

HEADQUARTERS
UNITED STATES EUROPEAN COMMAND
UNIT 30400, BOX 1000
APO AE 09128

STAFF MEMORANDUM
NUMBER 40-3

19 October 2000

INTELLIGENCE

Intelligence Support to Information Operations

1. **Summary.** This Staff Memorandum (SM) delineates the Intelligence Directorate's (ECJ2) responsibilities for all aspects of intelligence and counterintelligence (CI) support to Information Operations (IO) and establishes strategy, objectives, and procedures within ECJ2 on IO as well as Information Warfare (IW).
2. **Applicability.** This SM applies to all HQ USEUCOM intelligence organizations, to include the Joint Analysis Center (JAC) at RAF Molesworth, UK, and HQ USEUCOM directorates/staff offices which deal with Theater-level Intelligence and CI activities to support Information Operations. This SM is intended to complement guidance referenced in binding directives, publications or instructions.
3. **Internal Control System.** This SM contains no internal control provisions and is not subject to the requirements of the internal management control program. For HQ USEUCOM and subordinate joint activities, the applicable internal control directive is ED 50-8, Internal Management Control Program. This document will be reviewed and updated annually by the Intelligence Directorate, Production Requirements Division, ECJ22.
4. **Suggested Improvements.** The proponent for this SM is ECJ22. Suggested improvements should be forwarded to HQ USEUCOM/ECJ22, Unit 30400, Box 1000, APO AE 09128.
5. **References.**
 - a. DoD Directive S-3600.1, Information Operations (IO), 9 December 1996.
 - b. Joint Pub 2-0, Joint Doctrine for Intelligence Support to Operations, 9 March 2000.
 - c. Joint Pub 2-01, Joint Intelligence Support to Military Operations, 20 November 1996.
 - d. Joint Pub 2-01.2, Joint Doctrine, Tactics, Techniques, and Procedures for Counterintelligence Support to Operations, 5 April 1994.

- e. Joint Pub 2-02, National Intelligence Support to Joint Operations, 28 September 1998.
- f. Joint Pub 3-13, Joint Doctrine for Information Operations, 9 October 1998.
- g. Joint Pub 3-13, Appendix A to Joint Doctrine for Information Operations, 9 October 1998 (SECRET/US Only).
- h. C4ISR Handbook for Integrated Planning (CHIP), Revised, April 1998.
- i. Contingency C4ISR Handbook for Integrated Planning, Revised, August 1998.
- j. Communications Handbook for Intelligence Planners, Appendix A: U.S. European Command Communications Systems and Networks, Revised, April 1995 (SECRET/Not Releasable to Foreign Nationals).
- k. Defense Intelligence Management Document, DI-2700-75-99, Analyst Information Requirements for Information Operations/Information Warfare, February 1999.
- l. EUCOM Intelligence Tactics, Techniques and Procedures (ITTP) for Joint and Combined Operations, 15 Dec 99.

6. **Explanation of Terms.**

- a. **Counterintelligence (CI)**. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for, or on behalf of, foreign powers, organizations, persons, or terrorist activities.
- b. **Information assurance (IA)**. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.
- c. **Information operations (IO)**. Actions taken to affect adversary information and information systems while defending one's own information and information systems.
- d. **Information superiority**. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

e. **Information warfare (IW)**. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

f. **Intelligence**.

(1) The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas.

(2) Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.

g. **Intelligence preparation of the battlespace (IPB)**. Analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presented in graphic form. Intelligence preparation of the battlespace is a continuing process.

h. **Operational Intelligence**. Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within Theaters or areas of operations. Also see paragraph 6.f.

7. **Policy**

a. Information has taken on tangible value. Nations and non-state actors have realized the potential to influence political, economic and military events through coordinated use of information via propaganda, mass media, high-capacity communications and computers, providing goods and services, and the ability to disrupt, deny, destroy, or deceive information and information systems. The Department of Defense, realizing the impact of information on the nature of warfare, has provided guidance to its military forces for the conduct of IO (references f and g).

b. Intelligence and CI support are critical to planning, executing, and assessing IO. Intelligence and CI must be timely, accurate, usable, complete, relevant, objective, and sufficiently detailed to support the wide array of Department of Defense (DOD) IO support requirements, to include research, development, acquisition and operations. Intelligence preparation of the battlespace is also vital to successful IO. Support from non-DOD and non-U.S. sources also may be required.

(1) Intelligence has the mission to monitor adversaries, identify patterns of behavior, identify vulnerabilities, warn of threats and predict hostile activity. Intelligence will focus on:

- Identifying adversary capability to threaten U.S. and Allied forces
- Identifying adversary vulnerabilities
- Immediate threat warning of hostile action
- Predicting adversary activity through trend analysis and intelligence preparation of the battlespace (IPB)
- Preparing targeting information to support physical attack, electronic warfare, psychological operations, deception, and computer network attack

(2) CI has the mission to detect, identify, assess, counter, neutralize or exploit foreign intelligence service (FIS) efforts against DoD. In providing CI support to information operations, CI will focus on the following threats:

- Insider (especially FIS-directed)
- Unauthorized users
- Malicious software
- Other (implants, theft, human error, etc.)
- Intrusions
- Vulnerabilities of authorized users
- Computer networks as a tradecraft venue
- Low-level technological or unsophisticated threats that may be encountered in force-projection operations

8. **Responsibilities - Intelligence and CI Support to IO.** Intelligence and CI support are critical in the planning, execution, and assessment of IO. Efforts must be focused in order to provide support across the full spectrum of military operations, at all levels of war.

a. The Production Requirements Division, ECJ22, acts as the central point of contact for all intelligence support to IO for the headquarters ECJ2 staff. Coordination/interaction between the Intelligence Directorate and the Information Operations Division (ECJ39) will be through an on-site representative embedded within the USEUCOM IO Cell and through an IO staff officer assigned within ECJ22.

(1) The ECJ22 IO Cell Representative will:

- (a) Coordinate the development and prioritization of IO intelligence requirements.
- (b) Identify collection requirements based on specific needs identified by the IO Cell.

- (c) Coordinate development of targeting products to support IO campaign planning.
 - (d) Assist preparation of IO portions of USEUCOM exercises and operations plans.
 - (e) Inform ECJ2 of IO planning or execution activity in order to engage appropriate ISR capabilities for targeting and impact assessment.
 - (f) Notify other headquarters ECJ2 staff elements of decisions made within the HQ USEUCOM IO Cell which have potential impact on their functional areas of responsibility.
 - (g) Provide assistance (through the IO Cell) in assessing the operational impact and recommending appropriate recovery/response actions for computer intrusions affecting USEUCOM computer infrastructures in support of the ECJ6-I DIO mission supporting IA.
 - (h) Coordinate nomination of Protected Frequencies for inclusion into the Joint Restricted Frequencies List (JRFL).
 - (i) In concert with IO Cell, Guidance, Apportionment and Targeting (GAT) Cell, Joint Requirements Management Board or other appropriate organizations, coordinate development and prioritization of IO intelligence, surveillance and reconnaissance (ISR) requirements.
 - (j) In concert with ECJ3 and ECJ6, coordinate communications security (COMSEC) monitoring support from the Joint COMSEC Monitoring Activity (JCMA), including JCMA's own force protection communications support, during operations and exercises. Identify areas of operations security concern for JCMA focus. Integrate COMSEC monitoring activities with trusted agents (psychological operations [PSYOP], deception, operations security [OPSEC] and CI functions) to enhance proactive IO efforts.
 - (k) In coordination with headquarters staff representatives, identify critical USEUCOM information resources that fall outside the USEUCOM AOR. Prepare notification messages for supporting unified commands or agencies to highlight the need to monitor and protect these critical nodes.
- (2) The ECJ22 IO staff officer will:
- (a) Coordinate IO-related ISR issues with the Joint Staff, Intelligence Community, IO Centers; e.g., Information Operations Technology Center (IOTC), Joint Information Operations Center (JIOC), Joint Warfare Analysis Center (JWAC), and the component staffs.

- (b) Coordinate IO ISR requirements with JAC, ECJ22-P and appropriate ISR agencies.
- (c) Coordinate with ECJ23-ISR the development and prioritization of ISR collection required for assessment of IO effectiveness.
- (d) Develop, coordinate, implement and exercise processes/procedures to identify precise and timely ISR target intelligence, avenues of approach for information delivery, collection requirements, impact assessment and threat analysis for IO target selection and post-strike analysis through JAC and appropriate agencies.
- (e) Coordinate preparation of threat assessments for adversary and neutral nations that possess the capability to interfere with achievement of U.S., NATO or USEUCOM policy objectives. Prioritize these threats in coordination with ECJ3 and ECJ6.
- (f) In conjunction with the Joint Staff and Intelligence Community, coordinate the development of effective Indications & Warning (I&W) policy and processes for potential/actual IO threats in support of the ECJ6-I Defensive IO (DIO) mission support to computer network defense. Review/coordinate on plans to reconstitute and restore capabilities of ISR-related communications equipment.
- (g) Coordinate procedures and training necessary to provide HQ USEUCOM and subordinate commands with appropriate indications and warning of enemy IO or IW threats.
- (h) Coordinate on USEUCOM IO policy, tactics, techniques and procedures.
- (i) Develop, coordinate, implement and exercise procedures for nominating protected frequencies for incorporation into the JRFL. The JRFL should include those frequencies being exploited by national ISR resources, as well as Theater and Tactical ISR assets, and those frequencies critical to the operation of U.S. and Allied ISR assets. Protected frequencies should not be jammed without coordinating with intelligence representatives.
- (j) Develop, coordinate and ensure inclusion of ECJ2-nominated comments into EUCOM Critical Information List.
- (k) In concert with ECJ3, ECJ6 and national support agencies, coordinate, develop and implement training to sensitize USEUCOM personnel on potential adversary information exploitation and attack techniques.
- (l) Coordinate or request CI support for IO with ECJ23-CI.

(m) Immediately notify ECJ23-CI of any indications of the involvement or suspected involvement of foreign intelligence and security services (FISS), terrorists, espionage or sabotage impacting USEUCOM information systems.

(n) Coordinate with National Agency LNOs and ECJ25-S to identify and prioritize Intelligence Systems.

(o) Review National Agency and USEUCOM plans for reconstitution and restoration of critical ISR systems. Where none exist, identify requirements for these plans to the appropriate agency.

(3) The Force Application Branch, ECJ22-T, will provide targeting support, including support to Offensive IO and IW in accordance with EUCOM target architecture.

b. The Operations Division, ECJ23, acts as the central point of contact for all ISR and HUMINT collection support to IO for the ECJ2 staff. The Counterintelligence Branch, ECJ23-CI, acts as the central point of contact for all Theater CI support to IO within the ECJ2 staff and will provide a CI representative to the IO cell when requested by ECJ39. The Intelligence Operations Branch, ECJ23-O, conducts Deliberate and Crisis Action planning, and oversees deployed intelligence support functions.

c. The Plans Division, ECJ25, acts as the central point of contact for all intelligence planning support to IO for the ECJ2 staff. ECJ25 will:

(1) Integrate Theater intelligence support to IO into strategies and architectures.

(2) Plan, program, and budget for intelligence support to IO.

(3) Coordinate installation of IO-related C4ISR systems.

(4) Articulate Theater ISR shortfalls in support of IO through appropriate planning channels to Joint Staff, JROC, Congress, and national Agencies.

d. The Joint Analysis Center (JAC), RAF Molesworth, UK, will provide tailored intelligence for IO planning, execution and combat assessment, with increasing requirements to provide specialized IO support products to both CINC-level decision makers and JTF-level planners. The JAC will, in conjunction with the Joint Staff, J39, and key IO cells within the intelligence community, coordinate the development of effective Theater Indications & Warning (I&W) for potential/actual IO threats. The JAC will also leverage targeting, analytical and ISR management capabilities against Theater IO problem sets, as follows:

(1) Update the USEUCOM IO Cell on JAC IO indicators and warning status via collaborative exchanges between the USEUCOM Intelligence Operation Center, watch centers at the JAC, SHAPE and Theater components, or with individual analysts.

(2) Provide ISR asset management support to Senior Intelligence Officer (SIO) through proactive collection management IO profiles in conjunction with the IO Cell.

(3) Provide kinetic/non-kinetic targeting nominations for Theater IO targeting campaigns or special capabilities operations in conjunction with ECJ22-T and the IO Cell. Accomplish IO Battle Damage Assessment.

(4) Provide preliminary and follow-up analytical assessment of Theater adversary IO centers of gravity, leadership and vulnerabilities in conjunction with national entities. Accomplish IO IPB.

(5) The JAC Operations Division, JAC/DOO, will have the lead to document, generate and disseminate appropriate responses to IO Requests for Information in conjunction with the HQ USEUCOM/IO Cell.

(6) Accomplish Information Assurance (IA) for Theater intelligence systems (SCI, LOCE, and JAC SIPR/NIPRNET) through strategic IA programs and applications in conjunction with HQ USEUCOM/IO Cell, ECJ6 and DISA.

(7) Develop a strategic training plan ensuring that IO analytical applications; i.e., Counter Deception, Counter Propaganda, become standardized.

(8) Develop plan to restore/prioritize lost ISR communications connectivity to Theater and reachback nodes, and to operate in degraded C3 environments. Exercise this plan quarterly or in conjunction with Theater exercises.

e. National Agency Liaison Offices (LNO). Coordinated IO requires national agency liaison (LNO) participation. LNO roles must reflect current planning and established ECJ2 support structure.

(1) During the deliberate planning process, LNOs will maintain situational awareness of ongoing intelligence support to IO efforts with the IO staff officer and the ECJ2 IO Cell representative.

(2) During crisis planning, LNOs will assist in a direct support role providing assistance in working IO support issues with the home agencies in CONUS.

9. **Training.**

a. Intelligence support to IO places new demands on intelligence collection and processing, especially in the types of information required and the degree of detail necessary for IO planning and execution. It may alter priority intelligence requirements (PIR), reporting timelines, types of reports, and database maintenance priorities. The challenge is to make training available to ECJ2 personnel that will allow them to adequately understand all aspects of IO sufficiently to synchronize their activities.

b. The ECJ2 staff must become aware of the impact IO may have on their individual areas. Beyond a general indoctrination, selected staff members who come together at various times to form an IO cell need training to help them work together as a team. IO cell training should emphasize four planning imperatives of IO: synchronization, coordination, deconfliction, and fratricide avoidance.

FOR THE COMMANDER IN CHIEF:

OFFICIAL:

MICHAEL A. CANAVAN
Lieutenant General, USA
Chief of Staff

DAVID R. ELLIS
LTC, USA
Adjutant General

DISTRIBUTION:
P