GlobalResearch
Center for Research on Globalization

Assange's Fourteenth Day at the Old Bailey: Elections, Cracking Passwords and Failures of Proof

September 25. Central Criminal Court, London.

By Dr. Binoy Kampmark
Global Research, September 27, 2020

Region: USA
Theme: Intelligence, Law and Justice, Media Disinformation

On this Friday, the Assange trial moved into the rarefied realm of computer hacking and the less than rarefied world of when final arguments will be made. The WikiLeaks publisher is confronting the prospect of extradition to the United States for 17 charges under the US Espionage Act and one under the Computer Fraud and Abuse Act.

The defence first pushed for more time to prepare closing arguments. As Edward Fitzgerald QC explained,

> "It seems unlikely for you to make a judgment before Nov. 3 and you would have to bear in mind that the future is uncertain. Much of what we say about [US President Donald] Trump is because this proceeding was initiated by Trump ... and some elements of the case would be worse if Trump were [re-elected]."

The arguments worked, and Judge Vanessa Baraitser found herself admitting that the election outcome was "one of the factors going into my decision." She agreed to granting the defence four more weeks. "That means for your client there will be no more decision until the new year, if he appreciates that." A more than revealing nod that politics permeates this entire process.

The defence also attempted to confront US Assistant Attorney General Gordon Kromberg's rosy view of the US prison system, specifically regarding the conditions of the Alexandria Detention Center, destined venue for Assange's pre-trial time, and ADX Florence in Colorado, where he is likely to spend time if convicted. To date, the assistant attorney has been disinclined to surrender to cross-examination. This led Fitzgerald to attempt the submission of two defence statements to court, one from a former chief psychiatrist at the US Bureau of Prisons, another from a forensic psychiatrist well acquainted with ADX Florence. "We have no right to cross-examine Kromberg, who can say whatever he wants and we have no right to challenge him," submitted Fitzgerald. "They have no right to have the right word." Baraitser rejected the request, feeling that enough by way of defence testimony on the US prisons in question, had been heard.

Failure to prove conspiracy

The prosecution had been less than charitable in sending the defence documents at 11.30 pm the previous night. Such a move prompted Mark Summers QC to request Judge Vanessa

Baraitser to give their witness Patrick Eller an hour to peruse the prosecution material. Eller, chief executive of Metadata Forensics and former digital forensic examiner at the US Army Criminal Investigation Command headquarters at Quantico, had submitted his written testimony some nine months previously. Baraitser, on this occasion, acceded to the defence.

The day was further marked by a distinct lack of historical and computer literacy. The judicial bench seemed unblemished by an awareness of certain details of the Chelsea Manning court martial, along with its important terminology; the prosecution seemed ignorant of testimony supplied at the trial by the government's own forensic expert.

The indictment accuses Assange of conspiring with Manning to attempt to crack a password hash drawn from a conversation on the Jabber instant messaging service. On the surface, this reads like the basis of a narrowly crafted computer offence. The indictment is, however more broadly crafted, drawing upon the Espionage Act to target Assange for allegedly receiving pilfered data, including the Guantanamo Bay detainee assessment briefs, the US Department of State Cables, and the Iraq rules of engagement files. It is alleged that "Assange knew that Manning was unlawfully taking and disclosing them, and at the time Assange agreed to assist Manning in cracking the encrypted password hash [knowing] that Manning was taking and providing WikiLeaks with classified documents and records containing national defense information from classified databases." Both awareness, and action, become criminal ingredients.

Assange, allegedly using the name Nathaniel Frank, was asked by Manning whether he was capable of cracking a password hash containing an encrypted hash of half a password. Manning then sent a hexadecimal string taken from her computer network. The hash was passed on to an expert; Frank admitted to having "no luck so far" decrypting it.

Had this been possible, the prosecution claims that it would have "made it more difficult for investigators to identify Manning as the source of the unauthorised disclosures of classified information." Cracking the encryption would have also given Manning access to an FTP (File Transfer Protocol) user account with greater access privileges.

The grounds for the defence, fashioned by Eller's written testimony, are two-fold: "that the alleged passcode hash conspiracy was impossible, but even if it were possible, it has no utility to what is attributed to it."

Eller's analysis of Manning's court martial records was incisive. In his assessment, Manning never supplied the two necessary files vital in reconstructing the decryption key for the pass word hash. "At the time, it would not have been possible to crack an encrypted password hash, such as the one Manning obtained." What was "sent was insufficient to be able to crack the password in the way the government [has] prescribed."

James Lewis QC for the prosecution attempted to find some agreement with Eller that Manning and Assange had "thought they could crack the password and agreed to attempt to crack it." The answer from Eller was not assuring. A hash had been provided; they claimed to have "rainbow tables for it." (Rainbow tables being a decryption method applying different password values by means of guessing.) Nothing was ever stated on where the hash was from.

Even more troublingly for the prosecution, Eller reminded Lewis that, "The government's

own expert witness in the [Manning] court martial stated that was not enough for them to actually be able to do it." Bruised by this reversal of fortune, Lewis could only assay a weak question. "Are you aware Assange publicly boasted he is a fantastic hacker?"

Looming over the day's events in thick reminder were the proceedings of the Manning court martial. Consulting those records might have saved Lewis, and the court, some time. Kevin Gosztola reminds us of the testimony of special agent for the Army Computer Crimes Investigating Unit, David Shaver. On June 12, 2013, Shaver testified that the "hash value" was found in the chat, but was hardly the "full hash value". Major Thomas Hurley, for Manning's defence, asked whether "the hash value included in the chat wouldn't be enough to actually gain any passwords or user information". "Correct," came Shaver's response.

The "Nathaniel Frank" identity also proved slippery. In re-examination, Summers dug to see if there was any evidence linking Assange to it. None that he could see, came the reply from Eller, more than once. The prosecution now, just as in the Manning trial, continue to scrounge for an elusive link.

With Eller's testimony also came the seeds of doubt in the prosecution's conspiracy charge. Manning had, "[r]outinely and in the course of work," downloaded the war log documents so as to have "offline backups" in the event the Secret Internet Protocol Router Network (SIPRNet) were it to suffer "connectivity issues". The SIPRNet, segregated from the internet, could be accessed from a sensitive compartmentalised information facility (SCIF). By the time the alleged conversation with Assange took place on Jabber, Manning had already downloaded and leaked documents including the Iraq and Afghan war logs, the rules of engagement and "Collateral Murder" video and the Guantanamo detainee assessment briefs using her standard account on two secure computers. The "documents named in the indictment that Manning sent after the alleged cracking attempt were the State Department cables," which Manning was, in any case, authorised to access.

The US government claim that Assange made an agreement with Manning to crack a password in order to access the FTP user account collapses in a heap. As Eller notes in his submission, "Manning already had legitimate access to all the databases from which she downloaded data." To log "into another user account would not have provided her with more access than she already possessed." It was also "unclear" to Ellery "that any anonymity would be gained by cracking the password to gain access to the ftp user account."

This was certainly relevant in terms of downloading documents passed on to WikiLeaks, as doing so would have been tracked by the army, the user identifiable by means of the IP address. "Even if Manning was in fact logged into the ftp user account rather than her own normal account, this would have no effect on tracking," Eller's witness statement summarises the point. "Merely logging into a different local user account on the computer (such as ftp user) would not anonymise Manning at all because the IP address of the computer would remain the same regardless of what user account is in use."

Manning already had the means of accessing data via her own local computer, using a Linux CD which enabled her to read the files and bypass the security features of Windows. Eller's submission is sharply convincing. "The technical impossibility of using the ftp user account to download data anonymously, combined with Manning's past behaviour of downloading hundreds of thousands of documents from her own account, indicate that it is highly unlikely that Manning's attempt to crack the ftp user password had anything to do with leaking

documents."

Eller's testimony also gives an insight into how soldiers working with Manning at Forward Operating Base Hammer in Iraq frequently took breaks to play computer games and listen to music. Unauthorised software, stored on the T-drive of the SCIF, or on their work computers to chat, play games and music, were used. Manning's court martial revealed that soldiers often attempted to crack administrative passwords to gain access to such software. As Jason Milliman, a computer engineer retained to manage laptops at the base explained, "soldiers cracked his password in order to install a program and then deleted his administrator account."

The defence performance, in sinking the prosecution's feeble password-cracking conspiracy with testimony drawn from the US government's own forensic expert in the Manning trial, was impressive. But commentators such as Gosztola fear that a degree of obsolescence specific to the computer charge has crept in. The 2020 superseding indictment is a grab all rag bag of assertions claiming that Assange conspired with the hacktivist group LulzSec and propagandised his cause for reasons of recruiting sources in the US intelligence community as future WikiLeaks sources. It was the sort of material that should have been excised from the extradition proceedings, but Judge Baraitser refused. Show trials must have their scripts doctored for the occasion.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

Featured image is from HoweStreet.com
