IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

UNITED STATES	)	
	)	**DEFENSE MOTION FOR**
v.	)	**DIRECTED VERDICT:**
	)	**18 U.S.C. 1030 OFFENSE**
MANNING, Bradley E., PFC	)	
U.S. Army, (b) (7)(C)	)	
Headquarters and Headquarters Company, U.S.	)	
Army Garrison, Joint Base Myer-Henderson Hall,	)	DATED: 4 July 2013
Fort Myer, VA 22211	)	

RELIEF SOUGHT

1. COMES NOW PFC Bradley E. Manning, by counsel, pursuant to applicable case law and Rule for Courts Martial (R.C.M.) 917(a), requests this Court to enter a finding of not guilty for Specification 13 of Charge II.

STANDARD

2. A motion for a finding of not guilty should be granted when, viewing the evidence in the light most favorable to the prosecution, there is an "absence of some evidence which, together with all reasonable inferences and applicable presumptions, could reasonably tend to establish every essential element of an offense charged." R.C.M. 917(d).

ARGUMENT

A. The Government's Theory is Legally Deficient

3. During the motions phase of this case, the Defense brought two separate motions to dismiss the 18 U.S.C. §1030 offenses based upon the Government's failure to state an offense. The Court ruled, in response to the first motion, that the Court would adopt the narrow view of *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) such that the Government would not be able to bootstrap use restrictions (improper use of information) into access restrictions for the purposes of 18 U.S.C. §1030. The Government thereafter shifted its theory of criminality to focus on PFC Manning's use of an apparently unauthorized program to ground an offense under section 1030. The Court, not having the benefit of evidence on this point, did not dismiss the offenses and reiterated that the military justice system is a notice pleading jurisdiction and that the charge was sufficient to state an offense.

4. Now that the Court has had the full benefit of all the evidence on the issue of access to the NetCentric Diplomacy database, the Defense moves this Court to dismiss the charge under R.C.M. 917.

5. The Government's theory of liability is the following:

> In order for a person to access or obtain a diplomatic cable on the NCD website, the person has to individually "click" or "save" the diplomatic cable after searching for the cable or navigating to the cable in some manner. As the evidence will show, the accused bypassed the ordinary method of accessing information by adding unauthorized software to his SIPRNET computer and using that software to rapidly harvest or data-mine the information. Wget was not available on the computers used by the accused or authorized as a tool to download the information. Thus, the accused violated a restriction on access to the information - he bypassed a code-based restriction - by using Wget to obtain the cables in batches.

See Appellate Exhibit 188 at p. 5.

6. The Government has introduced evidence that PFC Manning used the program Wget to download the diplomatic cables. However, PFC Manning's purported use of this allegedly unauthorized program[1] to download the information specified in Specification 13 of Charge II does not change and cannot change the only fact that matters in the "exceeds authorized access" inquiry: PFC Manning was authorized to access each and every piece of information he accessed. The Government has not introduced any evidence to suggest that PFC Manning was not permitted to view the cables in question. The Government has not introduced any evidence to suggest that PFC Manning was not permitted to download the cables in question. The Government simply asserts that PFC Manning was not permitted to download them using a certain program, Wget.

7. The Government has not introduced evidence that Wget in some way expanded the access that PFC Manning had, such that it gave him access to information that he otherwise would not have had access to. The Government's witness, Agent Shaver, testified that: Wget does not give a user access to information that they otherwise would not have access to; Wget would not allow a user to grab information that they would not normally be able to see; Wget would not allow the user to circumvent any sort of restrictions that the Net-Centric Diplomacy database may place on the user; and Wget would not give a user any more access than they would have normally. *See* Testimony of Agent Shaver. The Government has thus not introduced evidence that PFC Manning by-passed any restrictions on access that would give PFC Manning access to information that he otherwise would not have had access to. All the Government has to hang its hat on is that PFC Manning used allegedly "unauthorized software" –as defined by an AUP that the Government could not even produce—in downloading the cables. This does not come close to establishing "exceeds authorized access" within the meaning of 18 U.S.C. §1030.

8. The Government is simply incorrect in asserting that the use of an unauthorized program to download information automatically converts what would otherwise be authorized access to that information into "exceeding authorized access." Whether or not PFC Manning used Wget to download the information he had access to is irrelevant; under the language of Section 1030, as well as this Court's ruling and all legal authorities, PFC Manning could not have exceeded his

[1] The Defense contests that this program was unauthorized, *infra* at C.

authorized access because he was authorized to obtain the *information* he obtained. That is, "exceeds authorized access" is not concerned with the *manner* in which information to which one has access is downloaded; it is rather concerned with whether the accused was *authorized to obtain or alter the information* that was obtained or altered.

9. Section 1030(e)(6) defines "exceeds authorized access" as follows: "the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6). This definition demonstrates that the Computer Fraud and Abuse Act (CFAA) is concerned with the relationship between the accesser and the *information*: is the accesser entitled to obtain or alter the information at issue? In *United States v. Nosal*, the en banc Ninth Circuit explicitly tied the concept of "exceeds authorized access" to the defendant's authorization to access the particular *information* at issue: "'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized *information or files*)." 676 F.3d 854, 858 (9th Cir. 2012) (en banc) (second emphasis supplied); *see also* Appellate Exhibit CXXXIX, at 7 ("*Nosal III* defines 'exceeds authorized access' to apply to *inside* hackers or individuals whose initial access to a computer is authorized but who accesses unauthorized information or files." (emphasis in original)). Nothing in the discussion of the narrow interpretation of "exceeds authorized access" in *Nosal* gives any indication that the manner in which a person downloads information has any bearing whatsoever on whether the person is authorized to access that information.

10. In this case, the Government does not dispute that PFC Manning was entitled to access the information and has offered no proof that PFC Manning was not authorized to access the cables. Similarly, the Government does not dispute that PFC Manning was entitled to download the information and has offered no proof that PFC Manning was not authorized to download the cables. The Government's Wget theory— that PFC Manning exceeded authorized access by using an unauthorized program to download the information—erroneously focuses on the manner in which PFC Manning downloaded the information. But the manner in which he downloaded the information is beside the point, since at all times he remained entitled to access the information in question.

11. The ridiculousness of the Government's theory is highlighted when one really distills what the Government is saying. If PFC Manning had downloaded the cables one-by-one (or with a program like Excel which was in the baseline package for the DCGS-A machines), then PFC Manning would not be facing a ten-year prison sentence under 18 U.S.C. §1030. However, because he is alleged to have used a program not technically approved on his DCGS-A machine, he is facing a ten-year prison sentence. A decade in jail cannot turn on what programs the Army happens to put on its "authorized software" list. While the Defense concedes that releasing the diplomatic cables was a criminal offense—one for which PFC Manning has accepted responsibility—it is not, under any stretch of the imagination, a computer crime within any rational meaning of 18 U.S.C. §1030.

12. If computer crimes will now turn on whether an accused uses unauthorized hardware or software to look at or download information that they otherwise have access to, this would be an extremely dangerous (not to mention unconstitutional) application of the statute. This is particularly so considering that 18 U.S.C. §1030(2)(C) criminalizes "exceeding authorized

access" and "thereby obtain[ing] information from any protected computer." In other words, simply "exceeding authorized access" and obtaining *any* information from a government computer would subject an accused to imprisonment. No particular type of information is required to have been accessed, nor does the information have to have been transmitted. It is simply "getting" the information by means of exceeding authorized access which is criminal. Consider what this would mean in practice if one could exceed authorized access simply by using unapproved hardware or software to view, download or print information that the accessor is otherwise entitled to view, download or print. A soldier who connected a commercial printer to a government computer (rather than a government-approved printer) would be exceeding authorized access if he printed any documents. A soldier who used an unapproved storage device (rather than a government-approved storage device) would be guilty of exceeding authorized access if he saved some documents onto it. A soldier who used the newest unapproved version of Excel to download information (rather than the government-approved version of Excel) would be guilty of exceeding authorized access. What most, and certainly those in PFC Manning's Brigade, would consider a minor breach of information assurance protocols would now be a felony.

13. There is absolutely no legal precedent for the Government's argument that the specific program with which information is downloaded can determine whether a person "exceeds authorized access" within the meaning of 18 U.S.C. §1030. A survey of the case law reveals that no criminal prosecutions have been maintained based on a theory in the nature of that advanced by the Government here (i.e. that the accessor was permitted to access the information, was permitted to download the information, but was not permitted to download the information using a certain program).

14. One civil case, however, made allegations very similar to those in the instant case. In *Wentworth-Douglass Hospital v. Young & Novis Professional Association*, 2012 WL 2522963 (D.N.H.), the plaintiff hospital alleged that certain doctors violated 18 U.S.C. §1030 on the basis that they downloaded information that they were otherwise entitled to access onto "extraordinarily large" unauthorized storage devices. The plaintiff pointed to the equivalent of the hospital's Acceptable Use Policy (WDH Policy Document IM-09) to show that the use of unauthorized storage devices to download information that one had authorized access to was prohibited by 18 U.S.C. §1030. The complaint laid out the relevant provisions of the hospital's computer policy (similar to the Army's policy) as well as the plaintiff's theory that the use of unauthorized hardware rendered the defendant's access to information unauthorized:

> 20. Pursuant to IM-09, Attachment 1, Section D ("Electronic Information"):
>
> > 4. No external hardware will be brought in and connected into the hospital information network without the approval of the Information Systems Department.
> >
> > 5. No software from external or unauthorized sources will be loaded on hospital computers without the approval of Information Systems. The hospital retains the right to remove any unauthorized or unlicensed

> software from any hospital computers. Any person found loading or using unapproved software will be considered in breach of this policy.
>
> ...
>
> 43. Between February 1, 2010 and February 28, 2010, removable storage devices or external hardware were connected to PY001, PY002 and the HP Laptop. Late on February 28, 2010, the last day when Dr. Moore and Dr. Littell had access to the desk top computers and laptop, *extraordinarily large removable storage devices* were attached to each of PY001, PY002 and the HP Laptop.
>
> ...
> 72. Defendants intentionally accessed computers without authorization or exceeded authorized access, and thereby obtained information from a protected computer in that Defendants, without the prior authorization and approval of the WDH Information Systems Department and in violation of IM-09, connected removable storage devices or external hardware to PY001, PY002 and the HP laptop computer, and obtained or altered information from WDH computers owned by WDH that Defendants were not entitled to obtain or alter.

See 2010 WL 4786559 (D.N.H.). In short, the plaintiff hospital alleged that the defendant doctors exceeded their authorized access under 18 U.S.C. §1030 because they downloaded information onto "extraordinarily large" removable storages devices or external hardware that was not authorized under the governing computer policy. Notably, the plaintiff did not allege that the defendants were not permitted to access the information in question or were not permitted to download the information in question. The plaintiff simply alleged that accessing information *in this particular manner*—i.e. by downloading that information onto "extraordinarily large" removable storage devices that were not authorized—violated 18 U.S.C. §1030. Thus, the allegations in *Wentworth-Douglass* mirror those in the instant case. In neither case is it disputed that the accessor of the information had permission to access or download the information. In both cases, the issue is whether the accessor had permission to download information *in a particular manner* (i.e. through an unauthorized storage device or through an unauthorized program).

15. The court in *Wentworth-Douglass* framed the issue as follows:

> Mirroring the language of the CFAA, count one of the amended complaint alleges that "Defendants intentionally accessed computers without authorization or exceeded authorized access, and thereby obtained information from a protected computer." Amended Complaint (document no. 68) at para. 82. But, in elaborating on that claim, the hospital says: Count I [of the amended complaint] alleges the Defendants violated [18 U.S.C. § 1030(a)(2)(C)] because, without the prior authorization and approval of the WDH Information Systems Department and in *violation of the IM–09, they connected removable storage devices* or external hardware to hospital computers and obtained or altered information from WDH computers owned by WDH that *they were not entitled to obtain or alter.*

> Plaintiff's Motion for Summary Judgment (document no. 81–1) at 13 (emphasis supplied).
>
> ...
>
> With respect to Dr. Cheryl Moore and Dr. Littell, the issue presented is whether they can be liable under section 1030(a)(2)(C) for having violated the hospital's computer use policy when they allegedly connected removable storage devices to hospital computers and then downloaded and/or copied data that they were otherwise authorized to access.

Wentworth-Douglass Hospital v. Young & Novis Professional Association, 2012 WL 2522963, *3 (D.N.H.). The court held that the defendants could *not* be liable under 18 U.S.C §1030 when they downloaded/copied data that they were otherwise authorized to access, onto unauthorized storage devices. Accordingly, the court entered a directed verdict for the defendants.

16. The court saw the relevant inquiry as whether or not the defendants were authorized to access the "hospital's computer and the data at issue," not whether the defendants were authorized to download the information onto unauthorized storage devices. *Id.* at *4. The plaintiff tried to characterize the hospital's computer policy prohibiting unauthorized hardware (the equivalent of the Army's AUP) as being an "access restriction" and not a use restriction. The court outright rejected this argument:

> The court disagrees. Of course, the distinction between an employer-imposed "use restriction" and an "access restriction" may sometimes be difficult to discern, since both emanate from policy decisions made by the employer—decisions about who should have what degree of access to the employer's computers and stored data, and, once given such access, the varying uses to which each employee may legitimately put those computers and the data stored on them. But, simply denominating limitations as "access restrictions" does not convert what is otherwise a use policy into an access restriction. Here, the hospital's policy prohibiting employees from accessing company data for the purpose of copying it to an external storage device is not an "access" restriction; it is a limitation on the use to which an employee may put data that he or she is otherwise authorized to access. An employee who is given access to hospital data need not "hack" the hospital's computers or circumvent any technological access barriers in order to impermissibly copy that data onto an external storage device. The offending conduct in such a case is misuse of data the employee was authorized to access, not an unauthorized access of protected computers and data.

Id. So too is the case here. In fact, the *Wentworth-Douglass* court's rejection of the possibility of *civil* liability under section 1030 in circumstances very similar to those alleged here should sound a note of extreme caution to a criminal court. If the "unauthorized hardware/software" theory is not sufficient to ground civil liability, surely it is not sufficient to ground criminal liability. And indeed, there is *no criminal* case that has accepted the narrow view of the Computer Fraud and Abuse Act (i.e. the *Nosal* view) where a theory like the Government's

(accused had access to download, but didn't have permission to download with a particular program) has even been advanced, much less where the theory has succeeded. Thus, under the authority of *Wentworth-Douglass*, the only case to make allegations similar to those in the instant case, PFC Manning cannot be found criminally liable under 18 U.S.C. §1030 for violating the terms of the Acceptable Use Policy when he was permitted to access the information in question and was permitted to download the information in question.

17. Additional authority that a violation of a computer use policy cannot turn what is otherwise authorized access into "exceeds authorized access" is found in the recent Fourth Circuit decision in *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199 (4th Cir. 2012). In that case, the plaintiffs advanced the argument that the defendants exceeded authorized access within the meaning of 18 U.S.C. §1030 because "under WEC's [the employer's] policies they were not permitted to download confidential and proprietary information to a personal computer." *Id.* at 202. The district court held that the complaint failed to state an offense because "Appellees' alleged conduct—the violation of policies regarding the use and downloading of confidential information—did not contravene any of these [section 1030] provisions." *Id.* On appeal, the Fourth Circuit affirmed the district court's judgment:

> WEC founds its CFAA claim on Miller's and Kelley's violations of its policies "prohibiting the use of any confidential information and trade secrets unless authorized" and prohibiting the "download[ing] [of] confidential and proprietary information to a personal computer." Notably, however, WEC fails to allege that Miller and Kelley accessed a computer or information on a computer without authorization. Indeed, WEC's complaint belies such a conclusion because it states that Miller "had access to WEC's intranet and computer servers" and "to numerous confidential and trade secret documents stored on these computer servers, including pricing, terms, pending projects [,] and the technical capabilities of WEC." Thus, we agree with the district court that although Miller and Kelley may have misappropriated information, they did not access a computer without authorization or exceed their authorized access.

Id. at 206-207.

18. The Fourth Circuit specifically held that the manner in which a defendant accessed information (in particular, by the unauthorized downloading onto a personal computer) could not ground civil liability, much less criminal liability, under 18 U.S.C. §1030. In this respect, it stated:

> Nevertheless, because WEC alleges that Miller and Kelley obtained information by downloading it to a personal computer in violation of company policy, we go a step further. Although we believe that interpreting "so" as "in that manner" fails to subject an employee to liability for violating a use policy, we nonetheless decline to adopt the *Nosal* panel's interpretation of the conjunction. The interpretation is certainly plausible, but it is not "clearly warranted by the text." Indeed, Congress may have intended "so" to mean "in that manner," but it "could just as well have included 'so' as a connector or for emphasis." Thus, faced with the option of two interpretations, we yield to the rule of lenity and choose the

more obliging route. "[W]hen [a] choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite."

Here, Congress has not clearly criminalized obtaining or altering information "in a manner" that is not authorized. Rather, it has simply criminalized obtaining or altering information that an individual lacked authorization to obtain or alter. And lest we appear to be needlessly splitting hairs, we maintain that the *Nosal* panel's interpretation would indeed be a harsher approach. For example, such an interpretation would impute liability to an employee who with commendable intentions disregards his employer's policy against download information to a personal computer so that he can work at home and make headway in meeting his employer's goals. Such an employee has authorization to obtain and alter the information that he downloaded. Moreover, he has no intent to defraud his employer. But under the *Nosal* panel's approach, because he obtained information "in a manner" that was not authorized (i.e., by downloading it to a personal computer), he nevertheless would be liable under the CFAA. *See* §1030(a)(2)(C). Believing that Congress did not clearly intend to criminalize such behavior, we decline to interpret "so" as "in that manner."

Id. at 205-206. Notably, the Fourth Circuit's passage referred to the Ninth Circuit panel's decision on the word "so" which was ultimately overruled *en banc* in *Nosal*, 676 F.3d 854 (9th Cir. 2012). Accordingly, and in light of the *en banc* decision in *Nosal*, the reasoning of the Fourth Circuit is even more persuasive that the manner in which information is downloaded is irrelevant to the "exceeds authorized access" inquiry.

19. In short, the Government has provided no evidence that PFC Manning was not authorized to access each and every piece of information covered in Specification 13 of Charge II. It instead argues that his use of Wget to download the information specified in Specification 13 renders his otherwise authorized access to that information an excess of his authorization. Such a theory finds no support in Section 1030, its legislative history, and the rulings of this Court and so many others that have adopted the narrow interpretation of "exceeds authorized access." Under that narrow interpretation of the phrase, the only inquiry is whether the accesser is entitled to obtain or alter the information at issue; the manner in which that information is downloaded does not provide an answer to that inquiry. Therefore, since PFC Manning was authorized to access all of the information covered in Specification 13 of Charge II, PFC Manning must be found not guilty.

B. The Government Has Not Introduced Evidence that Using Unauthorized Software was an Access Restriction

20. Even if one accepts that the Government's theory is not legally deficient, the Government has still not established that installing and using unauthorized software was an *access* restriction. According to the Government, the prohibition on using unauthorized software generally (but not Wget specifically) is found in the Army's Acceptable Use Policy (AUP). If the Army wanted to

create an access restriction, it must do so in a more clear way than burying it in a generic, multi-page, multi-topic AUP.[2] *See United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) ("Significant notice problems arise if we allow criminal liability to turn on the vagaries of private polices that are lengthy, opaque, subject to change and seldom read.").

21. Critically, the Government has not even presented the AUP signed by PFC Manning or anyone in his brigade. Thus, it is impossible to determine exactly what PFC Manning knew or should have known in terms of limitations on access and/or use.[3] Second, to state the obvious—the AUP refers to the Acceptable *Use* Policy, not the Acceptable *Access* Policy. This very fact shows that the policy focuses on *use* restrictions and not *access* restrictions. Third, the provision in the sample AUP regarding unauthorized software states, "d. I will *use* only authorized hardware and software I will not install or *use* any personally owned hardware, software, shareware, or public domain software." The fact that the word "use" appears twice in this sentence clearly shows that this is a "use" restriction and not an "access" restriction.[4]

22. The Government has provided no evidence to show that the prohibition against unauthorized software was an *access* restriction. The Government has called no witness to say that PFC Manning understood (or that soldiers in general understood) that the use of unauthorized software was a limitation on computer access, rather than use, and that any exceeding of that access could result in a felony conviction. Without an understanding that the use of unauthorized software constituted an access restriction, a soldier (in this case, PFC Manning) could not have *knowingly* exceeded authorized access by installing and using such software.

23. Further, the Government has introduced no evidence to show that computer access of soldiers who used unauthorized software was suspended. The evidence elicited showed that members of the S-2 section constantly added what would be considered "unauthorized software" to their DCGS-A computers. If the adding and using of unauthorized software was an "access" restriction, then presumably these soldiers would have had their access circumscribed or suspended for exceeding their authorized access. The testimony shows otherwise. CPT Cherepko testified that if he was able to identify the individual who added unauthorized software, he would "go to that soldier and explain the reasons why it's a bad idea." *See*

---

[2] The Defense adheres to the position that allowing employers, including the Army, to develop contract-based *access* restrictions would render 18 U.S.C. §1030 constitutionally vague and/or overbroad. *See United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). If the Army could simply make all use restrictions look like access restrictions (e.g. by stating "access to this computer system is conditioned upon a soldier using approved U.S. Government hardware and software"), this would criminalize a huge swath of conduct that is currently only punishable as a violation of a regulation. Moreover, to the extent that this Court believes that an AUP may contain both use and access restrictions, it needs to be clear to soldiers which one is which since an access restriction can render a soldier liable to imprisonment under 18 U.S.C. §1030, while a use restriction cannot.

[3] The testimony elicited by the Government established that there is a difference between "unauthorized software" (which is installed onto computers) and "executable files" (which are not installed onto the computer but only require a "double click"). Wget falls into the latter category. The Government has not provided any evidence that the AUP signed by PFC Manning even prohibited the use of executable files.

[4] No court that has accepted the narrow view of *Nosal* has found that an Acceptable Use Policy or the like can define *access* restrictions, rather than *use* restrictions. And for good reason. If all that is required to convert what otherwise is a use restriction into an access restriction is to change the phraseology of the provision, then employees will face criminal liability for breaches of contract that do not involve exceeding authorized access under any sensible understanding of the term.

Testimony of CPT Cherepko. Communicating that something is a "bad idea" is very different than communicating that something is an *access* restriction (i.e. that a soldier's access to a computer is contingent upon not using unauthorized software). It is clear that the installation and use of unauthorized software was always treated as a use restriction—and, as described below, one that was not ever enforced by the brigade.

24. The Government has also failed to introduce any evidence that there were any access restrictions on the Net-Centric Diplomacy database itself. The Government has not introduced evidence, for instance, that the Net-Centric Diplomacy database prevented downloading information using a program like Wget; indeed, the evidence was to the contrary—that there were no technical access restrictions on downloading the information or on the manner of downloading the information. Mr. Wisecarver testified that there were no access restrictions on the Net-Centric Diplomacy database. *See* Testimony of Mr. Wisecarver ("But, again, understanding that NCD was a web-based type of application, so I don't believe it was limited at all. If you had access to SIPRNET, you had that secret clearance, you were given authorization to use SIPRNET, then by default you would have access to NCD"). Mr. Wisecarver further testified that there were no individual access or authentication restrictions on the Net-Centric Diplomacy database and that a user could have multiple cables open at the same time which the user could download or print simultaneously.

25. Similarly, the Government has not introduced evidence of non-technical barriers on access, such as a banner on the Net-Centric Diplomacy database that said something to the effect of "This database must be accessed only with government-authorized hardware and software"[5] or "Information in this database may not be downloaded using automated tools." The banner that did appear on the Net-Centric Diplomacy database focused on the *use* of the information; it did not speak at all to the manner of access. *See* Testimony of Mr. Wisecarver (stating that the banner did not specify any restrictions on how information was accessed, or on the manner of downloading cables; nothing in the warning indicated that a user had to 'click, open, save'); *see also* Testimony of COL Miller (stating that the Brigade did not put out any restriction on the manner of downloading information from the SIPRNET or require that soldiers "click, open, and save" information). Accordingly, the Government has not established that anything resembling what might be considered an access restriction appeared on the Net-Centric Diplomacy database.

C. The Government Has Not Introduced Evidence that PFC Manning Knowingly Exceeded Authorized Access

26. The Government has presented evidence that Wget was not on the approved list of programs for the DCGS-A computer used by PFC Manning in downloading the cables. Thus, it argues that since PFC Manning downloaded information that he was otherwise entitled to download with "unauthorized software" he thereby exceeded his authorized access within the meaning of 18 U.S.C. §1030.

[5] The Defense submits that this would not actually be an access restriction. It would be a *use* restriction, masquerading as an access restriction.

27. The Government has not proven that Wget, which is an executable file, was "unauthorized software" in the particular environment in which PFC Manning worked.[6] While it may not have been officially approved for use on the DCGS-A computer, whether or not something is "authorized" or "unauthorized" is determined by a lot more than a piece of paper. For instance, Mr. Weaver, the Information Assurance manager who testified as to the scope and content of Army Regulation 25-2, was asked whether soldiers were authorized to use games, movies, music and other executable files. In response, he stated "You want the regulation answer or my opinion, sir?" *See* Testimony of Mr. Weaver. The answer and explanation given by Mr. Weaver demonstrates that there can be a disconnect between what the rules are "on paper" and what the rules are in practice. This disconnect is bolstered by the testimony of COL Miller. COL Miller testified that technically unauthorized media could be approved for morale and welfare purposes. *See* Testimony of COL Miller ("Because sometimes these risks -- the reason given for it's not authorized is because there's a document that says this is not authorized and therefore it's a risk. What I always want to get to is why, not the document, but what was the logic behind that being put in that document so I can get to the root reason."). This fact further highlights the distinction between what the rules were on paper as opposed to what the rules were in practice.

28. The Defense submits that the use of executable files was permitted by the S-2 section, and therefore Wget was not unauthorized. Every unit witness called by the Government testified that there was music, movies and games on the computers in the T-SCIF (whether on the T-drive or on the individual computers themselves). *See e.g.* Testimony of CPT Cherepko; Testimony of Mr. Maderas; Testimony of CW2 Balonek; Testimony of Ms. Showman; Testimony of COL Miller. Further testimony of some of these witnesses established that at least some of these music, movies and games took the form of executable files which were run directly from the desktop.

29. Mr. Maderas testified that PFC Manning added mIRC-chat to his computer and the computer of others as an executable file. mIRC-chat was not a standard program on the DCIGS-A machines. Mr. Maderas testified that he believed this was permitted and did not think it was a problem that the mIRC-chat executable file was added by PFC Manning rather than Mr. Millman. *See* Testimony of Mr. Maderas. Similarly, Ms. Showman also testified that she asked PFC Manning to put mIRC-chat on her computer and that he did. She did not believe that the adding of mIRC-chat by PFC Manning, as opposed to Mr. Millman, was a violation of the user agreement.

30. Unit witnesses testified that no soldier was, to their knowledge, ever punished for the placement or use of unauthorized software on the DCGS-A machines. *See e.g.* Testimony of Mr. Maderas. Testimony from CPT Cherepko confirmed that the command had actual knowledge of the use of executable files on the DCGS-A machines and did not do anything about it. CPT Cherepko confirmed that there was a command laxity with regard to the use of executable files.

---

[6] Both the Government and Defense elicted testimony that Wget was an executable file, meaning that the file is not a program that is "installed" onto the computer. Instead the program runs from the desktop after double-clicking or runs from a compact-disc. Executable files do not require administrative rights to run. *See* Testimony of CPT Cherepko ("There is no installation process. If you have it on a CD or thumb drive or on your desktop you can simply run it. There's no administrative rights required.").

See Testimony of CPT Cherepko. It is clear that soldiers in the S-2 shop were permitted to add executable files to their computers and did so on a regular basis. It is also clear that the chain of command knew about this rampant practice and did nothing about it. In short, soldiers in the T-SCIF were allowed to place executable files on their computer, despite the apparent on paper prohibition against adding "unauthorized software." In the S-2 shop, executable files were not considered "unauthorized software." Thus, in using an executable file, Wget, to download the cables, PFC Manning did not use "unauthorized" software. Instead, he used an executable file—a practice that had been sanctioned and approved of by the S-2 leadership and the chain of command.

31. If the Court nonetheless believes that, despite the practice in the S-2 shop, PFC Manning nonetheless used "unauthorized software", the Government has still failed to prove that PFC Manning *knowingly* exceeded his authorized access. If the Government's theory of exceeds authorized access is that PFC Manning used unauthorized software, then he must have *knowingly used* unauthorized software. Given the evidence elicited from all the unit witnesses as to what they believed was permitted and what they believed was not permitted, the Government has not introduced any evidence that PFC Manning *knew* he was exceeding his authorized access by using an executable file to download information that he had authorized access to.

32. For instance, CW2 Balonek testified that he did not know whether the use of executable files in the form of games, movies or music was authorized or not. He testified that he believed that games were allowed, if work was low. He further testified that the rules in garrison were different than the rules in theater ("different rules for different areas"). *See* Testimony of CW2 Balonek. Similarly, Mr. Maderas testified that he did not know whether the use of unauthorized software in the form of games, movies or music was prohibited. In response to the Court's question, he said that there was "silence" on whether this was authorized or not. *See* Testimony of Mr. Maderas. Ms. Showman testified that she believed that the S6 approved of music, movies and games on the DCGS-A computers, or at least she assumed they were authorized since the command knew about them and did nothing about it. *See* Testimony of Ms. Showman. It is clear that, at the very least, the rules of the game in the T-SCIF were unclear as to what was authorized and what was not. Accordingly, and against this backdrop, there is no evidence that PFC Manning knew that by using Wget, an executable file, he was exceeding authorized access.

33. Importantly, the fact that PFC Manning knew that ultimately transmitting the cables was wrong does not mean that he knew that his *use of the computer* in those circumstances was wrong. *See* 1996 Legislative History of 18 U.S.C. 1030 ("It is the *use of the computer* that is being proscribed, not the unauthorized possession of, access to, or control over the information itself.")(emphasis added). Section 1030 criminalizes those who "knowingly" exceed authorized access. Thus, the Government must show that PFC Manning knew that, by using an executable file to download information to which he otherwise had full access, PFC Manning was exceeding the access he was given. In light of what was permitted at the S-2 shop in terms of the use of executable files, the Government has introduced no evidence that PFC Manning had knowledge that by using Wget, he was exceeding his authorized access.

D. The Government Has Not Introduced Evidence of Its Own "Circumvention" Theory

34. The Government alleges that PFC Manning's use of "unauthorized software"—namely Wget—enabled him to rapidly download information. The fact that Wget rapidly downloads information has, in turn, led the Government to concoct a ridiculous "circumvention" argument whereby it alleges that PFC Manning circumvented the "normal" way of downloading information, thus making his action a computer crime within the meaning of 18 U.S.C. §1030.[7]

35. The circumvention argument is a complete red herring.[8] The Government's theory is that the use of "unauthorized software" can convert what is otherwise authorized access into "exceeds authorized access" within the meaning of section 1030. That unauthorized software in this case happens to be Wget. However, the unauthorized software could be anything, including an unapproved (and more recent) version of an approved program. So, for instance, if PFC Manning had downloaded the cables in an unapproved version of Excel, under the Government's view, he would still have exceeded his authorized access. Nothing turns on how fast or slow the download speed was—the crux of the Government's argument is the use of unauthorized software.

36. The Government now seeks to establish that the "normal" way of downloading information would be to manually press "click, open, and save" and that PFC Manning somehow by-passed or circumvented the process in contravention of Net-Centric Diplomacy access restrictions. The Defense believes that the Government has adopted this nomenclature to make it sound more like what PFC Manning did was hacking[9] or a computer crime under 18 U.S.C. §1030—when in reality it is clear that, at most, it is an Article 92 violation for the use of unauthorized software.

37. The Government has not introduced evidence that "click, open and save" was the normal way of downloading information on a SIPRnet computer. Indeed, analysts testified that they would often export large volumes of information using various tools, to include Excel. They would do this using an "export" function, not "click, open and save." *See e.g.* Testimony of CPT Fulton (explaining that PFC Manning was tasked to export SIGACTS into Excel to create a work product); Testimony of CW2 Balonek (explaining the use of Excel to import multiple amounts of points at the same time). Mr. Maderas, who was in PFC Manning's brigade, testified that he did not receive any training either at Fort Drum or during the deployment on *how* one had to download information from the SIPRNET. He testified that there was no formal guidance or statement that analysts had to download information in a particular way—specifically by using "click, open, save." He also testified that analysts often used Excel, which essentially automated the "click, open, save" function and allowed analysts to export large documents without having to manually "click, open and save." In using Excel, Mr. Maderas testified that the automated

---

[7] This argument is reminiscent of that advanced in *Douglass* where the plaintiff alleged that the defendant's exceeded their authorized access because they used "extraordinarily large" unauthorized storage devices to download information. Although not explicitly addressed in the case, the implication appears to be that the defendants were able to download more information than they otherwise would have been able to owing to the "extraordinarily large" storage devices (much like the Government's argument that PFC Manning was able to download much faster than he otherwise would have been able to do).

[8] Not surprisingly, there is not one case that the Defense was able to locate where the prosecution advanced a theory as attenuated as this.

[9] Agent Shaver testified that Wget is not synonymous with hacking and is just a "tool" that is used in a variety of contexts. In fact, Agent Shaver testified that he used Wget as part of his investigation to replicate the downloads that he identified from his forensic examination. *See* Testimony of Agent Shaver.

process was permitted and there was never anybody who told him he could not use an automated process. *See* Testimony of Mr. Maderas. Additionally, COL Miller testified that his Brigade did not put out any guidance on how soldiers had to download information on the SIPRNET and stated that there was no "click, open, save" requirement to download information. *See* Testimony of COL Miller.

38. Nor has the Government introduced evidence the Net-Centric Diplomacy database specifically was designed such that a user had to, *as an access restriction*, use the "click, open and save" method of downloading information. Mr. Wisecarver testified that he was not familiar with the design of Net-Centric Diplomacy (indeed, its design was outsourced to a private company). Accordingly, the Government has not introduced any evidence that it was a deliberate design feature of Net-Centric Diplomacy not to have a built-in mechanism for the automated downloading of cables. The lack of a technical feature to facilitate something is not at all indicative of an access restriction.[10] Moreover, the fact that Net-Centric Diplomacy was intended to facilitate "sharing of information" belies any argument that it was intended to have some sort of nonsensical "click, open and save" requirement (as such a requirement would actually inhibit the sharing of information). *See* Testimony of Mr. Wisecarver (indicating that there were no technical restrictions on access because the primary purpose of Net-Centric Diplomacy was information sharing).

39. Even if "click, open and save" were the normal way of downloading information on Net-Centric diplomacy and even if it were designed as some sort of access restriction, the Government has not established that the use of Wget by-passed this method. Indeed, Agent Shaver testified that Wget simply "automated" the process, it did not change it. *See* Testimony of Agent Shaver (noting that Wget did the "click, open, save" in an automated fashion). And, as indicated above, Mr. Wisecarver testified that there was no express prohibition on the Net-Centric Diplomacy database that warned that an automated downloading of information was not permitted. Any access restrictions, to the extent that they may have existed, did not originate with the Department of State, but rather were entrusted to the various government agencies that used Net-Centric Diplomacy. *See* Testimony of Mr. Wisecarver.

CONCLUSION

40. It is worth noting that the Government has adopted multiple theories of "exceeds authorized access" during the course of this proceeding. If the Government cannot even figure out what the objectionable conduct is which constitutes "exceeding authorized access" how can Soldiers be expected to know which actions are considered to be a "computer crime" and which actions are not? In other words, how could PFC Manning have knowingly exceeded authorized access at the time of the alleged offense if the Government did not even identify what conduct it considered criminal until it failed in its first attempt to state an offense? The fact that the Government is

[10] Consider, for instance, earlier versions of the Program Microsoft Word. Older versions of word did not have a function for "pdf"-ing documents (thus, one had to manually pdf a document). This was not indicative of a deliberate design *not* to permit something—i.e. it was not an access restriction. It was simply a feature that Word did not at the time possess.

clinging to a theory which hinges exclusively on the use of an apparently unauthorized program to ground imprisonment for 10 years shows just how weak this charge is.

41. There is not one case—not one—where any court in this country has premised criminal liability on a theory akin to the one the Government is advancing today. That fact alone speaks volumes. Consider, at base, what the Government is saying: the accused had authorized access to the database in question; the accused had authorized access to the information in question; the accused was entitled to download as much information as he wanted; but the accused used the wrong program to download that information. It would be a sad day indeed if a decade in jail could hinge exclusively on what program an accused used to download information he was otherwise entitled to access and otherwise entitled to download.

42. Accordingly, the Defense requests that this Court grant the R.C.M. 917 motion dismissing Specification 13 of Charge II.

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel