“I think unmanned aircraft are the future of flight in general.”

DAVID KIDD

Q&A

NVTC sat down with national security expert Richard Clarke to discuss his views on drones, their potential uses in the commercial sector, cybersecurity threats and his role as Co-Chair of the Virginia Cyber Security Commission.

By Allison Gilmore

nvtc While a work of fiction, your new book *Sting of the Drone* is obviously inspired by real events and scenarios. Can you share your thoughts on the military's current use of drones or UAVs? How will this new type of warfare impact America's future foreign and defense policies?

I think the military and the CIA have been using drones extensively for quite some time now. What they've found is that they offer additional capabilities that we didn't have otherwise, both for reconnaissance and intelligence collection, on the one hand, and for strikes on the other. The intelligence use I think is pretty non-controversial. Any time you can get more information about an area of concern, that's usually a good thing.

The use of weaponized drones in strikes has been controversial for a number of reasons. The first reason is a fear, a latent almost subconscious fear, on the part of many people about the possibility of killer robots. Of course, drones are not robots. They have a person in the loop, a pilot who is flying it and many people who are making decisions about whether or not to use the weapons. But nonetheless, there's a public perception of them as killer robots and that disturbs people.

There's also been a fear that they've been overused, particularly in Iraq, Afghanistan, and Pakistan. And that their overuse turned counterproductive by killing the wrong people sometimes, collateral damage, deaths of innocent people, and a general fear spreads throughout the public in some regions like Waziristan about the United States constantly flying overhead and being able to strike at any moment.

> “The government does need to have rules, not just about the traditional FAA concerns of safety, but also about privacy.”

So, they're a useful weapon in that they don't put American pilots at risk. But they have to be used in ways that take into account the potentially negative political psychological effects.

nvtc How do you think the U.S. should address those concerns and the psychological effects?

The President had authorized in his first term a great increase in the number of lethal drone operations. Then last year he issued a new policy that reduces the number of lethal strikes by setting up tougher criteria that must be met in order to use a lethal strike. It has to be an imminent threat to the United States or to American citizens or assets and it can't be used simply to support a friendly government that needs an air force. So, I think that's reduced the number of strikes considerably and that was appropriate.

I think unmanned aircraft, or remotely piloted vehicles (RPVs) is now the term the Pentagon likes, are the future of flight in general. I think the next heavy manned bomber that the United States is looking to develop has as one of the development criteria optional staffing, optional humans on board. There are clearly plans for fighter aircraft that will not have humans on board that allows the aircraft to be more capable. As long as the communications link is secure and unjammable that makes a lot of sense.

I think you'll see increased use of unmanned vehicles throughout the military in the United States and in other countries later, not just for reconnaissance, but for all missions. There was some discussion recently about whether or not the next generation of aerial refueling tankers needed to have pilots on board.

nvtc Clearly, drones are best known for their military and counter-terrorism applications. What other industries or uses do you foresee as being growth industries for UAVs or RPVs?

Well, we already see them being used in the United States for search and rescue, by the Coast Guard, police, and border patrol. We see them being used in agriculture for crop monitoring. I suspect they're going to be used instead of helicopters for pipeline security and pipeline safety. We've probably just begun to touch the number of opportunities. Clearly they're being used for news broadcasts and filming movies. People are even using them with GoPro cameras to film weddings apparently.

There's discussion by Google and Amazon and other companies of using them for delivery. I think that's not going to be happening any time soon because it presents a lot more problems than many of the applications we just discussed. Before we can see widespread commercial use, we've got to solve some of the safety problems and that means a vehicle needs to be aware of what's around it, not just what's in front of it. Most drones cannot see in 360 degree loop. They need to be able to see around them, above them, below them, and to the side of them so they don't bump into other drones or, worse yet, piloted aircraft.

nvtc What types of regulations do you believe are necessary to have this sector grow in the commercial space as well as use by private citizens?

I think it all comes back to not bumping into other things that are flying and, of course, things that are stationary. The stationary issue is easier to solve because the remotely piloted vehicle can tend to see where it's going and if there are high tension wires or a building, it can see them. And then that problem is solved by having rules about how close they can come to buildings, how close they can come to high tension wires and that sort of thing. But the problem of midair collisions is harder to solve without making the technology onboard the RPV a lot more sophisticated and therefore a lot more expensive.

I think we do need regulations and we need to enforce the ones we have. Right now the FAA has a regulation that you can't use RPVs for commercial use below a minimum height and they're not really enforcing it. So, real estate companies are using RPVs to film and advertise on their websites. That's clearly commercial use and clearly in violation of the FAA rules and the FAA is not doing anything about it. If they're going to be taken seriously they need to enforce whatever rules they come up with.

The government does need to have rules, not just about the traditional FAA concerns of safety, but also about privacy. None of us want to be laying in our backyard and have a drone come over and take pictures of us and continuously hover there, transmitting those pictures. None of us want a drone to come up to our bedroom window and hover there. It's not clear that the laws, Federal laws at least, are sufficient to protect privacy concerns from that kind of technology.

nvtc Earlier this year, Governor Terry McAuliffe named you co-chair of the Virginia Cyber Security Commission. What are your goals for the commission?

Yes. I come to the Commission having been the Cyber Advisor to the President and the White House in the past and now having spent the last decade in the private sector including as Senior Cyber Advisor and Counter-Terrorism Advisor at SRA, a Virginia-based technology company. The goals the governor has for the commission fall in two buckets. The first bucket is making sure that the Virginia state government and critical infrastructure, which is largely owned and operated by private companies, are appropriately secure from cyber attack.

The second bucket is developing further the commercial and business market in Virginia for cybersecurity. The internet was started in Virginia through DARPA grants and all the early nationwide routing hubs were in Northern Virginia. We've got a base of great companies in Northern Virginia, both big and little, that work on cybersecurity. Yet, we are prob-

ably the number two or three region in the country for cybersecurity. We're in competition with Silicon Valley. We're in competition with the area around Fort Meade in Maryland. There are also cybersecurity clusters in companies outside Boston, outside Atlanta, and in Texas, around San Antonio.

Virginia offers a lot for a cybersecurity company, either a new startup or a large company in terms of access to markets, access to trained personnel and quality of life. We would like to see more cybersecurity companies come and operate in Northern Virginia. All the economic estimates show that cybersecurity is a growth area. There will be a lot more people being hired, a lot more companies being formed. We'd like to see a lot of that happening in Northern Virginia.

> “The Commission is going to look at how we can help create a climate in which cybersecurity, as an economic sector in Virginia, can grow.”

One of the challenges we have is — and this is true everywhere in the country — is there aren't enough trained people in this field. And that's not just talking about PhDs and people with masters degrees in information technology. It's also talking about people with two year community college associate degrees, because a lot of the work that needs to be done can be done very, very well by people with associate degrees.

So, the Commission is going to look at how we can help create a climate in which cybersecurity, as an economic sector in Virginia, can grow. That means looking at our educational pipeline and at whatever incentives the state can offer companies. And we've just begun that process.

nvtc Where are the biggest cybersecurity threats likely to come from in the next two to five years and how should companies and the government be preparing?

They fall into two buckets. The first bucket is theft. That can be theft of money or identity, or intellectual property, research and development information. The second bucket, which we haven't seen much of thank God, is destruction, damage, and disruption. But we know that it's possible to do that second bucket even though not much of it has happened yet. So, both are of concern, obviously.

nvtc What are your thoughts on teaching hacking in order to have our cybersecurity professionals be trained to prevent against that kind of thing?

I think it's essential. I've been advocating for this for a long time. Over a decade ago, I realized that you could graduate from MIT with a masters degree in information technology without ever having taken one course or one class on security or on hacking. That kind of answers the question, why is so much of our software, so much of our hardware susceptible to attack and hacking? It's because it was designed by people who don't know how hackers work. I think it's essential to know the kinds of things that you can do to hardware and software to get in without authorization and to either steal information or to do damage.

nvtc Is there anything else you'd like to share with our readership in the technology sector here in Northern Virginia?

The Virginia Cyber Security Commission has a number of subgroups, on education and the workforce and on increasing the attractiveness of Virginia to the private sector in the cybersecurity area. As the Commission goes forward, we're looking for the people in Virginia to assist us with the working groups and we welcome suggestions and ideas. So, people can either submit ideas or actually affiliate themselves with the working groups. And under Virginia state law, all of our meetings are open to the public, either in person or online. So, people can follow our work. And we don't want people to wait until we issue some final big report and then be critical. We'd like to issue a number of reports as we go along and we'd like people to give us their ideas before we issue those reports rather than after.

Your members can give suggestions or volunteer to participate through the Commission's website, **http://cyberva.virginia.gov/**.

Allison Gilmore is NVTC's vice president of communications and strategic initiatives.