BEYOND INTERROGATIONS: AN ANALYSIS OF THE PROTECTION UNDER THE MILITARY COMMISSIONS ACT OF 2006 OF TECHNICAL CLASSIFIED SOURCES, METHODS AND ACTIVITIES EMPLOYED IN THE GLOBAL WAR ON TERROR

CAPTAIN NIKIFOROS MATHEWS*

"The necessity of procuring good intelligence is apparent and need not be further urged. All that remains for me to add is, that you keep the whole matter as secret as possible. For upon secrecy, success depends in most Enterprises of the kind, and for want of it they are generally defeated . . . ."

- Letter from George Washington to Colonel Elias Dayton, July 26, 1777[1]

The conduct of war, in the most classic sense, is the engagement in armed conflict either between states or within states.[2] In such a context, there is typically a recognized hierarchy of enemy actors, a recognized objective of the combatants, and a recognized beginning and end to the hostilities. In contrast, the Global War on Terror (GWOT) is an ongoing conflict involving non-state actors operating in the shadows across national borders. Therefore, "victory" in the classic sense is not attainable, as there is no enemy authority to accept the terms of surrender

---

* Judge Advocate, U.S. Army Reserve. Captain Mathews received his undergraduate degree from the University of Notre Dame (B.A., 1993) and his law degree from the Benjamin N. Cardozo School of Law (J.D., 1996). He deployed to Camp Arifjan, Kuwait, in 2005, where he served as an Operational and Administrative Law attorney for the Third U.S. Army (Coalition Forces Land Component Command) in support of Operations Iraqi Freedom and Enduring Freedom. Captain Mathews has traveled to both Afghanistan and Iraq in connection with detainee operations. The views expressed in this article are solely his own and do not reflect the views of any other organization or person. Captain Mathews wishes to thank Captain Sharad Samy for his thoughtful review and comment.

[1] 8 WRITINGS OF GEORGE WASHINGTON 478–79 (J. Patrick ed., 1933).

[2] While "war" itself is used to describe virtually any struggle—including those pitched on the fields of athletic endeavor—it is most commonly understood to be the state of international or internal armed conflict. *See, e.g.*, JOINT FORCES STAFF COLLEGE, PUB. 1, THE JOINT STAFF OFFICER'S GUIDE 1997 app. O (1997) (defining war as "[a] state of undeclared or declared armed hostile action characterized by the sustained use of armed force between nations or organized groups within a nation involving regular and irregular forces in a series of connected military operations or campaigns to achieve vital national objectives").

and act on behalf of the defeated.[3] The present conflict is so rooted in religious fanaticism, and so characterized by decentralized actions, that even if Osama bin Laden himself were to be captured and openly declare a cessation of hostilities, al Qaeda splinter groups, their associates, and their philosophical sympathizers undoubtedly would continue their efforts, perhaps with increased zeal and recklessness fostered by the evaporation of even limited command and control.[4] What this means for GWOT-related prosecutions is that, unlike the post-World War II trials at Nuremburg and more recent war crimes tribunals, there will not be an end to the hostilities before the relevant legal proceedings commence. In fact, these proceedings have already begun and there is no end to the hostilities in sight.[5]

The ongoing nature of the current conflict presents unique challenges in establishing a workable framework under which to prosecute GWOT detainees, particularly when it comes to determining the use and protection of sensitive information in legal proceedings. The prosecution of GWOT detainees has and will continue to require the use of sensitive

---

[3] Consider, for example, the definitive end of World War II with Emperor Hirohito's signature on the U.S.S. *Missouri* on 27 September 1945, or the symbolic and—for all practical purposes—military end of the U.S. Civil War with General Robert E. Lee's surrender at the Appomattox courthouse on 9 April 1865.

[4] As the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) noted:

> The problem is that al Qaeda represents an ideological movement, not a finite group of people. It initiates and inspires, even if it no longer directs. In this way it has transformed itself into a decentralized force. Bin Ladin may be limited in his ability to organize major attacks from his hideouts. Yet killing or capturing him, while extremely important, would not end terror. His message of inspiration to a new generation of terrorists would continue.

FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 16 (2004) [hereinafter 9/11 COMMISSION REPORT].

[5] The words of President George W. Bush in the wake of the September 11th attacks regarding the scope and expected duration of this conflict have held true:

> Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated. . . . Americans should not expect one battle, but a lengthy campaign, unlike any other we have ever seen.

President's Address to a Joint Session of Congress on the United States Response to the Terrorist Attacks of September 11, 37 WEEKLY COMP. PRES. DOC. 1347, 1349 (Sept. 20, 2001).

information as evidence. More relevant to this article, however, is that much of the prosecution's evidence will have been *obtained* from sensitive sources, methods, and activities employed by the Government, whether human or technical in nature.[6] Against the backdrop of an ongoing conflict, these sensitive sources, methods and activities—i.e., the means of obtaining evidence—used by the counterterrorism[7] community likely will not be stale at the time of a detainee's prosecution and, therefore, the disclosure of such means would compromise their future utility.[8]

This point has not been lost on those responsible for drafting procedural rules for GWOT prosecutions. The most recent effort in this regard is the Military Commissions Act of 2006 (the MCA).[9] The MCA's general approach to the protection of sensitive information is largely consistent with the approaches found in the Classified Information Procedures Act (CIPA)[10] and in Military Rule of Evidence (MRE) 505,[11] the federal statute and military evidentiary rule upon which much of the MCA's relevant provisions are based. However, the MCA

---

[6] The Department of Defense (DOD) has defined intelligence sources to include "people, documents, equipment, or technical sensors." U.S. DEP'T OF DEFENSE, JOINT PUB. 1-02, DICTIONARY OF MILITARY AND ASSOCIATED TERMS 269 (12 Apr. 2001, *as amended through* 12 July 2007) [hereinafter DOD DICTIONARY].

[7] According to the DOD Dictionary, counterterrorism is defined as "[o]perations that include the offensive measures taken to prevent, deter, preempt, and respond to terrorism." *Id.* at 130. As used in this article, "counterterrorism" has the meaning ascribed to it in the DOD Dictionary.

[8] As one commentator has noted, "[t]his is an unusual situation given that almost all war crimes and war-related offenses are prosecuted after the end of hostilities, when the need to protect national security information and safeguard participants in the trial is greatly reduced." Frederic L. Borch III, *Why Military Commissions Are the Proper Forum and Why Terrorists Will Have "Full and Fair" Trials: A Rebuttal to* Military Commissions: Trying American Justice, ARMY LAW., Nov. 2003, at 10 (responding to Kevin J. Barry, *Military Commissions: Trying American Justice*, ARMY LAW., Nov. 2003, at 1).

[9] Military Commissions Act (MCA) of 2006, 10 U.S.C.S. § 948a - 950w (LEXIS 2007) [hereinafter MCA]. The first conviction before a military commission convened under the MCA was that of David Hicks, an Australian trained by al Qaeda who pleaded guilty on 26 March 2007 to providing material support to a terrorist organization. *See* William Glaberson, *Plea of Guilty from Detainee in Guantánamo*, N.Y. TIMES, Mar. 27, 2007, at A1.

[10] 18 U.S.C. app. III (2000).

[11] MANUAL FOR COURTS-MARTIAL, UNITED STATES, MIL. R. EVID. 505 (2005) [hereinafter MCM].

also specifically protects from disclosure classified[12] sources, methods and activities through which admissible evidence was obtained.[13] The protection of sensitive counterintelligence means is not specified in either CIPA or MRE 505. As a result, the language of the MCA that provides this protection has come under attack as an instrument the prosecution may use to deny an accused his due process rights, particularly by restricting his ability to object to the admissibility of evidence obtained through questionable interrogation tactics.[14] Yet this myopic focus on interrogation methods has overshadowed what has become truly important to the counterintelligence community in this conflict and what was undoubtedly on the minds of the drafters of the MCA: the protection of *technical* means used to gather intelligence by penetrating terrorist communications and, especially, their finances.

This article tracks the development and content of the MCA as it relates to sensitive information, and examines whether the MCA's protection of technical counterintelligence means would withstand judicial scrutiny. Section I of this article provides background on how the MCA came to be and how it ultimately deals with the use and protection of sensitive information in military commission proceedings. Using the al Qaeda financial network as a vehicle, section II discusses the types of technical sources, methods and activities employed in the

---

[12] The drafters of the MCA decided to limit its protection of sensitive information to information that is actually classified, as discussed in greater detail below. *See infra* notes 27–31 and accompanying text.

[13] *See* 10 U.S.C.S. § 949d(f)(2)(B).

[14] *See, e.g.*, HUMAN RIGHTS WATCH, Q AND A: MILITARY COMMISSIONS ACT OF 2006, at 4 (2006), http://hrw.org/backgrounder/usa/qna1006/usqna1006web.pdf [hereinafter HUMAN RIGHTS WATCH Q & A] (stating that the protection of classified sources and methods of interrogations, in particular, will make it "extremely difficult for defendants to establish that evidence was obtained through torture or other coercive interrogation methods"); HUMAN RIGHTS FIRST, ANALYSIS OF PROPOSED RULES FOR MILITARY COMMISSIONS TRIALS 2 (2007), http://www.humanrightsfirst.info/pdf/07125-usls-hrf-rcm-analysis.pdf ("[T]he administration has claimed that the so-called 'alternative interrogation techniques' used on 14 former CIA detainees now held at Guantanamo are classified. . . . The Government could seek to include hearsay testimony derived from these interrogations, claim that the techniques used are classified, and defense lawyers would have a hard time showing that evidence should be excluded because it was obtained through torture."); Amnesty International, *Military Commissions Act of 2006—Turning Bad Policy Into Bad Law*, Sept. 29, 2006, http://web.amnesty.org/library/Index/ENGAMR511542006 (stating that an accused's inability "effectively to challenge the 'sources, methods or activities' by which the Government acquired the evidence . . . is of particular concern in light of the high level of secrecy and resort to national security arguments employed by the administration in the 'war on terror'").

GWOT against terrorist networks that the MCA intends in large part to protect. This section further highlights the importance of preventing the disclosure of such means. Finally, section III argues that, assuming proper vigilance by the military judge, the protection afforded under the MCA to technical counterintelligence means used to obtain incriminating evidence should not negatively impact the accused's defense. As such, these protections should withstand judicial scrutiny.

I. The Development of the Military Commissions Act of 2006 and Its Approach to Sensitive Information

Shortly after the attacks of September 11th, the President issued a military order establishing military commissions to prosecute suspected GWOT terrorists for law of war violations and directing the Secretary of Defense to issue the necessary orders and regulations for these commissions.[15] In March 2002, the Pentagon responded to this directive by issuing procedural rules for the commissions.[16] Thereafter, the General Counsel of the Department of Defense issued Military Commission Instructions specifying the crimes and elements of offenses to be prosecuted and providing administrative guidelines for the conduct of proceedings.[17] When it came to sensitive information, these rules and instructions broadly delineated what was to be safeguarded in proceedings, creating the concept of "protected information,"[18] and provided sweeping rules to prevent the disclosure of such information.[19]

---

[15] Military Order of November 13, 2001, 3 C.F.R. 918 (2002) [hereinafter Military Order].

[16] *See* U.S. Dep't of Defense, Military Commission Order No. 1 (21 Mar. 2002), 32 C.F.R. §§ 9.1–9.12 (2005) [hereinafter DOD MCO No. 1]. For instance, DOD MCO No. 1 set forth the number of military officers required for a panel, the powers vested in the presiding officer of the panel, and certain procedural safeguards afforded to the accused. *Id.* §§ 9.4(A)(2)–(A)(5), 9.5.

[17] *See* 32 C.F.R. §§ 10–18 (2005).

[18] DOD MCO No. 1 defined "protected information" to include:

> (A) information classified or classifiable pursuant to [Executive Order 12,958, now Executive Order 13,292]; (B) information protected by law or rule from unauthorized disclosure; (C) information the disclosure of which may endanger the physical safety of participants in Commission proceedings, including prospective witnesses; (D) information concerning intelligence and law enforcement sources, methods, or activities; or (E) information concerning other national security interests.

In 2006, the United States Supreme Court held in *Hamdan vs. Rumsfeld*[20] that military commissions, as then constituted, were not valid.[21] However, the Court left open the door for the President to obtain express authorization from Congress to employ the proposed military

---

DOD MCO No. 1, *supra* note 16, § 9.6(d)(5)(i).

[19] *See id.* §§ 9.6(d)(2)(iv), 9.6(d)(5)(ii) – (iv).

[20] 548 U.S. __, 126 S. Ct. 2749 (2006). Salim Ahmed Hamdan, a Yemeni national, allegedly worked as Osama bin Laden's bodyguard and chauffer. He was captured in Afghanistan in 2001 and was brought to Guantánamo Bay, Cuba, in 2002.

[21] *Id.* at 2778. Specifically, the Court concluded that the commissions lacked requisite Congressional authorization; that Common Article 3 of the Geneva Conventions applies to detainees; and that the military commissions procedures deviated substantially from those applicable under the Geneva Conventions and courts-martial. *See id.* at 2749. With respect to the lack of congressional authorization, the Court held that the power to create military commissions, if it exists, is among the "powers granted jointly to the President and Congress in time of war." *Id.* at 2773. It further held that Congress' authorization to use "all necessary and appropriate force against all nations, organizations, or persons" involved in the September 11th attacks which was granted under the Authorization for Use of Military Force, Pub. L. No. 1107-40, 115 Stat. 224, § 2(a) (2001), did not amount to a congressional authorization of military commissions. *Hamdan*, 126 S. Ct. at 2775. Specifically, the Court stated:

> [W]hile we assume that the AUMF [Authorization for Use of Military Force] activated the President's war powers, . . . and that those powers include authority to convene military commissions in appropriate circumstances, . . . there is nothing in the text or legislative history of the AUMF even hinting that Congress intended to expand or alter the authorization set forth in Article 21 of the UCMJ [Uniform Code of Military Justice] . . . . Together, the UCMJ, the AUMF, and the DTA [Detainee Treatment Act of 2005] at most acknowledge a general Presidential authority to convene military commissions in circumstances where justified under the "Constitution and laws," including the law of war. Absent a more specific congressional authorization, the task of this Court is . . . to decide whether Hamdan's military commission is so justified.

Id. Note that congressional sanction of the use of military commissions to try offenders of the law of war, as a general matter, was not at issue in *Hamdan*, as the Supreme Court had already determined that Congress had sanctioned the use of military commissions. *Ex parte* Quirin, 317 U.S. 1, 28 (1942) (pointing to UCMJ article 15, now UCMJ article 21, which states: "The jurisdiction [of] courts-martial shall not be construed as depriving military commissions . . . of concurrent jurisdiction in respect of offenders or offenses that by statute or by law of war may be tried by such . . . commissions."). Rather, what was at issue was whether the President was justified in convening the military commissions under the laws of war absent a specific congressional authorization.

commissions and for the President and Congress to address the Court's concerns over the rules governing these proceedings.[22]

In response to the Court's invitation in *Hamdan* to salvage the use of military commissions to try GWOT detainees, the President engaged Congress in an intense discourse intended to specifically authorize the President to create these commissions and to establish new procedural rules governing their proceedings. Following several key compromises, the Senate passed the bill that ultimately became the MCA on 28 September 2006.[23] Among the hotly-debated points on which the President and Congress reached compromise was the treatment of sensitive information in legal proceedings.[24] The primary reason for

---

[22] *See Hamdan*, 126 S. Ct. at 2799 (Breyer, J. concurring) ("Nothing prevents the President from returning to Congress to seek the authority he believes necessary.").

[23] 152 CONG. REC. S10,420 (daily ed. Sept. 28, 2006); *see also* Charles Babington & Jonathan Weisman, *Senate Approves Detainee Bill Backed by Bush*, WASH POST., Sept. 29, 2006, at A01. The House of Representatives passed the bill the following day, and the MCA was signed into law by the President on 17 October 2006. Upon signing the bill, the President noted:

> In the months after 9/11, I authorized a system of military commissions to try foreign terrorists accused of war crimes. . . . Yet the legality of the system I established was challenged in the court, and the Supreme Court ruled that the military commissions needed to be explicitly authorized by the United States Congress. And so I asked Congress for that authority, and they have provided it.

President Bush Signs Military Commissions Act of 2006, Oct. 17, 2006, *available at* http://www.whitehouse.gov/news/releases/2006/10/20061017-1.html.

[24] *See, e.g.*, *Agreement Is Reached on Detainee Bill*, N.Y. TIMES, Sept. 21, 2006, at A-1; R. Jeffrey Smith & Charles Babington, *Senators Near Pact on Interrogation Rules*, WASH. POST, Sept. 22, 2006, at A01. Finding middle ground with the President over how to deal with sensitive information in military commission proceedings was a concern for many Senators. For instance, Senator John McCain listed his priorities in the wake of *Hamdan* as follows:

> Ever since the Supreme Court announced its decision in the case of Hamdan v. Rumsfeld, I have made clear that my three primary goals for legislation authorizing military tribunals were: (1) Adjudicating the cases of detained terrorists in proceedings that are consistent with our values of justice, (2) *protecting classified information*, and (3) ensuring that our military and intelligence officers have clear standards for what is, and is not, permissible during detention and interrogation operations.

152 CONG. REC. S10,275 (daily ed. Sept. 27, 2006) (statement of Sen. McCain) (emphasis added).

such heavy negotiation on this topic was the harsh criticism of the expansive protection afforded to sensitive information under the Pentagon's procedural rules.[25] In particular, the legislators recognized the importance of allowing the accused to see the evidence brought against him in a manner that would withstand future Supreme Court scrutiny. Among other things, this would necessitate eliminating the Pentagon's procedural rules requiring the exclusion of the accused (and his civilian defense counsel) from portions of the proceedings that dealt with protected information.[26] At the same time, however, they struggled to devise a process that would enable the prosecution to admit evidence without exposing the sensitive sources, methods, or activities used to obtain that evidence to suspected terrorists, commission members, or the

---

[25] Those procedural rules were almost universally criticized by commentators both within and outside of the Judge Advocate community. *See, e.g.*, Kevin J. Barry, *Military Commissions: Trying American Justice*, ARMY LAW., Nov. 2003, at 1; Philip Allen Lacovara, *Trials and Error*, WASH. POST, Nov. 12, 2003, at A23 ("Further undermining the legitimacy of the process is the fact that the Defense Department's instructions for the military commissions grant broad discretion to the President and Secretary of Defense to close the entire proceeding, acting on undefined 'national security interests.'"); HUMAN RIGHTS FIRST, TRIALS UNDER MILITARY ORDER (2006), http://www.humanrightsfirst.org/us_law/PDF/detainees/trials_under_order0604.pdf.

[26] *See* DOD MCO No. 1, *supra* note 16, § 9.6(d)(5)(ii). Unlike those rules, the MCA does not allow for the exclusion of the accused from portions of his trial and does not permit the introduction of evidence before the commission without it being disclosed to the accused. Rather, it allows for the exclusion of the accused only for disruptive or dangerous conduct. *See* 10 U.S.C.S. § 949d(e) (LEXIS 2007). In drafting the rules for exclusion of the accused, legislators appear to have paid particular attention to the *Hamdan* Court's statement that "at least absent express statutory provision to the contrary, information used to convict a person of a crime must be disclosed to him." *Hamdan*, 126 S. Ct. at 2798. Legislators also apparently took to heart the concerns of senior Judge Advocates from the various armed services in this regard. *See, e.g.*, *Standards of Military Tribunals: Hearing Before the H. Comm. on Armed. Servs.*, 109th Cong. (2006) (statements of Major General Scott Black, United States Army, Judge Advocate General ("I can't imagine any military judge believing that an accused has had a full and fair hearing if all the Government's evidence that was introduced was all classified and the accused was not able to see any of it.") and Brigadier General James C. Walker, Staff Judge Advocate to the Commandant U.S. Marine Corps ("I concur with my colleagues that if we get to a point where the sole evidence against an accused is classified, he must be able to see that evidence. That's just essentially one of those elements of a full and fair trial."). In an editorial, *The New York Times*, a vociferous critic of the military commission procedures proposed under both the MCA and the Pentagon rules, noted the significance of the compromises that led to "Mr. Bush's agreement to drop his insistence on allowing prosecutors of suspected terrorists to introduce classified evidence kept secret from the defendant." N.Y. TIMES, Sept. 22, 2006, at A-20.

public at large, if such disclosure would be detrimental to national security.[27]

To begin with, the drafters of the MCA spurned the Pentagon procedural rules' concept of "protected information," deciding instead to limit protection to "classified information."[28] This greatly simplified the universe of information that could benefit from protection. The current Government information classification system was established in March of 2003 under Executive Order 13,292 (EO 13,292)[29] and sets forth the process through which information is to be classified and handled.[30] Among other things, it requires that information be classified according to its "sensitivity," or the degree to which the public disclosure of that

---

[27] Safeguarding counterintelligence means was clearly on the Senators' minds in the weeks leading up to the passage of the MCA. Weeks before it was passed, Senator William H. Frist noted that the bill which became the MCA "protects classified information—our critical sources and methods—from terrorists who could exploit it to plan another terrorist attack." 152 CONG. REC. S10,243 (daily ed. Sept. 27, 2006) (statement of Sen. Frist). Senator Levin added, "the bill does not permit the use of secret evidence that is not revealed to the defendant. Instead, the bill clarifies that information about sources, methods, or activities by which the United States obtained evidence may be redacted before the evidence is provided to the defendant and introduced at trial." 152 CONG. REC. S10,244 (daily ed. Sept. 27, 2006) (statement of Sen. Levin). Senator Lindsey Graham, a member of the Senate Armed Services Committee, remarked: "We're going to protect our classified information, and we're going to protect our methods and sources." James Rosen, *Graham Says Tribunal Bill Goes Too Far; Senator Upset By Clause to Withhold Relevant Evidence*, MYRTLE BEACH SUN-NEWS, Sept. 9, 2006, at A1.

[28] Classified information has been defined under the Classified Information Procedures Act (CIPA) as "any information or material that has been determined by the United States Government pursuant to an executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security." 18 U.S.C. app. III, § 1(a) (2000). CIPA defines "national security" as "the national defense and foreign relations of the United States." *Id*.

[29] Exec. Order No. 13,292, 3 C.F.R. 196 (2004).

[30] The stated purpose of the order is to establish "a uniform system for classifying, safeguarding and declassifying national security information, including information relating to defense against transnational terrorism." *Id.* With limited exception, the ability to classify information originally may be exercised only by the "original classification authorities," namely, the President, the Vice President (in the performance of executive duties) and agency heads and officials designated by the President in the *Federal Register*. *Id*. at 197. These original classification authorities must receive training on Executive Order No. 13,292 and its implementation directives (including possible criminal, civil and administrative sanctions in connection with unauthorized disclosures of the information) and may delegate their classification authority in writing to subordinate officials who have a "demonstrable and continuing" need to exercise it. *Id*. at 197-98.

information would damage national security.[31] By embracing the objective and recognized standard of classified information, the MCA provided a clear scope of information that would be afforded protection.

In addition to clarifying that only classified information is eligible for protection, the MCA established specific procedures for protecting classified information in military commission legal proceedings. As noted above, the MCA's provisions regarding the treatment of classified information were largely modeled after CIPA and MRE 505, a military evidentiary rule which itself is modeled after CIPA. The provisions of CIPA and MRE 505 do not apply to the MCA, as they apply to federal court proceedings and military law proceedings, respectively.[32]

---

[31] *See id*. at 215. Three classification sensitivity levels apply in the United States: (i) Top Secret, for information that, if publicly disclosed, reasonably could be expected to cause "exceptionally grave damage" to the national security; (ii) Secret, for information that, if publicly disclosed, reasonably could be expected to cause "serious damage" to the national security; and (iii) Confidential, for information that, if publicly disclosed, reasonably could be expected to cause "damage" to the national security if disclosed to the public. Note that it is impermissible to classify information in order to cover up illegal activities or merely because it would be embarrassing to state actors or others; information may only be classified to protect national security objectives. *See id*. at 200 (setting forth restrictions on reasons for classification).

[32] The availability of the federal courts and courts-martial as legal avenues that recognize and protect classified information has led some to assert that detainee prosecutions should take place in those systems. An examination of whether suspected terrorists should be tried either under these or other legal regimes instead of by military commissions is beyond the scope of this article. Nevertheless, with respect to the use of federal courts, the prosecution of Zacharias Moussaoui serves as a cautionary tale as far as disclosure of sensitive information is concerned. To the dismay of many, Moussaoui was prosecuted in federal court. *See, e.g.*, *Fox News Sunday* (Fox television broadcast Dec. 16, 2001) (statement of Sen. Joseph Lieberman) ("If [Moussaoui] is not a candidate for a military tribunal, who is?"); *Treatment and Trial of Certain Non-citizens in the War Against Terrorism, Hearing on Military Order on Detention Before the S. Armed Servs. Comm.*, 107th Cong. (2001) (statement of Sen. Carl Levin) ("The glove fits so perfectly here [for prosecution before a military commission]."); *see also* Editorial, *The Moussaoui Experiment*, WASH. POST, Jan. 27, 2003, at A18 (suggesting that Moussaoui's trial be moved to military court). Once Moussaoui was brought to the civilian courts, he benefited from the full range of rights afforded to criminal defendants who are American citizens, which he is not (he is a French citizen). For certain technical reasons, his case was not a CIPA case. Regardless, the prosecution had great difficulty restricting Moussaoui's access to sensitive information, and especially to sensitive sources. *See, e.g.*, United States v. Moussaoui, 365 F.3d 292 (4th Cir. 2004); A. John Rasdan, *The Moussaoui Case: The Mess from Minnesota*, 31 WM. MITCHELL L. REV. 1417 (2005) (discussing the challenges in prosecuting Moussaoui in the civil criminal courts). Trying Guantánamo detainees and other suspected terrorists in the federal court system would involve similar complications.

Nevertheless, before turning to the MCA itself, a brief overview of CIPA and MRE 505 procedures is helpful in understanding the relevant framework of laws existing at the time the drafters of the MCA established its military commission procedures.

According to the legislative history, CIPA was enacted primarily to deal with the issue of "graymail," a word-play on "blackmail" that essentially describes a situation where a criminal defendant attempts to force the Government to drop or reduce charges by threatening to disclose classified information.[33] However, CIPA ultimately dealt with the disclosure of classified information in federal proceedings in a more expansive way, addressing not only a defendant's threatened disclosures at trial,[34] but also providing a process for dealing with a defendant's discovery requests.[35] Specifically, when it comes to discovery, the court may authorize the Government to delete or substitute classified information contained in documents made available to a defendant.[36]

---

[33] *See* S. REP. NO. 96-823, at 2 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4294, 4295. The impetus for CIPA's passage was primarily to facilitate the criminal prosecution of Cold War-era spies. *See generally* Katherine L. Herbig & Martin F. Wiskoff, Defense Personnel Security Research Center, ESPIONAGE AGAINST THE UNITED STATES BY AMERICAN CITIZENS 1947-2001 (2002), *available at* http://www.fas.org/sgp/library/spies.pdf.

[34] *See* 18 U.S.C. app. III, § 5.

[35] *See id*. § 4 (allowing for the deletion, substitution or summarizing of classified information during discovery). "Congress intended section 4 to clarify the court's powers under Fed. R. Crim. P. 16(d)(1) to deny or restrict discovery in order to protect national security." United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988) (citing S. REP. NO. 823, at 6, *reprinted in* 1980 U.S.C.C.A.N. 4299-4300); *see also* United States v. Yunis, 867 F.2d 617, 621 (D.C. Cir. 1989) (stating that § 4 of CIPA "contemplates an application of the general law of discovery in criminal cases to the classified information area with limitations imposed based on the sensitive nature of classified information").

[36] 18 U.S.C. app. III § 4; *see also* Brian Z. Tamanaha, *A Critical Review of the Classified Information Procedures Act*, 13 AM. J. CRIM. L. 277, 291 n.73 (1986); Note, *Secret Evidence in the War on Terror*, 118 HARV. L. REV. 1962, 1962-63 (2005); United States v. Libby, 429 F. Supp. 2d 46, 48 (D.D.C. 2006). An authorization by the court to so delete or substitute requires a "sufficient showing" by the Government. Although "sufficient showing" is not defined in CIPA, as discussed in greater detail below, courts have fashioned standards and tests to determine whether defendants should prevail on CIPA discovery requests for classified information. *See infra* notes 84-97 and accompanying text.

Although beyond the scope of this article, note that CIPA also requires that a defendant file a notice describing the classified information he "reasonably expects to disclose or cause the disclosures of" at trial. 18 U.S.C. app. III, § 5(a). Hence, if classified information is disclosed to (or otherwise possessed by) a defendant who intends to use it in the proceedings, the Government may request a hearing to determine the "use, relevance or admissibility" of the information. *Id*. § 6(a). If the court then rules that the

In the military context, MRE 505 generally protects classified information from disclosure during criminal proceedings if the head of the executive or military department or Government agency concerned with the information asserts privilege over it by finding that the information itself is properly classified and that its disclosure "would be detrimental to national security."[37] When it comes to discovery, like CIPA, MRE 505 allows the Government to delete or substitute classified information in response to requests from an accused.[38] In relevant part, MRE 505 permits the military judge to authorize the deletion or substitution of classified information at the discovery stage, "unless the military judge determines that disclosure of the classified information itself is necessary to enable the accused to prepare for trial."[39]

Much like MRE 505, the MCA deploys a shield over classified information sought by an accused, establishing a process through which a "national security" privilege may be asserted.[40] This shield is deployed

---

classified information is admissible, the Government may move to substitute or summarize the information. *Id*. § 6 (c)(1). In fact, the court is *required* to grant the Government's motion for an alternative to outright disclosure if that alternative will provide the defendant "with substantially the same ability to make his defense as would disclosure of the specified classified information." *Id*.

[37] MCM, *supra* note 11, MIL. R. EVID. 505(c).

[38] *See id.* MIL. R. EVID. 505(g)(2). This evidentiary rule provides:

> Limited disclosure. The military judge, upon motion of the Government, shall authorize (A) the deletion of specified items of classified information from documents to be made available to the defendant, (B) the substitution of a portion or summary of the information for such classified documents, or (C) the substitution of a statement admitting relevant facts that the classified information would tend to prove, unless the military judge determines that disclosure of the classified information itself is necessary to enable the accused to prepare for trial. The Government's motion and any materials submitted in support thereof shall, upon request of the Government, be considered by the military judge in camera and shall not be disclosed to the accused.

Id.

[39] *Id*. Similar to § 6(a) of CIPA, MRE 505 allows the Government to make a motion for an in camera proceeding to determine whether, and in what form, classified information may be disclosed and used during the court-martial trial proceeding. *Id.* MIL. R. EVID. 505(i)(4). Classified information may only be disclosed if it is "relevant and necessary to an element of the offense or a legally cognizable defense." *Id.* MIL. R. EVID. 505(i)(4)(B); *see also* United States v. Lonetree, 31 M.J. 849, 856 (N.M.C.M.R. 1990), *aff'd* 35 M.J. 396 (C.M.A. 1992), *cert. denied,* 507 U.S. 1017 (1993).

[40] Specifically, § 949d(f)(1) of the MCA states:

during all stages of the proceedings, and hinges upon a finding by the head (or his designee) of the executive or military department or Government agency concerned that (i) the information is properly classified, and (ii) its disclosure would be detrimental to national security.[41] Once privilege is asserted, the accused may not disclose (or compel the disclosure of) the subject information.[42] The MCA also permits the military judge to authorize the prosecution to introduce either redacted documents or summary information to protect classified information from disclosure at trial.[43]

> (f) Protection of Classified Information-
>
> (1) NATIONAL SECURITY PRIVILEGE- (A) Classified information shall be protected and is privileged from disclosure if disclosure would be detrimental to the national security. The rule in the preceding sentence applies to all stages of the proceedings of military commissions under this chapter.
>
> (B) The privilege referred to in subparagraph (A) may be claimed by the head of the executive or military department or Government agency concerned based on a finding by the head of that department or agency that--
>
> (i) the information is properly classified; and
>
> (ii) disclosure of the information would be detrimental to the national security.

Note that the military judge may not assess the validity of the national security privilege. Rather, it appears that Congress intended to defer exclusively to the department or agency head on the substance of the privilege assertion, as determined in accordance with § 949d(f)(1)(B), and that the military judge's review consists merely of ensuring that the relevant department or agency head has made the required *finding* as to (i) the proper classification of the information at issue, and (ii) the potential impact of its disclosure.

[41] 10 U.S.C.S. § 949d(f)(1) (LEXIS 2007). In the words of Senator John McCain, "[W]hile ensuring a full and fair process, the legislation [that became the MCA] also recognizes the important role that classified information is likely to play in these trials. The legislation expressly provides the Government with a privilege to protect classified information." 152 CONG. REC. at S10,275 (daily ed. Sept. 7, 2006) (statement of Sen. McCain).

[42] Note that even after discovery, during an examination of a witness, trial counsel may object to admission into evidence of any classified information and the military judge (who may choose to review trial counsel's claim of privilege in camera and on an ex parte basis) must thereafter safeguard the information. 10 U.S.C.S. § 949d(f)(2)(C) (stating, in relevant part: "During the examination of any witness, trial counsel may object to any question, line of inquiry, or motion to admit evidence that would require the disclosure of classified information. Following such an objection, the military judge shall take suitable action to safeguard such classified information."). A parallel to this is found in CIPA, which requires that the court take protective action when the defense's questioning of a witness may require the disclosure of classified information. 18 U.S.C. app. III § 8(c) (2000).

[43] Section 949d(f)(2)(A) of the MCA states as follows:

However, unlike CIPA and MRE 505, the MCA specifically provides a mechanism for the protection of classified sources, methods or activities. In relevant part, § 949d(f)(2)(B) of the MCA states:

> (2) INTRODUCTION OF CLASSIFIED INFORMATION-
>
> * * *
>
> (B) PROTECTION OF SOURCES, METHODS, OR ACTIVITIES- The military judge, upon motion of trial counsel, shall permit trial counsel to introduce otherwise admissible evidence before the military commission, while protecting from disclosure the sources, methods, or activities by which the United States acquired the evidence if the military judge finds that (i) the sources, methods, or activities by which the United States acquired the evidence are classified, and (ii) the evidence is reliable. The military judge may require trial counsel to present to the military commission and the defense, to the extent practicable and consistent with national security, an unclassified summary of the sources, methods, or activities by which the United States acquired the evidence.[44]

In short, if the military judge determines that certain evidence is reliable and otherwise admissible, and permits the introduction of that evidence, he must protect the classified sources, methods or activities used to obtain that evidence, although he may require a summary of those counterintelligence means. Therefore, although the MCA brings the use and protection of sensitive information in military commission proceedings more in line with federal and military procedural law and closer to the expectations of the legal community, it goes out of its way to explicitly protect counterintelligence means from disclosure.[45]

> (A) ALTERNATIVES TO DISCLOSURE.—To protect classified information from disclosure, the military judge, upon motion of trial counsel, shall authorize, to the extent practicable—(i) the deletion of specified items of classified information from documents to be introduced as evidence before the military commission; (ii) the substitution of a portion or summary of the information for such classified documents; or (iii) the substitution of a statement of relevant facts that the classified information would tend to prove.

Id.

[44] *Id.* § 949d(f)(2)(B).

[45] This explicit protection of counterintelligence means was obviously intentional. In the words of Senator Lindsey Graham,

II. Technical Sources, Methods and Activities Employed in the GWOT

As previously discussed, the protection afforded to classified information under the MCA is largely consistent with that afforded under CIPA and MRE 505, with the notable exception of the explicit protection afforded under § 949d(f)(2)(B) of the MCA to sources, methods and activities used to obtain admissible evidence. But why is this the case? What prompted the drafters to take such an interest in—and such specific precautions concerning—the protection of GWOT counterintelligence means? The answer lies in the counterintelligence community's wide-ranging response to the September 11th attacks, and particularly on its heavy reliance upon technical counterintelligence means.

The Government has traditionally placed great emphasis on protecting its classified sources, methods and activities from disclosure, whether to the media through leaks or to the public at large through legal proceedings.[46] Its efforts in the GWOT are no exception. Of the

---

> We struck a great balance. . . . We need to be very clear that, in prosecuting the terrorists during a time of war, we do not have to reveal our sources and methods to protect us, our classified procedures. . . . But if the Government decides to provide information to the jury that would result in a conviction, sending someone to jail for a long period of time, or to the death chamber, an American trial must allow that person to know what the jury found them guilty of so they can confront the evidence.

Byron York, *The Detainee Deal: The White House Won—and So Did McCain*, NAT'L REV. ONLINE, Sept. 22, 2006, *available at* http://article.nationalreview.com/?q=YWYONTjhOGVjMGRkNTBkZGY1NTZkYTg4MGViY2I1ZTE=.

[46] The Government's protectiveness over such information in legal proceedings is not limited to restricting disclosure in U.S. courts; rather, it also has gone to great pains to protect its classified sources and methods in the context of international criminal justice. *See, e.g.*, Laura Moranchek, *Protecting National Security Evidence While Prosecuting War Crimes: Problems and Lessons for International Justice from the ICTY*, 31 YALE J. INT'L L. 477 (2006). For instance, the U.S. Government allowed its former officials to testify before the ICTY at Slobodan Milošević's trial only in a closed session with two Government officials present and with permission to delete any testimony from the record that it believed compromised U.S. national security. *Id*. at 484. The reason given for these conditions to testimony was as follows: "It is a matter of intelligence collection and a fear that sources and methods of obtaining information could be jeopardized if [the former officials] have to testify in open court." *Id*.; *see also* Ian Black, *Wesley Clark Testifies in Secret at Milosevic Trial*, GUARDIAN, Dec. 16, 2003, at 11; *Closed Session Ordered for Envoy's War Crimes Testimony*, AUSTRALIAN, June 14, 2002, at 9; Elaine Sciolino, *Clark Testifies Against Milosevic at Hague Tribunal*, N.Y. TIMES, Dec. 16, 2003, at A3.

counterintelligence means that have come to the public light, interrogation methods have dominated the headlines.[47] This public fascination with intelligence gathered through interrogations is understandable; it is a manifestation of our concern for the humane treatment of detainees and, as such, touches upon our core societal values. And yet, in the context of what has been—and will continue to be—truly important in the daily prosecution of the GWOT, it is a mistake to focus solely on interrogation tactics.[48] A wide array of other

---

[47] An examination of the validity or morality of detainee interrogation techniques employed by any DOD or governmental agency program is beyond the scope of this article. Nevertheless, it cannot be disputed that interrogations of suspected high-ranking terrorists have, at times, proved modestly effective in yielding useful intelligence. The CIA's High Value Terrorist Detainee Program has been particularly effective in this regard, reporting success in using interrogation methods that have led to the capture of al Qaeda operations chief Khalid Shaykh Mohammad, better known as the mastermind of the September 11 attacks, and Ramzi bin al-Shibh, another September 11 plotter. *See* OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, SUMMARY OF THE HIGH VALUE TERRORIST DETAINEE PROGRAM (2006), http://www.dni.gov/announcements/content/TheHighValueDetaineeProgram.pdf. Once captured, Khalid Shaykh Mohammad himself appears to have provided a plethora of information about other terrorists and planned operations. *See id*. Information from interrogations has also played an important part in averting additional terrorist plots, including one involving the destruction of commercial airliners from London in the summer of 2006. *See* Mark Mazzetti, *The Reach of War; New Generation of Qaeda Chiefs Is Seen on Rise*, N.Y. TIMES, Apr. 2, 2007, at A-1.

[48] As noted above, some critics have focused exclusively on potential invocation of privilege over counterintelligence sources, methods and activities to conceal in commission proceedings abusive and/or illegal interrogation techniques that may either embarrass the Government or permit coerced statements. *See supra* note 14. As one commentator states bluntly:

> The bill [that became the MCA] includes a number of provisions that protect classified "sources, methods, or activities" against being revealed. The likely impact of such provisions is to bar any inquiry into the CIA's abusive interrogation practices. (For sources, substitute "disappeared" detainees; for methods, substitute torture, and for activities, substitute water-boarding, stress positions, and days without sleep.)

Joanne Mariner, *The Military Commissions Act of 2006: A Short Primer*, Oct. 9, 2006, http://writ.news.findlaw.com/mariner/20061009.html; *see also* HUMAN RIGHTS WATCH Q & A, *supra* note 14, at 4 ("Unless military commission judges are extremely vigilant [in the application of protection over classified sources, methods and activities], the prohibition on evidence obtained through torture could be become virtually meaningless.").

While beyond the scope of this article, the admission of potentially "coerced" evidence is quite limited under the MCA. A statement obtained prior to the enactment of the Detainee Treatment Act of 2005 (42 U.S.C.S. § 2000dd (LEXIS 2007) [hereinafter DTA 2005]) where the degree of coercion is disputed, may be admitted *only* if the military judge

means have been employed with modest success and warrant protection from disclosure. Infiltration efforts and classic techniques involving human intelligence certainly are being used with increased vigor.[49] Most significant, however, and the central focus of this article, are those activities and methods that gather intelligence through technical means.

Technical means have been employed to monitor both terrorist communications and financial activity. On the communications front, one program that has been the subject of intense public scrutiny involves monitoring by the National Security Agency of communications where one party is located outside of the United States.[50] This program, known as the Terrorist Surveillance Program (TSP),[51] and similar "wire-tapping"

---

concludes that (i) the statement is reliable and possesses sufficient probative value, and (ii) that the interests of justice would be best served by admitting the statement; for statement obtained after enactment of DTA 2005, the military judge also must conclude that the interrogation methods used were not cruel, inhuman, or degrading. 10 U.S.C.S. § 948r.

[49] Improving human intelligence has been a common theme in administrative and congressional reviews since the September 11th attacks. *See, e.g.*, H. SUBCOMM. ON TERRORISM & HOMELAND SEC., H. PERM. SELECT COMM. ON INTELLIGENCE, REPORT ON COUNTERTERRORISM INTELLIGENCE CAPABILITIES AND PERFORMANCE PRIOR TO 9-11, 107th Cong. 2 (2002), *available at* http://fl1.findlaw.com/newsfindlaw.com/cnn/docs/terrorism/hsint1.71702thsrpt.pdf [hereinafter COUNTERTERRORISM CAPABILITIES REPORT] (recommending that CIA leadership "penetrate terrorist cells, disrupt terrorist operations and capture and render terrorists to law enforcement. . . . More core collectors need to be put on the streets."). The lack of human intelligence in Afghanistan and Iraq prior to the September 11th attacks is viewed as a major intelligence community failure. In fact, former National Security Advisor Samuel Berger testified before Congress that the United States maintained no significant intelligence assets in Afghanistan after 1989. *Joint Investigation into September 11th: Second Public Hearing Before the Joint H. & S. Intelligence Comms*., 107th Cong. (2002), *available at* http://www.fas.org/irp/congress/2002_hr/091902berger.pdf (statement by Samuel Berger); *see also* COUNTERTERRORISM CAPABILITIES REPORT, *supra*, at 2 ("CIA did not sufficiently penetrate the al-Qa'ida organization before September 11th. Because of the perceived reduction in the threat environment . . . and the concomitant reduction in resources for basic human intelligence collection, there were fewer operations, officers, fewer stations, fewer agents, and fewer intelligence reports produced.").

[50] According to a Department of Justice publication, this program is narrowly focused on international calls for which there is a reasonable basis to believe that one party to the communication is affiliated with al Qaeda. U.S. DEP'T OF JUSTICE, THE NSA PROGRAM TO DETECT AND PREVENT TERRORIST ATTACKS: MYTH V. REALITY 2 (2006), http://www.usdoj.gov/opa/documents/nsa_myth_v_reality.pdf.

[51] Although not aimed at intercepting an enemy nation's signals, the TSP nevertheless falls within classic signals intelligence. According to the DOD Definitions, signals intelligence is defined as "communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence, however transmitted." DOD DICTIONARY, *supra* note 6, at 492. The use of signals intelligence to track and capture non-state figures through their communications is not new. One noted case where it has been used is that

programs intended to monitor potential terrorist communications, have been the focus of the media and the public because of the privacy concerns they engender.[52] Nevertheless, the more novel and, quite possibly, more effective use of technical means has been to access and monitor *financial* activity and records to establish links between and among actors of interest and their funds. Using al Qaeda's financial network as a vehicle, the following subsection examines the financial networks (i.e., the "cycle" of their funds—generation, investment, and movement) of modern terrorist organizations and explores how certain technical counterintelligence means are being employed in the GWOT to exploit these financial networks.

---

of Kurdistan Workers' Party leader Abdullah Oçalan, who led a bloody war in the 1990s against Turkish forces for an independent Kurdish state. (There are approximately twenty-five million Kurds, primarily in Iraq, Iran, Syria and southeast Turkey, making them the largest ethnic population without a state in the world.) Oçalan was captured in 1999 in Kenya after being expelled some years earlier from Syria and subsequently being freed from house arrest in Italy. The exact circumstances of how he was located and apprehended are not clear, although *The New York Times* published a report citing unnamed U.S. sources claiming that U.S., British and Israeli intelligence agents tracked his mobile phone activity and passed on information about his whereabouts to Turkey. Tim Weiner, *U.S. Helped Turkey Find and Capture Kurd Rebel*, N. Y. TIMES, Feb. 20, 1999, at 1. The United States officially maintains it did not participate in the capture of Oçalan.

[52] The TSP was disclosed to the public in December 2005. *See, e.g.*, James Risen & Eric Lichtabu, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A-1. In a recent suit brought by the American Civil Liberties Union (ACLU) and certain journalists, academics and lawyers, a U.S. district court judge in Michigan held that the program's warrantless monitoring violated the Separation of Powers doctrine, the Administrative Procedures Act, the First and Fourth Amendments to the United States Constitution, and statutory law. *See* ACLU vs. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006). The Sixth Circuit, however, vacated the district court's order and remanded the case with instructions that it be dismissed for lack of jurisdiction based on the plaintiffs' inability to establish standing for any of their asserted claims. *See* ACLU v. NSA, Nos. 06-2095/2140, at 35 (6th Cir. July 6, 2007). The Government had argued that the President had the "inherent" authority under the Constitution to engage in signals intelligence as Commander-in-Chief, that the AUMF implicitly authorized the activity and that the telephone conversations were intercepted only where the Government "has a reasonable basis to conclude that one party to the communication is a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda." Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence, White House Press Briefing, Dec. 19, 2005, *available at* http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html.

A. Understanding Terrorist Organization Financial Networks

Relatively little money is required to implement any one terror operation. In fact, according to the 9/11 Commission, the attacks of September 11th, which were the most expensive operation ever undertaken by al Qaeda, cost "somewhere between $400,000 and $500,000 to plan and conduct."[53] Nevertheless, weapons, training, preparation for operations, and the day-to-day subsistence of operatives all require the generation, management and movement of funds. As a result, "follow the money" has been a lynchpin in the counterterrorism community's plan to locate al Qaeda associates and frustrate the organization's operational capabilities.[54] Indeed, President Bush emphasized the importance of crippling terrorist financial networks in an executive order issued soon after the September 11th attacks.[55]

---

[53] 9/11 COMMISSION REPORT, *supra* note 4, at 169. The operatives spent more than $270,000 in the United States and incurred "additional expenses includ[ing] travel to obtain passports and visas, travel to the United States, expenses incurred by the plot leader and facilitators outside the United States, and expenses incurred by the people selected to be hijackers who ultimately did not participate." *Id*. at 499 n.131.

[54] As the future co-Chairman of the 9/11 Commission, Lee H. Hamilton, noted:

> [T]racking al Qaeda financing is an effective way to locate terrorist operatives and supporters and to disrupt terrorist plots. . . . Following the money to identify terrorist operatives and sympathizers provides a particularly powerful tool in the fight against terrorist groups. Use of this tool almost always remains invisible to the general public, but it is a critical part of the overall campaign against al Qaeda.

National Commission on Terrorist Attacks Upon the United States, Statement Before the S. Comm. on Banking, Housing & Urban Affairs, 108th Cong. (2004) (statement of former Vice Chair Lee H. Hamilton and Commissioner Slade Gorton), *available at* http://banking.senate.gov/_files/joint_st.pdf.

[55] This executive order states, in relevant part:

> [B]ecause of the pervasiveness and expansiveness of the financial foundations of foreign terrorists, [this] Order authorizes the U.S. Government to block the assets of individuals and entities that provide support, services, or assistance to, or otherwise associate with, terrorists and terrorist organizations designated under [this] Order, as well as their subsidiaries, front organizations, agents, and associates. . . . I also find that because of the pervasiveness and expansiveness of the financial foundation of foreign terrorists, financial sanctions may be appropriate for those foreign persons that support or otherwise associate with these foreign terrorists. I also find that a need exists for further consultation and cooperation with, and sharing of information by, United States and foreign financial

Considering the depth and sophistication of the al Qaeda financial network, leveraging technical means to accomplish the ends envisioned by this executive order was clearly born of necessity.

It is now well-known that al Qaeda has generated millions of dollars from multiple sources, actively managed its financial investments and operated small businesses throughout the world.[56] In fact, the organization has its own finance and business committee charged with the management and transfer of its funds around four continents.[57] Financial training and acumen is viewed as a critical aspect of al Qaeda's operational capability, as evidenced by the detailed instructions provided in its military training manual, *Declaration of Jihad Against the Country's Tyrants*.[58] The organization's financial network has truly proven resilient, primarily because of the limited information disclosed to the web of players involved and the diversification of its activities in the generation, management, and movement of funds.

Al Qaeda and its associates have been extremely successful in generating income from public and private donations, as well as crime. Donations have come from wealthy individuals, but appear mostly to derive from legitimate government and private Islamic benevolent organizations and charities.[59] In Saudi Arabia, in particular, government

---

> institutions as an additional tool to enable the United States to combat the financing of terrorism.

Exec. Order No. 13,224, 3 C.F.R. 786 (2002). Through this executive order, President Bush froze the assets of twenty-seven organizations and individuals having suspected links to terrorists. Thirty-nine names were added within the next month.

[56] As the 9/11 Commission noted, "al Qaeda had many sources of funding and a pre-September 11th annual budget estimated at $30 million." 9/11 COMMISSION REPORT, *supra* note 4, at 170.

[57] ROHAN GUNARATNA, INSIDE AL QAEDA: GLOBAL NETWORK OF TERROR 81 (2003). It also uses regional financial officers to further manage its funds. *Id*.

[58] *Id*. at 83-84. Among other things, this document instructs the reader how to counterfeit currency and credit cards and forge official documents. *Id*. Interestingly, it articulates several financial security principles, including the following: (i) funds should be either invested for financial return or set aside (and scattered) for use in operations; (ii) very few members should know the location of funds at any one time; and (iii) monies should be left with non-members of the organization. *Id*. at 84.

[59] As the 9/11 Commission pointed out, "Al Qaeda and its friends took advantage of Islam's strong calls for charitable giving, *zakat*. These financial facilitators also appeared to rely heavily on certain imams at mosques who were willing to divert *zakat* donations to al Qaeda's cause." 9/11 COMMISSION REPORT, *supra* note 4, at 170. Some of these donations have been generated from unwitting philanthropic organizations. *See, e.g.*, William E. Wechsler, *Strangling the Hydra: Targeting al Qaeda's Finances*, *in* HOW

officials have failed to effectively curb the open support provided to groups suspected of supporting terrorist organizations.[60] And yet, al Qaeda does not subsist on donations alone. Another primary source of income generation for the organization is crime. In fact, intelligence sources estimate that al Qaeda's European network raises approximately $1 million per month through credit card fraud alone.[61]

Once terrorist organizations generate and accumulate funds, they must deposit, manage and, at times, invest them until such time as they are needed for operational purposes.[62] Al Qaeda's investments have been exceptionally diverse, both geographically and substantively. For instance, it has invested in fishing, hospital equipment, the dairy industry and paper mills.[63] Although definitive proof is lacking, al Qaeda funds have also been tied to the illegal diamond trade.[64]

Effecting operational plans necessarily requires the movement of funds. Criminals throughout history have devised creative ways to move funds. Islamic terrorist networks, in particular, appear to use three primary methods: the formal banking system, cash couriers, and *hawala*, a traditional and unregulated arrangement for capital transfer

---

DID THIS HAPPEN? TERRORISM AND THE NEW WAR 137 (James F. Hodge, Jr. & Gideon Rose eds., 2001).

[60] Indeed, it appears "al Qaeda found fertile fund-raising ground in Saudi Arabia, where extreme religious views are common and charitable giving was both essential to the culture and subject to very limited oversight." 9/11 COMMISSION REPORT, *supra* note 4, at 171.

[61] GUNARATNA, *supra* note 57, at 87.

[62] Note that "operational purposes" may mean expenditures directly related to terrorist acts, such as the rental of a Ryder® truck by convicted terrorist Muhammad Salameh and his co-bombers in connection with the 1993 World Trade Center bombing. However, it may also mean day-to-day expenditures, such as rent payments for sleeper cells and training facility necessities.

[63] GUNARATNA, *supra* note 57, at 90.

[64] *See generally* DOUGLAS FARAH, BLOOD FROM STONES (2004). *See also* Douglas Farah, *Al Qaeda Cash Tied to Diamond Trade: Sale of Gems From Sierra Leone Rebels Raised Millions, Sources Say*, WASH. POST, Nov. 2, 2001, at A01 (reporting that one European investigator opined: "I now believe that to cut off al Qaeda funds and laundering activities you have to cut off the diamond pipeline. . . . We are talking about millions and maybe tens of millions of dollars in profits and laundering."); *Al Qaeda Bought Diamonds Before 9/11*, USA TODAY, Aug. 7, 2004 (reporting witness accounts that six senior al Qaeda associates dealt directly with then-Liberian President Charles Taylor and other warlords beginning in 1999). Nevertheless, the 9/11 Commission concluded: "we have seen no persuasive evidence that al-Qaeda funded itself by trading in African conflict diamonds." 9/11 COMMISSION REPORT, *supra* note 4, at 171.

based on trust.[65] Current intelligence indicates that al Qaeda increasingly relies on transferring funds through *hawala* and simple cash couriers.[66]

---

[65] Several forms of *hawala* exist, mostly in South Asia and in the Middle East. In its simplest form, it consists of a broker located in one location taking a fee to transfer money to a recipient in a different location through a trusted contact of the broker. The steps of a typical *hawala* transaction are as follows: (i) the sender gives the broker the amount to be transferred, plus his fee (typically about one percent of the transaction), (ii) the broker notifies a personal contact in proximity of the recipient of the intended transfer through e-mail, instant message, phone, or fax, (ii) the contact approaches the recipient, who often must provide a pre-designated password or detail to complete the transaction, (iii) the contact extends the money to the recipient, and (iv) the broker and his contact keep detailed ledgers and either cancel existing debt or physically settle the transaction by falsifying invoices for phantom goods and services or by providing goods (including commodities such as gold and diamonds) or services of equivalent value as an alternative to cash. The system relies on a high level of trust between the broker and his contact, as their bilateral settlement is not secured.

Large-scale use of *hawala* appears to have begun in the 1940s when, for a variety of reasons, an enormous number of people migrated from South Asian rural areas to cities throughout the world, transferring what wealth they could through trusted friends and extended family. Michelle Cottle, *Hawalah v. The War on Terrorism*, NEW REPUBLIC, Oct. 15, 2001, at 1-2. *Hawala* exploded in the 1960s and 1970s, as migrants of Asian and Middle Eastern expatriates arranged to send earnings to family members in their country of origin without paying the high banking and exchange rates required of such transfers in the official banking system. *Id*.

> Hawala remains a significant method for large numbers of businesses of all sizes and individuals to repatriate funds and purchase gold . . . . It is favoured because it usually costs less than moving funds through the banking system, it operates 24 hours per day and every day of the year, it is virtually completely reliable, and there is minimal paperwork required."

ORG. FOR ECON. CO-OPERATION AND DEV. (OECD) FIN. ACTION TASK FORCE ON MONEY LAUNDERING, REPORT ON MONEY LAUNDERING TYPOLOGIES 1999–2000 (2000), http://www.fatf-gafi.org/dataoecd/29/37/34038120.pdf.

[66] In fact, the Department of the Treasury Under Secretary for Terrorism and Financial Intelligence noted in 2004:

> As the formal and informal financial sectors become increasingly inhospitable to financiers of terrorism, we have witnessed an increasing reliance by al-Qaida and terrorist groups on cash couriers. The movement of money via cash couriers is now one of the principle methods that terrorists use to move funds.

Legislative Proposals to Implement the Recommendations of the 9/11 Commission: Hearing Before the H. Comm. on Fin. Servs., 108th Cong. 35 (2004) (Prepared testimony of Stuart A. Levey, Undersecretary for Terrorism and Financial Intelligence, U.S. Department of the Treasury) [hereinafter Levey FSC Testimony]). Charitable organizations also may be used by terrorist organizations to move funds.

Although the transfer of money using cash couriers is inherently invisible to technical monitoring, this is not the case for transfers effected through the formal banking system and, to a lesser extent, *hawala*, which itself often makes use of the formal banking system.

With respect to with *hawala*, it is important to note that its link to terrorist financing is not theoretical. In fact, the 9/11 Commission concluded that al Qaeda frequently moved money through *hawala* prior to the September 11th attacks.[67] The vast scope of *hawala* in areas of al Qaeda influence is also telling.[68] At first blush, *hawala* transactions may appear impossible to uncover or monitor. Yet there are components of *hawala* that utilize the formal banking system, most significantly the ultimate settlement between the broker and his contact, which may be effected through traditional money transfers or deposits.

Despite a heavy reliance on *hawala*, terrorist organizations such as al Qaeda also move funds directly through the formal banking system, relying on the low level of scrutiny over money transfers where the amount transferred does not raise suspicion.[69] As the 9/11 Commission

---

[67] 9/11 COMMISSION REPORT, *supra* note 4, at 171. One notable such case is that of Dihab Shill, a Somali-based *hawaladar* (broker) that was identified as the financier of the 1998 attacks on the American embassies in Kenya and Tanzania. One terrorist involved in the attack, Mohamed Al-Owhali, apparently had no money or identity papers, but was nevertheless able to receive funds from Dihab Shill because the al Qaeda contact who sent him cash from Yemen had written a note on the transfer which, according to the Dihab Shill owner in Nairobi, Kenya, said: "This person doesn't have any proper documents . . . please give him without documents." John Willman, *Trail of Terrorist Dollars That Spans the World*, FIN. TIMES, Nov. 29, 2001, at https://specials.ft.com/attack onterrorism/FT3RNR3XMUC.html. Note, however, that the 9/11 Commission found no evidence of *hawala* being used in connection with the September 11 attacks. 9/11 COMMISSION REPORT, *supra* note 4, at 499 n.131.

[68] For instance, according to the estimates of Shaukut Aziz, Pakistan's Minister of Finance and a former executive vice president of Citibank in New York, as of 2001, Pakistani *hawala* networks accounted for transfers of between two and five billion U.S. dollars per year; on the higher end, this is many multiples greater than the amount of foreign transfers made annually through the official Pakistani banking system. *See* Douglas Frantz, *A Nation Challenged: Ancient Secret System Moves Money Globally*, N.Y. TIMES, Oct. 3, 2001, at 2.

[69] *See* U.S. Dep't of Treasury Secretary John W. Snow, Letter to the Editor, N.Y. TIMES, June 29, 2006 [hereinafter Secretary Snow Letter] (stating "[w]hile terrorists are relying more heavily than before on cumbersome methods to move money, such as cash couriers, we have continued to see them using the formal financial system . . ."). It stands to reason that the lower the amount involved, the less the ability of the bank to flag and scrutinize a cash transaction due to the sheer volume of daily transactions. The Bank Secrecy Act of 1970, which was amended by the USA PATRIOT Act of 2001,

concluded, "[t]he conspiracy made extensive use of banks in the United States. The hijackers opened accounts in their own names, using passports and other identification documents. Their transactions were unremarkable and essentially invisible amid the billions of dollars flowing around the world every day."[70] Nevertheless, despite terrorist financial networks' efforts to fly under the wire of financial scrutiny, the fact remains that whether as a component of *hawala* or otherwise, they have used and, to some extent, must continue to use, the formal banking system to subsist and to effect their operations.

B. Counterintelligence Means for Financial Monitoring Used in the GWOT

As the preceding subsection highlights, terrorist organizations such as al Qaeda must generate, manage and move funds for operational purposes, much like a legitimate enterprise. In taking each of these steps, they often leave behind banking or other financial tracks that the counterintelligence community could uncover and exploit. A sophisticated surveillance program may be able to sift through mounds of financial data and capture critical information.

Based on this potential, intelligence, law enforcement, and other agencies scrambled to arm themselves with enhanced financial monitoring abilities in the wake of September 11th, often enlisting the help of private sector companies.[71] Among other efforts, programs were established to monitor the formal money transfer, credit card charge and banking system—i.e., the banking footprints—of terrorists. Tracking the formal banking system has provided concrete leads on terrorists and their intended operations.[72] One early tracking effort was a Department of

---

established an arbitrary threshold of $10,000 for daily cash transactions, above which U.S. banks must file a report known as a "Currency Transaction Report." 31 U.S.C. §§ 5313, 5316(a) (2000). Note, however, that U.S. banks must also file a "Suspicious Activity Report" where the bank "knows, suspects or has reason to suspect" that questionable cash transactions are being effected. *Id.* § 5318(g).

[70] 9/11 COMMISSION REPORT, *supra* note 4, at 14 (Executive Summary).

[71] *See id.* at 382 (noting that the world financial community has provided strong cooperation in supplying relevant information for investigations).

[72] According to Treasury Department Undersecretary Levey:

> [W]hile terrorist supporters may use code names on the phone, when they send or receive money through the banking system, they often provide information that yields the kind of concrete leads that can

Defense collaboration with a company named First Data, which at the time owned the money-transfer company, Western Union.[73] But a more prominent program that has recently come to light is not operated by the intelligence agencies or traditional law enforcement. Rather, it is run by the Treasury Department and is named the Terrorist Finance Tracking Program (TFTP).[74] A critical aspect of this program is the ability to make queries into the vast database of international wire transactions managed by a Belgian firm named SWIFT (Society for Worldwide Interbank Financial Telecommunication). SWIFT is an industry-owned cooperative managing much of the world's financial-message traffic, processing millions of electronic messages daily from banks, brokerages, and investment managers in connection with international transactions.[75]

> advance an investigation. For these reasons, counter-terrorism officials place a heavy premium on financial intelligence. . . . Despite attempts at secrecy, terrorist facilitators have continued to use the international banking system to send money to one another, even after September 11th.

The Terror Finance Tracking Program: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Fin. Servs., 108th Cong. 44 (2006) (Prepared testimony of Stuart A. Levey) [hereinafter Levey HFSSOI Testimony].

[73] First Data, which operates globally, processes massive volumes of credit charge charges and, as such, has access to who purchases what and where they live. *See* RON SUSKIND, THE ONE PERCENT DOCTRINE 38 (2006). According to its web site, a sender may send money through Western Union to 245,000 agent locations in over 200 countries. WesternUnion, http://www.westernunion.com/info/selectCountry.asp?origination=global (last visited Oct. 4, 2007).

[74] The first public admission of the existence of the program was made on 22 June 2006. *See* Glen R. Simpson, *U.S. Is Moving on Several Fronts to Police Financial Transactions*, WALL ST. J., June 24, 2006, at A4; *see also* Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A-1; Barton Gellman, et al., *Bank Records Secretly Tapped*, WASH. POST, June 23, 2006, at A-1; Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A-1.

[75] According to its web site, SWIFT was founded in 1973 with the mission of "creating a shared worldwide data processing and communications link and a common language for international financial transactions." SWIFT, About SWIFT, http://www.swift.com/index.cfm?item_id=1243 (last visited Oct. 4, 2007). SWIFT's web site indicates exactly how expansive its reach is, reporting that it currently provides messaging services and interface software to nearly 8,100 financial institutions in 206 countries. SWIFT, About SWIFT, http://www.swift.com/index.cfm?item_id=62272 (last visited Oct. 4, 2007). Once the TFTP was publicly acknowledged by a U.S. Government official, SWIFT issued the following statement to help allay fear in the financial markets of abuse:

> In the aftermath of the September 11th attacks, SWIFT responded to compulsory subpoenas for limited sets of data from the Office of Foreign Assets Control of the United States Department of the

SWIFT does not handle funds per se, but does handle over 2.5 billion sets of transfer instructions and transaction confirmations each year.[76]

According to Treasury officials, the TFTP has been highly successful, leading not only to the apprehension of suspected terrorists, but also to the disruption of existing terrorist cells and pending operations.[77] The program's successes are believed to include information leading to arrests in connection with the 2002 Bali bombings and the arrest of a key player in Iraqi terrorism, as well as useful information related to the 2005 London bombings.[78]

The importance of these and similar (whether not yet publicly disclosed or not yet developed or implemented) governmental efforts warrants their protection from unnecessary disclosure. Disclosures from media leaks have already damaged programs employing technical counterintelligence means in the GWOT. The TFTP is one such example. In a letter to the editors of The New York Times, Treasury Secretary John W. Snow underscored the damage to intelligence efforts caused by the program's disclosure, stating that the newspaper had "undermined a highly successful counter-terrorism program and alerted terrorists to the methods and sources used to track their money trails."[79]

> Treasury. Our fundamental principle has been to preserve the confidentiality of our users' data while complying with the lawful obligations in countries where we operate.

Press Release, Statement on Compliance by SWIFT, June 23, 2006, *available at* http://www.swift.com/index.cfm?item_id=59904.

[76] Glen R. Simpson, *Treasury Tracks Financial Data in Secret Program*, WALL ST. J., June 23, 2006, at A1.

[77] In the words of then-Treasury Secretary John W. Snow: "I am particularly proud of our Terrorist Finance Tracking Program which, based on intelligence leads, carefully targets financial transactions of suspected foreign terrorists." U.S. Department of the Treasury Press Release, John W. Snow, Secretary of the Treasury (June 22, 2006), *available at* http://www.treas.gov/press/releases/js4332.htm.

[78] *See* Levey HFSSOI Testimony, *supra* note 72 (noting that the program "played an important role in the investigation that eventually culminated in the capture of Hambali, Jemaah Islamiyya's Operations Chief, who masterminded the 2002 Bali bombings" and uncovered "a key piece of evidence that confirmed the identity of a major Iraqi terrorist facilitator and financier").

[79] In relevant part, Secretary Snow's letter stated:

> The decision by The New York Times to disclose the Terrorist Finance Tracking Program, a robust and classified effort to map terrorist networks through the use of financial data, was irresponsible and harmful to the security of Americans and freedom-loving people

Unnecessarily disclosing the existence and workings of classified sources, methods and activities such as the TFTP in military commission proceedings would exacerbate damage which has already been inflicted by media leaks, and would substantially impair—or, in some cases, render worthless—those means. Disclosing similar programs (whether tracking finances, physical movement, communications, internet use, etc.) would have the same practical effect on intelligence gathering as executing scores of trusted agents and informants. This is something the counterintelligence community could ill afford.

III. An Analysis of the MCA's Protection of Technical Sources, Methods and Activities under CIPA

The preceding sections have established that technical classified sources, methods and activities employed in the GWOT—particularly those monitoring terrorist financial networks—are a critical component of the overall counterintelligence effort. Furthermore, these technical classified means often will not be stale at the time of the relevant legal proceedings, and the drafters of the MCA recognized that their disclosure may cause significant damage to ongoing counterintelligence programs. The remaining question is whether the specific protections afforded to these means under § 949d(f)(2)(B) of the MCA would withstand judicial scrutiny.[80] This section argues that they should.

The courts have recognized the Government's strong interest in protecting classified counterintelligence means in the context of terrorism cases.[81] In fact, when it comes to counterintelligence means,

---

> worldwide. In choosing to [expose this program], The Times undermined a highly successful counter-terrorism program and alerted terrorists to the methods and sources used to track their money trails.

Secretary Snow Letter, *supra* note 69. Following the disclosure of the program, Treasury Undersecretary Levey testified: "The Terrorist Finance Tracking Program was . . . an invisible tool. Its exposure represents a grave loss to our overall efforts to combat al Qaida and other terrorist groups." Levey HFSSOI Testimony, *supra* note 72.

[80] *See* 10 U.S.C.S. § 949d(f)(2)(B) (LEXIS 2007).

[81] *See, e.g.*, United States v. Walker-Lindh, 198 F. Supp. 2d 739, 742 (E.D. Va. 2002); United States v. Bin Laden, 58 F. Supp. 2d 113, 121 (S.D.N.Y. 1999). As one court stated in an attempt to disclose surveillance information under the Foreign Intelligence Surveillance Act, "[i]n the area of foreign intelligence gathering, the need for extreme

judicial concern with the protection of sources and methods in connection with terrorism cases, particularly where investigations are ongoing, predates the September 11th attacks[82] and extends even to interrogation techniques.[83] As the *Hamdan* Court noted, the Government "has a compelling interest in denying [the accused] access to certain sensitive information."[84] Outside of the terrorism context, the Supreme Court clearly stated in a case dealing with the threatened disclosure of intelligence sources and methods that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation. . . . Measures to protect the secrecy of our Government's foreign intelligence operations plainly serve these interests."[85] Nevertheless, judicial trends and sweeping dicta merely provide us with an interesting historical backdrop; they cannot accurately predict how the courts would deal with a challenge to the MCA's protection under § 949d(f)(2)(B) of classified counterintelligence means, particularly as they apply to technical means. Rather, support for the position that the MCA should withstand judicial scrutiny is found by comparing the MCA's protection

---

caution and sometimes even secrecy may not be overemphasized." United States v. Ott, 637 F. Supp. 62, 65 (E.D. Ca. 1986), *aff'd*, 827 F.2d 473, 475 (9th Cir. 1987).

[82] *See Bin Laden*, 58 F. Supp. 2d at 121 (In considering whether to require security clearances for defense counsel, the court stated that concern over the disclosure of classified information is "heightened in this case because the Government's investigation is ongoing, which increases the possibility that unauthorized disclosures might place additional lives in danger.").

[83] For instance, in the prosecution of John Walker-Lindh in 2002, a federal district court acknowledged that "given the nature of al Qaeda and its activities, and the ongoing federal law enforcement investigation into al Qaeda, the identities of the [interviewed] detainees, as well as the questions asked and the techniques employed by law enforcement agents in the interviews are highly sensitive and confidential." *Walker-Lindh*, 198 F. Supp. 2d at 742.

[84] Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2798 (2006). Sources of intelligence information have been protected across the federal legal landscape, and not just in connection with terrorism trials. For example, in *CIA v. Sims*, 471 U.S. 159, 175 (1985), the Supreme Court recognized the broad authority of the director of Central Intelligence to withhold intelligence sources from Freedom of Information Act disclosure requests, reiterating its position in *Snepp v. United States*, 444 U.S. 507, 509 n.3 (1980) (per curiam), that "the [g]overnment has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."

[85] Haig v. Agee, 453 U.S. 280, 307 (1981) (quoting Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964), a case where the public disclosure of the CIA station chief in Athens, Greece, was quickly followed by his assassination).

of such means with CIPA's well-established and recognized procedures.[86]

Consider the simple example of a classified counterintelligence program that tracks global money transfers, much like the TFTP. Let us assume that this hypothetical program uncovers the existence of a wire transfer confirmation, demonstrating that an accused received funds from a bank account held by a charitable organization with purported ties to al Qaeda. Let us further assume that the prosecution intends to admit the wire confirmation into evidence at trial, and that the confirmation is otherwise discoverable and admissible.

Before embarking on our analysis, it is helpful to frame the circumstances under which the identity of the hypothetical financial monitoring program could be disclosed in the proceedings, so as to isolate which provisions of CIPA and the MCA are relevant to the analysis. Classified information may be disclosed during legal proceedings by either the accused or the prosecution. With respect to the prosecution, such disclosure may be intentional, as part of the prosecution's case or in response to a discovery request. It is highly unlikely that an accused would know of the existence of the financial monitoring program that led to the collection of evidence against him; as such, the accused himself would not be in a position to disclose the existence of the program.[87] Also, for obvious reasons, the Government would want to maintain the program's anonymity and would not disclose it as part of its case if the court did not require it to do so. Hence, a disclosure of the program during legal proceedings is most likely to occur only if the prosecution's response to the accused's discovery request identifies the source of the wire confirmation. This section contends that CIPA and the MCA would prevent such a disclosure in similar ways.

---

[86] As the original statute addressing the procedures for disclosure of classified information in legal proceedings, CIPA has more developed case law than MRE 505. Hence, this analysis focuses solely on CIPA. CIPA itself has withstood the test of time and its provisions have repeatedly been found constitutional. *See, e.g.*, United States v. Pringle, 751 F.2d 419, 427-28 (1st Cir. 1984); United States v. Wilson, 750 F.2d 7 (2d Cir. 1984); *see also* Timothy J. Shea, Note, *CIPA Under Siege: The Use and Abuse of Classified Information in Criminal Trials*, 27 AM. CRIM. L. REV. 657 (1990).

[87] Note further that § 5 of CIPA and § 949d(f)(1) of the MCA would prevent the accused from disclosing such information unless and until vetted by the court.

A. Analysis of the Discovery Request Under CIPA

As Congress and the courts have made clear, CIPA was not intended to create new rules of relevance and admissibility.[88] Rather, "CIPA's fundamental purpose is to protect and restrict the discovery of classified information in a way that does not impair the defendant's right to a fair trial. It is essentially a procedural tool . . . ."[89] Under CIPA discovery procedures, the Government may petition the court to delete or substitute information contained in documents to be made available to a defendant.[90] To this end, the prosecution may submit documents—which the court may review in camera and ex parte—to make the "sufficient showing" required in support of its motion.[91] Upon such a petition, the Court essentially must determine how important the requested information is to the defendant's case. The standard for making this

---

[88] *See* S. REP. NO. 96-823, at 8 (1980); H.R. NO. 96-1436, at 12 (1980) (Conf. Rep.); United States v. Johnson, 139 F.3d 1359, 1365 (11th Cir. 1998) ("CIPA has no substantive impact on the admissibility or relevance of probative evidence.") (citations omitted).

[89] United States v. Dumeisi, 424 F.3d 566, 578 (7th Cir. 2005) (citations and quotations omitted); *see also* United States v. Smith, 780 F.2d 1102, 1106 (4th Cir. 1985) (en banc) (stating that "[t]he circuits that have considered the matter agree with the legislative history . . . that ordinary rules of evidence determine admissibility under CIPA") (citations omitted).

[90] 18 U.S.C. app. III, § 4; *see also Pringle*, 751 F.2d at 427; United States v. Libby, 429 F. Supp. 2d 46, 47 (D.D.C. 2006). Irrespective of the CIPA discovery procedures, the Government's obligation to disclose any evidence in its possession that is exculpatory to a defendant in accordance with *Brady v. Maryland*, 373 U.S. 83, 87 (1963), remains. Although the Supreme Court has stated that "[t]here is no general constitutional right to discovery in a criminal case and *Brady* did not create one," *Weatherford v. Bursey*, 429 U.S. 545, 559 (1977), the Government would withhold such evidence at its own risk. *See* United States v. Ramirez, 54 F. Supp. 2d 25, 33 (D.D.C. 1999). To properly comply with its *Brady* obligations, the Government would need to assess whether the evidence in its possession was arguably exculpatory and, if so, should submit the evidence to the court for an in camera and ex parte review to secure judicial approval for withholding it from the defense. *See* United States v. Felt, 491 F. Supp. 179, 184 (D.D.C. 1979).

[91] *See* 18 U.S.C. app. III, § 4; *see also* H.R. REP. NO. 96-831, at 27 n.22 (1980), *reprinted in* 1980 U.S.C.C.A.N. 4307 (stating that an adversarial proceeding at this stage "would defeat the very purpose" of the Government's request to withhold discovery of the classified materials at issue); United States v. Clegg, 740 F.2d 16, 17 (6th Cir. 1984) (noting that the district court allowed the Government to submit classified and unclassified documents for in camera ex parte review to establish their materiality to the defense); *Libby*, 429 F. Supp. 2d at 48 (stating that the court can envision making determinations regarding the materiality of classified information in the preparation of the defense ex parte "if the Government is of the view that simply disclosing the nature or mere existence of certain classified information would alone pose significant harm to national security").

determination is that a defendant should have "substantially the same ability to make his defense" whether or not disclosure occurs.[92] The requested information must be more than theoretically relevant to the defense; rather, it must be material and helpful to the defendant's preparation of his case.[93] In practical terms, a defendant first must demonstrate that the requested information is "relevant" to his case.[94] Once a defendant has met this low threshold, the Government may assert a "colorable" claim of privilege over the information.[95] Upon doing so, the defendant must then demonstrate that the information would be helpful to his defense.[96]

Applying the above standards and steps to our hypothetical wire transfer confirmation, let us examine how a court would apply CIPA to deal with a Government petition to remove references to the classified counterintelligence program in materials it is to make available to a defendant. A defendant certainly should be able to demonstrate that the methods used by the Government to acquire the confirmation are relevant to his case. Similarly, the Government should be able demonstrate a colorable claim of privilege over its classified financial monitoring program, as disclosure of its mere existence could have disastrous consequences on its continued utility. Hence, it would be left to the court to determine whether the identity (and, perhaps, certain details) of the program at issue is material and helpful to the defense and, therefore, warrant disclosure.

---

[92] Note that this standard is explicitly set forth for determinations regarding substitutions for classified information *at trial*, and not for responses to discovery requests. 18 U.S.C. app. III, § 6(c). Nevertheless, courts have applied this same standard for substitution determinations at the discovery stage, as doing so is in line with the underlying purpose of the Act.

[93] *See* United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) (stating that classified information must be at least helpful to the defense, and not just theoretically relevant); *Smith*, 780 F.2d at 1110 (stating that courts should order the disclosure of classified information only if it is "at least essential to [the] defense, necessary to the defense, and neither merely cumulative nor corroborative") (internal citation and quotation marks omitted); *see also* United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998); *Libby*, 429 F. Supp. 2d at 48.

[94] *See Yunis*, 867 F.2d at 623.

[95] *Id*.

[96] *Id*. In connection with its determinations, some circuit courts have adopted balancing tests to weigh the defendant's right to prepare his defense against the public's interest in preventing disclosure of classified information. *See, e.g.*, United States v. Sarkissian, 841 F.2d 959, 965 (9th Cir. 1988); *Smith*, 780 F.2d at 1110.

Such disclosure is highly unlikely to be material or helpful to the defense. An insightful parallel may be drawn here with *U.S. v. Pringle*, where the defendants sought discovery under Federal Rule of Criminal Procedure 16 of "materials related in any conceivable way to the surveillance, boarding and seizure" of their vessel by the U.S. Coast Guard.[97] The Government moved for protection of its classified information under, *inter alia*, CIPA §§ 3 and 4.[98] The district court concluded, following an ex parte, in camera review of the materials at issue, that when it came to surveillance information, it "was neither relevant nor helpful to the defense of the accused, nor otherwise essential to the fair adjudication of the case and, hence, not discoverable under [Rule 16]."[99] The circuit court agreed, noting that such information was not relevant to the guilt or innocence of the defendants.[100]

Technical classified means, such as the surveillance methods used by the U.S. Coast Guard in *Pringle*, are by their very nature unlikely to be exculpatory or even helpful to the defense. In our hypothetical case, the defendant likely would focus his defense on avenues such as his lack of personal involvement in the transfer, a legitimate business purpose for accepting funds from the organization's account, or his lack of knowledge as to the organization's illicit activities, and not on attacking the program that discovered the wire transfer communication. Scenarios certainly could be envisioned where the reliability or accuracy of the program is compromised.[101] And yet, by and large, technical means such

---

[97] United States v. Pringle, 751 F.2d 419, 425 (1st Cir. 1984). In relevant part, Rule 16(d)(1) provides as follows:

> (1) *Protective and Modifying Orders*. Upon a sufficient showing the court may at any time order that the discovery or inspection be denied, restricted or deferred, or make such other order as is appropriate. Upon motion by a party, the court may permit the party to make such showing, in whole or in part, in the form of a written statement to be inspected by the judge alone.

FED. R. CRIM. P. 16.

[98] *Pringle*, 751 F.2d at 425.

[99] *Id*. As the court pointed out, the legislative history makes clear that §§ 3 and 4 of CIPA "were intended to make explicitly the . . . limitation of discovery of classified information pursuant to [Rule 16]." *Id*. at 427.

[100] *Id*. at 427-28 (stating "[w]e have reviewed the classified information and agree with the district court that 'it was not relevant to the determination of the guilt or innocence of the defendants, was not helpful to the defense and was not essential to a fair determination of the cause.'") (quoting Brady v. Maryland, 373 U.S. 83 (1963)).

[101] For instance, in the course of examining the evidence identifying the financial monitoring program under CIPA's procedures, the court itself could determine that the

as the hypothetical financial monitoring program, are by their very nature disinterested and unemotional. As such, little can be gained by revealing and probing them.[102]

Hence, applying the CIPA procedures, a judge most likely would conclude that disclosure of the identity and details of the counterintelligence program that uncovered the confirmation were not material to the defense. At most, the judge may allow for a summary or statement concerning the means through which the confirmation was acquired.

B. Analysis of the Discovery Request Under the MCA

It could be argued that § 949d(f)(2)(B)—the section of the MCA explicitly protecting sources, methods and activities from disclosure[103]—is superfluous, as counterintelligence means would benefit from similar protection under § 949d(f)(1)[104] of the MCA. As discussed in section II above, § 949d(f)(1) of the MCA generally protects classified information from disclosure at *all* stages of military commission proceedings, if the head of the relevant department or agency finds that such disclosure would be detrimental to the national security.[105] In accordance with EO 13,292, counterintelligence means themselves may constitute classified information, separate and apart from the substantive evidence they produce. Specifically, the executive order states that information may be considered for classification if it concerns "*intelligence activities, intelligence sources or methods*, or scientific, technological, or economic matters relating to the national security, including defense against

---

reliability and/or accuracy of the program warrants adversarial probing. And yet, a court likely would proceed down this road with great caution. In short, where "the Government is seeking to withhold classified information from the defendant, an adversary hearing with defense knowledge would defeat the very purpose of the discovery rules." *Sarkissian*, 841 F.2d at 965 (quotation and citation omitted).

[102] The same cannot be said for human sources of intelligence, whether Government agents, informants or interrogated persons. This is especially true where information is obtained through the interrogation of either the defendant himself or another detainee and the military judge must determine whether the resulting evidence is reliable. For example, evidence may be obtained through an informant with malicious motives or through the testimony of another detainee during an interrogation involving questionable tactics. *See supra* note 48. The MCA specifically deals with coerced testimony. *See* 10 U.S.C.S. § 948r (2007).

[103] *See supra* note 44 and accompanying text.

[104] *See supra* note 40.

[105] 10 U.S.C.S. § 949d(f)(1).

transnational terrorism."[106] Applying the language of the executive order to our example, the counterintelligence program that intercepted the wire transfer confirmation should be protected from disclosure under § 949d(f)(1) of the MCA, even absent § 949d(f)(2)(B), so long as the appropriate official finds that the program is properly classified and that its disclosure would be detrimental to national security.

Nevertheless, for the reasons articulated in section I above, legislators wanted to specifically protect classified sources, methods, and activities used to obtain admissible evidence.[107] In accordance with § 949d(f)(2)(B) of the MCA, the Government would be allowed to admit the wire transfer confirmation into evidence without disclosing the existence or details of the classified program, so long as the military judge concluded that the confirmation itself is otherwise admissible and reliable.[108] It follows from the unambiguous and mandatory language of § 949d(f)(2)(B), bolstered by the clear intent of § 949d(f)(1), that an accused's discovery request for disclosure of the means used to discover the confirmation would prove fruitless. At the time of admission of the evidence, the judge at most may permit an unclassified summary of the sources, methods or activities used to obtain the confirmation "to the extent practicable and consistent with national security,"[109] thereby providing the accused some context for the admitted evidence. If the military judge makes appropriately-supported reliability determinations (inter alia, to ensure that counterintelligence operators do not themselves manipulate technical means to manufacture or enhance evidence), and applies the requirement that alternative disclosures be practicable and consistent with national security in such a manner as to allow for an unclassified summary, then (for the same reasons as those articulated above in the context of CIPA) the defense should not suffer. In short, the defense gains little by discovering the identity and details of the hypothetical financial monitoring program.

In summary, the MCA should protect technical counterintelligence means, such as the hypothetical financial monitoring program in the example above, from disclosure during discovery in a similar manner, and with similar alternatives to outright disclosure, as CIPA. Assuming the military judge's vigilance, such protection should not negatively

---

[106] Exec. Order No. 13,292, 3 C.F.R. 196, 198 (2004) (emphasis added).
[107] *See supra* note 27 and accompanying text.
[108] *See* 10 U.S.C.S. § 949d(f)(2)(B).
[109] *See id*.

impact the accused's defense, as there is little to be gained by an accused's probing the existence and details of such a program. Consequently, a challenge to the MCA's explicit protection from disclosure of technical sources through which evidence is obtained is likely to fail, resulting in the admission of the evidence—assuming that it is otherwise reliable, as the MCA requires.[110]

IV. Conclusion

The employment of classified sources, methods and activities by the counterintelligence community is a vital component of our national security effort in the GWOT. The disjointed nature of the terrorist organizations involved and the disparate ethnic, racial and cultural composition of its members and sympathizers has necessitated significant reliance on technical means to gather intelligence. Such means have increasingly been used to monitor communications, especially financial transactions, in search of golden nuggets of information. The MCA properly recognizes that these means are critical to counterintelligence efforts and should be protected, while allowing for a summary to be provided to the accused as an alternative to outright disclosure. Provided that the military judge is vigilant in determining reliability and liberally allows for such summaries, the MCA will protect technical classified sources, methods and activities employed by the Government in the GWOT in a manner consistent with CIPA and without negatively impacting the accused's ability to mount an adequate defense. Thus, the protections afforded to such technical counterintelligence means under the MCA should withstand judicial scrutiny.

[110] *See supra* notes 44–45 and accompanying text.