

Just Drones as a Growing Threat

Intro [00:00:01] RTI International's Justice Practice Area presents Just Science.

Intro [00:00:09] Welcome to Just Science, a podcast for justice professionals and anyone interested in learning more about forensic science, innovative technology, current research, and actionable strategies to improve the criminal justice system. In episode one of our Domestic Radicalization season, Just Science sat down with Neil Parsons, senior research scientist at RTI international, to discuss the growing threat of drone use and how the American criminal justice system is responding. Most people think of drones as a benign hobby or a tool to take aerial photos and videos. However, recent research reveals that drones are increasingly being used for malicious purposes. Drones are easily accessible to the masses and can be used to transport contraband, violate privacy, and even drop explosives. Listen along as Neil describes exactly what a drone is. The many ways that drones are being used to commit crimes, and evolving strategies for the detection, regulation and mitigation of drone threats. This episode is funded by RTI International's Justice Practice area. Some content in this podcast may be considered sensitive and may evoke emotional responses or may not be appropriate for younger audiences. Here's your host, Michael Planty.

Michael Planty [00:01:13] Hello and welcome to Just Science. I'm your host, Michael Planty, with the Justice Practice Area at RTI international. Our topic today is around drones, also referred to as unmanned or uncrewed aircraft systems or UAS. Drones have been used for lots of exciting purposes from the hobbyist with personal interest in photography and film. They also have value in applications in commercial and government sectors for delivery, operations, search and rescue, infrastructure inspection, agriculture and disaster response. And of course, outside of the US, they have a significant presence in conflicts and war settings for defensive purposes. But with this rise in drones, we're also seeing an increase in drones used for nefarious purposes. Unauthorized drones have been flown over stadiums, causing disruptions to games, concerns around drones being weaponized for terrorist attacks, and drones being used to fly drugs and contraband in our prisons and over our borders. There's also the major concerns around invasion of privacy, both individual and corporate. Today, we're specifically interested in the use of drones for malicious purposes for our U.S. domestic setting and a related criminal justice response to these threats. So today, we're excited to speak with Mr. Neil Parsons. Welcome to the podcast, Neil.

Neil Parsons [00:02:19] Thank you Mike I appreciate it. Good to be here.

Michael Planty [00:02:21] Neil is a senior research scientist at RTI international. His career and experience includes supporting the operational research initiatives for U.S. military, intelligence and law enforcement communities. Currently, Neil leads the research, testing and evaluation activities for project out of the Department of Justice called the Criminal Justice Technology and Evaluation Center, also known as CJ tech. This project involves testing and evaluating various technologies that criminal justice practitioners would use to improve efficiency in operations with their day-to-day activities. So, to kick us off, Neil, tell us about what led you to focus on this issue of drone threats in the criminal justice system?

Neil Parsons [00:02:57] So first of all. Through the Criminal Justice Testing and Evaluation Consortium, or CJ Tech, which is a program of the National Institute of Justice, which RTI runs here, we developed a series of research reports around contraband. Those

reports included everything from, you know, drugs and cell phones and other types of contraband that are getting into prisons. And one thing we realized after going through the research and looking into the threats, is that contraband is actually making its way into the prison facilities via drone on a regular basis. And we came to this determination by not only seeing it in news reports, but actually speaking with practitioners, talked to multiple practitioners around the country that are operating correctional facilities. They're saying that drugs and contraband, particularly cell phones, are actually being brought into prison facilities on a daily basis. So, they're really seeing this as a threat just to the overall safety of their staff and inmates.

Michael Planty [00:03:58] Before we go any further, let's level set with our listeners. Let's talk about some of the basic concepts related to current drone market and how they're currently regulating. For the audience, what do we mean when we refer to a drone or a UAS? And what are the most common vendors and capabilities?

Neil Parsons [00:04:13] Drones in UAS or unmanned aircraft systems, also known as unmanned aerial vehicles or UAVs. So, there's quite a few acronyms for them but drones is the most common. However, drones can also be used and expanded to other systems such as nautical or terrestrial type drones. So, you can have a boat that is, you know, fashioned to be a drone or autonomous vehicle, as well as some type of land based vehicle, like a small rover or something. So, the rovers they put up on to the moon or technically drones, knowing that the actual number of drones in the United States, or at least aerial drones, is estimated between 850,000 to 1.1 million drones. And this market is significantly dominated by Chinese manufactured aircraft, particularly the company DJI. That company accounts for approximately 70% of the market. They are producing drones that are mostly multi rotor aircraft that are battery powered. They're operated by RF controllers and or smartphones. So, you can actually use a smartphone to control the drones.

Michael Planty [00:05:18] So RF meaning radio frequency?

Neil Parsons [00:05:21] Yes. So, the reason behind DJI's dominance is they produce highly capable drones at a very low barrier cost point. So, they're accessible to the masses.

Michael Planty [00:05:30] When you say masses, I mean people can just go into any hobby store and pick up a drone, and the drones come in all different types of sizes and applications. Right? Can you describe some of the different applications or uses in the residential and commercial sector?

Neil Parsons [00:05:42] Sure. So yeah, the multi rotor aircraft has really expanded in use. Right? So, for the most part when you think of a drone, you're thinking of a group one drone, which is categorized as a drone that weighs less than 20 pounds. There is different size grouping of drones out there, whether it's 2 or 3. And you'll see some of those fit into the category of agricultural type drones. So, they'll have drones that are 55 pounds. Those are typically out of the reach of your common consumer right there, tens of thousands, if not hundreds of thousands of dollars for those larger type agricultural drones. But we're mainly looking at here is drones that are, you know, 20 pounds or less. You can buy them on Amazon, you can go to Best Buy. They're easy to use. They proliferated within the industry for a lot of reasons for hobbyists and industries because they have great photography and video capture, potential for movies and commercials and real estate marketing. They essentially provide that bird's eye view for various industry for

construction projects, insurance claims, power companies use it to maintain our power infrastructure and as well as agricultural practices.

Michael Planty [00:06:50] Yeah. So, when you think about it, you know, these are 500 bucks, a thousand bucks and you can get a really high end, drone. And with the ease of use, that really is a game changer. So, when you talk about remote control planes and other products, they've been around for many, many years, right? Yeah, I Google that and you'll probably find a bunch of old guys standing in a field playing with their planes. What is it about today's drones that really are making it a game changer for threats in terms of their operation in use?

Neil Parsons [00:07:14] I thought about this myself after going down the path of researching the drone threat, and I wondered what, you know, RC planes have been around since the 1930s. You know, they were initially used in World War two, for combat training. So, they would put these RC planes up in the air and actually shoot them down to simulate how anti-aircraft guns would work in a war setting, but recently, essentially over the last decade, these aircraft have turned into a much more accessible aircraft for the masses. They're easy to fly, they're inexpensive, and they don't require, you know, the necessary skill level as a winged aircraft or an RC airplane would require. This allows, you know, a lot of different people to use them. And like I said, they're so simple to operate now that they can actually fly autonomously. So, you don't necessarily even need to control the aircraft. You can actually put in various GPS waypoints, and the drone itself will fly from waypoint to waypoint to its destination, and then can return back to the operator and land on its own. So, you essentially don't even need to have any control over the aircraft. It can be done through, you know, these automated programs.

Michael Planty [00:08:24] So given the use and proliferation, I mean, these things are going to be flying all over the skies. Can you talk a little bit about the current regulations in terms of who can operate these and under what circumstances?

Neil Parsons [00:08:34] The use of drones are regulated by the FAA specifically under part 107 regulations. Now, part 107 dictates who can fly drones, where they can be flown, and how they can be operated in the national airspace. And really, this is specific to drones that are over 250g and weight, which is roughly about a half a pound. They're medium, I would say they're still small drones. A drone that is, you know, three fourths of a pound is still a small drone. But the capabilities on these drones are fairly expansive. And so, the FAA has taken an approach where the reasonably fly one of these. You need to take the FAA aeronautical knowledge exam, which exists of various topic areas such as aircraft operation, airspace restrictions, safety measures, things like that. And so that is typically how the FAA is regulating drone use. There's a other few caveats. For the most part, you're not allowed to fly drones at night. You're not allowed to fly drones over people, and you're not allowed to fly drones above 400ft above ground level, which provides a safe space for, you know, manned aircraft flying in the airspace.

Michael Planty [00:09:37] So you're saying if I go to Best Buy and buy a drone, I'm not able to fly this over restricted airspace right to the White House or fly to 2000ft or to fly it at night?

Neil Parsons [00:09:48] Therein lies the problem. Because the technology the drones are capable of flying above 400, having those restrictions is purely being established by the FAA. And it's one of these things where it's regulated pretty much on trust within the community.

Michael Planty [00:10:03] Circling back our talk today around the use of these drones. So, we now know something about the specs related to how these drones operate to ease their capabilities. And it really sets up a real tough problem for our criminal justice system when they're used for malicious activities. So, let's turn back to the types of threat we mentioned briefly at the beginning of the discussion. What are the major threats to public safety and privacy, when in fact, you know, regulation is only going to carry you so far? The bad guys are not going to follow regulation when they might increase their visibility, right?

Neil Parsons [00:10:31] That's correct. It's not just nefarious actors, right? There's a category of operations called clueless and careless. Right? So, it's people who go out and buy these drones and they fly them, and they don't know you're not supposed to go above 400ft above ground level. And therefore, it can create some significant issues just by somebody not knowing the regulations. And to buy a drone doesn't mean you have to have the license. Really, the threat level of drone incursions is really the scary part of this discussion. The advancements in drone technology have really enabled them, again, to be operated with a minimal technical skill set and at a very low-cost point. You know, they're fast, they're quiet, they're able to travel long distances now. In addition, they're also now able to transport and drop sizable payloads with precision. And all these qualities are very enticing to the nefarious act.

Michael Planty [00:11:24] And beyond the visual line of sight, right, as we call it, you could be a person who's flying this thing miles away from where you actually are. So, in terms of law enforcement, detecting the operator or even the drone, there's a distance issue there that the actor can actually operate this without any visual sight of the drone.

Neil Parsons [00:11:42] That's correct. And that's one of the regulations outlined by part 107. You are not supposed to fly your drone where you do not have visual line of sight of it. That's pretty easy to do. Some of these drones can on a charge can go several kilometers. Definitely, that's an issue and a common occurrence with drone operators who are either clueless or careless and or nefarious in their actions. We're seeing drones being used more and more for illicit activities, and at the same time, we're also witnessing drone warfare evolve in real time, particularly in the war in Ukraine. We're really starting to see more drones that are still Group one type drones having a very significant impact on infrastructure and, you know, lives of people in those war environments. So, you have a \$1,500 drone that is essentially capable of destroying or disabling a \$4 million tank. And that is pretty much the definition of asymmetrical warfare. You can guarantee that bad actors are taking note of how to perform those exact operations of dropping payloads that either have explosive type munitions on them, and it really creates another level of threat that potentially, you know, capable of being used in the United States.

Michael Planty [00:12:55] So, yeah, let's get to those specific threats. The first one you just mentioned, the threat of weaponizing drones for malicious activities, whether it's targeting infrastructure, soft targets such as schools or outdoor events or other mass gatherings.

Neil Parsons [00:13:08] You look at the soft targets, you know, you have a stadium full of people, and if you have a drone that comes over and is able to drop, you know, a small explosive, a chemical or biological agent, that specific payload may cause damage. But, you know, the real fall out of that scenario, maybe the thousands of people that get trampled in trying to exit the area all at once. I speak regularly with federal law

enforcement agencies. This is a real concern. Obviously, that hasn't happened in the United States yet. We have had some instances. In 2018, a drone flew into a 49er's game and dropped leaflets throughout the stadium. The reality is, is that was very simple for that operator to do that could have been a lot worse. But in reality, we're seeing threats from drones on a daily basis. And those are, you know, anything from contraband being delivered to prisons, which again, destabilizes the prison system. And then there's other things like the potential for cyber-attacks and the potential for voyeurism and personal privacy protections. I mean, there's surveillance capabilities of these drones with their high-definition cameras that generate a real threat to the community.

Michael Planty [00:14:19] I was at the beach one time, and I look up and I'm like, well, that's kind of creepy, but not only that, but you're like, well, who's controlling it? Is it going to crash on me? I'm trying to just, you know, relax at the beach and this thing's flying, you know, 100ft above my head, and I don't have to worry about, you know, this device falling out of the sky and hitting me or something of that nature. And of course, individual privacy is one thing, right? At one point, will we have drones flying over our heads just like we have cars on the roads? And what are our expectations there?

Neil Parsons [00:14:45] It's a dynamic environment. You know, you have multiple companies right now establishing various delivery systems using drones, right? You're going to be able to order supplies and materials online and have them delivered by drone. You think about that. You don't really know what drone in the sky is a threat or is a delivery service. You don't know the friend from the foe just by looking at a drone that's hovering over your head. You know, for a lot of people, just having that drone within your vicinity, not knowing who the operator is, it's a very uneasy feeling. If it is, there could be a malicious intent drone or scenarios where that drone is being used for stalking, could be used for casing homes and property for theft and burglary. I think one of the bigger things, and I've been reading several articles on this recently, is the potential for cyber attacks in the summer of 2023. There was a financial institution that discovered two DJI drones that were on the roof of the building. Those drones were actually equipped with a Wi-Fi sniffer and a penetration test capability, so they were able to actually get into the network system there by hacking into the various access, by sniffing out other people's login credentials. And so, you're going to have different scenarios like that. And there's actually there's a research entity in Israel that demonstrated they could actually fly a drone in proximity of a building and actually use a system to deliver or spread a malicious IOT update. And this research entity showed that they were able to disable all the light bulbs within a building, that in a much larger scale and potentially blackout entire city blocks. So, I think that is something, you know, we're just on the precipice of. But it's a real concern and a real threat to our way of life here in the States.

Michael Planty [00:16:31] So when we think about public safety, what is the process that public safety and criminal justice practitioners have to go through in terms of detection, identification and mitigation?

Neil Parsons [00:16:41] Yeah, so there's really four steps to the process Right? Initially detecting the drone is your first step. Once you have detected that drone you need to be able to track that drone movement within the airspace. The second step would be to attempt to identify that UAV and or to operate and determine whether the aircraft is actually a threat. The third step there is you're going to have to react to that aircraft if there's malicious intent behind that flight, alerting the appropriate authorities or response team such as the FAA or a law enforcement agency. And then the final step, the mitigation

of UAV is essentially the defeat or the ability to bring that drone to the ground and or remove it from the scenario where it is actually becoming a threat.

Michael Planty [00:17:27] So what are some of the products and technology that are out there to help practitioners with this process of identification?

Neil Parsons [00:17:33] You know, considering the discrete nature of drones, how they operate, how quiet they are, how fast they can travel, how far they can travel, depending on human observation, is just not a reliable technique. A lot of the human observers that I've spoken to, especially in like a prison setting, there's a lot of time they misidentify a drone versus a small manned aircraft, especially at night. There's multiple technologies out there that provide capabilities in this space to allow for detection of the drone, which is the first step, right? So, you have to start with detection. And these technologies for the most part include radio frequency detection, radar systems, acoustic sensors, as well as camera systems.

Michael Planty [00:18:15] They use different technology, but they have to be trained. Right? Because the confusion between a drone and a bird or anything else on the sky, you have to be able to discern the differences between that and to be able to act right and within a specific period of time, the latency on this. So, if it takes you five minutes to pick something up, it's going to be in and out and the threat is going to be either there or it's going to be gone.

Neil Parsons [00:18:36] Yeah, so all the systems that I mentioned, they all have their strengths and weaknesses in real world settings. And this can be seen as, you know, what is the range of efficacy. So how far are you able to detect the drone out from the establishment you're protecting line of sight requirements. Does the system or the sensor need to have a good line of sight to that drone? Is there buildings in the way or are there trees in the way? You have impact of ambient noise levels. So, a lot of other RF transmissions happening out there, is that going to confuse the RF sensor, or is it going to make it more complicated for it to pinpoint it in space and time, airspace and ground clutter. So, we use the word clutter a lot when we're talking about radar. That's because anything that flies in the air or anything that is actually traveling on the ground, will be picked up by radar. The systems need to be smart enough to differentiate a bird from a drone. It can have the ability to differentiate those things, but that requires, you know, a level of analysis, whether it's done automatically through an algorithm or it's actually somebody there monitoring the radar system and determining that in real time.

Michael Planty [00:19:44] And what about costs? What are the cost specs related to these types of technologies?

Neil Parsons [00:19:48] Yeah, so they vary significantly in cost. I would say they're not cheap. You know, you're looking at hundreds of thousands of dollars to establish a system that works effectively. What I mean by that is that there's no one system that does everything extremely well at this point. It really does require a combination of sensors that fits within a specific scenario. And I think that's what you're getting to here that, you know, if you're using an ad detection systems at the Indy 500 is be much different if you're using it in, you know, New York City on New Year's Eve, it's a much different scenario. There's a much different ambient noise levels happening there. There's much more clutter. You have to really tailor the systems that you're using to the environment that it's being used in. And how they're regulated is also a concern. Right? So not just anybody can use these systems. They are regulated by the, FCC and the FAA, you are required to get approval

prior to using specifically RF systems and radar systems. It's really a dynamic situation. It's challenging, especially for, you know, law enforcement and the criminal justice community to really understand what is available to them to use in these various scenarios.

Michael Planty [00:21:00] So we talked a little bit about detection and identification. But now the big thing is mitigation. So, you see a threat. What are the options? What are the concerns? What are the potential consequences to mitigation?

Neil Parsons [00:21:10] Congress through the Preventing Emerging Threats Act, which was in 2018, more specifically, the 124 in that has exclusively authorized the departments of Defense, Energy, Justice and Homeland Security to engage in limited counter UAS detection and mitigation specifically for credible threats to covert facilities or assets. The one thing about using mitigation techniques is that there's really two different camps. There's kinetic and non-kinetic mitigation techniques and the non-kinetic techniques. Employees jamming or the takeover of communication signals to the drone. You know, it allows for the drone to be taken over by the mitigation system, typically RF, and either land it safely in a designated area or disabled to where it lands, where it is currently at in space, and it can actually drop to the ground land. But one of the issues with that technology is that there is the capability of bad actors to actually program their drones to return to home or make their home location the actual destination for a place where they would like to drop a payload. Potentially, there are some issues with that. Now, you also have kinetic mitigation techniques, and these are more along the lines of electronic warfare type systems, lasers. They also use attack drones, one drone hitting another drone or throwing a net around another drone while it's in flight to actually capture it. And as well as using munitions such as projectiles, bullets and however, I have never heard of one instance where kinetic mitigation techniques have been used domestically. And there's probably a really good reason for that, right? I mean, you're going to have potential for collateral damage, which, you know, could include injuries or loss of life or destruction of the property.

Michael Planty [00:23:01] Those concerns are all raised in terms of your ability to first detect. And then again, you're trying to protect a parade or stadium and to think you're going to blow something out of the air over a stadium kind of defeats the whole purpose in many ways, especially these carrying a payload. So, a really complicated issue in terms of how to address these threats to public safety. As we get close to wrapping up here, where do you think the future research needs are? There are many different things as this technology advances, right? So, the minute you understand one system, the rapid advancements in this space seems to create somewhat of an arms race.

Neil Parsons [00:23:36] Yeah, I mean, that's one of the biggest hurdles that we've seen in our research. That's what we're hearing from all of our federal components. This game where they're trying to catch up to the bad guys. So, you're having new technologies being developed every day to counter UAS threats. The bad actors are also making changes to their systems to counter the counter UAS. It's a big game of cat and mouse. Our end users such as the Department of Justice, Department of Homeland Security, the need to have a very rigorous research, testing and evaluation program to actually vet these products and these technologies before they are deployed in the field is absolutely necessary to see how effective they are. I mean, it's much different to use a counter UAS system in the middle of nowhere at a high max prison facility versus a stadium within a big city. The technology is going to need to be tailored specifically to those situations, and the only way you can get there is by actually implementing a very thorough and rigorous testing approach evaluation approach that shows that they're effective in those very scenarios. So

that is necessary. And what we're doing right now, as far as the research that we're doing here, is actually doing that for our partners and our federal partners.

Michael Planty [00:24:54] Yeah. And when we think down the line, some of these things, we often think about drone as a drone. But now drones are working in concert with other drones, with different roles. One may play surveillance, another one may be carrying a payload or a weapon. We have the increased use of camouflage and stealth, battery life and speed have increased so you can fly longer and faster. Thinking of malicious actors, this helps to avoid detection and actually to do their operations, right? If you're flying drugs over a border, you're flying rooftop to rooftop within minutes, avoiding your detection of the offender by detection of the actual transaction. And then the customization of some of these drones in terms of their ability to withstand weather and various other conditions. It's really causing a lot of concern in terms of how to best approach and detect these public safety concerns.

Neil Parsons [00:25:42] Yeah, exactly. I mean, if you were to purchase, you know, reasonably priced drone, let's say \$1,000, \$1,000 a drone can get you a fairly capable drone, just off of Amazon. And you can just go to another search query in Amazon and look up payload mechanisms. They develop payload mechanisms for almost every commercial off the shelf drone that's out there. And, you know, that is a concern because now you have the capability of dropping, you know, payloads from these aircraft. And if you look at it, some of these drones that maybe they weigh 1.5kg can actually carry a kilogram of payload. And if you look at how much a kilogram of payload and what that means is that you have a kilogram of fentanyl, a kilogram fentanyl can be pressed into 500,000 pills. And like I said before, you had 10,000 incursions over the U.S. border in 2023, in a very small span of area. What's the amount of drugs that is actually getting over the US border? How much drugs are actually infiltrating our prisons? You don't think that a kilogram is a lot, but it is when you're delivering such concentrated type drugs and explosives. I mean, you look at C-4, it doesn't weigh that much. You can easily put a kilogram of C-4 on one of these things, and it could do significant damage to infrastructure and take out entire buildings.

Michael Planty [00:27:01] Yeah, this seems like this is an emerging area that's been on our radar, no pun intended, for many years. And it's not going away, right? This is all the time we have for today. It was excellent conversation. Thank you so much for your time today and for sitting down with Just Science to discuss, drone threats and solutions for practitioners to keep us all safe.

Neil Parsons [00:27:19] Thanks, Mike, I appreciate it.

Michael Planty [00:27:20] I also like to thank, you, the listener, for tuning in today. If you enjoyed this conversation, be sure to like and follow Just Science on your podcast platform of choice. I'm Mike Planty and this has been another episode of Just Science.

Outro [00:27:32] Next week, Just Science sits down with Matthew de Michelle to discuss his research on former white supremacists. Opinions or points of views expressed in this podcast, represent a consensus of the authors, and do not necessarily represent the official position or policies of its funding.