

**All-Source Analyst**

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

**Category:** Analyze

**Specialty Area:** All-Source Analysis

# Knowledge

K0001:	Knowledge of computer networking concepts and protocols, and network security methodologies.
K0002:	Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).
K0003:	Knowledge of laws, regulations, policies, and ethics as they relate to cybersecurity and privacy.
K0004:	Knowledge of cybersecurity and privacy principles.
K0005:	Knowledge of cyber threats and vulnerabilities.
K0006:	Knowledge of specific operational impacts of cybersecurity lapses.
K0036:	Knowledge of human-computer interaction principles.
K0058:	Knowledge of network traffic analysis methods.
K0108:	Knowledge of concepts, terminology, and operations of a wide range of communications media (computer and
K0109:	Knowledge of physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).
K0177:	Knowledge of cyber attack stages (e.g., reconnaissance, scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).
K0221:	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
K0349:	Knowledge of website types, administration, functions, and content management system (CMS).
K0357:	Knowledge of analytical constructs and their use in assessing the operational environment.
K0362:	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).
K0377:	Knowledge of classification and control markings standards, policies and procedures.
K0392:	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).
K0395:	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.).
K0405:	Knowledge of current computer-based intrusion sets.
K0409:	Knowledge of cyber intelligence/information collection capabilities and repositories.
K0410:	Knowledge of cyber laws and their effect on Cyber planning.
K0427:	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).
K0431:	Knowledge of evolving/emerging communications technologies.
K0436:	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber-attack, cyber defense), principles, capabilities, limitations, and effects.

## All-Source Analyst

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

**Category:** Analyze

**Specialty Area:** All-Source Analysis

# Knowledge

K0437:	Knowledge of general Supervisory control and data acquisition (SCADA) system components.
K0440:	Knowledge of host-based security products and how those products affect exploitation and reduce vulnerability.
K0444:	Knowledge of how Internet applications work (SMTP email, web-based email, chat clients, VOIP).
K0445:	Knowledge of how modern digital and telephony networks impact cyber operations.
K0446:	Knowledge of how modern wireless communications systems impact cyber operations.
K0449:	Knowledge of how to extract, analyze, and use metadata.
K0457:	Knowledge of intelligence confidence levels.
K0458:	Knowledge of intelligence disciplines.
K0460:	Knowledge of intelligence preparation of the environment and similar processes.
K0464:	Knowledge of intelligence support to planning, execution, and assessment.
K0465:	Knowledge of internal and external partner cyber operations capabilities and tools.
K0469:	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.
K0471:	Knowledge of Internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).
K0480:	Knowledge of malware.
K0507:	Knowledge of organization or partner exploitation of digital networks.
K0511:	Knowledge of organizational hierarchy and cyber decision-making processes.
K0516:	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.
K0533:	Knowledge of specific target identifiers, and their usage.
K0542:	Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).
K0549:	Knowledge of target vetting and validation procedures.
K0551:	Knowledge of targeting cycles.
K0556:	Knowledge of telecommunications fundamentals.
K0560:	Knowledge of the basic structure, architecture, and design of modern communication networks.
K0561:	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).
K0565:	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.

## All-Source Analyst

Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

**Category:** Analyze

**Specialty Area:** All-Source Analysis

# Knowledge

K0577:	Knowledge of the intelligence frameworks, processes, and related systems.
K0598:	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.
K0603:	Knowledge of the ways in which targets or threats use the Internet.
K0604:	Knowledge of threat and/or target systems.
K0610:	Knowledge of virtualization products (VMware, Virtual PC).
K0612:	Knowledge of what constitutes a "threat" to a network.
K0614:	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.