From Information Clearing House | Original Article

Full Transcript

This statement below was read by Private First Class Bradley E. Bradley at a providence inquiry for his formal plea of guilty to one specification as charged and nine specifications for lesser included offenses. He pled not guilty to 12 other specifications. This rush transcript was taken by journalist Alexa O'Brien at the Article 39(a) session of United States v. Pfc. Bradley Manning on February 28, 2013 at Fort Meade, MD, USA.

Judge Lind: Pfc. Manning you may read your statement.

Pfc. Bradley Manning: Yes, your Honor. I wrote this statement in the confinement facility. The following facts are provided in support of the providence inquiry for my court martial, United States v. Pfc. Bradley E. Manning.

Personal Facts.

I am a twenty-five year old Private First Class in the United States Army currently assigned to Headquarters and Headquarters Company, HHC, US Army Garrison (USAG), Joint Base Myer, Henderson Hall, Fort Meyer, Virginia.

My [missed word] assignment I was assigned to HHC, 2nd Brigade Combat Team, 10th Mountain Division at Fort Drum, NY. My primary military occupational specialty or MOS is 35 Foxtrot intelligence analyst. I entered active duty status on 2 October 2007. I enlisted with the hope of obtaining both real world experience and earning benefits under the GI Bill for college opportunities.

Facts regarding my position as an intelligence analyst.

In order   to enlist in the Army I took the Standard Armed Services   Aptitude Battery or [ASVAB?]. My score on this battery was high   enough for me to qualify for any enlisted MOS positon. My   recruiter informed me that I should select an MOS that   complimented my interests outside the military. In response, I   told him that I was interested in geopolitical matters and   information technology. He suggested that I consider becoming an intelligence analyst.

After   researching the intelligence analyst position, I agreed that   this would be a good fit for me. In particular, I enjoyed the   fact that an analyst could use information derived from a   variety of sources to create work products that informed the   command of its available choices for determining the best course   of action or COA's. Although the MOS required working knowledge   of computers, it primarily required me to consider how raw   information can be combined with other available intelligence   sources in order to create products that assisted the command in   it's situational awareness or SA.

I accessed   that my natural interest in geopolitical affairs and my computer   skills would make me an excellent intelligence analyst. After   enlisting I reported to the Fort Meade military entrance   processing station on 1 October 2007. I then traveled to and   reported at Fort Leonard Wood, Missouri on 2 October 2007 to   begin basic combat training or BCT.

Once at   Fort Leonard Wood I quickly realized that I was neither   physically nor mentally prepared for the requirements of basic   training. My BCT experience lasted six months instead of the   normal ten weeks. Due to medical issues, I was placed on a hold   status. A physical examination indicated that I sustained   injuries to my right soldier and left foot.

Due to   those injuries I was unable to continue 'basic'. During medical   hold, I was informed that I may be out processed from the Army,   however, I resisted being chaptered out because I felt that I   could overcome my medical issues and continue to serve. On 2[8   or 20?] January 2008, I returned to basic combat training. This   time I was better prepared and I completed training on 2 April   2008.

I then   reported for the MOS specific Advanced Individual Training or   AIT on 7 April 2008.

AIT was an enjoyable experience for me.   Unlike basic training where I felt different from the other   soldiers, I fit in did well. I preferred the mental challenges   of reviewing a large amount of information from various sources   and trying to create useful or actionable products. I especially   enjoyed the practice of analysis through the use of computer applications and methods that I was familiar with.

I   graduated from AIT on 16 August 2008 and reported to my first   duty station, Fort Drum, NY on 28 August 2008. As an analyst,   Significant Activities or SigActs were a frequent source of   information for me to use in creating work products. I started   working extensively with SigActs early after my arrival at Fort   Drum. My computer background allowed me to use the tools of   organic to the Distributed Common Ground System-Army or D6-A   computers to create polished work products for the 2nd Brigade   Combat Team chain of command.

The   non-commissioned officer in charge, or NCOIC, of the S2 section,   then Master Sergeant David P. Adkins recognized my skills and   potential and tasked me to work on a tool abandoned by a   previously assigned analyst, the incident tracker. The incident   tracker was viewed as a back up to the Combined Information Data   Network Exchange or CIDNE and as a unit, historical reference to   work with.

In the   months preceding my upcoming deployment, I worked on creating a   new version of the incident tracker and used SigActs to populate   it. The SigActs I used were from Afghanistan, because at the   time our unit was scheduled to deploy to the Logar and Wardak   Provinces of Afghanistan. Later my unit was reassigned to deploy   to Eastern Baghdad, Iraq. At that point, I removed the   Afghanistan SigActs and switched to Iraq SigActs.

As and   analyst I viewed the SigActs as historical data. I believed this   view is shared by other all-source analysts as well. SigActs   give a first look impression of a specific or isolated event.   This event can be an improvised explosive device attack or IED,   small arms fire engagement or SAF engagement with a hostile   force, or any other event a specific unit documented and   recorded in real time.

In my   perspective the information contained within a single SigAct or   group of SigActs is not very sensitive. The events encapsulated   within most SigActs involve either enemy engagements or   causalities. Most of this information is publicly reported by   the public affairs office or PAO, embedded media pools, or host   nation HN media.

As I   started working with SigActs I felt they were similar to a daily   journal or log that a person may keep. They capture what happens   on a particular day in time. They are created immediately after   the event, and are potentially updated over a period of hours   until final version is published on the Combined Information   Data Network Exchange. Each unit has it's own Standard Operating   Procedure or SOP for reporting recording SigActs. The SOP may   differ between reporting in a particular deployment and   reporting in garrison.

In   garrison a SigAct normally involves personnel issues such as   driving under the influence or DUI incidents or an automobile   accident involving the death or serious injury of a soldier. The   reports starts at the company level and goes up to the   battalion, brigade, and even up to the division level.

In   deployed environment a unit may observe or participate in an   event and a platoon leader or platoon sergeant may report the   event as a SigAct to the company headquarters and the radio   transmission operator or RTO. The commander or RTO will then   forward the report to the battalion battle captain or battle   non-commissioned officer or NCO. Once the battalion battle   captain or battle NCO receives the report they will either (1)   notify the battalion operations officer or S3; (2) conduct an   action, such as launching a quick reaction force; or (3) record   the event and report and further report it up the chain of   command to the brigade.

The   reporting of each event is done by radio or over the Secret   Internet Protocol Router Network or SIPRNet, normally by an   assigned soldier, usually junior enlisted E-4 and below. Once   the SigAct is recorded, the SigAct is further sent up the chain   of command. At each level, additional information can either be   added or corrected as needed. Normally within 24 to 48 hours,   the updating and reporting or a particular SigAct is complete.   Eventually all reports and SigActs go through the chain of   command from brigade to division and division to corp. At corp   level the SigAct is finalized and [missed word].

The CIDNE   system contains a database that is used by thousands of   Department of Defense--DoD personel including soldiers,   civilians, and contractors support. It was the United States   Central Command or CENTCOM reporting tool for operational   reporting in Iraq and Afghanistan. Two separate but similar   databases were maintained for each theater-- CIDNE-I for Iraq   and CIDNE-A for Afghanistan. Each database encompasses over a   hundred types of reports and other historical information for   access. They contain millions of vetted and finalized   directories including operational intelligence reporting.

CIDNE was   created to collect and analyze battle-space data to provide   daily operational and Intelligence Community (IC) reporting   relevant to a commander's daily decision making process. The   CIDNE-I and CIDNE-A databases contain reporting and analysis   fields for multiple disciplines including Human Intelligence or   HUMINT reports, Psychological Operations or PSYOP reports,   Engagement reports, Counter Improvised Explosive Device or CIED   reports, SigAct reports, Targeting reports, Social and Cultural   reports, Civil Affairs reports, and Human Terrain reporting.

As an   intelligence analyst, I had unlimited access to the CIDNE-I and   CIDNE-A databases and the information contained within them.   Although each table within the database is important, I   primarily dealt with HUMINT reports, SigAct reports and Counter IED reports, because these reports were used to create a   work-product I was required to published as an analyst.

In working   on an assignment I looked anywhere and everywhere for   information. As an all-source analyst, this was something that   was expected. The D6-A systems had databases built in, and I   utilized them on a daily basis. This simply was--the search   tools available on the D6-A systems on SIPRNet such as Query   Tree and the DoD and Intellink search engines.

Primarily,   I utilized the CIDNE database using the historical and HUMINT   reporting to conduct my analysis and provide a back up for my   work product. I did statistical analysis on historical data   including SigActs to back up analysis that were based on HUMINT reporting and produce charts, graphs, and tables. I also created   maps and charts to conduct predictive analysis based on   statistical trends. The SigAct reporting provided a reference point for what occurred and provided myself and other analysts   with the information to conclude possible outcome.

Although   SigAct reporting is sensitive at the time of their creation,   their sensitivity normally dissipates within 48 to 72 hours as   the information is either publicly released or the unit involved   is no longer in the area and not in danger.

It is my   understanding that the SigAct reports remain classified only   because they are maintained within CIDNE-- because it is only   accessible on SIPRnet. Everything on CIDNE-I

and CIDNE-A to   include SigAct reporting was treated as classified information.

Facts regarding the storage of SigAct Reports.

As part of   my training at Fort Drum, I was instructed to ensure that I   create back ups of my work product. The need to create back ups   was particularly acute given the relative instability and   reliability of the computer systems we used in the field during   deployment. These computer systems included both organic and   theater provided equipment (TPE) D6-A machines.

The   organic D6-A machines we brought with us into the field on our   deployment were Dell [missed word] laptops and the TPE D6-A   machines were Alienware brand laptops. The [M90?] D6-A laptops   were the preferred machine to use as they were slightly faster   and had fewer problems with dust and temperature than the   theater provided Alienware laptops. I used several D6-A machines   during the deployment due to various technical problems with the   laptops.

With these   issues several analysts lost information, but I never lost   information due to the multiple backups I created. I attempted   to backup as much relevant information as possible. I would save   the information so that I or another analyst could quickly   access it whenever a machine crashed, SIPRnet connectivity was   down, or I forgot where the data was stored.

When   backing up information I would do one or all of the following   things based on my training:

[(1)]   Physical back up. I tried to keep physical back up copies of   information on paper so that the information could be grabbed   quickly. Also, it was easier to brief from hard copies of   research and HUMINT reports.

(2) Local   drive back up. I tried to sort out information I deemed relevant   and keep complete copies of the information on each of the   computers I used in the Temporary Sensitive Compartmented   Information Facility or T-SCIF, including my primary and

secondary D6-A machines. This was stored under my user profile   on the desktop.

[(3)]   Shared drive backup. Each analyst had access to a 'T' drive--   what we called 'T' drive shared across the SIPRnet. It allowed   others to access information that was stored on it. S6 operated   the 'T' drive.

[(4)]   Compact disk rewritable or CD-RW back up. For larger datasets I   saved the information onto a re-writable disk, labeled the   disks, and stored them in the conference room of the T-SCIF.   This redundancy permitted us to not worry about information   loss. If the system crashed, I could easily pull the information   from a secondary computer, the 'T' drive, or one of the CD-RWs.

If another   analysts wanted to access my data, but I was unavailable she   could find my published products directory on the 'T' drive or   on the CD-RWs. I sorted all of my products or research by date,   time, and group; and updated the information on each of the   storage methods to ensure that the latest information was   available to them.

During the   deployment I had several of the D6-A machines crash on me.   Whenever one of the computer crashed, I usually lost information   but the redundancy method ensured my ability to quickly restore   old backup data and add my current information to the machine when it was repaired or replaced.

I stored   the backup CD-RW with larger datasets in the conference room of   the T-SCIF or next to my workstation. I marked the CD-RWs based   on the classification level and its content. Unclassified CD-RWs   were only labeled with the content type and not marked with   classification markings. Early on in the deployment, I only   saved and stored the SigActs that were within or near   operational environment.

Later I   thought it would be easier to just to save all of the SigActs   onto a CD-RW. The process would not take very long to complete   and so I downloaded the SigActs from CIDNE-I onto a CD-RW. After   finishing with CIDNE-I, I did the same with CIDNE-A. By retrieving the CIDNE-I and CIDNE-A SigActs I was able to   retrieve the information whenever I needed it, and not rely upon   the unreliable and slow SIPRnet connectivity needed to pull. Instead, I could just find the CD-RW and open up a pre-loaded   spreadsheet.

This   process began in late December 2009 and continued through early   January 2010. I could quickly export one month of the SigAct   data at a time and download in the background as I did other   tasks.

The   process took approximately a week for each table. After   downloading the SigAct tables, I periodically updated them, by   pulling the most recent SigActs and simply copying them and   pasting them into the database saved on the CD-RW. I never hid   the fact that I had downloaded copies of both the SigAct tables   from CIDNE-I and CIDNE-A. They were stored on appropriately   labeled and marked CD-RW, stored in the open.

I viewed   this the saving copies of CIDNE-I and CIDNE-A as for both for my   use and the use of anyone within the S2 section during the   SIPRnet connectivity issues.

In   addition to the SigAct tables, I had a large repository of   HUMINT reports and Counter IED reports downloaded from CIDNE-I.   These contained reports that were relevant to the area in and   around our operational environment in Eastern Baghdad and the   Diyala Province of Iraq.

In order   to compress the data to fit onto a CD-RW, I used a compression   algorithm called 'bzip2'. The program used to compress the data   is called 'WinRAR'. WinRAR is an application that is free, and   can be easily downloaded from the internet via the Non-Secure Internet Relay Protocol Network or NIPRnet. I downloaded WinRAR   on NIPRnet and transfered it to the D6-A machine user profile   desktop using a CD-RW. I did not try to hide the fact that I was   downloading WinRAR onto my SIPRnet D6-A machine or computer.

With the   assistance of the bzip2 algorithm using the WinRAR program, I   was able to fit All of the SigActs onto a single CD-RW and   relevant HUMINT and Counter ID reports onto a separate CD-RW.

 Facts regarding my knowledge of the WikiLeaks Organization or   WLO.

I first became vaguely aware of the WLO during my AIT at Fort Huachuca, Arizona, although I did not fully pay attention until the WLO released purported Short Messaging System or SMS messages from 11 September 2001 on 25 November 2009. At that time references to the release and the WLO website showed up in my daily Google news open source search for information related to US foreign policy.

The stories were about how WLO published about approximately 500,000 messages. I then reviewed the messages myself and realized that the posted messages were very likely real given the sheer volume and detail of the content.

After this, I began conducting research on WLO. I conducted searched on both NIPRnet and SIPRnet on WLO beginning in late November 2009 and early December 2009. At this time I also began to routinely monitor the WLO website. In response to one of my searches in 2009, I found the United States Army Counter Intelligence Center or USACIC report on the WikiLeaks organization. After reviewing the report, I believed that this report was possibly the one that my AIT referenced in early 2008.

I may or may not have saved the report on my D6-A workstation. I know I reviewed the document on other occasions throughout early 2010, and saved it on both my primary and secondary laptops. After reviewing the report, I continued doing research on WLO. However, based upon my open-source collection, I discovered information that contradicted the 2008 USACIC report including information that indicated that similar to other press agencies, WLO seemed to be dedicated to exposing illegal activities and corruption.

WLO received numerous award and recognition for its reporting activities. Also, in reviewing the WLO website, I found information regarding US military SOPs for Camp Delta at Guantanamo Bay, Cuba and information on the then outdated rules of engagement for ROE in Iraq for cross-border pursuits of former members of Saddam Hussein [missed word] government.

After seeing the information available on the WLO website, I continued following it and collecting open sources information from it. During this time period, I followed several organizations and groups including wire press agencies such as the Associated Press and Reuters and private intelligence agencies including Strategic Forecasting or Stratfor. This practice was something I was trained to do during AIT, and was something that good analysts were expected to do.

During the   searches of WLO, I found several pieces of information that I   found useful in my work product in my work as an analyst,   specifically I recall WLO publishing documents related to   weapons trafficking between two nations that affected my OP. I   integrated this information into one or more of my work   products.

In   addition to visiting the WLO website, I began following WLO   using Instand Relay Chat or IRC Client called 'XChat' sometime   in early January 2010.

IRC is a   protocol for real time internet communications by messaging and   conferencing, colloquially referred to as chat rooms or chats.   The IRC chat rooms are designed for group communication   discussion forums. Each IRC chat room is called a channel--   similar to a Television where you can tune in or follow a   channel-- so long as it is open and does not require [missed   word].

Once you   [missed word] a specific IRC conversation, other users in the   conversation can see that you have joined the room. On the   Internet there are millions of different IRC channels across   several services. Channel topics span a range of topics covering   all kinds of interests and hobbies. The primary reason for   following WLO on IRC was curiosity-- particularly in regards to   how and why they obtained the SMS messages referenced above. I   believed that collecting information on the WLO would assist me   in this goal.

Initially   I simply observed the IRC conversations. I wanted to know how   the organization was structured, and how they obtained their   data. The conversations I viewed were usually technical in   nature but sometimes switched to a lively debate on issue the   particular individual may have felt strongly about.

Over a   period of time I became more involved in these discussions   especially when conversations turned to geopolitical events and   information technology topics, such as networking and encryption   methods. Based on these observations, I would describe the WL   organization as almost academic in nature. In addition to the   WLO conversations, I participated in numerous other IRC channels   acros at least three different networks. The other IRC channels   I participated in normally dealt with technical topics including   with Linux and Berkley Secure Distribution BSD operating systems   or OS's, networking, encryption algorithms and techniques and   other more political topics, such as politics and

[missed word].

I normally   engaged in multiple IRC conversations simultaneously--mostly   publicly, but often privately. The XChat client enabled me to   manage these multiple conversations across different channels   and servers. The screen for XChat was often busy, but its   screens enabled me to see when something was interesting. I   would then select the conversation and either observe or   participate.

I really   enjoyed the IRC conversations pertaining to and involving the   WLO, however, at some point in late February or early March of   2010, the WLO IRC channel was no longer accessible. Instead,   regular participants of this channel switched to using the   Jabber server. Jabber is another internet communication [missed   word] similar but more sophisticated than IRC.

The IRC   and Jabber conversations, allowed me to feel connected to others   even when alone. They helped pass the time and keep motivated   throughout the deployment.