Sentencing Complexities in National Security Cases

CHRIS JENKS*

Assistant Professor and Criminal Justice Clinic Director, SMU Dedman School of Law

To discuss the sentencing complexities in military national security cases, first defining a national security case and then distinguishing Department of Defense (DOD) prosecutions from those by the Department of Justice (DOJ) is helpful. Following that, this article explains the challenges national security cases present, including the introduction of classified information and the difficulty in correlating degrees of potential harm to national security to a level of punishment.

I. What is a National Security Case?

There is no agreed upon definition of a "national security case." Civil liberties groups litigating U.S. government travel watch lists, monitoring of cell phone call data, or overseas targeted killing operations are civil national security cases. So too are certain criminal cases brought by the DOJ in U.S. District Courts and the DOD in military prosecutions or courts-martial. Some of the federal and military prosecutions are considered national security cases by the charges, the federal law, or Uniform Code of Military Justice (UCMJ) article allegedly violated. Other federal and military cases are considered national security cases not by the charges but by the overall context of the prosecution. This article employs a useful but admittedly not dispositive indicator of a national security case—whether the proceeding involves classified information.

The DOJ is involved in the vast majority of national security cases, prosecuting criminal cases and defending the U.S. government in civil cases. The role of the DOD is triggered when the individuals who allegedly committed the offense(s) are subject to the UCMJ.[1] Although servicemembers are not the only category of individuals subject to the UCMJ,[2] in practice U.S. military justice is essentially limited to the DOD prosecuting members of the U.S. military.

II. What is a Military National Security Case?

The UCMJ allows for assimilating and charging federal law violations.[3] But the military only does so when there is not an applicable punitive UCMJ article. Thus, almost all military national security cases only involve violation(s) of military law. There are several articles of the UCMJ the violation of which would almost always be considered a national security case, and there are other articles the violation of which may qualify based on the details or context of an individual case.[4]

The articles of the UCMJ which presumptively yield a national security case include:

> Article 104—Aiding the Enemy: This charge encompasses servicemembers who aid or attempt to aid the enemy with arms, ammunition, supplies or other things.[5]
>
> Article 106—Spies: This charge encompasses spying. It's more a notional than practical charge as the punishment is per se unconstitutional. The *mandatory* punishment for someone convicted of spying is death.[6]
>
> Article 106a—Espionage: A servicemember violates this article in much the same way as a violation of Article 104. The key distinction is that Article 104 involves an enemy (any hostile body that the U.S. military is opposing), whereas espionage involves a foreign enemy against whom the U.S. is not engaged in armed conflict.[7]

Other military prosecutions involve facially neutral charges and qualify as national security cases on an individual basis. Examples include the 2013 court-martial of Private First Class Bradley Manning for aiding the enemy in violation of Article 104 and then a host of violations of Article 92 (failure to obey a lawful order or regulation) stemming from his role in providing information to WikiLeaks. The Article 104 charge is a *per se* national security charge, but you would need to know the context of the Article 92 violations in order to say the same of them. The vast majority of the time Article 92 violations have nothing to do with national security, so context is key. In Manning's case the Article 92 charges referred to his violating the Army's regulation on information assurance, which details how to properly store, protect, and transmit unclassified and classified information. Manning violated the regulation, and thus Article 92, by wrongfully moving classified files, cables, videos, and presentations from a secure government system onto his personal computer, a nonsecure system.

Similarly, when two U.S. servicemembers attacked and killed fellow servicemembers in separate incidents—in Kuwait shortly before the United States invaded Iraq in 2003,[8] and at Ft. Hood, Texas, in 2009[9]—the U.S. Army charged both with murder and attempted murder under the UCMJ. It is the context of these crimes—that the servicemember defendants were Muslim and purportedly acting in support of the Islamic extremist groups the United States

Federal Sentencing Reporter, Vol. 27, No. 3, pp. 151–155, ISSN 1053-9867, electronic ISSN 1533-8363.
 DOI: 10.1525/fsr.2015.27.3.151.

was fighting and against U.S. servicemembers either in, or preparing to deploy to, the Middle East—that renders these prosecutions national security cases.[10]

Thus, the military will, on rare occasion, prosecute a servicemember for UMCJ violations that presumptively and/or contextually render the process a national security case. The rarity of such proceedings is itself a challenge; the military prosecutor and defense counsel are very unlikely to have previously tried a case involving classified information. And although a court-martial need not technically involve classified information to constitute a national security case, the overwhelming majority of them do.[11]

The introduction of classified information significantly alters the contours of a court-martial, before the proceedings, during the merits, on sentencing, and even posttrial and on appellate matters. In general classified information creates a tension that does not exist in other cases, between the competing values of the government's interest to protect national security information from disclosure and the accused's right to a fair trial. This tension is exacerbated in the military at the pretrial stage as the military practices open-file discovery, which is made functionally impossible in the need-to-know environment of classified information. Further, the presence of classified information, and the difficulty in correlating degrees of potential harm to national security to a level of punishment in the absence of sentencing guidelines, both add complexity to the sentencing process in these cases.

III. Sentencing Complexities in National Security Cases

Classified information often poses the largest challenge in sentencing. The challenges begin before trial with the byzantine manner by which material is determined to be classified and only increases when the material is introduced in court. Concern about safeguarding classified material dictates any number of aspects of the conduct of sentencing proceedings. And a mistake regarding handling of classified evidence is at best glaring hypocrisy[12] and may even constitute a criminal violation.[13]

A. Classified Information

Under Military Rule of Evidence 505, classified information "means any information or material that has been determined by the Unites States Government pursuant to an executive order, statute or regulations, to require protection against unauthorized disclosure for reasons of national security, and any restricted data, as defined in 42 U.S.C. § 2014(y)."[14] The required basis for classifying material is that its unauthorized release would harm national security. The level of classification corresponds to the amount of damage the unauthorized release would cause, ranging from grave damage equating to top secret, serious damage to secret, and damage to confidential.

Determining the existence of classified information is a process that in equal parts resembles *Alice In Wonderland* and Joseph Heller's *Catch-22*. A U.S. Army prosecution of a federalized National Guard soldier who attempted to aid al-Qaeda is instructive. The soldier, Ryan Anderson, was lower ranking and did not possess a security clearance and thus did not have access to classified material. Anderson exchanged a number of text messages and participated in two meetings with people whom he thought were members of al-Qaeda, but who were in fact federal agents. Between the text messages, materials he delivered, and what he said at the meetings, Anderson provided information concerning the vulnerabilities of U.S. Army vehicles and of individual soldier equipment used in Iraq. Much of what Anderson said proved correct. It also proved to be classified. Because Anderson did not have a security clearance, this led to his military defense counsel, who did have a security clearance, not being able to discuss Anderson's statements with Anderson. The reverse of this problem occurred in a U.S. Air Force court-martial; the military accused, a fighter pilot, could not, at least initially, discuss classified aspects of his case, notably the rules of engagement, with his civilian defense counsel.[15]

The process by which information is reviewed and accessed to determine whether it's classified is beyond the scope of this chapter. And there is an entirely differently process by which unclassified governmental information the disclosure of which would be detrimental to the public interest is privileged.[16] Suffice to say both are cumbersome and slow processes, made more so when the entity making the determination is outside the DOD. The processes are so onerous that sometimes defense counsel will seek to include classified information in a proceeding as a form of leverage against the prosecution, a technique known as "graymail."[17] And yet the complexities only increase following a determination that relevant information is classified and introduced in court. Table 1 highlights the differences and similarities between how the different federal criminal forums—federal court, military courts-martial, and military commissions—treat classified information.

B. Impact of Classified Information on Sentencing Process

The complexities include dictating which courtrooms may and may not be used, a host of requirements on counsel for both sides, and even how the military judge, court personnel, witnesses, and the panel (military jury) operate.

The starting point for understanding the enormous complexity added by the introduction of classified information is to recognize that all personnel and facilities must be cleared to handle or receive classified information. Thus security managers must inspect and approve the courtroom itself as a location in which classified information may be discussed and stored. In terms of personnel, although many servicemembers possess security clearances, many do not. And civilian witnesses or counsel generally don't have security clearances, which leads to considerable delays in the progress of the trial as counsel go through the clearance process.

Table 1. Classified Information Comparison

Use of Classified Information
- **CIPA** — Classified Information Procedure Act codified at 18 U.S.C. App. 3. CIPA is a procedural tool, not an evidentiary priviledge.[a]
- **MRE 505** — Military Rule of Evidence 505, Classified Information. Created through authority under 10 U.S.C. § 836. Hybrid rule of both priviledge (national security and executive) and procedure. MRE 505 is based on the unreacted House version of CIPA.
- **Military Commissions** — Formally recognizes a classified information priviledge. Military Commissions Act of 2009 (MCA), subchapter V, 10 U.S.C. §§ 949p 1–949p 7.

Discovery
- **CIPA** — Does not on its face include standards for discovery, yet "six of the federal circuit courts of appeal have adopted a 'relevant and helpful' standard for determining whether the defense is entitled to discovery of classified information."[b]
- **MRE 505** — Allows for discovery of "noncumulative, relevant, and helpful to a legally cognizable defense, rebuttal of the prosecution's case, or to sentencing."[c] MRE 505 clearly envisions litigation over classified information discovery.
- **Military Commissions** — Provides for discovery of classified information after a demonstration that the evidence is "noncumulative, relevant, and helpful to a legally cognizable defense, rebuttal of the prosecution's case, or to sentencing."[c]

Use of Precedent
- **CIPA** — "Extensive jurisprudence interpreting CIPA in the more than 30 years since it was enacted."[d]
- **MRE 505** — Few courts-martial involve classified information, thus there are few reported decisions.
- **Military Commissions** — Relies on CIPA case law as precedent.

Closing Proceedings to the Public
- **CIPA** — Does not allow closed sessions during which classified evidence may be admitted.
- **MRE 505** — Allows closed sessions during which classified evidence may be admitted.
- **Military Commissions** — Allows closed sessions during which classified evidence may be admitted.

Declassification
- **CIPA** — Does not provide a mechanism.
- **MRE 505** — Does not provide a mechanism.
- **Military Commissions** — "[P]rovides a mechanism (and through its implementing regulations, the personnel and resources) to accomplish it."[e]

[a] *See* Jennifer K. Elesa, *Comparison of Rights in Military Commission Trials and Trials in Federal Court*, Congressional Research Service (Mar. 21, 2014); Edward C. Liu & Todd Garvey, *Protecting Classified Information and the Rights of Criminal Defendants: The Classified Information Procedures Act*, Congressional Research Service (Apr. 2, 2012).
[b] Christopher W. Behan, *Military Commissions and Conundrum of Classified Evidence: A Semi-Panglossian Solution*, 37 So. Ill. L.J. 643, 665 (2013), *available at* http://www.law.siu.edu/our-people/deans/behan-publication.html.
[c] MCA 2009 § 949p-4(a)(2).
[d] Behan, *supra* [b] at 667.
[e] Behan, *supra* [b] at 666–67.

In addition to impacting where national security trials may be held and the personnel who may be involved, classified information dictates the conduct of the trial. Classified information may only be introduced or discussed in closed sessions, meaning that the only people present have the requisite security clearance and need to know the information being discussed. But given both the accused's and public's rights to a public trial, the military judge may close the courtroom for only those portions that involve classified information.[18] This leads to both advocacy and organizational challenges for counsel and the military judge.

To limit the number of times the courtroom needs to be closed and then reopened, most military judges require that each side introduce all unclassified information in one open session and then all the classified information in one closed session. The result is that unless a witness's testimony is either completely unclassified or completely classified, their testimony is bifurcated. Likewise, to the extent counsel's sentencing arguments involve classified information, counsel will need to make their unclassified argument in open court, and then that portion of their argument that involves classified evidence in a closed session. This presents challenges in terms of maintaining a coherent case presentation.

The military judge in a national security case is constantly striving for a balance—maintaining as much of the court-martial open to the public as possible while properly safeguarding classified information. One technique military judges will utilize is to have a security manager present in court. When in open session, the security manager will signal when either a question or part of a witness's testimony approaches or crosses the line of classified information. Both counsel and witnesses tend to become timid during discussion of any issue close to the classified boundary. Both counsel and witnesses start to build in long pauses between sentences and even in the middle of sentences to allow for the security manager to signal. The result is a process that safeguards classified information but can be an awkward and atypical example of military justice and advocacy, which is even more unfortunate as national security cases are more likely to be high-profile and involve media attention.

Counsel, court personnel, and jurors all must separate unclassified from classified information. That sounds straightforward enough, but the constant vigilance required by all involved, coupled with fear of a misstep, is taxing. For jurors, one technique is to have different colored notepads for unclassified and classified sessions. For counsel, ensuring the proper handling of classified material present in the courtroom involves meeting with a security manager before and after court to recover and redeposit the items from a safe. Ideally the prosecution and defense will each have their own safe for storage of classified material, but that's not always possible, which then creates additional

challenges. On breaks during the proceedings, counsel must ensure that any classified information is appropriately safeguarded.

If counsel wish to use a computer to store notes, arguments, and other case-related material, if any of the material is classified, then the laptop must be certified to store such material. And unless and until the information is properly removed, the computer is considered a classified storage device and must be treated as such. This means not being able to leave the laptop unattended, storing it in a safe at a night, and not taking it home.

Members of the court staff are not immune from the challenges classified information presents. Similar to counsel's laptop, the court reporter must have any computer used to transcribe testimony during classified sessions certified, and once used the computer is then, and must be treated as, a classified storage device. Likewise, court staff members are responsible for the proper handling and storage of classified information admitted as evidence.

C. Determining Punishment

In many national security cases, reducing amorphous concepts like grave or serious damage to national security to how long the convicted servicemember should spend in confinement is yet another challenge. In cases like *Anderson*, where the accused was communicating with federal agents, not al-Qaeda, no classified information ever reached the terrorist group. This leaves the military prosecutor to argue for punishment based on the accused's intent, but not actual harm following consummated acts. And the "victims" are often conceptual—the good order and discipline and morale of a military unit. Although those concepts are critically important, in advocacy terms they tend not to lend themselves as well to a sentencing arguments focusing on human victims.

Even in cases where the accused did convey information determined to be classified to an unauthorized person or entity, identifying the harm that directly resulted from the disclosure is difficult. In the *Manning* case, the prosecution called an intelligence expert to testify to the harm Manning's leak caused. For more than three hours he testified about the DOD's concerns that Manning's leaks "would erode trust between nations, between citizens and leaders, and between American soldiers and civilians in places like Afghanistan . . ."[19] But on cross-examination he "could not cite specific data showing the effect of the leak on the number of foreign civilians and emissaries talking to the United States."[20]

These challenges are made greater by the lack of military sentencing guidelines, which might serve as a base from which upward or downward departures would be considered.[21] Instead, for the vast majority of punitive articles of the UCMJ, there is no minimum mandated punishment.[22] And for cases involving the per se national security charges of aiding the enemy or espionage, the potential punishment ranges from no punishment up to and including the death penalty. Such a range better allows for individualized sentencing. But it can also lead to wildly disparate sentences in different courts-martial for similar offenses.

IV. Conclusion

Military national security courts-martial infrequently occur. When they do occur, military counsel, judges, and court personnel endeavor to perform their function at a high level. Unfortunately, the process by which the U.S. government conducts classification reviews and the military's inexperience in national security cases often results in the form of safeguarding classified information trumping the substantive function of the underlying trial process. And by the time the sentencing phase is reached, understandable but unfortunate focus is placed on simply concluding the trial without mishandling classified information.

Notes

* Professor Jenks previously served as a Judge Advocate in the U.S. Army, including as lead counsel for the Army's first counter-terrorism case, a classified, fully contested court-martial of an activated National Guard Soldier who attempted to aid al-Qaeda. The Department of Defense recognized the case with the Counterintelligence/Law Enforcement National Security Investigation of the Year Award and the Department of Justice Counterterrorism Section nominated then Major Jenks for John Marshall Interagency Cooperation Award.

1 U.S. Dep't of Def. Dir. 5525.7 Implementation of the Memorandum of Understanding (mou) Between the Departments of Justice (doj) and Defense Relating to the Investigation and Prosecution of Certain Crimes, Jun. 18, 2007.

2 10 U.S.C. § 802. This includes that "[i]n time of declared war or contingency operation, persons serving with or accompanying an armed force in the field" are subject to the UCMJ. *Id.* at § 802(a)(10). There has only been one recent instance of the U.S. court-martialing a civilian accompanying the force, the 2008 court-martial of one non-U.S. national contractor for, among other offenses, assaulting another non-U.S. national contractor. U.S. v. Ali, 71 M.J. 256 (C.A.A.F 2012), Cert. later denied by Ali v. U.S. 133 S.Ct. 2338 (May 13, 2013). In terms of other categories of individuals subject to the UCMJ, the U.S. military could have court-martialed the members of al-Qaeda and the Taliban currently facing a different form of military justice, military commission proceedings at Guantanamo Bay Naval Base in Cuba. *Id.* at § 818.

3 10 U.S.C. § 934.

4 DOJ faces a similar challenge. Some federal charges are per se national security cases, charges involving terrorism such as hijacking, whereas others are contextual, violent crimes, weapons violations, racketeering, and drug crimes, among them. This latter category may or may not constitute a national security case depending on the facts of the individual case. Federal prosecutions are straightforward enough that New York University issues a "Terrorist Trial Report Card" that breaks down the different kinds of possible national security cases in federal court. New York University School of Law, Center on Law and Security, Terrorist Trial Report Card: September 11, 2001–September 11, 2011, *available at* http://www.lawandsecurity.org/Portals/0/Documents/TTRC%20Ten%20Year%20Issue.pdf.

5 10 U.S.C. § 904. *See also* U.S. v. Anderson, 68 M.J. 378 (C.A. A.F. 2010).

6 10 U.S.C. § 906. *See also* Major David A. Anderson, *Spying in Violation of Article 106, UCMJ: The Offense and the*

Constitutionality of Its Mandatory Death Penalty, 127 Mil. L. Rev. 1 (1990).

7 10 U.S.C. § 906a. *See also* U.S. v. Sombolay, 37 M.J. 647 (A.C. M.R. 1993).

8 U.S. v. Akbar, 2012 WL 2887230 (A. Ct. Crim. App. 2012). Final disposition of Akbar remains pending; as of this writing the Court of Appeals for the Armed Forces is reviewing Akbar's petition for relief. The Court granted Akbar's motion for oral argument, which was held on November 18, 2014.

9 U.S. v. Hasan (III Corps, Ft. Hood, Tx. 2013). Courts-martial decisions are not reported decisions; appellate decisions are.

10 Despite evidence that Major Hasan had been in contact with Anwar Al-Awlaki, a prominent member of al-Qaeda, and that Hasan attacked U.S. servicemembers preparing to deploy to the Middle East and yelled "Allahu Akbar" ("God is great" in Arabic), the DOD initially labeled the Ft. Hood shootings as "workplace violence." Manny Fernandex & Alan Blinder, *At Fort Hood, Wrestling with Label of Terrorism*, N.Y. Times, Apr. 8, 2014. Congress modified the eligibility criteria for the Purple Heart in the National Defense Authorization Act of 2015, which led the Army to announce it would award the Purple Heart to Hasan's service member victims. Ashley Southall, *Purple Heart to be Awarded to Victims at Fort Hood*, N.Y. Times, Feb. 6, 2015.

11 One example of a military proceeding that, depending on one's perspective, may constitute a national security case but not involve classified evidence would be where a servicemember refuses to deploy to armed conflict. The military routinely court-martials such servicemembers who unsuccessfully attempt to use the trial as platform to challenge the President's decision to deploy the military. The resulting trials tend to be very straightforward affairs. The prosecution charges a violation of Article 87, "missing movement," which only requires the government to prove that (1) the accused was required to move with his or her unit, (2) the accused knew of the movement, and (3) the accused missed that movement. 10 U.S.C. § 892. The DOD would likely consider these cases as simply reinforcing good order and discipline and the requirement to follow lawful orders, which underpin military service, whereas opponents would describe the cases in a broader, national security, context.

12 It is one of a military prosecutor's worst nightmares to mishandle classified evidence when prosecuting a servicemember for . . . mishandling classified evidence. This occurred in public fashion in 2003 during an ill-fated U.S. Army prosecution of an Army chaplain for allegedly aiding the enemy. *See Classified Material Mishandled in Muslim Chaplain's Case*, A.P., Dec. 3, 2003, *available at* http://usatoday30.usatoday.com/news/washington/2003-12-03-chaplain-case_x.htm.

13 The U.S. Navy established an office devoted to classified litigation issues, purportedly in the wake of botched prosecutions in which military prosecutors mishandled classified material. *See* National Security Litigation Division (Code 30), *available at* http://www.jag.navy.mil/organization/code_30.htm.

14 Manual For Courts-martial, United States, Mil. R. Evid. 505(b)(1) (2012). Pursuant to an Executive Order:

> Information may be originally classified under the terms of this order only if all of the following conditions are met:
>
> (1) an original classification authority is classifying the information;
> (2) the information is owned by, produced by or for, or is under the control of the United States Government;
> (3) the information falls within one or more of the following categories of information (Military plans, weapons systems, or operations; Foreign government information; Intelligence activities (including covert action), intelligence sources or methods, or cryptology; Foreign relations or foreign activities of the United States, including confidential sources; Scientific, technological, or economic matters relating to national security; U.S. Government programs for safeguarding nuclear materials or facilities; Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to national security; and Weapons of mass destruction)
> (4) the original classification authority determines that the unauthorized disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism, and the original classification authority is able to identify or describe the damage.

Exec. Order No. 13526 Classified National Security Information (Dec. 29, 2009).

15 U.S. v. Schmidt, 60 M.J. 1 (2004). The pilot was involved in an air-to-ground bombing incident that killed four Canadian soldiers in Afghanistan.

16 *See* MCM, *supra* note 14, Mil. R. Evid. 506 (2012) (Government Information Other Than Classified Evidence).

17 *See* Sam A. Schmidt & Joshua L. Dratel, *Turning the Tables: Using the Government's Secrecy and Security Arsenal for the Benefit of the Client in Terrorism Prosecutions*, 48 N.Y.L. Sch. L. Rev. 69 (2003); Major Stephen A.J. Eisenberg, *Graymail and Grayhairs: The Classified and Official Information Privileges Under the Military Rules of Evidence*, Army Law (Mar. 1981).

18 Reporters Committee for Freedom of the Press, *Court Rules Army Officer Illegally Closed Investigative Hearing*, Feb. 24, 2005 *available at* http://www.rcfp.org/browse-media-law-resources/news/court-rules-army-officer-illegally-closed-investigative-hearing.

19 Emmarie Huetteman, *In Sentencing, U.S. Tries to Prove Harm by Manning*, N.Y. Times, Jul. 31, 2013.

20 *Id.* Asked directly by defense counsel whether he was aware of anyone harmed by Manning's disclosures, the intelligence expert first claimed to know of one Afghan national who had been killed by the Taliban, but later conceded that the name of the Afghan national was not among the documents Manning leaked. *Id.*

21 *See* U.S. Sentencing Commission Sentencing Guidelines Manual, *available at* http://www.ussc.gov/guidelines-manual/guidelines-manual.

22 Indeed, one defense tactic for striking prospective court-martial panel (jury) members is to ask them whether, if they found the accused guilty, they could consider awarding a sentence of no punishment. For those that deny they could consider no punishment, military prosecutors will attempt to rehabilitate them by stressing that they are only required to consider no punishment and such consideration can be extremely brief.