

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

GOVERNMENT RESPONSE TO
DEFENSE MOTION FOR DIRECTED
VERDICT: 18 U.S.C. 1030 OFFENSE

11 July 2013

RELIEF SOUGHT

COMES NOW the United States of America, by and through undersigned counsel, and respectfully requests this Court deny the Defense Motion for Directed Verdict: 18 U.S.C. § 1030 Offense.

STANDARD

"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 charged." Rule for Courts-Martial (hereinafter "RCM") 917(d). "The evidence shall be viewed in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*

WITNESSES/EVIDENCE

The United States requests the Court consider all previous submissions by the parties relating to the offenses alleging misconduct in violation of 18 U.S.C. § 1030(a)(1) (Appellate Exhibits 90, 91, 170, and 188), the Court's two previous rulings on this issue (AEs 139 and 218), and the testimony and evidence cited herein.

LEGAL AUTHORITY AND ARGUMENT

"The military judge, on motion by the accused or *sua sponte*, shall enter a finding of not guilty of one or more offenses charged after the evidence on either side is closed and before findings on the general issue of guilt are announced if the evidence is insufficient to sustain a conviction of the offense affected." RCM 917(a). The motion by the accused shall state with specificity where the evidence is insufficient to enable the trial counsel to respond to the motion, and the Court shall give each party an opportunity to be heard on the matter. *See* RCM 917(b); RCM 917(c); RCM 917(c), discussion (stating that the military judge ordinarily should permit the trial counsel to reopen the case as to the insufficiency specified in the motion).

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 charged." RCM 917(d). The Court shall view the evidence "in the light most favorable to the prosecution, without an evaluation of the credibility of witnesses." *Id.*; *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). The standard of "some evidence" required 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"); *United States v. Jenkins*, 59 M.J. 893, 898 (A. Ct. Crim. App. 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) (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 R.C.M. 917(d)") (quoting RCM 917(d)). 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).

The defense motion for a directed verdict with respect to Specification 13 of Charge II should be denied. For the third time in this court-martial, the defense argues that the United States has failed to allege the accused "exceeded authorized access" within the meaning of 18 U.S.C. § 1030(a)(1) because the accused "was authorized to access each and every piece of information he accessed." Def. Mot. at 2; see AE 170 at 4 ("PFC Manning was authorized to access each and every piece of information he allegedly accessed"); AE 90 at 27 ("PFC Manning had access to the relevant SIPRNET computers and was authorized to access every piece of information that he allegedly accessed on the SIPRNET"). The defense argument over three separate filings is virtually verbatim—the only change is that the defense has dropped the word "allegedly." This Court has ruled that restrictions on access "can include manner of access." AE 218 at 2. In filing this motion for a directed verdict, the defense appears to have ignored the Court's statement of the law. See Def. Mot. at 3 ("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."). The Government's theory for Specification 13 of Charge II is a valid application of the statute. See AE 218. The Government presented evidence in accordance with that theory during its case-in-chief, including evidence relating to each essential element. No further inquiry is necessary.

I. THE GOVERNMENT'S PROFFERED THEORY WAS CONSIDERED BY THE COURT.

Prior to trial, the Government proffered that the accused "exceeded authorized access" within the meaning of 18 U.S.C. § 1030(a)(1) when he obtained the information at issue using an unauthorized program (Wget). See AE 188 at 2. In that same filing, the Government stated that "Wget can be used as a 'web crawler' by extracting resources linked from web pages and downloading them in sequence... Wget can be used to rapidly mine data from websites." *Id.* The Government cited evidence presented at the Article 32 investigation, which showed that "the accused added Wget to his [SIPRNET] computer and used the program to access and harvest more than 250,000 Department of State diplomatic cables from the Net-Centric Diplomacy

(NCD) website.” *Id.* The Government proffered that evidence presented at the court-martial would establish that Wget was not authorized software for Army computers. *Id.*

Thereafter, this Court considered the proffer of the Government, *the defense legal authority and argument*, and ruled:

Restrictions on access to classified information are not limited to code based or technical restrictions on access. Restrictions on access to classified information can arise from a variety of sources, to include regulations, user agreements, and command policies. Restrictions on access can include manner of access. User agreements can also contain restrictions on access as well as restrictions on use. The two are not mutually exclusive.

AE 218 at 2. This Court made it clear that criminal liability for exceeding authorized access under 18 U.S.C. § 1030(a)(1) was “not limited to code breaking restrictions on access.” *Id.*

II. THE GOVERNMENT PRESENTED EVIDENCE IN ACCORDANCE WITH ITS PROFFERED THEORY.

The United States is puzzled. It would be one thing if the Government proffered a theory to the Court that was not borne out at trial by the facts—facts that must be viewed in the light most favorable to the prosecution. It is another thing entirely when the defense articulates, on the first page of its motion, the Court’s ruling on the issue of “exceeds authorized access” with an incomplete reference to the record and without further elaboration. *See* Def. Mot. at 1 (“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.”).

As stated above, the proffered theory for “exceeds authorized access” was that the accused obtained the information at issue using an unauthorized program. For purposes of this motion, it is important to note four separate conclusions of law by this Court. First, “restrictions on access can include manner of access.” AE 218. Second, “user agreements can also contain restrictions on access as well as restrictions on use.” *Id.* Third, access and use “are not mutually exclusive.” *Id.* Finally, “exceeds authorized access” is not limited to code breaking restrictions on access.” *Id.* The defense concedes that the United States introduced evidence that the accused used the program Wget to download more than 250,000 Department of State cables. *See* Def. Mot. at 2 (“The Government has introduced evidence that PFC Manning used the program Wget to download the diplomatic cables.”). Thus, the only inquiry left is whether the prosecution presented evidence that Wget was an unauthorized program. Fortunately for the Court’s determination of this issue, the United States has presented overwhelming evidence that Wget – whether characterized as software, freeware, or an executable – was not authorized on Army computers generally, and the Defense Common Ground System-Army (DCGS-A) computers specifically. *See* Testimony of SA David Shaver (stating that Wget is not a standard

program on Army computers and was not part of the Army Gold Master, and that there is no difference between software and executables); Testimony of Mr. Jason Milliman (stating that only the DCGS-A Field Software Engineer (FSE) was authorized to put an executable file on DCGS-A machines); Testimony of CPT Thomas Cherepko (stating that the Acceptable Use Policy and AR 25-2 prohibited introducing software, freeware, or executables, and that Wget was not an authorized executable file); Testimony of Mark Kitz (stating that Wget is not on the DCGS-A baseline system, and that Wget did not go through the process and was never authorized).

III. THE GOVERNMENT PRESENTED EVIDENCE WITH RESPECT TO EACH ESSENTIAL ELEMENT OF THE OFFENSE.

This Court must determine whether the evidence presented could reasonably tend to sustain a conviction for the relevant offense. *See* RCM 917(a). 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 charged." RCM 917(d). In order to find the accused guilty of Specification 13 of Charge II, the Court must find:

- (1) That at or near Contingency Operating Station Hammer, Iraq, between on or about 28 March 2010 and on or about 27 May 2010, the accused knowingly accessed a computer exceeding authorized access on a Secret Internet Protocol Router Network;
- (2) the accused obtained information that has been determined by the United States Government by Executive Order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, to wit: more than 75 classified United States Department of State cables;
- (3) the accused had reason to believe the information obtained could be used to the injury of the United States or to the advantage of any foreign nation;
- (4) the accused communicated, delivered, transmitted, or caused to be communicated, delivered or transmitted the information to a person not entitled to receive it;
- (5) the accused acted willfully; and
- (6) under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

See AE 410.

The United States presented evidence with respect to each essential element of the offense during its case-in-chief. Although the defense did not raise the issue of whether the United States presented evidence with respect to element (3) above, the testimony of several witnesses, as well as the charged diplomatic cables themselves, establish that the accused had

"reason to believe" the cables he obtained could be used to the injury of the United States or to the advantage of any foreign nation. *See, e.g.,* Testimony of Troy Moul (AIT instruction); PEs 169-178 (diplomatic cables were marked with classification). The only other contested element is whether the accused "knowingly" exceeded authorized access on the SIPRNET. On this point, the prosecution presented overwhelming evidence that the misconduct was "knowing." SA Shaver testified that Wget was under the accused's user profile and not in the program files. Thus, the program was only available to the accused on the computer he was using. *See* Testimony of SA Shaver. SA Shaver also testified that to run Wget, the accused had to create a program or script in order to download the cables from NCD and the detainee assessments from the Intellipedia site. *Id.* Mr. Milliman, the DCGS-A FSE and administrator, was never approached to put Wget on a computer, nor had he heard of Wget before his involvement in this case. *See* Testimony of Mr. Milliman. There is also no evidence the accused asked any of his superiors whether he could download Wget to his SIPRNET computer; in fact, none of the unit witnesses testified that they even knew what Wget was until recently. *See* Testimony of Unit Witnesses. Further, the evidence showed that the accused specifically enabled private browsing in Mozilla Firefox to prevent the recording of search and activity history on the SIPRNET. *See* Testimony of SA Shaver. As such, there is overwhelming evidence that when the accused downloaded Wget and put it on his computer (on at least two separate occasions), he did so in a manner that hid the program from other users, his supervisors, and the administrator. The logical inference is that the accused knew the program was not authorized to be used to rapidly harvest more than 250,000 cables from NCD, and more than 700 detainee assessments from an Intellipedia site.

IV. THE EVIDENCE PRESENTED ALSO ESTABLISHED THAT WGET OR SOMETHING LIKE IT WAS NOT EMBEDDED WITHIN NET-CENTRIC DIPLOMACY.

The evidence presented established that the "manner" of accessing or obtaining the cables in this case was the use of a Wget, an unauthorized program. Wget was not part of the Department of State Net-Centric Diplomacy (NCD) website, and there was no mechanism to allow users of NCD to download or print multiple cables at one time. *See* Testimony of Charles Wisecarver; Testimony of SA Shaver (Wget was not embedded as part of the NCD server). Mr. Wisecarver also testified that diplomatic cables downloaded from NCD came with a banner embedded. *See* Testimony of Mr. Wisecarver. Although Mr. Wisecarver could not remember the exact wording of the banner, the banner reads as follows:

USE OF THIS DoS COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO MONITORING OF THIS SYSTEM. UNLESS SPECIFICALLY LABELED AS RELEASABLE TO FOREIGN NATIONALS, CONTENT IN THIS DoS INFORMATION SYSTEM IS NOT RELEASABLE TO FOREIGN NATIONALS. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR

ADMINISTRATIVE, CRIMINAL, OR OTHER ADVERSE
ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT
TO MONITORING FOR THESE PURPOSES.

See, e.g., Prosecution Exhibit 173c (example of banner embedded in cables downloaded from NCD). The defense characterizes the database banner as focused on the “*use* of the information.” Def. Mot. at 10. Fortunately, the Court does not have to rely on the defense to be candid. The “*use*” in the banner above clearly refers to use of the system itself. As the Court stated, access and use “are not mutually exclusive.” AE 218. The banner can fairly be read as “unauthorized use [of this computer system] may subject you to criminal prosecution”, which is separate and apart from the prohibition on releasing “content” or information in the system to foreign nationals. It also appears the defense is attempting to confuse the Court by intimating that because Microsoft Excel was part of the baseline package for the DCGS-A machines, there was some kind of authorized mechanism the accused could have used to download cables rapidly from NCD. *See* Def. Mot. at 3. Microsoft Excel is a program used by analysts to create spreadsheets and tables. *See* Testimony of CW2 Kyle Balonek (all Soldiers within the S-2 section used Microsoft Excel spreadsheets for simple tasks). The idea that a spreadsheet program like Excel doubles as a program that could download webpages rapidly is preposterous and one example of the way the defense has mischaracterized evidence. The Court should note, however, that the Combined Information Data Network Exchange (CIDNE) database allowed a user to export significant activity reports in monthly increments to a comma separated value file or Excel file—an example of a database containing a design feature which allowed downloading in batches. *See* Testimony of Chad Madaras; Stipulation of Expected Testimony for Patrick Hoeffel (CIDNE allows a user to export SIGACTs into a “.csv” format)

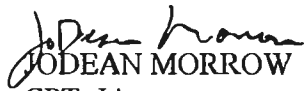
V. A DECADE IN JAIL IS THE MAXIMUM PENALTY FOR A VIOLATION OF 18
U.S.C. § 1030(a)(1).

The defense asserts at several points that a “decade in jail cannot turn on what programs the Army happens to put on its ‘authorized software’ list.” Def. Mot. at 3; *see also* Def. Mot. at 15 (“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.”). Aside from whether this is an appropriate argument for a motion under RCM 917, the legislative branch determined that the maximum penalty for a violation of 18 U.S.C. § 1030(a)(1) was ten years in prison. In its focus on whether the use of “unauthorized software” should be relevant to the “exceeding authorized access” inquiry, the defense forgets that § 1030(a)(1) as a whole criminalizes serious misconduct. *See* 18 U.S.C. § 1030(a)(1) (punishing individuals who obtain and communicate classified information to unauthorized persons). Additionally, the evidence presented during the prosecution’s case-in-chief established that Wget is a dangerous program for the SIPRNET. *See, e.g.*, Testimony of CW4 Armond Rouillard (stating that he used Wget in his OPFOR capacity for attacking the Army network, and he was specifically authorized to install Wget; Wget is only for individuals who are penetration testers and OPFOR); Testimony of SA Shaver (Wget downloaded information faster than humanly possible); Testimony of CPT Cherepko (Wget “scrapes” websites and retrieves any data that is set in the program to retrieve); Testimony of Mr. Weaver (Wget allows you to do entire content


downloading of a website). Accordingly, policies prohibiting Wget on SIPRNET computers seem more than appropriate.

CONCLUSION

The United States respectfully requests this Court DENY the Defense Motion for Directed Verdict: 18 U.S.C. 1030 Offense. For the reasons stated above, the United States has presented evidence with respect to each essential element of Specification 13 of Charge II.


JODEAN MORROW
CPT, JA
Assistant Trial Counsel

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


JODEAN MORROW
CPT, JA
Assistant Trial Counsel