

UNITED STATES OF AMERICA

v.

Manning, Bradley E.
PFC, U.S. Army,
HHC, U.S. Army Garrison,
Joint Base Myer-Henderson Hall
Fort Myer, Virginia 22211

Prosecution Response

to Defense Motion for
Directed Verdict: Article 104

11 July 2013

RELIEF SOUGHT

The prosecution in the above case respectfully requests the Court deny the defense request to enter a finding of not guilty as to the Specification of Charge I (pursuant to Rule for Courts-Martial (RCM) 917(a)).

BURDEN OF PERSUASION AND BURDEN OF PROOF

A motion for a finding of not guilty shall be granted only in the absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense most favorable to the prosecution, with an evaluation of the credibility of witnesses. RCM 917(d).

FACTS

The prosecution began its case in chief on 3 June 2013 and rested on 2 July 2013. The defense filed its motions for directed verdict on 4 July 2013.

WITNESSES/EVIDENCE

PE 1: OMPF

PE 5: 35F Program of Instruction and Lesson Plan

PE 6: 35F AIT Student Evaluation Plan

PE 11: Hard drive - DN #073-10 Item 1 - Classified (Accused's External Hard Drive)

PE 12: Hard drive - DN #073-10 Item 1 - Classified (.22)

PE 25: Powerpoint "Operations Security" dtd 13 Jun 08

PE 30: Wired.com chat logs (Manning/Laino)

PE 35: Stipulation of Expected Testimony, Elisa Ivory, 10 May 13

PE 36: Stipulation of Expected Testimony, SSG Alejandro Marin, 30 May 13

PE 42: Readme.txt

PE 43: Chaos Communication Congress report by SSG Matthew Hosburgh, dtd 7 Jan 2010 (declassified)

PE 45: ACIC Special Report, Wikileaks.org-an Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups? (unclassified w/out references)

PE 51: Power Point slides "Issue: Islamic Extremism"

PE 52: Power Point slides "Information Security AR 380-5" from 305th MI Battalion

PE 58: Email from Manning to Ehresman and Hack, dtd 12 Jan 10 - Classified
PE 59: Manning Non-Disclosure Agreement witnesses by Rubin (aka Ivory), dtd 7 Apr 08
PE 60: Manning Non-Disclosure Agreement witnessed by Balonek, dtd 17 Sep 08
PE 61: CD Containing Intelink Logs for .22 and .40 - Classified
PE 63: ACIC Website Logs
PE 64: ACIC Webserver Logs
PE 70: Stipulation of Expected Testimony, Mr. Peter Artale
PE 85: Intelink Log Summary (C3 and NCIS Documents)
PE 99: NCIS_IIR
PE 120: Buddy List from PFC Manning's Personal Mac Listing Press Association Contact Information
PE 123: Chats recovered from PFC Manning's Personal Mac between Press Association and dawgnetwork
PE 127: Volumes.txt
AE 81: Court Ruling, Def Motion Dismiss The Sp of Ch I, FTSAO, 26 Apr 12
AE 410: Court's Draft Instructions
DE J: Report of Examination of PFC Manning's Personal Laptop Classified
Testimony of CPT Fulton
Testimony of CW2 Balonek
Testimony of CW2 Hack
Testimony of Mr. Hosburgh
Testimony of Mr. Johnson
Testimony of Mr. Madrid
Testimony of Mr. Moul
Testimony of SA Mander
Testimony of SA Shaver
Testimony of SA Smith
Testimony of SFC Anica

LEGAL AUTHORITY AND ARGUMENT

The sole allegation in the defense's motion with regard to Article 104 is that the prosecution did not present evidence that the accused had "actual knowledge" that by giving information to WikiLeaks, he was giving information to an enemy of the United States. Defense RCM 917 Motion for Article 104 at 1.

Only "some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged" is necessary to withstand a motion for a directed verdict. RCM 917(c). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*; see also *United States v. Perez*, 40 M.J. 373 (C.M.A. 1994) (upholding the military judge's decision not to enter a finding of not guilty because the testimony of three witnesses, construed in the light most favorable to the prosecution, could reasonably tend to establish the overt act). Courts agree the "some evidence" standard to survive a motion for a finding of not guilty is a low one. See *United States v. Escochea-Sanchez*, 2013 WL 561356 (N-M.Ct.Crim.App. 2013) (concurring with the military judge who "noted repeatedly while hearing

argument on the RCM 917 motion [that] the standard for surviving such a motion is very low"); *see also United States v. Jenkins*, 59 M.J. 893, 898 (A.C.C.A. 2004) (encouraging trial judges to view the standard used to decide whether to grant a motion for a finding of guilty as a mirror image of the standard used to decide whether to give an instruction on an affirmative defense); *United States v. Athearn*, 1994 WL 711894 (A-F.Ct.Crim.App. 1994) (quoting RCM 917(d)) (noting that "[t]he military judge was obviously correct in denying the motion for a finding of not guilty under the low, 'some evidence' standard set out in RCM 917(d)").

According to the Court's draft instructions for the Specification of Charge I,

"knowingly" requires actual knowledge by the accused that by giving the intelligence to the 3rd party or intermediary or in some other indirect way, that he was actually giving intelligence to the enemy through this indirect means. This offense requires that the accused had a general evil intent in that the accused had to know he was dealing, directly or indirectly, with an enemy of the United States. 'Knowingly' means to act voluntarily or deliberately. A person cannot violate Article 104 by committing an act inadvertently, accidentally, or negligently that has the effect of aiding the enemy.

Appellate Exhibit (AE) 410 at 2; *see also United States v. Batchelor*, 22 C.M.R. 44 (C.M.A. 1956). The explanation of "Knowledge" in Article 104(c)(5)(c) for "Giving intelligence to the enemy" also states that "Actual knowledge is required but may be proved by circumstantial evidence." Article 104(c)(5)(c), Uniform Code of Military Justice (UCMJ). This definition is quoted in "The Law: Article 104" portion of the Court's Ruling on the Defense Motion to Dismiss for Failure to State an Offense. AE 81; *see also* RCM 918(c) (Findings may be based on direct or circumstantial evidence.). "There is no general rule for determining or comparing the weight to be given to direct or circumstantial evidence." RCM 918(c), discussion. Direct or circumstantial evidence satisfies the "some evidence" standard. *See United States v. Parker*, 59 M.J. 195 (C.A.A.F. 2003); *United States v. Varkonyi*, 645 F.2d 453, 458 (5th Cir. 1981). Although not explicitly enumerated in the draft instruction of "knowingly" for Article 104, in the draft instruction for "knowledge" in Specification 1 of Charge II the Court specifically notes that, "Knowledge, like any other fact, may be proved by circumstantial evidence, including the accused's training, experience, and military occupational specialty." AE 410 at 3.

The prosecution elicited a plethora of evidence in its case in chief to prove that the accused had the requisite knowledge for the Specification of Charge I. The evidence that the prosecution presented to establish the accused's actual knowledge can be broadly defined under three categories: (1) Military education and training; (2) information the accused reviewed during the course of his misconduct; and (3) statements by the accused.

1. Military Education and Training

The defense acknowledged that the prosecution introduced evidence that, in his training, the accused was instructed that the enemy uses the internet generally. *See* Defense RCM 917 Motion at 2. The defense, however, argues that the prosecution has not proffered any evidence

that shows that the accused was instructed that a particular enemy looks at or uses the WikiLeaks website.

The prosecution notes a factual inaccuracy in paragraph 5 of the defense's argument. In response to the defense in cross-examination, Mr. Johnson testified he did not look at or recover any websites that were associated with terrorism or with a hatred of America or anti-American beliefs in his forensic examination of the accused's personal Macintosh computer, rather than what the defense proffered. Testimony of Mr. Mark Johnson. Mr. Mark Johnson did not say "that his forensic investigation of PFC Manning's computer revealed no searches for the enemy, anything related to terrorism, or anything remotely anti-American." Defense RCM 917 Motion for Article 104 at 2.

a. AIT Training

The prosecution established in its case-in-chief that the accused is an all-source intelligence analyst (35F). *See, e.g.*, Prosecution Exhibit (PE) 1 (OMPF).

The prosecution presented evidence that during AIT, the accused committed an operational security (OPSEC) violation and, as part of corrective training, was specifically required to research and brief the importance of OPSEC and the potential damage or harm to national security by having an OPSEC violation. *See* Testimony of Mr. Madrid. The accused presented three different types of corrective training (a brief, a Power Point, and a written report) that covered the importance of OPSEC. *See* Testimony of Mr. Madrid; PE 25 (Power Point presented by the accused on OPSEC). The accused's Power Point was found on his external hard drive, which was recovered from the Accused's CHU in Iraq. *See* Testimony of SA Smith; Testimony of Mr. Johnson; DE J. In his Power Point, the accused noted that, among others, adversaries included foreign governments, terrorists, activists, and hackers. Testimony of Mr. Madrid; PE 25 (Power Point presented by the accused on OPSEC). In his Power Point, the accused also documented "Common OPSEC Leaks" which included the Internet and concluded that disclosure of information, including posting on the Internet, must be avoided and that one must use common sense because there are many enemies and it is a free and open society. *Id.*

The prosecution also presented evidence on the accused's training as an all-source intelligence analyst and that training included training on the identities of terrorist groups, which included Al-Qaeda. *See* Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan); PE 51 (Power Point slides on the enemy). The prosecution also presented evidence that the accused was trained that the enemy used the internet and that anything that the enemy can use or piece together to use against the United States should be protected, in include, among other things, PII and unit identification and movement information. *See* Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan); PE 51 (Power Point slides on the enemy); PE 52 (Power Point slides from AIT on INFOSEC); PE 36 (Stipulation of Expected Testimony, SSG Marin); PE 35 (Stipulation of Expected Testimony, Ms. Ivory). For example, slide 71, which is supplemented by the text in the corresponding 35F AIT lesson plan, and was taught to the accused by Mr. Moul states, "The enemy will attempt to discover how and when we are conducting operations, knowing this, we must protect our activities from detection. We do this

by: •Identifying - Critical Information •Analyzing - Threat." See PE 52 (Power Point slides from AIT on INFOSEC); Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan). Slide 72 defines "Critical Information" as, among other things, installation maps with highlights of designated points of interest, SOPs, TTPs, unit capabilities and intent, and personal/family information. *Id.* Slide 73, entitled "Prevent Disclosures" says "DON'T DISCUSS OPERATIONAL ACTIVITIES ON THE WEB". *Id.* Training slide 73 that the accused received at AIT goes on to say, "Ensure information posted has no significant value to the adversary"; "Always assume the adversary is reading your material"; and "Remember it is called the World Wide Web for a reason." *Id.* The accused also received training on the different types of recruiting utilized by terrorist organizations, particularly by Al-Qaeda, and that the number of terrorist websites have jumped from less than 100 to as many as 4,000 in the last ten years and many insurgency groups have many sites and message boards to help their network. Testimony of Mr. Moul; PE 51 (Power Point slides on the enemy and their use of the Internet). The accused had to pass a test on INFOSEC/OPSEC in order to proceed in the course. See Testimony of Mr. Moul; PE 5 (35F Program of Instruction and Lesson Plan); PE 6 (35F AIT Student Evaluation Plan).

The training demonstrates that the accused knew who the enemy was and that the enemy used the internet. The accused passing a test on INFOSEC/OPSEC and his corrective training further demonstrate that he was not only taught the information, but he learned it and had an appreciation for its importance. A reasonable inference follows that since Wikileaks.org is a website on the Internet, and the accused knew that the enemy was looking for any and all information on the Internet, that the Accused knew that by putting information on the Internet, he was giving the information to the enemy. This is particularly true in light of the information that the accused was giving to Wikileaks.org, which he was specifically trained was of interest to the enemy. The accused's knowledge of enemy receipt is an inevitable conclusion given the evidence the prosecution presented on the accused's knowledge of the type of website that Wikileaks.org was at the time the accused unlawfully transmitted the information to them (discussed below). This is circumstantial evidence of the accused's actual knowledge.

b. Non-Disclosure Agreements

In addition, the prosecution offered evidence that the accused had to sign non-disclosure agreements (SF 312). See Testimony of Mr. Moul; PE 35 (Stipulation of Expected Testimony, Ms. Ivory); PE 59 (Accused NDA, dtd 7 Apr 08); Testimony of CW2 Balonek; PE 60 (Accused NDA, dtd 17 Sep 08). The non-disclosure agreements described the responsibilities and special trust and confidence associated with having access to classified information. See PE 59 (accused NDA, dtd 7 Apr 08); PE 60 (accused NDA, dtd 17 Sep 08). The non-disclosure agreements explain the potential damage and consequences associated with the unauthorized disclosure of that information. *Id.* Furthermore, the non-disclosure agreements highlights that the classified information was the property of the US government. *Id.* The significance of the NDA was also explained to the accused. Testimony of Mr. Moul; PE 35 (Stipulation of Expected Testimony, Ms. Ivory); Testimony of CW2 Balonek. The accused even raised his right hand and vowed to uphold the responsibilities contained in the non-disclosure agreement. See PE 35 (Stipulation of Expected Testimony, Ms. Ivory). Understanding and signing the non-disclosure agreements further ensured that the accused understood the importance of protecting classified information

and the consequences of its unauthorized release. This is circumstantial evidence of the accused's actual knowledge.

c. Additional Information on the Accused's External Hard Drive

The prosecution admitted the accused's external hard drive. *See* PE 11. That external hard drive contains a wealth of training information in addition to the accused's OPSEC slideshow discussed above. *Id.* Specifically, it contained the following:

- the accused had a Microsoft PowerPoint brief titled "Insurgent Propaganda TTPs" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\Lessons Learned\Lessons Learned\Threat\UFOUO_Iraqi_Propaganda_TTPs_Brief_26Jan05.ppt).¹ Slide 17 says "Insurgent Information operations (IO) becoming increasingly sophisticated – videos on the internet and favorable news coverage on Arab media Al Jazeera (see list of pro-insurgent websites)." *Id.*

- the accused had a copy of FM 2-0 titled "Intelligence" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Field Manuals\FM_2_0-intel.pdf). The document states adversaries "weaponry may range from a computer connected to the Internet to WMD." *Id.*

- the accused had a copy of AR 525-13 titled "Antiterrorism" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\O&I\OIP\SOP's_AR's\AR525_13 Anti-Terrorism.pdf). It states that terrorists use "instances of web site tampering to further their cause." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\fm7_100x1.pdf). This document states "Rapid advances in technology have produced an incredibly complex global information environment. Information and communications technologies have grown exponentially in recent years. Satellite and cellular communications, direct-broadcast television (expanding the awareness of events, issues, and military activities), personal computers, global positioning system (GPS) technologies, wireless communication capabilities, and the Internet are a few examples of the capabilities widely available to nations, as well as independent organizations and individuals. Given such advances, the capabilities of both the OPFOR and its potential adversaries are increasing in both sophistication and lethality. The OPFOR tries to exploit such technologies to gain the operational advantage." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\fm7_100x1.pdf). This document

¹ PE 11 and PE 12 are compilation exhibits that were admitted and contain computer images of the accused's external hard drive (PE 11) and ".22" SIPRNET computer (PE 12). The prosecution can provide the Court with the appropriate viewing equipment or can print each item referenced within this motion for the Court.

states "In contrast to other forms of warfare, IW [(Information Warfare)] actions might occur without access to large financial resources or backing or without state sponsorship. Information weapons could be software logic bombs or computer worms and viruses. IW could be conducted with such easily accessible means such as cellular telephones and the Internet." *Id.*

- the accused has a copy of FM 7-100.1 titled "Opposing Force Operations" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\fin7_100x1.pdf). Chapter 5 of this document provides an overarching discussion of Information Warfare. *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states that "Depending on the size, nature, and focus of the insurgent organization, the direct action cell (IW) may be capable of several functions. Some example functions . . . [include assisting] . . . in the cyber-mining for intelligence. All of these functions are integrated to further short- and long-range goals." *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states "Close coordination is maintained with the IW cell for Internet communications." *Id.*

- the accused has a copy of FM 7-100.4 titled "Opposing Force Organization Guide" on his personal HDD. PE 11 (\PFC MANNING External HDD\0055-28May10\MANNING-External\1 Manning\Manning\Documents\Analyst\Reference Material\pdf\FM 7-100-4.pdf). Appendix C of this document, in providing an example of a local insurgent organization, states "The internet is a powerful recruitment tool. The recruiting cell maintains close coordination with the information warfare cell." *Id.*

The accused's possession of all the above information is additional circumstantial evidence that the accused knew and understood all of the above information, leading to the reasonable inference that the accused knew that by disclosing information to WikiLeaks.org he was giving the information to the enemy, and specifically Al-Qaeda.

d. Accused Knowledge of SIGACTs

In addition to offering evidence on the type of information the accused would be seeking on the Internet, the prosecution also offered evidence that the accused was aware that SIGACTs included the type of information that the enemy would be seeking and that the accused knew that the SIGACTs were valuable and useful intelligence as discussed below. The accused acknowledged the value by stating in the text file that accompanied the disclosed CIDNE databases on the accused's SD Card stating, "This is possibly one of the more significant

documents of our time, removing the fog of war, and revealing the true nature of 21st century asymmetric warfare." PE 42 (Readme.txt); *see* Testimony of SA Shaver.

The prosecution offered numerous witnesses to testify regarding the accused's knowledge of SIGACTs. *See, e.g.*, Testimony of SFC Anica; Testimony of CW2 Hack; Testimony of CPT Fulton; Testimony of CW2 Balonek. According to SFC Anica, it was part of the accused's job, in garrison, to combine information from the SIGACTs and pick out the most relevant and important data and then create PowerPoint presentations to brief the S2; vehicle-borne IEDs were particularly significant at the time. Testimony of SFC Anica. According to CW2 Hack, the accused had many SIGACTs organized in his folder on his unit's share drive in an extremely meticulous manner. Testimony of CW2 Hack. The SIGACTs and other intelligence reports were organized by geographical locations that were tied to an enemy threat group that the leadership had prioritized. *Id.* The accused knew of the value and usefulness of SIGACT reports when conducting an analysis of unit activity, as he used the SIGACTs to create work product. *See id.*; PE 58. Specifically, the accused gave CW2 Hack a SIGACT report of an IED attack that had a unit in the same area of operation that 2d Brigade, 10th Mountain was in, two years before they arrived to assist CW2 Hack with his targeting mission as the Accused thought the SIGACT would be assist in the capture of a high value target. *Id.* The attack described the type of weapon system that was used, as well as damage and equipment that was used. *Id.* It also included an S2 assessment of the event. *Id.* Similarly, the accused pulled SIGACTs for CPT Fulton, which would typically focus on IEDs, small arms, and direct and indirect fire. Testimony of CPT Fulton. The accused would mine the information, organize the information, sort the information, and then plot the SIGACT information on the map, so it was represented visually and so analysis could be conducted based on enemy patterns and engagement areas represented. *Id.* The accused also pulled SIGACTs from CIDNE, and organized them on an excel spreadsheet to show enemy trends. *Id.* CPT Fulton also testified that, in garrison, the Accused helped her prepare the intelligence portion of the OPORD for the deployment. *Id.* Specifically, the accused gave CPT Fulton the basis of knowledge on all of the enemy threat groups. *Id.* Finally, according to CW2 Balonek, the accused put together an intelligence product that compared the past three years of Iraq SIGACTs, and specifically looked at locations of different types of attacks, such as IED attacks and small arms fire against convoys. Testimony of CW2 Balonek.

The evidence offered by the prosecution is a reasonable inference to show the accused knew the value of the SIGACTS from an intelligence point of view. He knew that individual SIGACTS could be used to create actionable intelligence products for the Commander. He also knew the value of having numerous SIGACTs and the products that could be created from the SIGACTs. He knew a group of SIGACTS could be used to decipher patterns of behavior of friendly and enemy units. Just as the accused would use SIGACTS to decipher enemy tactics, techniques, and procedures (TTPs), the accused knew that the enemy would find the same value in the ability to decipher our TTPs, and would find similar value in the ability to create actionable intelligence products from the SIGACTS. All the above leads to a reasonable inference that the accused knew of this value prior to disclosing the SIGACTs to Wikileaks.org to be posted on the internet, to be accessible to all people globally, including the enemy. The above also leads to a reasonable inference that the accused knew that this information was

exactly the type of information that the enemy would seek out and access and that the enemy would have access to all the information as leaked on Wikileaks.org.

2. Information Accused Accessed During the Course of his Misconduct

a. ACIC Report

The defense acknowledged that the prosecution introduced evidence to show that the accused accessed the ACIC report titled "Wikileaks.org--An Online Reference to Foreign Intelligence Services, Insurgents, or Terrorist Groups?)" charged in Specification 15 of Charge II. *See* Defense RCM 917 Motion at 2. The defense, however, argues that accessing this article does not show that the accused had actual knowledge that by giving information to Wikileaks, he was giving it to the enemy. *Id.* The defense argues how the accused interpreted the report in their motion; however, there is no evidence of that interpretation by the accused. *Id.* These are the defense's interpretations and reserved for argument, thus not appropriate for a RCM 917 motion. RCM 917(c) requires the Court to view the evidence "in the light most favorable to the prosecution." RCM 917(c).

The purpose of the ACIC report, which was published on 18 March 2008, was to "assess the counterintelligence threat posed to the US Army by the Wikileaks.org Web site." PE 45 (Unclassified ACIC Report). The ACIC report describes in detail what the author's research of Wikileaks.org revealed about Wikileaks.org, their actions, and how they operated in 2008. *See* PE 45 (Unclassified ACIC Report). The first bulleted "Key Judgment" of the ACIC report is that "Wikileaks.org represents a potential force protection, counterintelligence, OPSEC, and INFOSEC threat to the US Army." PE 45 (Unclassified ACIC Report). The second bullet states, "Recent unauthorized release of DoD sensitive and classified documents provide FISS, foreign terrorist groups, insurgents, and other foreign adversaries with potentially actionable information for targeting US forces." *Id.* The sixth bullet says that "Wikileaks.org most likely has other DoD sensitive and classified information in its possession and will continue to post the information to the Wikileaks.org Website." *Id.* The ACIC report goes on to discuss the DoD and classified information that Wikileaks.org has released in the past and how Wikileaks.org posts all information that they receive without editorial oversight. *Id.* The ACIC report concludes that "it must also be presumed that foreign adversaries will review and assess any DoD sensitive or classified information posted to the WL.org web site" and warns of adversaries increased ability to complete rapid data compilation to more efficiently develop actionable information for their use for intelligence collection, planning, or targeting purposes. *Id.*

The prosecution also offered evidence that the accused searched for Wikileaks.org or variations of that term over 100 times between 1 December 2009 and 15 March 2010 on SIPRNET. Testimony of SA Shaver; PE 61 (Intelink logs). The logs further prove that he further supplemented his knowledge of Wikileaks.org through these searches. *Id.* The prosecution also admitted the image of the accused's .22 computer. *See* PE 12. That image contains an email that the accused sent to members of the S2 section (CPT Lim, CPT Martin, CW2 Ehresman, 1LT Gaab, CW2 Balonek, SPC Madaras, SPC Cooley) on 15 March 2010, classified FOUO. PE 12 (PFC MANNING Primary SIPR\2251-27May10\2251-27May10\C\Documents and Settings\bradley.manning\Local Settings\Application

Data\Microsoft\Outlook\archive.pst\Root folder\Top of Personal Folders\Deleted Items\Sent Items1\[UNCLASSIFIED//FOR OFFICIAL USE ONLY] ACIC Cyber Collaboration Portal [UNCLASSIFIED//FOR OFFICIAL USE ONLY]). In that email, the accused states, "Occasionally has good hits from extremist websites in our OE! Found it earlier this evening. <http://acicportal.north-inscom.army.smil.mil/cyber/default.aspx>". *Id.* According to the ACIC logs, the ACIC report (Product ID # RB08-0617) is available at the URL "<http://acicportal.north-inscom.army.smil.mil/cyber/default.aspx>" and the accused linked to the ACIC report through that URL. *See* PE 64 (ACIC Webserver logs); PE 45 (Unclassified ACIC Report).

The prosecution offered evidence that the accused accessed the website containing the ACIC report on 1 December 2009, 29 December 2009, 1 March 2010, and 7 March 2010. PE 70 (Stipulation of Expected Testimony, Mr. Artale); PE 63 (ACIC metrics for the ACIC report). The prosecution also offered evidence that the accused viewed the ACIC document on 14 February 2010 and 1 March 2010. Testimony of SA Shaver; PE 61 (Intelink logs).

The above evidence leads to a reasonable inference that based on the accused's repeated access to the report, he not only read the ACIC report charged in Specification 15 of Charge II but that he read it multiple times. This is circumstantial evidence that the accused was put on notice that by giving information to Wikileaks.org, the enemy would have access to and use the information. The accused was also put on notice by the ACIC report that Wikileaks.org was not a legitimate media organization, since, according to the report, Wikileaks.org posts all information they receive with no editorial oversight. PE 45 (Unclassified ACIC Report). It is a reasonable inference that given the accused's specific training on Al-Qaeda, he knew the enemy would be Al-Qaeda based on the time period of the misconduct and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet.

b. IIR 5 391 0014 08

Similarly, the prosecution offered evidence of the accused's knowledge through IIR 5 391 0014 08. The subject of this IIR was "Internet Web Postings of Classified and for Official Use Only Documents." PE 99 (IIR 5 391 0014 08). The IIR discussed Wikileaks.org, and according to the report, in December 2006, "Wikileaks.org was established to encourage the anonymous posting of sensitive government and corporate documents." PE 99 (IIR 5 391 0014 08); *see also* Testimony of SA Mark Mander. According to the IIR, "Wikileaks.org self-describes as (quote) an uncensorable Wikipedia for untraceable mass document leaking and analysis (unquote)." *Id.* According to the 2008 report, numerous classified and FOUO documents have been posted and continue to be available on Wikileaks.org and its mirror sites. *Id.*

The prosecution offered evidence that the accused searched for the IIR on 14 February 2010. *See* PE 85 (Intelink logs); Testimony of Mr. Mark Johnson. The prosecution also offered evidence that the accused moved a copy of the IIR to his personal Macintosh computer on 15 February 2010. *See* PE 127 (Volumes.txt which showed the IIR was on the accused's personal Macintosh computer).

The above evidence leads to a reasonable inference that the accused's accessing the individual IIR and moving it to his personal computer demonstrates that the accused read the

document. Again, by reading the IIR, the accused was put on notice that by giving information to Wikileaks.org, a site that was quickly gaining a reputation for encouraging leaks of classified government information and a website that seemingly posted everything it received, would be used by the enemy. This is circumstantial evidence that the accused knew the enemy would be Al-Qaeda based on the priorities of the United States and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet. This inference is reasonable considering the type of information the accused was disclosing to the website, and his training that made him aware of the type of information and the enemy's use of the Internet.

c. C3 Document

The prosecution also offered evidence of the accused's knowledge through the Chaos Communication Congress (C3) report, which reported on the December 2009 C3 conference, an annual event that attracts hackers, security researchers, computer hobbyists and malicious computer users. The C3 report states that "the Internet is an essential communication tool for terrorists." PE 43 (C3 report). In regard to Wikileaks.org, the report explains that it is "a publicly accessible Internet Website where individuals can contact with leaked information and have it published to the public anonymously without fear of being held legally liable." *Id.* The report further states, "[t]he information that can be disclosed includes, but is not limited to, classified information, trade secrets, corporate information, personally identifiable information, and even operational data." *Id.* The report also discusses the threat from the insider leaking information to Wikileaks.org, as Mr. Julian Assange was encouraging the leaking of classified and proprietary information at the conference. Testimony of Mr. Hosburgh; *see also* PE 43 (C3 report).

The prosecution offered evidence that the accused searched for the report on 14 February 2010, just one day after returning from R&R leave. *See* Testimony of SA Shaver; PE 85 (Intelink logs). The prosecution also offered evidence that the accused moved a copy of the C3 report to his personal Macintosh computer on 15 February 2010. Testimony of Mr. Mark Johnson; PE 127 (Volumes.txt which showed the C3 document was on the accused's personal Macintosh computer).

The above evidence leads to a reasonable inference that the accused's accessing the individual report and moving it to his personal computer demonstrates that the accused read the document. Again, by reading the report, the accused was put on notice that by giving information to Wikileaks.org, a site that was quickly gaining a reputation for encouraging leaks of classified government information and a website that seemingly posted everything it received, would be used by the enemy. This is circumstantial evidence that the accused knew the enemy would be Al-Qaeda based on the priorities of the United States and the accused's knowledge and training on who our enemy was and our enemy's use of the Internet.

3. Statements by accused

The prosecution introduced evidence of the accused's own statements that documented his knowledge that by giving information to Wikileaks.org, he was giving it to the enemy.

a. Chats with Mr. Adrian Lamo

The prosecution offered evidence that in his chats with Adrian Lamo, the accused called the disclosed Department of State cables "world-wide anarchy" in CSV format." PE 30 (Wired.com chat logs of the accused and Mr. Lamo). The accused also asserted that the DoS cables will affect "everybody on earth." *Id.* The accused further noted that "Hilary Clinton, and several thousand diplomats around the world are going to have a heart attack when they wake up one morning, and finds an entire repository of classified foreign policy is available, in searchable format to the public...=L". *Id.* It is a reasonable inference that if the accused knew that everyone in the world would have access to the information on Wikileaks.org, that the enemy, namely Al-Qaeda would have access. This information further reveals that the accused knew the value of the US government information contained in the Department of State cables, which further requires the conclusion that by disclosing that information to Wikileaks, that the accused knew he was giving the information to the enemy, as he knew the information would be valuable to the enemy.

Additionally, as pointed out in the defense brief, the accused acknowledged that he "could've sold [the information] to Russia or China, and made bank" but he did not "because it's public data" and "because another state would just take advantage of the information . . . try to get some edge." *Id.* The defense argues that this statement shows the accused's "focus was on getting certain information to the American public in order to hopefully spark change and reform." Defense RCM 917 Motion for Article 104 at 3. However, there is no evidence supports the defense interpretation of the chat, and should be left for argument. The accused never once mentions the American public or the United States being any sort of motivation for his crimes in any of his chats or emails. The statement cited by the defense instead requires the opposite conclusion, as it shows that the accused did not want to limit access to the information to one group, but wanted everyone to see the information.

b. Chats with Mr. Julian Assange

The prosecution also offered evidence that the accused (dawgnetwork) was chatting with Mr. Julian Assange (pressassociation). Testimony of Mr. Johnson; PE 120 (Buddy List from the Accused's personal computer listing pressassociation's contact information); PE 123 (Chats recovered for the accused's personal computer between pressassociation and dawgnetwork). In those chats, on 10 March 2010, the accused called Wikileaks.org the first "Intelligence Agency" for the general public. *See* PE 123 (Chats recovered for the accused's personal Mac between pressassociation and dawgnetwork). This demonstrates that the accused does not think of Wikileaks.org as a news organization. The chats with Mr. Assange also show that the accused knew the information that he transmitted to Wikileaks.org would be published on the Internet. *See* PE 123 (Chats recovered for the accused's personal computer between pressassociation and dawgnetwork). On 6 March 2010, the accused asked Mr. Assange if he was "gonna give release a shot?" Mr. Assange responded, "yes." *Id.* The accused also asks Mr. Assange, "is it like the entire world is uploading to you?" Mr. Assange responds with examples of information releases from Hungary, Haiti, and Germany, indicating the international interest in his website. *See* PE 123 (Chats recovered for the accused's personal Mac between pressassociation and dawgnetwork).

In summary, it is a reasonable inference that based on the above evidence that the accused knew the enemy used the Internet, the accused knew who the enemy was, and the accused knew the Wikileaks.org website was on the Internet and commonly contained classified official US government information and was about to contain a lot more classified government information that would be of value to the enemy courtesy of the accused.

Although not appropriate for a RCM 917 motion, the defense argues in their motion that the accused did not have actual knowledge that by giving the classified US government information to the enemy that the accused was giving the information to Wikileaks.org, the evidence supports the opposite conclusion through circumstantial evidence. Based on the evidence presented by the prosecution, it is a reasonable inference that the accused was trained by the military on the enemy (particularly Al-Qaeda and Usama Bin Laden) and its use of the Internet, the accused was trained by the military on the types of information the enemy would be seeking on the Internet, the accused was informed of how Wikileaks.org conducted business by his own searches during the commission of his misconduct, and the accused acknowledged in his discussions during the commission of his misconduct that he knew exactly what he was doing in disclosing the charged information. Ultimately, a reasonable inference can be drawn based on the circumstantial evidence that the accused knew that by giving information to Wikileaks.org, he was giving information to the enemy, specifically Al-Qaeda.

CONCLUSION

Since the prosecution has presented evidence on every element of the Specification of Charge I (Article 104), the defense request to enter a finding of not guilty as to the Specification of Charge I should be denied. This is particularly true given the lower burden on the prosecution to withstand an RCM 917 motion and the requirement that the Court must view the evidence "in the light most favorable to the prosecution." RCM 917(c).



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel

I certify that I served or caused to be served a true copy of the above on the Defense Counsel, via electronic mail, on 11 July 2013.



ANGEL M. OVERGAARD
CPT, JA
Assistant Trial Counsel