ROYAL UNITED SERVICES INSTITUTE OF NOVA SCOTIA

Comment Paper

6 July 2015

Comments on RCMP "H" Division & Unmanned Aerial Systems

by James Birchall

(Note: These comments follow a demonstration of the RCMP "H" Division Unmanned Aerial System to the Royal United Services Institute of Nova Scotia, 8 April 2015. An earlier paper on the event, titled "RCMP "H" Division & Unmanned Aerial Systems," is available at http://rusi.ca/wp-content/uploads/2014/01/RCMP-UAS.pdf.)

The Unmanned Aerial System (UAS) model demonstrated by RCMP "H" Division was an unmodified DraganFly X4-ES [1] mounted with a Sony QX100 camera payload. It is not easily identifiable as a piece of RCMP equipment. The UAS has a flight time of 20-25 minutes and a working range of ~200m in moderate weather. The pilot is required to keep the UAS in sight at all times and the RCMP notifies Transport Canada and local air traffic control that they are operating and what their general mission is. Accidents, even minor ones, are reported to the Transport Safety Board. This limits the system's mission scope to short range and short duration with some lead time - the UAS is simply not capable of practical persistent surveillance.

From a data communications perspective, the UAS radiates in the consumer 2.4/5 Ghz spectrum using the 802.11g/WPA2 protocol for video while the radio controls are a paired set of frequency hopping spread spectrum algorithms over 900Mhz/TEA. Data is recorded unencrypted on the camera and then downloaded from the UAS via a USB cable to a workstation as a standard camera drive or via the SD card itself to a dedicated card reader once the aircraft has landed. There is no encryption between the camera card and any workstation.

In flight, the UAS creates an 802.11g WLAN encrypted with WPA2. Applications on phones / tablets / laptops can connect to the UAS to receive real time video and telemetry once they provide the network password. The flight control channels and the video channels are physically separate - taking over the WLAN video stream has no effect on where the aircraft flies.

This communications platform is commercial grade and possibly compromisable [2][3], though the flight controls operate on a relatively unusual frequency. DraganFly has active R&D to upgrade the security to AES with strong pre-shared user-defined keys.

While the technical platform could be improved from a security perspective, disappointing was the lack of unique policy around the treatment of UAS data, specifically the flight logs, software logs and video imagery.

First and most importantly, we noticed an exemplary ethic on the part of the briefer, RCMP Constable Skinner. His desire to always act honestly and honourably was apparent, as was support of that position by the senior RCMP officer attending, Superintendent Ferguson, regardless of what kind of shame and disrepute that may bring if anything ever goes wrong. While it should go without saying, we must stress how important this is.

However, the constable noted that he would "delete the logs after the flight" if, in his sole discretion, he deemed them to be irrelevant (as he promised to do with the data from our presentation). We did not hear what workstation or tools he is actually using to do the work and there appears to be nothing but his own ethics stopping him from using the data inappropriately.

Further, we did not hear how we would be able to verify independently that the video of us was actually destroyed as promised and that additional copies were not made. We did not hear that there was any leadership oversight or organisational follow up to confirm that the data was destroyed in a responsible manner or that the pilot was trained to dispose of the digital data properly or that the UAS was protected against tampering.

In short, while we know that we are on video, we cannot verify what happened to that video other than trusting the assurances of the pilot. The same is true of any bystander accidentally filmed during a mission.

Like all cameras in public in Canada, there is a legislated duty [4] (Sec. 5.2) to notify anyone who may have been recorded accidentally unless the imagery is involved in an investigation covered by a search warrant and notifying a person would compromise the mission. While we were required to sign in for the demonstration, in the field receiving sign off from every possible bystander before every mission is impractical. We heard and could find no policy or facility allowing the general public to see if they have been captured by an RCMP UAS camera.

While it is clear that the people operating the equipment are of the highest integrity, policy needs to be developed in the RCMP to ensure that this remains the case. The privacy commissioners of Ontario [5] and the federal government [6] and the US Department of Justice [7] have all released policy recommendations to aid UAS operators in this regard.

[1] http://www.draganfly.com/uav-helicopter/draganflyer-x4es/index.php
[2] http://www.aircrack-ng.org/doku.php?id=aircrack-ng&DokuWiki=baccf676281e2887e32cfd5229169acd
[3] https://github.com/samyk/skyjack
[4] http://laws-lois.justice.gc.ca/eng/acts/P-21/
[5] https://www.ipc.on.ca/images/resources/video-e.pdf
[6] https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.asp
[7] http://www.justice.gov/file/441266/download

James Birchall is a professional systems analyst with over 15 years of industry experience. He holds a BSc. hon in Computer Science from Dalhousie University, a CIPS Information Systems Professional designation, and has software patents. This work is the sole opinion of the author and does not represent the views of the Royal Canadian Mounted Police, the Canadian Armed Forces, the Canadian Department of National Defence, the Royal United Services Institute of Nova Scotia, DraganFly Innovations Incorporated or the author’s employers. The author may be contacted at RUSINovaScotia@gmail.com.

Recommended citation: James Birchall, Comments on RCMP “H” Division & Unmanned Aerial Systems, Royal United Services Institute of Nova Scotia, July 6, 2015