Chapter 8

Charges in Classified Information and National Security Cases

As in any court-martial, how the charges are drafted in classified information cases affects the shape of the case from discovery through trial, whether contested or by plea. There are a number of considerations that need to be taken into account prior to drafting charges in any case involving classified information. Most importantly, the authority to use classified information as evidence at trial. Other concerns are the amount and classification level of the information, as well as issues that arise due to the presence of classified information on electronic media. Those considerations are discussed in section A. Sections B and C discuss the specific non-capital and capital offenses that are most commonly charged in cases involving classified information, including those federal offenses that are charged under Clause 3 of Article 134, UCMJ (Crimes and Offenses Not Capital).

A. Charging Considerations.

1. Permission to Use the Classified Information. The most important question to be considered at the early stage of any classified information court-martial is what classified information the government will be able to use as evidence in the case. It should NOT be assumed that simply because the accused is alleged to have committed a crime, even the crime of espionage, that the classified information will be available for use at trial. This is especially true for information that originates outside the Department of Defense. The intelligence community's first priority is protection of its sources and methods, not prosecution. This colors their approach to these cases. The presence of civilian counsel representing the accused heightens these concerns. Members of the intelligence community, and the National Security Agency (NSA) in particular, have been known to refuse to allow their information to be turned over in discovery, much less used at trial. Alternatively, it is not uncommon for an agency such as NSA to place limits on the material that may be used, such as only allowing Secret or non-Sensitive Compartmented Information to be used.

It is important for the staff judge advocate to develop a full understanding of the quantity and quality of classified information as early as possible. To that end, NCIS should complete all forensic examinations as soon as possible. It is critical that trial counsel review all potential evidence prior to drafting charges.[1] The charges should not be drafted until counsel has a full and complete understanding

[1] This is a lesson learned from the King case, where trial counsel was not cleared to review all of the evidence prior to the preferral of charges. The fact that Petty Officer King was in pre-trial confinement drove the sense of urgency behind preferring charges against him so early in the investigation.

of what evidence will be available[2] and what restrictions, if any, the intelligence community places on the use of the classified information as evidence.

2. Amount of Classified Information. The amount of classified material present is an important consideration in any case because large amount of classified material require more classification reviews. It is possible to write a broadly worded charge that implicates all of the classified information, but then pick only certain documents to use as evidence at trial and just have those documents undergo a classification review. In such a case, the defense will often ask for a bill of particulars because the broadly worded charge does not provide sufficient detail as to what actual information was lost, mishandled, or compromised. Even if the government cherry picks particular documents to use as evidence, some or all of the remaining documents may still be discoverable. After all, the defense counsel has the obligation to test any characterization that the government makes about the remaining documents or about the overall group of documents. In cases involving large amounts of classified information, especially when the Original Classification Authority (OCA) has placed use restrictions on some of the information, trial counsel should consider listing specific classified documents in the specification in order to minimize potential discovery and evidence necessary for the trial. Therefore, everything not listed in the specification is not relevant to the case and effectively "fenced off" from discovery.[3] Such a charging strategy can assist any use limits imposed by OCAs and address and drastically limit the number of classification reviews required. It also provides for a more focused case, however, the full scope of the accused's misconduct may be obscured from the finder of fact.

3. Classification Level. The classification level of the material in the case needs to be considered prior to drafting charges. The higher the classification level, or if there is Sensitive Compartmented Information or Special Access Program material present in the case, the more complicated the case becomes, both from an evidentiary and logistical standpoint. Both types of information can only be discussed in a Sensitive Compartmented Information Facility (SCIF), which means that all closed pre-trial and trial sessions would have to be held in such a location. Other extra security precautions immeasurably complicates the case. This is especially true in mishandling cases where there is no allegation of espionage or willful compromise. Serious consideration should be given to charging in such a way as to NOT implicate these two types of information. This can be done by enumerating specific documents in the specification, as discussed in the last section, or by putting a specific classification level into the specification. For instance, charging the accused with mishandling "information

[2] The convening authority staff judge advocate and trial counsel need to have the proper clearance to review the evidence in the case and should apply for any required upgrades in clearance level as early in the process as possible.

[3] Of course, trial counsel could not then refer in any way to the greater body of classified documents/information. The enumerated documents could not be characterized as being "representative," or a "sampling" in any way of the entirety of the classified information.

classified at the Secret level" rather than the more generic "classified information." However, it should be emphasized that charging in such a manner carries a risk if the classification review does not confirm the classification level. This risk can be dramatically reduced by having good, thorough classification reviews completed prior to charging or ensuring that multiple Secret documents are charged and then reviewed. When the evidence in a case does not go above the Secret level, then the more conservative approach is to simply charge loss of "classified information."

4. Electronic Media. The cases involving the largest quantities of highly classified information are usually cases where the classified information was located on electronic media such as laptop hard drives, CDs, or thumb drives. Electronic media should not be charged in the specification, especially if efforts are being made to fence off amounts or levels of classified information. The electronic media is not the classified information. It is merely the holder of the classified information, much like a file folder of classified information found at someone's house. It is the classified information inside the folder that is charged, not the folder. Case law and the facts of each case need to be carefully examined to determine whether or not the entire forensic examination is subject to discovery, especially in cases where efforts have been made to limit the scope of the material at issue. In such cases, when a decision is made to provide the entirety of the forensic examination, the titles of the non-relevant documents/files on the electronic media should be carefully screened to ensure that classified subject lines are not mistakenly provided in discovery.

B. Non-Capital Offenses.

1. Article 92 – Failure to Obey Order or Regulation. Article 92 violations are the most commonly charged UCMJ offenses in classified information cases. It is often the only charge available in mishandling cases. Article 92 can also be charged in espionage and willful compromise cases as such conduct also violates the safeguarding and handling regulations.

The applicable regulation is SECNAV M-5510.36, the Department of the Navy Information Security Regulation.[4] It is important to note that, although the instruction is expressly punitive, most of the affirmative duties are placed on commanding officers. Only a few provisions place affirmative duties on service members generally. The facts of each case need to be carefully evaluated to determine if they constitute a specific violation of SECNAV M-5510.36. Judge advocates should become familiar with provisions in chapters 7 (Safeguarding), 10 (Storage and Destruction), and 12 (Loss or Compromise of Classified Information) as these chapters are the most likely to support an orders violation charge. In Chapter 7, the regulation requires the Commanding Officer to set administrative procedures for controlling the various levels of classified information. Individuals must take care to properly log classified materials,

[4] Army: AR 380-5; USAF: AFI31-401

conduct end-of-the-day security checks, and take care when discussing classified information. While Chapter 10 places much of the burden on commanding officers to establish proper procedures for the storage and destruction of classified information, be aware of situations involving unauthorized storage at residences or within workspaces by individuals. Chapter 12 places an affirmative burden on individuals to notify their security manager and commanding officer upon discovering a loss or compromise of classified information.

Another option for trial counsel is to charge a violation of the Classified Information Executive Order. Section 4.2(c) of Executive Order (E.O.)12958 states that classified information may not be removed from official premises without proper authorization. This is a prohibition that applies to everyone, not just COs, and would seem to be specific enough to support a charge of disobedience of a general order. Section 5.7(b) of E. O. 12958 also contains language that simply and clearly prohibits unauthorized disclosures of classified information.

Trial counsel can also use Article 92 to charge a dereliction of duty. The principle is that all service members have a duty to safeguard classified information. This duty is a long-standing custom of the service and is known, or should be known, because it is discussed in several regulations, including SECNAV M-5510.36 and E.O. 12958. In many cases, the service member was indoctrinated upon being granted a clearance and signed a non-disclosure agreement (SF-312) or other form. Copies of the SF-312 are usually available in the service member's service record. SECNAV M-5510.36 can be used to establish certain duties pertaining to classified information. A failure to safeguard information marked as classified would constitute a dereliction of this duty and, depending on the facts, could be charged either as willful or negligent.

2. Article 134 - The General Article. Article 134, clause 3 permits the assimilation of non-capital crimes and offenses under the United States Code that are not otherwise specifically contained in the UCMJ. Article 134's preemption doctrine prohibits the assimilation of offenses specified under the U.S. Code if the conduct is already covered by Articles 80-132 of the UCMJ. There are several federal statutes that prohibit conduct not already covered under standard UCMJ articles. These are frequently charged in national security cases and cases involving classified information. JAGMAN § 0126 lists some of the federal statutes that relate to national security. Sample specifications are provided in Appendix 8-A. Note, however, that 18 U.S.C. § 794 cannot be charged under Article 134 because it is a capital offense.

When charging Article 134 violations, remember that the applicable statute of limitations is Article 43, UCMJ, which provides for a five year period for most violations. If, however, the offense is punishable by death, there is no statute of limitations.

(a) 18 U.S.C. § 793**.** 18 U.S.C. § 793 is one of the primary federal espionage statutes. Section 793 is titled "Gathering, transmitting, or losing defense information," and is subdivided into six separate offenses. Each offense carries a maximum sentence of 10 years confinement. Section 793 does not require any intent or attempt to give the information to a foreign entity, unlike Article 106a, discussed below in section C. Section 793 is not preempted by Article 134 because it is, in effect, a lesser offense of Article 106a, and is aimed at preventing the possession of national defense information by any person who is not authorized to possess it, not just foreigners. Just as with Article 106a, Section 793 does not specifically require that the information be classified. It only requires that the information be related to the national defense. Each subsection differs slightly with respect to the manner in which the accused comes into possession of the information and other minor details. See Appendix 11-B for a detailed breakdown of the elements of the various subsections of 18 U.S.C. § 793.

(b) 18 U.S.C. § 1924**.** Section 1924 is titled "Unauthorized removal and retention of classified documents or material." This section is appropriately charged when the evidence indicates mishandling of classified information, but does not suggest the accused made any attempt or had any intent to give the information to an unauthorized person. It is a misdemeanor and carries a maximum sentence of one year of confinement. This offense, by itself, would not likely be a national security case, because it does not involve a compromise. However, it often is charged in conjunction with other offenses in a national security case. The main focus of section 1924 is to prevent unauthorized handling of classified information by persons who might otherwise be authorized to possess the information. In contrast, the focus of section 793 is to prevent unauthorized people from possessing classified information. Section 1924 also differs from section 793 in that it does specifically require that the information be classified.

(c) Other Federal Statutes**.** Titles 18, 42, and 50 describe several additional offenses which may be applicable in cases involving classified information. Within title 18, counsel should consider section 792 (harboring or concealing persons), section 795 (photographing defense installations), section 798 (disclosure of classified information), and section 1001 (false statements when the falsification or concealment concerns any actual, prospective, or attempted commission of a crime against national security). In addition, sections 2151 through 2156 of title 18 (chapter105) describe offenses of sabotage, and sections 2331-2339B of title 18 (chapter 113B) describe offenses of terrorism. Other title 18 offenses include sections 2381 (treason), 2382 (misprision of treason), 2383 (rebellion or insurrection), 2384 (seditious conspiracy), 2385 (advocating overthrow of Government), 2388 (activities affecting armed forces during war), 2389

(recruiting for service against the United States), and 2390 (enlistment to serve against the United States).

Title 42 and title 50 describe offenses that may be chargeable in national security cases for specific categories of evidence. If the case involves restricted data, counsel should consult title 42. Offenses under title 42 include sections 2272 (violation of specific sections), 2273 (violation of sections generally), 2274 (communication of restricted data), 2275 (receipt of restricted data), 2276 (tampering with restricted data), and 2277 (disclosure of restricted data). If the case involves classified information, counsel should consult title 50. Within title 50, section 783 makes it a crime to communicate classified information, or conspire to do so, to any person whom one knows or has reason to believe to be an agent of a foreign government. 50 U.S.C. § 421, the Intelligence Identities Protection Action prohibits the unauthorized disclosure of information identifying certain U.S. intelligence officers, agents, informants, or sources.

3. Miscellaneous Articles. One should not overlook traditional offenses when drafting a charge sheet involving classified information. Judges and counsel are generally more familiar with traditional UCMJ violations than federally assimilated statutes. There is usually established military case law applicable as well. Furthermore, traditional charges may be less difficult to prove and may not require the use of classified information during the presentation of evidence. Some possible charges include Articles 81 (Conspiracy), 107 (False Official Statement), and 131 (Perjury). Cases involving the taking or removal of classified information from a workplace or command can be charged under Articles 108 (military property) and 121 (larceny) because classified information is property of the United States, according to SECNAV M-5510.36, Section 7-1.

C. Death penalty eligible charges

1. Art 104 – Aiding the enemy (if referred capital). Any person who aids, or attempts to aid, the enemy with arms, ammunition, supplies, money, or other things, is guilty of aiding the enemy. Further, any person who, without proper authority, harbors, protects or gives intelligence to or communicates or corresponds with the enemy, either directly or indirectly, is guilty of this offense. "Enemy" is defined in Part IV, paragraph 23c.(1)(b) of the MCM and includes organized forces of the enemy in the time of war, any hostile body that our forces may be opposing, and includes civilians as well as members of hostile military establishments. For the offense of aiding the enemy, either a court-martial or a military commission may award the death penalty. This is the most applicable of the death penalty offenses to instances of a service member assisting a terrorist organization such as Al Qaeda.

2. Art 106 – Spies (mandatory). Any person, regardless of nationality or status, who, in time of war, is found to be acting clandestinely or under false pretenses

and collecting or attempting to collect certain information, with the intent to convey this information to the enemy, is guilty of this offense. The phrase "time of war" is defined in R.C.M. 103(1) as either a period of war declared by Congress, or the factual determination by the President that the existence of hostilities warrants a finding that a "time of war" exists for purposes of R.C.M. 1004(c)(6) and Parts IV and V of the MCM. The accused shall be tried by general court-martial or military commission and, if convicted under this Article shall be punished by death. There is no lesser-included offense.

3. Art 106a – Espionage (if referred capital). Article 106a was created in 1985 to establish a peacetime espionage offense. Prior to its enactment, espionage and espionage-like acts could only be punished, if committed in a time of war, under Article 106, Spies. Article 106a was modeled after 18 U.S.C. § 794, the Federal Espionage Act. This particular section of the federal code could not be assimilated under Article 134 since it is a capital offense and Article 134 prohibits the assimilation of capital offenses. Congress responded to this deficiency by creating Article 106a. Article 106a may be used to charge an individual, who communicates, delivers or transmits or attempts to communicate, deliver or transmit any "thing" relating to the national defense to an entity or agent of what is best described generically as a "foreign power." A terrorist organization, such as Al Qaeda, does not fit neatly within the definitions of "entity" contained within the definitions of this section. Trial counsel must prove that the accused acted with intent or with reason to believe that "thing" at issue would be used to the injury of the United States or to the advantage of a foreign nation. "Thing" is a defined term which, in its broadest term, includes "information relating to the national defense," which parallels the language used in the pertinent sections of Title 18 of the U.S. Code.

Transmission of certain types of information may be punishable by death. Article 106a states that the information warranting a capital charge is anything that directly concerns nuclear weaponry, military spacecraft or satellites, war plans, communications intelligence and or any other major weapons system or major element of defense strategy.

Trial counsel must be able to show the subject did, or did attempt to, transmit, deliver, or communicate, national defense information to a specified entity, such as a foreign government; a faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the U.S.; or a representative, officer, agent, employee, subject, or citizen of such a government, faction, party or force. It is important to note that the information does not have to be classified. It only needs to relate to the national defense. In circumstances where the information is not classified,[5] the trial counsel must show the accused acted in bad faith, without lawful authority with respect to information that is not

[5] The Department of Justice, as a matter of policy and practice, does not prosecute cases under 18 U.S.C. §§ 793 and 794 unless the information was, in fact, classified. Code 17 recommends that convening authorities follow DoJ's lead on this issue.

lawfully accessible to the public, and that the accused did so with the intent or reason to believe that the information would be used to the injury of the U.S., or to the advantage of a foreign nation.

When Article 106a is charged as a capital offense, the court martial must find unanimously and beyond a reasonable doubt one or more of the following aggravating factors: the accused has been convicted of another offense involving espionage or treason for which the sentence of death or imprisonment for life was authorized by statute; the accused knowingly created a grave risk of substantial damage to the national security in the commission of the offense; the accused knowingly created a grave risk of death to another person in the commission of the offense; or any other factor that may be prescribed by the President pursuant to Article 36 of the UCMJ. As already stated, only information which directly concerns nuclear weaponry, military spacecraft or satellites, war plans, communications intelligence and or any other major weapons system or major element of defense strategy, has the potential to satisfy this requirement.

As a final note, *attempted* espionage is not charged under Article 80 like most other attempted crimes under the UCMJ. Attempted espionage is charged under Article 106a. Sample specifications are provided in the Appendix.

4. Aggravating Factors. For the death penalty to be imposed for the foregoing offenses, the members must find, beyond a reasonable doubt, one or more of R.C.M. 1004 aggravating factors are present. While trial counsel should plead the element that makes the charge capital when seeking a capital referral, it is not required to plead the aggravating factors. It is imperative for counsel to be certified for capital litigation before litigating a national security case which has been referred capital.

APPENDIX 8-A

Sample Specifications

§ 793(b):

Specification: In that _____ , on active duty, did, on board _____ _____, from on or about _____ to on or about _____, for the purpose of obtaining information respecting the national defense of the United States of America, with intent or reason to believe that the said information was to be used to the injury of the United States or to the advantage of a foreign nation, violate Title 18, United States Code, Section 793(b), by knowingly and willfully [taking photographs or equipment; making a writing; containing information] connected with the national defense.

§ 793(e):

Specification: In that _____ , on active duty, did, at or near _____, on or about _____, having unauthorized possession of information relating to the national defense of the United States of America, which information the said _____ had reason to believe could be used to the injury of the United States or to the advantage of a foreign nation, violate Title 18, United States Code, Section 793(e), by knowingly and willfully [communicating; delivering] information relative to the national defense to persons not entitled to receive said information.

§ 793(f):

Specification: In that_____, on active duty, did, at or near_____, on or about_____ violate Title 18, United States Code, Section 793(f), by permitting, through gross negligence, a computer disk containing information pertaining to the national defense, of which he had lawful control, to be removed from its proper place of custody on board_____ and ultimately to his private residence.

§ 795(a):

Specification: In that _____ , on active duty, did, on board _____ _____, from on or about _____ to on or about _____, violate Title 18, United States Code, Section 795(a), by unlawfully making photographs of vital naval equipment, relating to the national defense and requiring protection against general dissemination, without first obtaining permission from the naval command concerned and submitting said photographs to such command for censorship or such other action as deemed appropriate.

§ 1924:

Specification: In that _____ , on active duty, did, on board _____ _____, from on or about _____ to on or about _____, violate Title 18, United States Code, Section 1924, by becoming possessed, by virtue of his office, of materials containing classified information of the United States and knowingly removing such materials without authority and with the intent to retain such materials at an unauthorized location.

ADDITIONAL SAMPLE CHARGES AND SPECIFICATIONS

Charge: Violation of the UCMJ, Article 81

Specification: In that _____, on active duty, did, at or near_____, on or about _____, conspire with Mr. and Mrs. Bin Laden, to commit an offense under the Uniform Code of Military Justice, to wit: espionage, in violation of Article 106a, and in order to effect the object of the conspiracy, _____ did deliver documents titled "Super Secret Squirrel" to Mr. Bin Laden.

Charge: Violation of the UCMJ, Article 92

Specification 1: In that _____, on active duty, did, at or near_____, on or about_____, violate a lawful general regulation, to wit: Paragraph X of SECNAV M-5510.36, by wrongfully disclosing documents titled "Super Secret Squirrel", classified SECRET and TOP SECRET, in his possession and under his control, to persons not authorized to receive said classified information.

Specification 2: In that _____, on active duty, did, at or near _____, on or about_____, violate a lawful general regulation, to wit: Paragraphs X of SECNAV M-5510.36, by wrongfully failing to properly safeguard and store documents titled "Super Secret Squirrel", classified SECRET and TOP SECRET, in his possession, Paragraph X of SECNAV M-5510.36, by wrongfully possessing and storing said classified information at locations not authorized for such storage, and Paragraphs X of SECNAV M-5510.36, dated 23 Jan 01, by wrongfully reproducing SECRET and TOP SECRET classified material without authorization.

Specification 3: In that_____, on active duty, did, at or near_____, on or about_____, having knowledge of his duties concerning the proper handling of classified material, was derelict in the performance of those duties by having, without proper authority, wrongfully and negligently removed classified material, to wit: documents titled "Super Secret Squirrel".

Charge: Violation of the UCMJ, Article 104

Specification: In that_____, on active duty, did, at or near_____, on or about_____, attempt to, without proper authority, knowingly give intelligence to the enemy, by providing documents concerning SIGINT operations.

Specification: In that _____, on active duty, did, at or near_____, on or about_____, aid the enemy with maps of Naval installations, by furnishing and delivering said maps to members of al Qaida.

Charge: Violation of the UCMJ, Article 106a

Specification: In that_____, on active duty, did, at or near_____, on or about_____, with the intent or reason to believe that it would be used to the injury of the United States or to the advantage of a foreign nation, attempt to deliver classified SECRET and TOP SECRET information, to wit: documents titled “Super Secret Squirrel”, relating to the national defense to a representative of a foreign government.

Charge: Violation of the UCMJ, Article 108

Specification: In that _____, on active duty, did, at or near_____, on or about_____, without proper authority, sell to Mr. Bin Laden, documents titled “Super Secret Squirrel”, of some value, military property of the United States.

Charge: Violation of the UCMJ, Article 121

Specification: In that_____, on active duty, did, at or near_____, on or about_____, steal documents classified SECRET, of some value, the military property of the United States.

This page intentionally left blank