This chapter implements STANAG 2363

Chapter 3
OPERATIONS AND TECHNIQUES

GENERAL

Counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements of foreign organizations, persons, or international terrorist activities. See Joint Publication 1-02. This chapter identifies and focuses on CI operations and techniques as they support force protection, operations, and other military and civilian requirements.

OPERATIONS

There are two types of CI operations—special operations and general operations. Special operations involve direct or indirect engagement with FIS through human source or technical efforts. General operations are usually defensive in nature and are aimed at supporting force protection programs and formal security programs of Army commanders at all levels.

Essentially, all CI operations and activities support force protection. CI operations are not operations in the conventional combat arms sense. CI activities that do not fall under the other functional areas of investigations, collection, or analysis and production are characterized as operations. CI personnel are soldiers first. They are not equipped or trained to conduct standard military operations as a unit nor replace combat arms units, other combat support, or combat service support personnel. CI personnel support operations in peace, war, and OOTW. It is the commander's responsibility to direct execution. Once the decision to execute is made, operations will generally be carried out by combat forces. For example, in conflict, CI may identify threat collection assets that are legitimate tactical targets and recommend neutralization by appropriate artillery or air defense artillery fires.

CI information is developed through the intelligence cycle. The cycle consists of five phases: planning and directing, collecting, processing, producing, and disseminating. It is a continuous process and, even though

each phase is conducted in sequence, all phases are conducted concurrently.

CI information without proper dissemination and action is useless. It is the role of the MDCI analyst working with other CI and intelligence specialists in the analysis and control element (ACE) to analyze threat data and determine countermeasures to deny the enemy collection capabilities or other threats. CI personnel recommend countermeasures through the S2/G2/J2 to the commander.

SPECIAL OPERATIONS:

CI special operations are generally carried out under the auspices of the National Foreign Counterintelligence Program. Normally, these operations involve direct or indirect engagement of FIS through human source or technical means. CI special operations are governed by AR 381-47(S) and consist of offensive CI operations, CE projects, and defensive source programs. Normally, these operations involve engagement of a FIS. Only those agencies approved by Headquarters, Department of the Army (HQDA), in implementing classified memorandums conduct defensive source programs. Defensive source programs are designed to protect designated Army activities against confirmed HUMINT threat.

GENERAL OPERATIONS:

As stated in Chapter 2, CI general operations are essentially defensive in nature and are aimed at supporting the force protection programs and formal security programs of Army commanders at all levels. Included in general operations are—

- Advice and assistance programs.
- Technical support activities.
- Support to acquisition and SAP.
- Support to intelligence disciplines.
- Support to treaty verification.
- Support to domestic civil disturbances.
- Support to natural disaster operations.
- Support to HUMINT.

***Advice and* Assistance Programs.** Advice and assistance programs are conducted by CI teams at all levels to improve the security posture of supported organizations. These programs aid security managers in

developing or improving security plans and SOPs. This support can be programmed or unprogrammed. Advice and assistance can help identify and neutralize threats to security from FIS or others who attempt to obtain information about US Army forces, programs, and operations. They provide threat information and identify specific vulnerabilities to security beyond the capability of a security manager. Advice and assistance can include but is not limited to—

- Conduct of inspections, security planning, the resolution of security problems, or development of classification guides.
- CI surveys, technical inspections, and preconstruction technical assistance.
- SAEDA training, providing SAEDA materials, and training security managers in the SAEDA programs.
- Security investigations under AR 15-6 and AR 380-5.

Technical Support Activities. Technical support activities include TSCM, TEMPEST, polygraph, counter-surreptitious entry, and C-SIGINT (COMSEC monitoring). TSCM are specialized CI investigations governed by AR 381-14 (S). Intelligence polygraph is a technical investigative technique or tool and is governed by AR 195-6 and AR 381-20. TSCM and polygraph apply to intelligence as well as CI operations. INSCOM and the 650th MI Group conduct TSCM. INSCOM conducts intelligence polygraph. For more information on polygraph, see Section III to Appendix A.

Automated Systems Security. Automated systems security includes all of the technological safeguards and managerial procedures established and applied to computer hardware, software, and developed data. INSCOM, under the technical direction of DCSINT (DAMI-CI), operates the automatic data processing system security enhancement program (ADPSSEP). Through that program, INSCOM has evaluation teams available to visit Army, and as directed, selected DOD contractor-operated data processing facilities to advise, assist, and evaluate automated systems on aspects of automated system security. Each evaluation performed by the teams identifies to management, potential vulnerabilities of the total automated operation by analyzing areas of personnel, physical, document, communication, hardware, software, procedural, and management security. The team will provide the commander or Data Processing Activity (DPA) manager with an assessment of the vulnerabilities to the system and prescribe countermeasures which must be implemented or accounted for in the risk management program.

Support to Acquisition and SAPs. INSCOM provides CI support to research, development, test, and evaluation (RDTE); acquisition elements

through the Acquisition Systems Protection Program (ASPP); and the safeguarding of defense systems anywhere in the acquisition process as defined in DODD 5000.1. Acquisition systems protection integrates all security disciplines, CI, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver our forces uncompromised combat effectiveness over the life of the system. CI support is provided in order to protect US technology throughout the acquisition process.

SAPs usually involve military acquisition, operations, or intelligence activities. When applicable, CI support to SAPs extends to government and industrial security enhancement; DOD contractors and their facilities in coordination with DIS as appropriate; and the full range of RDTE activities, military operations, and intelligence activities for which DA is the proponent or executive agent. INSCOM is responsible for providing life cycle CI support to SAPs. See AR 380-381.

Support to Intelligence Disciplines. CI supports the collection of HUMINT, SIGINT, and IMINT. As threats are identified and located, US Army intelligence systems are used to provide early warning, situation development, and other IEW functions. By crosswalking CI information to intelligence collection and vice versa, it eliminates possible conflict and compromise and provides a value added to the total intelligence community.

Support to Treaty Verification. A security consequence of arms control is overt presence of FIS at US facilities. CI is concerned with non-treaty related activities of FIS visits to Army installations, and protecting installation activities and facilities not subject to treaty verification. CI personnel provide advice and assistance to installation commanders, and debrief Army personnel who may have come in contact with inspectors.

The On-Site Inspection Agency has overall responsibility for CI support to treaty verification. INSCOM with United States Army Forces Command (FORSCOM) support is responsible for treaty verification support within CONUS, OCONUS and all CI elements provide CI support as directed by affected unified or allied command Commanders in Chief (CINCs).

Support to Domestic Civil Disturbance. The primary CI function is to support unit force protection through close and continuous liaison with civilian law enforcement agencies (LEAs). Civilian LEAs are the primary information collectors and retention agencies.

Since military support to civilian LEAs is a law enforcement function, EO 12333 and AR 381-10 do not apply; however, DODD 5200.27, AR 380-13, and AR 381-20 do apply. Any activity by CI personnel must comply with the following:

- Prior to execution, CI support is coordinated with the task force senior intelligence officer and legal advisor, and is approved by the task force commander's designated law enforcement representative. Support should be confined to analytical and situation development activities.

- CI personnel assigned to the task force work in uniform and do not use a CI badge and credentials.

To avoid questionable or illegal activities by CI personnel participating in this type of OOTW, thorough training prior to deployment is crucial. CI personnel must understand they do not conduct any activity without prior approval, and do not collect or maintain information on US persons beyond that specifically authorized for the deployment duration.

Support to Natural Disaster Operations. Without an identifiable threat to US Army security interests, use of CI personnel is not recommended since there is no viable mission for them.

Support to HUMINT. Countering foreign HUMINT capabilities and efforts is a key part of accomplishing the CI mission. Again, the CI agent or CI team cannot do this task alone. CI is a total Army mission that relies on our ability to—

- Identify the hostile HUMINT collector.

- Neutralize or exploit the collector or deny information.

- Control our own information and indicators of operations so they are not readily accessible to foreign collectors.

- Support C-HUMINT commanders through effective and stringent adherence to physical, information, and personnel security procedures governed by Army regulations. They apply force or assets to ensure security daily. The IEW organization provides continuous and current threat information so the command can carry out its security responsibilities.

C-HUMINT Operations. C-HUMINT requires effective and aggressive offensive and defensive measures as shown in Figure 3-1. Our adversaries collect against our forces using both sophisticated and unsophisticated methods. On the battlefield we must combat all of these methods to protect our force and to ensure the success of our operations. The CI agent recommends countermeasures developed by CI analysts that the commander can take against enemy collection activities.

OFFENSIVE	DEFENSIVE
Targeting for fire and maneuver	Deception operations (OPSEC)
Counterespionage operations	Physical security
Counterreconnaissance	Information security
Countersabotage	Personnel security
Counterterrorism	
Penetration and exploitation operations	

Figure 3-1. C-HUMINT operations.

To accomplish C-HUMINT, the CI agent, individually or as part of a CI team, conducts investigations, operations, and collection. A detailed description and instructions on how to conduct investigations are included in Chapter 4 and Section I to Appendix A. Other tasks include—

- Developing, maintaining, and disseminating multidiscipline threat data and intelligence fries on organizations, locations, and individuals of CI interest. This includes insurgent and terrorist infrastructure and individuals who can assist in the CI mission.

- Performing PSIs and records checks on persons in sensitive positions and those whose loyaity is questionable. Procedures for these investigations and checks are outlined in Chapter 4 and Section VII to Appendix A.

- Educating personnel in ail fields of security. A component of this is the muitidiscipline threat briefing. Briefings can and should be tailored, both in scope and classification level. Briefings could then be used to familiarize supported commands with the nature of the multidiscipline threat posed against the command or activity.

- Searching for people who pose an intelligence collection or terrorist threat to US Forces. Should CI investigations result in identifying the location of terrorists, their apprehension is done in conjunction with civil and law enforcement authorities.

- Debriefing selected personnel (friendly and hostile) including combat patrols, aircraft pilots, or other elements which may possess information of CI interest. Individuals and types of information which may be of interest to CI personnel are identified in the paragraphs below.

- Recognizing that the circumstances of combat and CI operations in tactical areas make the tasks of the CI agent more challenging. There may be many people who are looked upon as threats to security, perhaps solely because of their presence in the combat zone.

The CI agent must conduct preliminary screening to permit concentration on those of greatest potential interest or value. The CI agent is extremely dependent on such agencies as the MP, Civil Affairs (CA) units, Defense HUMINT Services (DHS), and interrogation prisoner of war (IPW) to identify persons of CI interest. CI personnel must keep these agencies posted on individuals of CI interest and the procedures to notify CI personnel of their detention.

Such personnel are usually apprehended as they try to enter or leave a zone of operations. If they are foreign agents, they will have cover stories closely paralleling their true environments and identities. It is, therefore, necessary that CI agents know about the AO and adjacent areas as well as the intellectual, cultural, and psychological peculiarities of the population. CI agents must also develop their linguistic and interrogation skills. Individuals who may be of interest include—

- Refugees or displaced persons with knowledge of hostile or terrorist activities, intentions, locations, or sympathizers.
- Members of underground resistance organizations seeking to join friendly forces.
- Collaborators with the adversary.
- Deserters from adversary units.
- Target personalities, such as those identified on the “detain” and “of interest” lists. (See Section V to Appendix A.)
- Individuals previously holding political or civic positions of influence within the AO.
- Individuals with knowledge of the adversary force’s strategic capabilities, resources, and intentions.

CI teams of technicians, agents, interrogators, and analysts not only improve the overall effectiveness of CI efforts but also expand the scope and knowledge of both. Although CI agent personnel are not interrogators, they should be knowledgeable in these areas:

- They must be capable of expeditiously recognizing, detecting, exploiting, and reporting tactical and order of battle (OB) data.

- All members of the CI team should know which units of the opposition their unit is facing and which units are in the AO.

- The team should maintain current OB information for possible exploitation of EPW. Interrogators use any and all information about adversary disposition, strength, weaknesses, composition, training, equipment, activities, history, and personalities.

- The linguistic capabilities of interrogators.

In most cases, deployment of CI agent personnel is in rear areas rather than forward with the combat units. However, CI personnel are prepared to operate whenever and wherever indications of adversary activities require a CI effort. By the very nature of their mission, CI agents provide area
coverage and are in a position to provide valuable assistance to supported commands in countering adversary activities in those areas. Other missions of the CI team include—

- Developing civilian human source networks dispersed throughout the area which can provide timely and pertinent force protection information. See FM 34-5 (S).

- Providing security advice and assistance to critical installations and activities.

- Conducting continued briefings to MP, CA personnel, interrogators, and G2/S2 staffs on adversary intelligence activity and method of operation, as well as other threats to force protection.

- Providing assistance to and support of the continuing program of security orientation and indoctrination of all command personnel, emphasizing the SAEDA regulation.

- Recommending specific countermeasures to unit and installation commanders for enhancing security practices, including detecting behavioral patterns detrimental to the security of the command.

- Conducting evaluations and surveys on the effectiveness of security measures.

CI personnel maintain contact and conduct continuous liaison with adjacent units and staffs. Many adjacent units have a concurrent requirement to collect intelligence on the threat, insurgent, and adversary organizations. The exchange of information is a normal function of CI personnel among adjacent units and agencies. CI personnel conduct liaison with key agencies such as MP and CA. CA personnel are great sources of initial

operational, threat, and source lead information, since they are often some of the first personnel to arrive in an area. Although CA is valuable during wartime, it is even more important in OOTW.

A close working relationship and continuous coordination between CA and CI elements are essential at all levels of operation and aid in the exchange of information. CA units, which have as their primary goal the reestablishment of civil order within a troubled country, can be of great assistance in the following areas:

- The identification of a subversion, espionage, or sabotage threat to US Forces.

- Thorough contact with civilian organizations, leaders, and political enemies of the government. CA units can compile personnel rosters or identify possible adversary infiltrators for screening by CI.

- Both CA and CI personnel must continuously monitor the feelings and attitudes of the civilian population. Although CI personnel orient their monitoring mission primarily on subversion, espionage, and sabotage, they must also work with CA on programs designed to counter and neutralize a hostile threat.

- CA personnel often deal with both personnel and material which can be of assistance to CI agents. Some sources which CA personnel are likely to locate may include—

  — Civilians who were associated with our adversaries.

  — Leaders of fraternal, civic, religious, or patriotic organizations.

  — Persons employed in recreational areas.

  — Governmental documents, libraries, or archives.

  — Industrial and commercial records.

  — Technical equipment, blueprints, or plans.

- Other CA personnel are in contact with leaders of civil organizations having direct contact or support activities with the military installation or population. Civil security measures requiring close coordination between CA and CI personnel include—

  — Population and resources control.

  — Civil censorship.

— Security screening of civilian labor.

— Monitoring of suspect political groups.

— Industrial plant protection.

Coordination of efforts and the exchange of information between MP and CI agent personnel must be continuous. MP and CI agents have a mutual interest in many areas and may find themselves interfacing in a variety of circumstances. Both MP and CI elements frequently develop information which may fall into the jurisdiction of the other. The following information should be shared at the lowest practical level consistent with command policy on coordination:

- **MP Investigations.** MP investigations are concerned with the impact of crime on the war effort. They are concerned with the ties criminals might have with local leaders, political parties, labor unions, legitimate businesses, and governmental agencies. Those criminal actions and parties may extend into the subversive and sabotage arenas. Terrorism through sabotage is a criminal act and may well be a coordinated enemy effort. Both MP and CI elements can develop offensive and defensive measures to deny the enemy information and material for hostile actions.

- **MP and CI Elements.** MP and CI elements require coordination. MP and CI personnel jointly conduct raids, cordon and search operations, and apprehend persons of CI interest. See Section VI to Appendix A. They operate joint mobile and static checkpoints for either MP control purposes or CI spot-checks for infiltrators. The intelligence exchange between these two elements is critical. The exchange may be conducted formally through staff elements, or on a liaison-type basis.

C-SIGINT Operations. C-SIGINT operations, including COMSEC monitoring (see AR 380-53) conducted during peace, war, and OOTW, are performed to enhance force protection, survivability, mobility and training; provide data to identify friendly C-E vulnerabilities; provide countermeasures recommendations; and when implemented, determine if countermeasures are effective. C-SIGINT includes full identification of the threat and an integrated set of offensive and defensive actions designed to counter the threat as shown in Figure 3-2. C-SIGINT is addressed in greater detail in Appendix B.

OFFENSIVE	DEFENSIVE
Targeting for fire and maneuver	Radio OPSEC countermeasures
Electronic attack	Use of secure telephone
	Signals security (SIGSEC) procedures
	Deception operations

Figure 3-2. C-SIGINT operations.

C-SIGINT provides the commander with the knowledge to assess the risk and probable success of alternatives before a plan is implemented. C-SIGINT is a cyclic process requiring a strong analytical approach. The key is to be predictive. C-SIGINT is based on a thorough knowledge of—

- Foreign SIGINT.
- Friendly force Communications-Electronics profile.
- Foreign forces operations and plans.
- Realistic security measures that can be taken to deny information to the enemy.

The Joint COMSEC Monitoring Activity and INSCOM MI group or brigade will provide C-SIGINT operational support at all echelons as outlined in DODD 4640.6 and NACSI 4000.

Acquiring the necessary information on foreign SIGINT collectors as well as information to support maintenance of friendly communications nodes database at all echelons is, at best, difficult. Presently, we gather adversary information from the existing SIGINT and electronic warfare (EW) collection capability of the IEW force. We also gather it through electronic preparation of the battlefield based on what we know foreign SIGINT or radio electronic combat doctrine to be.

Friendly C-E patterns and signatures information are gathered by examining our technical manuals; getting anomaly emissions information from electronics maintenance personnel; and getting procedural information from operations staffs and signal command and staff personnel.

Currently, there is no dedicated capability to accurately and completely capture friendly C-E emissions in the same way our adversaries do. Our

analysis efforts attempt to make up for this shortcoming on the doctrinal portrayal of our C-E assets. At all echelons, the goals are the same:

- Force protection.
- Reliable use of the electromagnetic spectrum for friendly C^2.
- Degradation or neutralization of hostile SIGINT and radio electronic combat assets.

These goals are achieved through vigorous application of a five-step C-SIGINT process:

- Threat assessment.
- Vulnerability assessment.
- Recommendation of countermeasures options.
- Countermeasures implementation.
- Evaluation of countermeasures effectiveness.

Threat assessment must be done first if the remaining steps are to be viable. When we determine that a threat exists for a given area, the MDCI analyst assesses friendly C-E systems within that area to determine which are vulnerable to the threat. Once this has been done, the MDCI analyst develops countermeasures that will reduce or eliminate the threat, the vulnerability, or both. The commander then directs countermeasures implementation. Recommended countermeasures include—

- OPSEC (all COMSEC and electronic security measures).
- Targeting.
- Electronic attack (EA).
- Electronic deception.

The last step is evaluating the measure of success for any implemented countermeasures. This may be done by—

- COMSEC monitoring.
- Analyzing reports received.
- Analyzing air and ground operational situation reports.

Analyzing of data collected during or after countermeasures implementation.

C-IMINT Operations. C-IMINT is a total force mission that includes full identification of the adversary and an integrated set of actions to counter the threat. These actions range from offensive action to the use of OPSEC techniques and deception designed to deny adversaries information as shown in Figure 3-3.

OFFENSIVE	DEFENSIVE
Action of ADA	Deception operations
	OPSEC countermeasures
Targeting for fire and maneuver	Aerial platform tracking

Figure 3-3. C-IMINT operations.

Threat. As with all CI operations, detailed analysis of the adversary is necessary. To help protect our force from exploitation, our analysts must fully understand the adversary and its capabilities.

Any adversary may possess or acquire systems or products with a comprehensive an-d "sophisticated IMINT capability. We must have in place a carefully developed counterprogram to negate any tactical and strategic threat. An adversary or belligerent acquires IMINT information through a variety of ways from handheld cameras to sophisticated satellite reconnaissance systems. Adversary IMINT systems may include—

- Aerial cameras.
- Infrared sensors.
- Imaging radars.
- Electro-optical sensors (TV).
- Multispectral and digital imagery products.

Adversaries know that to maximize the effect of their massed fire-power and mobility, their IMINT capabilities must be accurate and timely. They know their IMINT operations will be met by our countermeasures and deception operations. For this reason, they may use diverse multisensory collection means to obtain information. Sometimes the various collection means and sensors overlap and are redundant.

Adversary commanders and staffs of all combat arms and services organize reconnaissance operations. Adversary doctrine indicates that reconnaissance is effective only if it is actively and continuously conducted under all conditions and circumstances. Continuity of action, timeliness, and accuracy of information are constantly stressed.

Tactical air reconnaissance is a good source of IMINT. Adversaries use air reconnaissance at all levels with organic or supporting manned and unmanned aviation assets.

Adversary IMINT collection efforts directed against US and allied forces vary according to weather, terrain, and the depth and density of friendly forces and their collection capabilities. Reconnaissance aircraft, in general, also carry weapons and are capable of attacking ground targets of opportunity.

C-IMINT Collection. We must view a potential adversary's use of IMINT to develop intelligence and targeting information as potentially damaging to our interests. We get information on adversary IMINT operations from many different sources:

- Enemy prisoner of war (EPW) reports.
- US Air Force reports.
- Tactical and strategic reconnaissance.
- HUMINT operations.
- SATRAN. See DIAM DJS-1400-7-85 (S).
- Air defense artillery (ADA) reports.
- SPOT reports in size, activity, location, unit, time, and equipment (SALUTE) format.
- CI threat assessments, estimates, and summaries from higher, lower, and adjacent units.
- OPSEC surveys, estimates, and assessments.

TECHNIQUES

CI techniques are means used to accomplish the mission efficiently and effectively. Selection of techniques occurs at the lowest level possible by the on-scene CI element to meet the needs of the supported military

commander within the constraints of the operation and applicable regulations. Techniques include vulnerability assessments, hostile intelligence simulation (Red Team), and covering agent support.

VULNERABILITY ASSESSMENTS:

Vulnerability assessments are studies conducted by CI personnel to provide a supported command or agency a picture of its susceptibility to foreign intelligence collection. These assessments may be conducted on a command, agency, installation, subordinate element, HQ, operation, or program and are tailored to the needs of each requestor.

The objective is to provide a supported command or agency a realistic tool with which to evaluate internal force protection or security programs, and to provide a decisionmaking aid for the enhancement of these programs. Vulnerability assessments include—

- Evaluating FIS multidiscipline intelligence collection capabilities, collection and other activities, and PIR.
- Identifying friendly activity patterns (physical and electronic), friendly physical and electronic signatures, and resulting profiles.
- Monitoring or collecting C-E transmissions to aid in vulnerability assessments, and providing a more realistic and stable basis from which to recommend countermeasures.
- Identifying vulnerabilities based upon analysis of collected information and recommendations of countermeasures.
- Analyzing the effectiveness of implemented countermeasures.

HOSTILE INTELLIGENCE SIMULATION (RED TEAM):

Upon request by a commander or program manager, CI personnel may plan and execute a simulation of a foreign intelligence penetration of a specified target, such as an installation, operation, or program. Such simulations are informally known as Red Team operations.

There is no single structure or composition for a Red Team. It is an array of MDCI resources which are selectively employed during the operation. Red Team operations include the full range of MDCI activities to include those activities formerly performed as vulnerability assessments that may be applied to replicate the FIS threat.

Red Team operations provide a supported command or agency a tool to evaluate internal force protection or security programs, and a decisionmaking aid for the enhancement of these programs. Red Team operations assist the commander or program manager and his security

staff by identifying vulnerabilities based upon analysis of the collected information and recommending countermeasures to reduce or negate those vulnerabilities.

Red Team operations should be carried out as realistically as possible in accordance with AR 381-10 and AR 381-20. Red Team operations should be conducted by the most experienced CI personnel available after thorough coordination with the unit commander and security manager. These operations require extensive preparation. A full multidiscipline Red Team operation would require support from EAC CI elements.

Commanders must ensure compliance with laws, policy, and regulations when employing COMSEC monitoring, electronic surveillance, or other technical CI collection activities as part of Red Team simulation operations.

Because of the complexity and high resource requirements, Red Team operations generally should be limited to extremely sensitive activities, such as SAPs, although Red Team operations may be useful in conjunction with major tactical exercises and deployments. For more information on Red Team operations, see AR 381-20.

Red Team proposals will be documented in an OPLAN and approved by the activity head or commander who requested the service.

Red Team findings will be used to inform and educate commanders and their security staffs on the effectiveness of their security policies and practices. CI personnel also assist the command in enacting countermeasures to any vulnerabilities detected by Red Team operation.

COVERING AGENT SUPPORT:

CI covering agent support is the technique of assigning a primary supporting special agent to a command or agency. This agent will conduct all routine liaison and advice and assistance with the supported element. It ensures detailed familiarity with the supported element's operations, personnel, security, and vulnerabilities, and in turn provides the element with a point of contact for reporting matters of actual or potential CI interest.