-suited for the task they are assigned. This article will explore the necessary skills to conduct cyber threat intelligence support, describe what types of intelligence products are necessary to support various cyberspace operations at various levels of command, and will advocate for an interdisciplinary approach to building intelligence support sections with a shared additional MOS to build and retain human talent that will professionalize cyber threat intelligence in the Marine Corps—making the Service more adaptable and lethal in the cyberspace warfighting domain.

There seems to be a lack of consensus on what cyber threat intelligence is. The Director of National Intelligence defines it as:

> the collection, processing, analysis, and dissemination of information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, tactics, targets, operational activities and indicators, and their impact or potential effects on U.S. national security interests. Cyber threat intelligence also includes information on cyber threat actor information systems, infrastructure, and data; and network characterization, or insight into the components, structures, use, and vulnerabilities of foreign cyber program information systems.[1]

CrowdStrike, a commercial cybersecurity entity, defines cyber threat intelligence as:

> Threat intelligence is data that is collected, processed, and analyzed to understand a threat actor's motives, targets, and attack behaviors. Threat intelligence enables us to make faster, more informed, data-backed security decisions and change their behavior from reactive to proactive in the fight against threat actors.[2]

Though the Director of National Intelligence and CrowdStrike differ in their definitions, both describe *technical cyberspace sources* as the foundation of characterizing the threat. In order for an analyst to effectively evaluate and characterize a threat, they must have a foundational understanding of the subject in which they are analyzing. In the cyberspace warfighting domain, the analyst's foundation must be the technical data, sources, systems, and networks contained within cyberspace. The commercial cyberspace community and intelligence community both recognize the technical requirements to analyze and produce cyber threat intelligence, yet the Marine Corps has not developed this skillset within its ranks. Developing this capability requires bringing cyberspace skillsets to bear for network collection requirements, coupled with all-source intelligence analysts.

The Office of the Director of National Intelligence utilizes a unifying intelligence strategy to comprehensively bring collection and analysis to bear on issues of importance to national security. The Office of the Director of National Intelligence utilizes a unifying intelligence strategy to comprehensively bring collection and analysis to bear on issues of importance to national security. These focus areas are divided up between regional and transnational issues. There are seven regional issues—Africa, East Asia, Europe and Eurasia, Near East, South Asia, Western Hemisphere, and Iran—and there are nine transnational issue areas: counterterrorism, counterproliferation, counterintelligence, cyber, economics, military, space, technical intel, and threat finance.[3] This gives us a baseline understanding for how we tackle the functions of intelligence

>Capt Connatser is currently serving as the Intelligence Officer at Marine Corps Cyberspace Operations Group. The Marine Corps Cyberspace Operations Group is the Service's sole cybersecurity service provider and is charged with the secure, operate, and defend mission for the Marine Corps Enterprise Network. She previously served in numerous billets throughout 3d MAW and deployed with SPMAGTF-CR-CC 18.2.

analysis: analysts are versed in either a geographic area, which can be broken down further into country-specific focus (China, Russia, etc), or they are versed in transnational issues like counterterrorism or, notably, cyber. The three intelligence agencies responsible for all-source intelligence analysis, the Central Intelligence Agency, Defense Intelligence Agency, and the Bureau of Intelligence and Research at the State Department, provide ample insight into the hiring and training of analysts.

Analysts are hired into topic-specific analytic positions, such as: cyber analyst: economic analyst; leadership analyst; military analyst; political analyst; or science, technology, and weapons analyst. The requirements for these analytic positions require a degree/background in the topic area. (Economic analyst requires a degree in economics, technology requires an engineering degree, cyber requires cybersecurity or cyber operations, etc).[4] This means the Agency will teach new hires the analytic methodologies, building on the base of knowledge the analyst will bring to bear. Junior intelligence Marines have the daunting task of developing both analytic tradecraft skills and a knowledge base for their assigned unit or billet. 0231's conducting analysis at an infantry battalion must build upon their analytic tradecraft taught at the entry-level schoolhouse while also developing understanding of friendly and enemy infantry unit capabilities, such as armored troop carriers and learning their armor thickness, small and medium arms weapons and their employment, and the cultural and doctrinal employment methods of adversaries like China and Russia. If we understand analysis to be a methodology used to understand a threat problem-set that the analyst understands, it immediately becomes clear that a foundational knowledge of a topic is essential for conducting analysis.

Cyberspace was designated as the fifth domain of warfare in 2010.[5] The U.S. military now engages in military operations on land, sea, in the air, space, and now cyberspace. If we understand intelligence analysis is conducted on topics or geographic areas, military intelligence analysis should be understood to focus on transnational military threat topics and geographic areas within these warfare domains. The Navy focuses on the sea domain and its premiere maritime threat intelligence agency is the Office of Naval Intelligence.[6] The Army and Air Force respectively focus on land and air domains with the National Ground Intelligence Center and the National Air and Space Intelligence Center, respectively.[7] Each domain has unique threat systems with differing tactics, techniques, and procedures that require dedicated intelligence professional competency to evaluate the threat and relate it to the capabilities of friendly systems and forces within that domain. The air domain has aircraft, surface-to-air missile systems, varying capabilities for multiple generations of systems, and systems of command and control and tactics, techniques, and procedures for engagement unique to various adversary countries.

Within the Marine Corps, we have dedicated intelligence analytic competency to the air and land domains to support MAW units and various ground units within the MLGs and Marine divisions. Our Marines receive extra professional competency training in these domains through attending Weapons Tactics Instructor School, where students are awarded the 0277 additional MOS, and through the Intelligence Tactics Instructor (ITI) course, which awards the 0233 additional MOS (AMOS). We have not yet developed professional competency in the cyberspace domain of warfare. Addressing this gap will require both the intelligence and cyberspace occupational fields to work in tandem to support intelligence analysis and intelligence operations in cyberspace.

There are key distinctions in the cyberspace domain as compared to the other domains of warfare, which necessitate the development of technical cyberspace expertise for intelligence personnel assigned to cyberspace units. The first distinction is the cyberspace environment, or battlespace, itself. Intelligence personnel must have intimate knowledge of the operating environment, yet 0231 Marines are not trained in cyberspace. Entry-level training develops the 0231's ability to understand the difference between a T72 (tank) and a Boyevaya Mashina Pekhoty (BMP/ Infantry Fighting Vehicle) and apply their understanding of the BMP's capabilities and limitations to the threat characterization of the enemy in the intelligence preparation of the battlespace planning process. They are not taught the difference between a router and a switch, the purpose of a Domain Controller, nor the purpose of the Domain Name System. Our current method of training and employment of 0231 Marines assigned to cyberspace units is backwards from the foundational model of teaching analytic tradecraft on top of an area of intelligence focus. Instead, they are taught entry-level analytic tradecraft in the schoolhouse and are then assigned to cyberspace units per the needs of the Marine Corps wherein they must learn cyberspace-specific skills. Current training for 0231 Marines assigned to the Marine Corps Cyberspace Operations Group and other defensive cyberspace units includes having those Marines acquire Sec+ certification, attend training courses at the Defense Cyber Investigations Training Academy, and other various cyber-specific certification and training events. This training develops foundational knowledge of cyberspace

Marines assigned to the Marine Corps Cyberspace Operations Group … includes … Sec+ certification … training courses at the Defense Cyber Investigations Training Academy, and other … cyber-specific certification and training events.

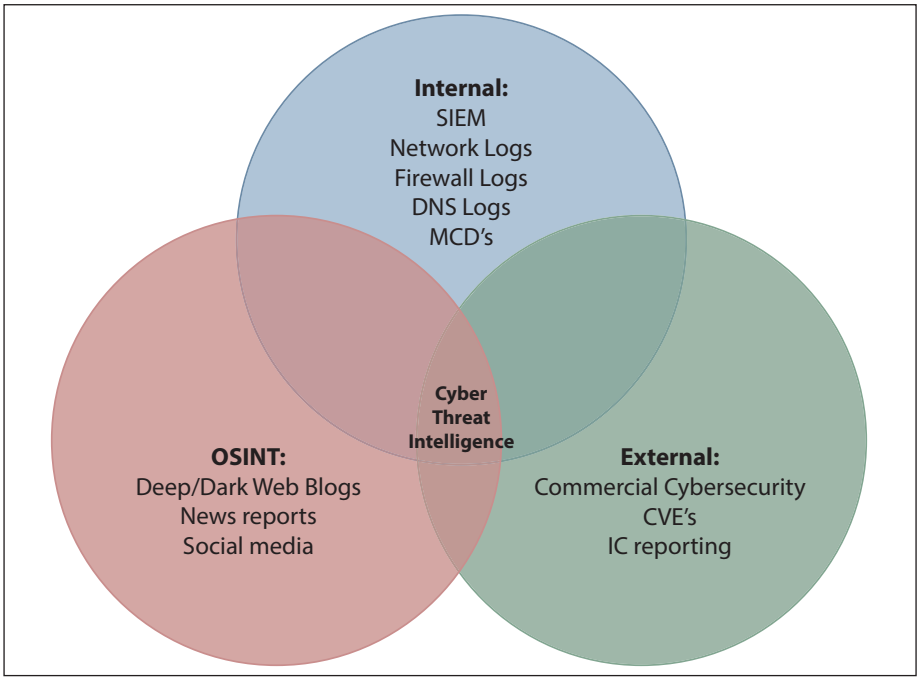

Figure 1. *(Figure provided by author.)*

terrain, terms, and capabilities which are essential for being able to support the development of cyber intelligence. This is an excessive amount of training to ask of a junior Marine—or anyone for that matter—to develop an entire knowledge base outside of their primary MOS. The acquisition of these certifications and the pursuit of cyberspace skills results in the atrophy of their fundamental MOS skill sets as outlined in their *MOS Manual* and the individual training and readiness events they are charged with demonstrably executing. The allocation of the right mix of human talent is essential to developing intelligence in the cyberspace environment.

Cyberspace threat intelligence is less reliant on traditional intelligence sources. Traditional intelligence collection platforms collect intelligence within various intelligence disciplines. Human intelligence, signals intelligence, measurement and signature intelligence, geospatial intelligence, imagery intelligence, and open-source intelligence (OSINT) are all used together to collect on areas of interest in the *physical* warfighting domains. It is not controversial to say some intelligence disciplines, like geospatial intelligence, have limited applicability in the cyberspace environment, especially in the defensive environment. Within the cyberspace domain, there are essentially two categories for sources of intelligence: internal threat network intelligence and external threat network intelligence. External threat intelligence can be divided in two subsections that address OSINT and commercial and intelligence community reports. Figure 1 provides a graphical depiction of how these sources relate together.

Internal threat intelligence requires information technology organizations to source and analyze data from their network(s) inside the DOD Information Networks (DODIN) boundaries, commonly referred to as blue space. Each federal agency and Service in the armed forces operate and maintain their own networks within the DODIN, creating adjacent sources and entities within blue space. The sources for internal threat intelligence for the Marine Corps come from the Marine Corps' primary information network—the Marine Corps Enterprise Network (MCEN). The sources of MCEN internal threat intelligence are the security information and event management software, Domain Name Systems logs, firewall logs, Marine Collection Database investigations, and other sources as the MCEN adapts and implements new technologies.

External intelligence sources are the more traditional sources of intelligence with the addition of the rapidly expanding commercial cybersecurity sector that collects and produces cyberspace intelligence from grey space reporting. Grey space is the commercial internet outside of the boundaries of the DODIN. OSINT is where analysts can collect within the deep and dark web and gain access to malicious cyber actors selling cyber tools, discussing intentions, and discover stolen Marine Corps credentials. Red space is defined as the adversary's networks. Intelligence from within red space will come from traditional technical intelligence sources, like signals intelligence, in the form of

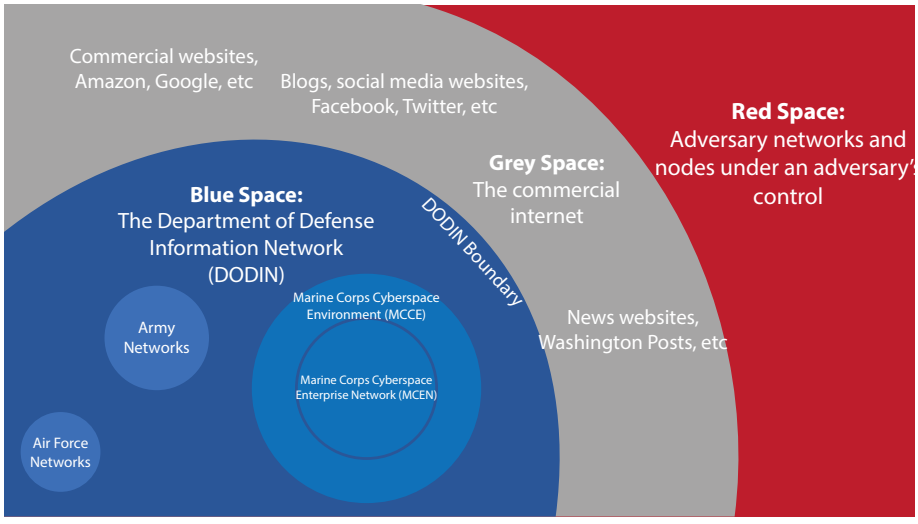

Figure 2. *(Figure provided by author.)*

reporting from the intelligence community agencies. Understanding these sources of cyber threat intelligence allows us to align specific techniques to the collection and analysis of cyber threat intelligence. A graphical depiction of the cyberspace domain of warfare is depicted in Figure 2.

The most challenging mindset shift for intelligence to support defensive cyberspace operations and the secure, operate, and defend mission requires all personnel to understand that the blue force network, or the Marine Corps Cyberspace Environment network sensors are a collection asset. It is counterintuitive to think of any blue terrain, or friendly terrain, as the area requiring intelligence collection. However, when it comes to deriving intelligence of value, the defended network itself is the primary source of critical intelligence because it contains the adversary's activity.

Reducing the burden of developing cyber specific skills in 0231s can be accomplished through employing the currently existing MOS of 1721 Defensive Cyberspace Operator or the newly developing 1731 Marine in intelligence sections, who bring foundational cyber knowledge to bear; 1721 training and readiness events have an intelligence flavor that suit the conduct of intelligence support. These events include: 1003: conduct forensic analysis; 1005: conduct system research; 2002: identify potential compromise; 2003: analyze system architecture; 2004: identify anomalous network behavior; and 2005: conduct risk analysis.[8] These 1000- and 2000-level events are skillsets the 1721 Marine would immediately be able to bring to bear to the intelligence section upon assignment. These specific skills are necessary for the conduct of intelligence support to defensive cyberspace operations in a multidiscipline fashion. Partnering 0231's with 17XX's creates a multi-disciplinary intelligence section that leverages the cyber skillsets of the 17XX and the analytic tradecraft skillsets of the 0231 to develop cyber intelligence in support of cyberspace units with the secure, operate, and defend mission.

Employing 17XX's in an intelligence section allows them to bring their expertise of blue-force capabilities, cyber weapons, and understanding of networks to the intelligence section. 17XX's can play many roles in the intelligence section. The primary function will be to conduct collection operations using network sensors and creating intelligence reports from this data. Intelligence reports derived from the data acquired by network sensors will characterize network activity, looking for anomalous behaviors and events. 17XX's can also characterize threats from community reporting. There are thousands of cyber intelligence threat reports from commercial vendors, but quickly discerning which reports are applicable to the defended network is the most important part of the process of producing meaningful and actionable intelligence. For example, a report about Iran using destructive malware on Saudi Arabia is of intelligence value. A 17XX can quickly characterize that threat in relation to the blue force network through understanding what aspects of that malware are blocked at various DODIN boundaries or firewalls, and which are not, and how the blue-force network may be vulnerable to that threat. The 0231 can then leverage their analytic skillsets to combine network event data with intelligence community reporting and fusing it with their understanding of adversary capabilities and intent in order to develop the most likely and most dangerous courses of action. This framework is not meant to absolve 0231s of developing cyber knowledge and skills entirely. 0231s absolutely must learn cyberweapons, capabilities, and have a basic competency in networks while they are serving in a cyberspace billet. The employment of 17XXs in the intelligence section rather allows the intelligence to be more technical, more network-specific, and enhanced in understanding of the threats posed to the defended network.

The proposed employment model seeks to recognize the cyberspace occupational field is not yet at full capacity and is low on manpower. It also seeks to recognize that not all 17XXs possess the same knowledge set, in the same way it acknowledges not all 0231s possesses the same analytic competencies. The 0231 community is also being pulled in myriad directions, and professionally developing them and employing them in roles within their skillsets is essential for the health and retention of the community. To optimally employ both 17XXs and 0231s, the forthcoming model seeks to provide commanders greater flexibility while enhancing the Marine's skillsets and expertise. These billets would be filled for one year and would be sourced internally on a rotational basis within the command. The rotational basis with one year in the billet (or less, based on the commander's needs) allows the 17XXs to develop the network-specific knowledge of their unit that is required to optimally understand it and subsequently defend it. Further, a "tour" in the intelligence section professionalizes the 17XX by imbuing them with threat expertise that they would not get otherwise. The goal is to enhance each Marine's career and professional development, and a tour in the intelligence section would allow 17XXs to become familiar with threat trends, adversary cyberweapons, and increase basic knowledge and understanding of the adversary. Pilots develop expertise on threats to their aircraft through briefing requirements for various flights and qualifications. Infantry Marines develop competency in adversary tactics through professional reading and military education. Defensive Cyberspace Operators, 1721, currently do not have a professional requirement for education in the adversary's threat capabilities they are expected to defend

Defensive cyberspace operators … currently do not have a professional requirement for education in the adversary's threat capabilities …

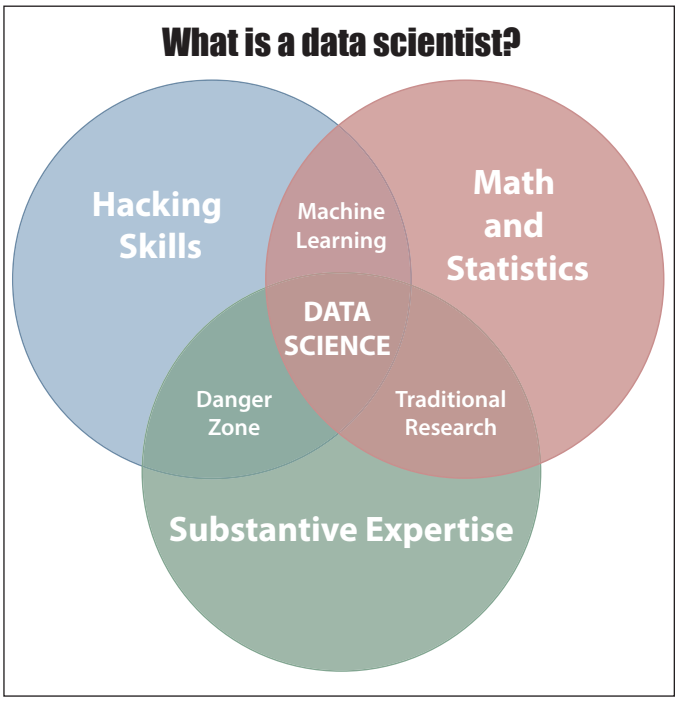

Figure 3. *(Figure provided by author.)*

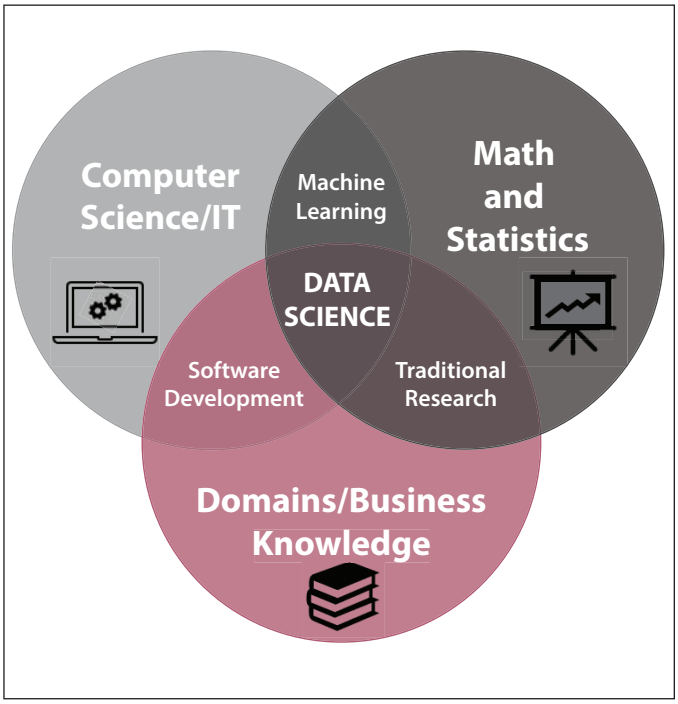

Figure 4. *(Figure provided by author.)*

against. Employment in the intelligence section can bridge that knowledge gap. A tour in the intelligence section should result in the awarding of an additional AMOS, such as 0217, Cyber Threat Intelligence Analyst, to allow the Marine Corps occupational fields responsible managing talent and personnel to see how many Marines have developed cyber intelligence skillsets and knowledge. Until a formal MOS producing school is created, the 0217 AMOS would be awarded after a one-year tour in the intelligence section for both 17XX Marines and 0231s. The AMOS allows for the monitoring of population skill and potential follow-on assignment to Marine cyberspace units or joint cyberspace billets. This experience should be recognized by the wider Marine Corps community on promotion and selection boards, so the Marine Corps is able to appropriately manage and develop technical talent within the ranks.

The Marine Corps is developing the 2652, Intelligence Data Engineer, who will be trained in data science tradecraft. This occupational specialty is essential to meet the demands of aggregating and synthesizing voluminous amounts of data in order to sense and make sense of otherwise imperceptible pieces of data. Data science is defined as "an inter-disciplinary field that uses scientific methods, processes, algorithms, and systems to extract knowledge and insights from many structural and unstructured data."[9] A data scientist's skills are outlined in Figures 3 and 4.

As we can see in Figures 3 and 4, data scientists possess the mix of cyber and analytic skills that are essential for trending cyber incidents on the network that can then be correlated against intelligence community reporting to discern potential malicious cyber actor activity against the MCEN.[10] As our network software and sensors develop, it will not be sufficient to simply send this data from the sensor operators to the intelligence section as part of staff coordination. The intelligence section must have access to the sensors and must be able to make sense and aggregate data in order to support sensor operators with incident responses with fused intelligence. Employing a data scientist at the enterprise level within the intelligence section will enhance intelligence production that is specific to the supported command and will generate *network specific* intelligence.

The Marine Corps is developing the 2652 Intelligence Data Engineer who will be trained in data science tradecraft. This occupational specialty is essential … to sense and make sense of otherwise imperceptible pieces of data.

The size of the intelligence section will vary with the mission of the unit they are supporting. Tactical-level operations require tailored technical support. For example, hunt missions need technical intelligence of advanced persistent threat in the form of the signatures of their malware and various exploit tools are essential for finding the adversary. At the enterprise level, intel-

ligence support ranges from situational awareness of threat actors and recent events that affect network hardening decisionmaking to supporting specific operations ranging from DCO web assessment missions to prioritizing patching vulnerabilities in DODIN operations. Mission enhancement, professional development, and career enhancement are the goals of this manning proposal. Figure 3 depicts the proposed structure of the intelligence sections at the Marine Corps Cyberspace Operations Group and subordinate units charged with conducting DCO missions.

Generating better intelligence support is essential to meet the demanding needs of the information environment during great power competition. At the end of 2020, Russia conducted the greatest cyberattack on American government networks and infrastructure in history via the SolarWinds intrusion.[11] The analysis of this event is still ongoing, and it will likely take months to years to fully assess the damage. The assumption moving forward should be that compromises shall continue and will only grow more lethal in tradecraft that is harder to detect. The solution to the commander's requirement for cyber threat intelligence is the employment of 17XX's alongside 0231s to appropriately provide the technical and analytical tradecraft requirements. Intelligence sections must take an interdisciplinary, fusion approach, and no longer task only 0231s with meeting the challenge at the group level and below. Mixing professional skills focused on the cyber threat intelligence problem will enhance threat assessment and intelligence collection in support of cyberspace operations. The 1721 or 1731 Marines who serve intelligence tours in cyberspace units must be recognized with the 0217 AMOS, which enables the Service to track their progression for follow-on assignment throughout the cyberspace community. Additionally, 0231 Marines serving in cyberspace units should earn the 0217 AMOS to track their progression as well. This talent management is essential for developing and professionalizing the intelligence and cyberspace forces who are meeting the realtime challenges in the cyberspace domain. This will enable MARFORCYBER, the fleet operating forces, and the Marine Corps as a Service to leverage technically trained, developed, and experienced intelligence and cyberspace personnel in a multidomain warfare environment. The threat grows and adapts daily, and it is imperative that we adjust our personnel management and employment to meet the challenges we will continue to face.

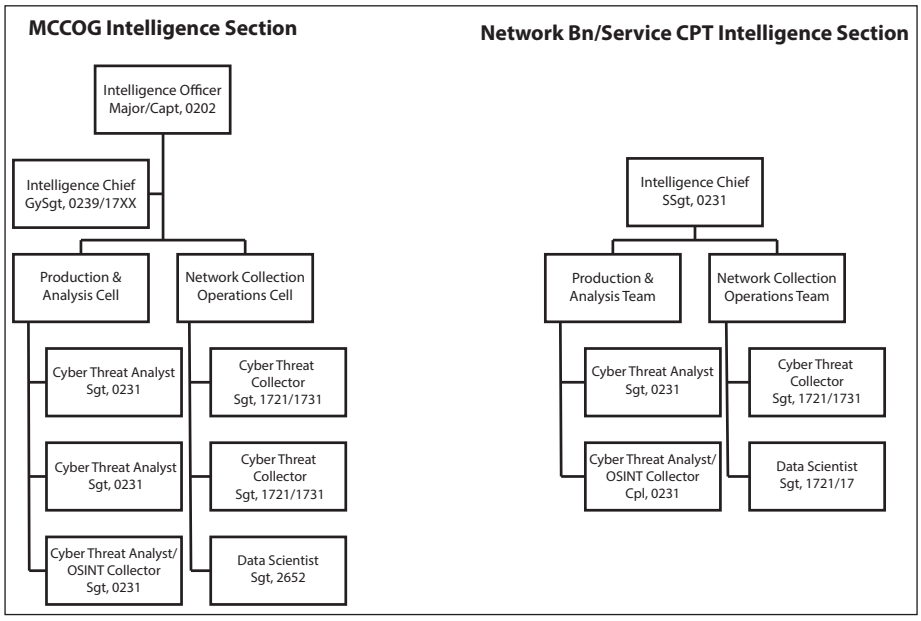

Figure 5. *(Figure provided by author.)*

Notes

1. Office of the Director of National Intelligence, *National Intelligence Strategy 2019*, (Washington, DC: 2019).

2. Kurt Baker, "What is Cyber Threat Intelligence?" *CrowdStrike*, (July 2019), available at https://www.crowdstrike.com.

3. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed., (Washington, DC: CQ Press, 2017).

4. Staff, "Analytic Positions," Central Intelligence Agency, (September 2020), available at https://www.cia.gov.

5. Lesley Seebeck, "Why the Fifth Domain Is Different," *The Strategist*, (September 2019), available at https://www.aspistrategist.org.

6. Staff, "Our Mission," Office of Naval Intelligence, (n.d.), available at https://www.oni.navy.mil.

7. Office of the Director of National Intelligence, *Intelligence Consumers Guide*, (2009), https://www.dni.gov.

8. Headquarters Marine Corps, *NAVMC 3500.124, Cyberspace Training and Readiness Manual*, (Washington, DC: 2018).

9. Jeff Leek, "The Key Word in 'Data Science' Is Not Data, It Is Science," *Simply Statistics*, (December 2013), available https://simplystatistics.org.

10. Chairman of the Joint Chiefs Staff, "Cyber Incident Handling Program," (Washington, DC: December 2014).

11. Ellen Nakashima, "U.S. Intelligence Community Says Russia Is Behind Major Cyberhacks Of Federal Agencies," *Washington Post*, (January 2021), available at https://www.washingtonpost.com.