



WHARTON AEROSPACE & DEFENSE REPORT

Your Knowledge Source on the Aerospace & Defense Industry

Drowning in Drone Data

How Can the Military Handle the Huge Data Volumes Collected by Unmanned Vehicles?

June 2010

The U.S. Air Force has successfully harnessed the power of unmanned aerial vehicles, commonly known as drones, to identify, track and kill insurgents in Iraq, Yemen and Afghanistan. But these drones are really anything but "unmanned." They require a growing number of military personnel to guide them during combat air patrols (CAPs) and to provide accurate analysis of all the video and sensor data they collect each hour they fly.

"To support each new CAP, we will need 140 more Airmen, half of whom are intelligence professionals to process the raw data, exploit and fuse it with other sources, and disseminate actionable information to the field," Air Force's General Norty Schwartz told a group of cadets recently. The cadets were graduating from a "beta" program training for unmanned pilots and sensor operators.

The reality, however, is that humans are probably not up to the task of analyzing all the data drones will generate. Air Force records shows that the amount of video collected jumped 300% from 2007 to 2008. The New York Times notes that the footage captured in 2008 would take about 24 years to watch if a person never slept or blinked.

And the amount of video will only increase exponentially as the Air Force introduces drones with up to 10 simultaneous video feeds. That number will jump to 30 video feeds this fall and to 65 feeds later this year. And that the number likely will continue to increase.

"How do we find the relevant nuggets," asks Gen. David A. Deptula, the Air Force's deputy chief of staff for Intelligence, Surveillance and Reconnaissance, adding that intelligence officers are not looking for a needle in a haystack but for "a needle in a needle-stack." The bottom line, he says, is that while today's systems are smart, the military will have to deploy even smarter systems that can isolate the useful information, connect it to other data, and then disseminate this information to tactical operators.

To get a better understanding of the implications of the new technologies, Knowledge@Wharton spoke to Rex Buddenberg, a professor at the Naval Postgraduate School, who specializes in the interoperability of information systems. He described military networks (and the computers and sensors connected to those networks) as information systems made up of "sense, decide and act end nodes" -- much like a human nervous system. To manage the growing amount of data collected by drones, these military systems will have to inch closer to the efficiency of the human nervous system. Buddenberg, who noted that his statements are his own and not official opinions of the Navy's, discussed in the following edited interview how the military can face the challenges from its growing mountain of data:

Knowledge@Wharton: How do you manage the growing amount of data produced by drones so it's useful and quickly accessible?

Rex Buddenberg: If you have an information system where all the data is concentrated at one place and then redistributed, you are not going to have something that is successful. Take a

look at how data has become very distributed on the commercial Internet area. You need a system that allows many-to-many distribution.

Knowledge@Wharton: The data that is being gathered will all soon be high definition video. How will the drones handle the increased demand for bandwidth?

Buddenberg: There are some limitations on any radio communication system -- even though it is agnostic about the kind of data that it can deal with. Radio links are four orders of magnitude less capacious than the wired Internet. So you are going to hit a bottleneck that is not manageable with engineering solutions. It is a physics-imposed bottleneck. There is an old adage that "God only made so much spectrum."

Knowledge@Wharton: That's not a comforting thought given that we'll have all this data that needs to be transmitted. At what point is all this data counterproductive?

Buddenberg: Drowning yourself in data is not necessarily a good thing. And we have discovered this many, many times. Better information makes for better decisions but we have to transform the data into information. And then you have to present it to the decision maker and in a form that he can understand. There are several bits of esoteric [system modules] in there that will need to be worked. We won't get it all right the first time. So we need to be building evolutionary systems that can easily be upgraded and refined as we go. Circling back, the drone sensory package itself is simply going to have to get smarter and refine some of the data that it sees -- so it only sends the data that needs to be sent rather than sending all of it.

Knowledge@Wharton: And is that something that sensor makers are already working on or is that something that they need to start working on?

Buddenberg: Let me give you an example that you might have in your own house. Many of us have webcams. Some people use them for baby monitors, some people use them for security and most of them have a motion sensor in them. So they only snap a picture when they see motion. They don't send you an image of your living room, except when the cat walks across the floor.

Knowledge@Wharton: To do that in at a more specialized scale sounds rather difficult. If you are scanning a whole territory -- with people walking and trucks moving -- it still would register data that is not that useful because of all the movement down there.

Buddenberg: I am not a sensor-manufacturing specialist and so I am not really qualified to answer that kind of question. But if you step back you are simply going to have to have some sort of compromise between what the sensor does and the amount of communications capacity available.

Knowledge@Wharton: The military services all have different infrastructure for accessing and sharing data. How will the growing amount of data be shared effectively across services?

Buddenberg: It has to be shared across platforms, programs, and service boundaries. And, unfortunately, that is a part of the information systems business that we haven't gotten very good at it.

But let's back up and parse the problem first. There is communications interoperability; there is data interoperability; and there is data dictionary synchronization. There are a whole slew of other issues: processes interoperability, software reuse, data presentation and fusion, along with a bunch of procedural and cognitive interoperability issues.

It is a wonderfully complex and fascinating area. The law says the CIOs [chief information officers] are supposed to do this but I haven't seen any of the CIOs in the services actually doing it.

The modularity is crucially important to interoperability across the domains that you are talking about or any other domain. Show me somebody anywhere in federal government, and the Department of Defense is certainly included, who is in charge of modularity.

Knowledge@Wharton: Companies building drones specialize in avionics design, not networking and security. What are the potential flaws or actual flaws in their data security that they don't realize are there, given that is not their expertise?

Buddenberg: Let's start at the top: the radio networks are designed to handle Internet protocol. This modularizes the radio network away from Local Area Networks. Once you understand the design of the Radio WAN and the Local Area Network within the platform, you realize that the security measures there can only protect the infrastructure. You cannot protect the data end-to-end because the data is traveling with multiple hops across the Internet. That means that you have to protect the data. So the principle should be that no unprotected data exists in any end system that is placed on the Internet.

Conversely no data acceptor accepts data that is not protected. That gives you end-to-end protection, which eliminates the vulnerabilities that comes as unprotected data travels across the Internet or on open Radio frequencies.

Knowledge@Wharton: So why do they not send data in a protected encrypted format? Is it because it slows the whole process, because it has to be encrypted and then decrypted at the other end?

Buddenberg: That used to be a valid argument because it required CPU (central processing unit) cycles to do the encryption and to do the decryption. However, that is not a valid argument anymore. CPU horsepower is cheap and plentiful these days. This is the way we have always done it and a lot of the security measures both in the commercial world and in the military. We have not really caught up with the concept of internal networks that are really multiple networks routed together.

