Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

Drones, the New Threat from the Sky

Dominique C. Brack

This paper is about drones. Drone risks and countermeasures. Drones have become an inherent risk not just for critical infrastructure but also public events (sports, concerts) and privacy. I wrote about the exclusive risk catalogue I have developed for a small highly secialised startup called DroneGuard. The catalogue contains over 140 detailed drone related risks. From payload of drones (explosives, chemicals, etc.) to cyberrisks like Signal Hacking and Disruption (WiFi, GSM, Bluetooth, RFID, etc.). Since Deepsec is a more technically oriented event I will highlight the risk management frame work, my experience with our personal payload drone and the cyber risks. This talk will help you if you have to protect critical infrastructure from a physical perspective, or if you have to protect yourself or your company from privacy implications.

Keywords: Drones, Risks, Countermeasures, Critical Infrastructure, Risk Management, Signal Hacking and Disruption

Citation: Brack, D. C. (2019). Drones, the new threat from the sky. *Magdeburger Journal zur Sicherheitsforschung*, *18*, 969–976. Retrieved October 17, 2019, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_067_Brack_Drones.pdf

I'll talk about drones, a topic I worked on for over a year. For drones and the respective threats they can represent there is no framework or guidance available. So I had to develop the whole story from scratch from methodology to threats and countermeasures and threat modeling.

I'm not so much involved with the positive side of the drones, like delivering medication, delivering blood samples, dropping packets for human disaster relief, etc. That's all fine, but I'm on the dark side of the drones. I'm talking about defense, I'm talking about attacks, I'm talking about threats, etc.

We have typically two types of drones. We have the cooperative drones, the nice ones. There are the pilots that stay within restrictions, the drones that don't fly where they shouldn't fly, and everyone is looking after themselves in a safe way and is happily ever after. To make an analogy to the IT world: If you'd have more drone pilots like this, we wouldn't need firewalls and antivirus because people would just get along great.

But there's the other side, my side. The non-cooperative drones. For the non-cooperative drones you need to understand what they can do, you need to try to predict the next steps, you need to be preemptive about it, and you need to know what capabilities are out there.

What can hit you? You need to plan ahed so that you can actually prepare an adequate defense. Usually, if money is not an issue, you can build anything; but you need to justify what defenses you are building. From this perspective, the framework we'll look at will help you, because you cannot use $50,000 for a drone defense system if the risk you're protecting against is way smaller than $50,000 for instance.

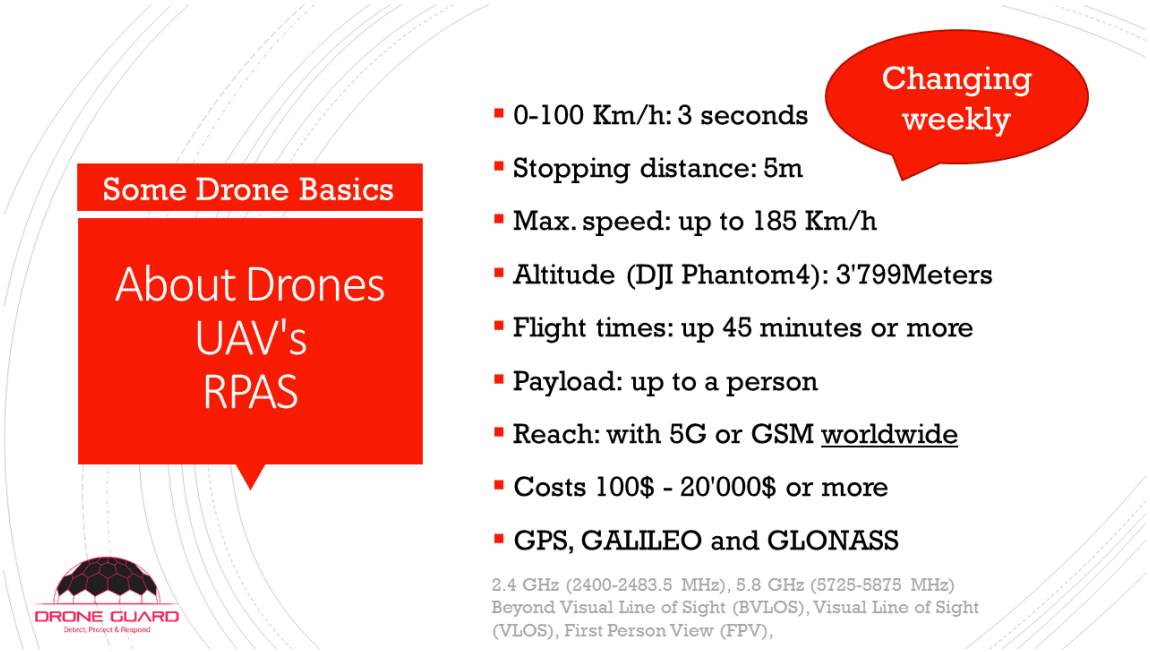
The drone itself is just a representation of what's coming in the future of the IT world. It's like autonomous vehicles. You will have the same problems there. For instance, one use case I usually bring to the table is if Google Autonomous Drive (or for that matter, just any autonomous car) is bringing me to the hospital. I call, they bring me there, emergency services, I get in, then the car stops. What do you do as the owner of the hospital? Do you have to pull the car away or not? There's no driver you can look for, there is no one there. There may even be no GPS reception at this location. So what do you do?

Okay, first, you need to write policies. As usual, on paper. But after the paper, you need to set some actions. Maybe you need to have new sensors, or new signs signaling that this is not a zone for autonomous vehicles or self-driving cars, or robots for that matter. So, what you will learn from drones, you can apply to other areas in the future. I believe there'll be a lot of work involved for everyone, from technical to architectural work to security.

Why are drones an InfoSec topic? Because it's all about data, it's all about locations, where did they fly, what did they transport. It's all about the space and the area, so it's three dimensional. It's just like you build wings on a firewall and the firewall is up in the air. It's the same thing, so this is very, very much an InfoSec topic. The physical world and the digital world are merging, and I think with new technologies like drones and autonomous vehicles, even more so. It's like "CyPhys" or "PhyCy". It's a new discipline: Cyber Physical. You can see that in the area of SCADA much better, because SCADA has more of a direct impact on the physical world than other components. Drones are the worst flying IoT device you can imagine.

- To successfully working on drone based risks Cybersecurity must join Physical Security

Here, we'll give you some real basics about drones. If you work with drones and on the topic of drones, it's all about the lingo of the dingo. You need to know what you're talking about. Just to give you some facts: Drones can be really fast, fly extremely high and can be basically controlled from around the world. In risk scenarios people talk about reach/distance, but forget the discussion about distance. I can sit in Central Park with my phone and control a drone in Vienna if someone opens the box for me. If you go over the mobile network to fly a drone you can do it from everywhere in the world.



Testing your drone defenses is one of the most important factors in your defense. Why testing? Because you can get promised everything, but you really need to look under the hood to see if the defense system works, and I did that. At the beginning, they seem great, and on paper, they look awesome. But in real life, it's a different story. I can tell you here right now that none of these drone defense systems work a hundred percent. You need to decide for yourself what's acceptable as a risk and what's not. Some of these systems are based on different technologies. Some of these systems will detect birds as drones, some of them will identify trucks with cooling systems and vents on their roofs as drones. Some will even not detect some drones at all. It depends on the criticality of your infrastructure, or your event or place which system will suit you best.

[3F?]Really do some testing. I can highly recommend that.

So after all this experiences made with drones, we decided to get into the topic very structured and methodically.

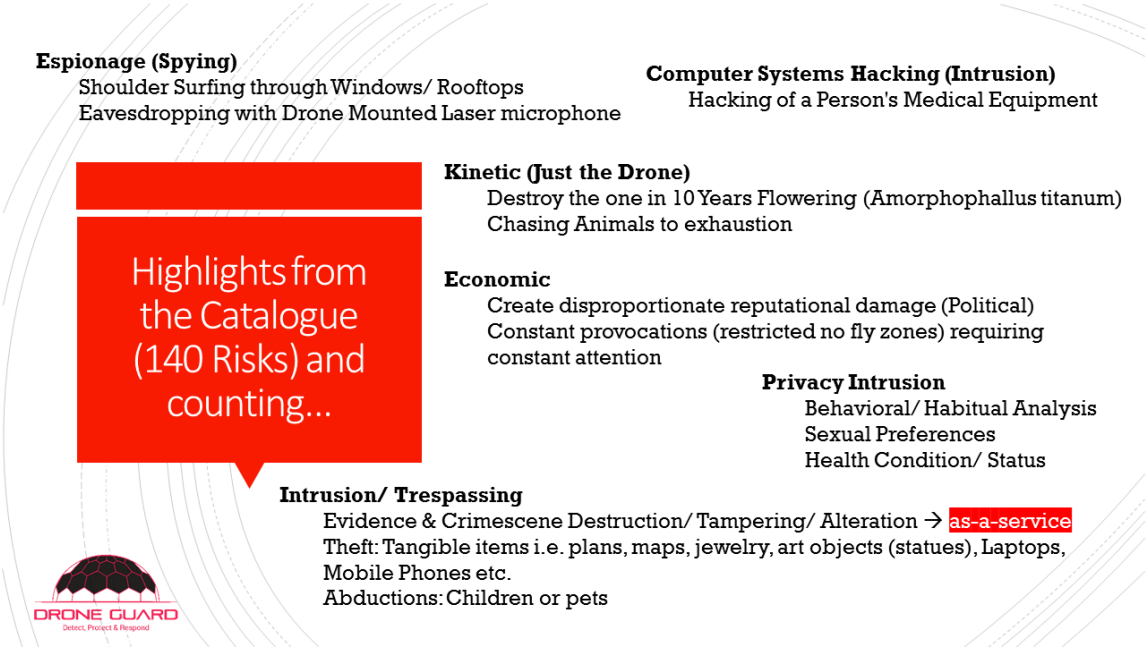
We needed to create structures and methods to assess risks, and to do some effective testing on what's working and what's really the risk with these drones.

Since there were no standards, we've started with creating our own. We first developed a threat catalog: What's out there, what has been reported, what really has been a drone case. Next we catalogued the drone threats and countermeasures and categorized them. Then we added additional criteria to see what really feasible solutions for drone detection and defense are.

1 Drone Threat Catalogue

Our drone threat catalogue contains 140 items. Some of them are typical ones like payload. There is also espionage and industrial espionage. You can use drones for carrying laser microphones. You can use drones for social engineering, because a memory stick dropped inside a nuclear plant on the parking lot works so much better than dropping the memory stick outside that facility. There is a NATO fence, three meter high, with a three meter divider where the dogs are, with another fence inside, and you feel somehow inherently safe in there. You feel that you're in a protected facility. Yes, you are in a way, but with drones, you can forget about it. With a drone, I'm in the third dimension. I can drop anything anywhere. Things that can be dropped by a drone: access points, repeaters, memory sticks, trackers, etc. whatever you like.

IoT hacking, hacking of medical equipment of a person are other examples. With a drone you also have access to rooftop apartments, you have access to artworks that might be there (theft, destruction, arson etc.). If someone has a very expensive statue in his rooftop apartment, you can go and steal it with a drone. It's very easy. You can go and steal the phones, the purse, and the dog, whatever you like. There are people flying their drones into geysers, or people who were chasing animals with drones, so they are threatening wildlife and also plants. Of course you can use drones for surveillance or as an espionage tool. Or for economic attacks. In an economic attack you can tie up resources, police for instance, and keep them busy with drones, which are very cheap, so you can generate a disproportionate response. If you send up 100 drones, you will have 100 incidents where in some way or another, people have to respond to these 100 incidents. So this is an economic attack. These are just some of the drone risks from the threat catalogue we've put together.

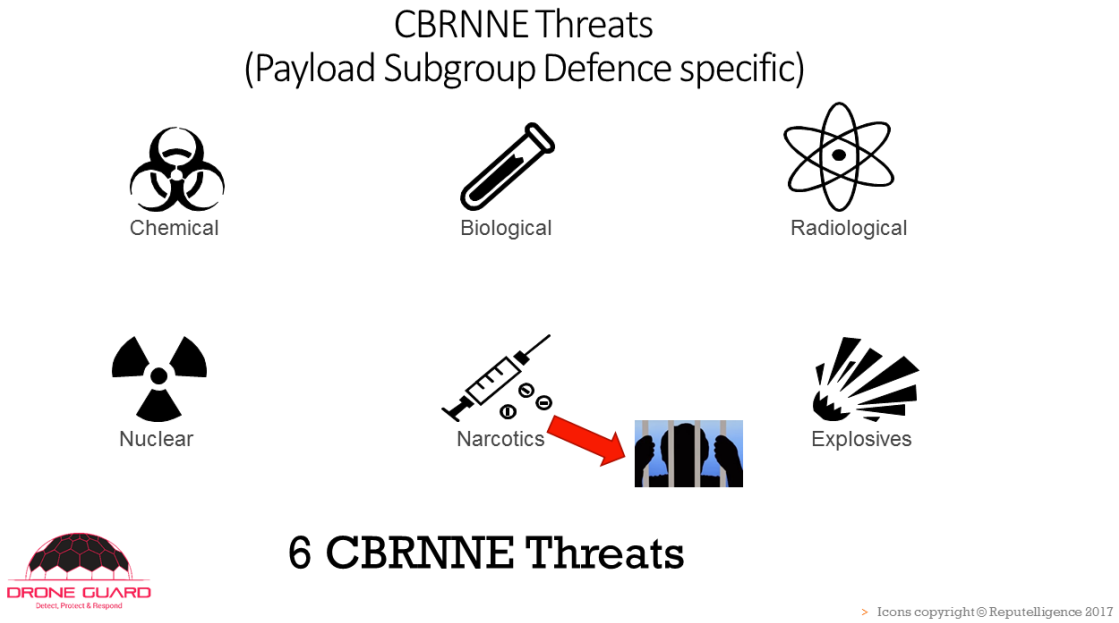


2 Drone Attack Vectors

The aforementioned risks have then been processed into drone attack vectors. The drone attack vectors combine the collected risks into logical categories. These categories should be detailed enough to place any current and future drone threats into corresponding categories.

3 CBRNNE Threats (Payload Subgroup)

A specific group within the payload attacks consists of CBRNNE payloads. CBRNNE is jargon and stands for: Chemical, Biological, Radiological, Narcotics, Nuclear, and Explosives.



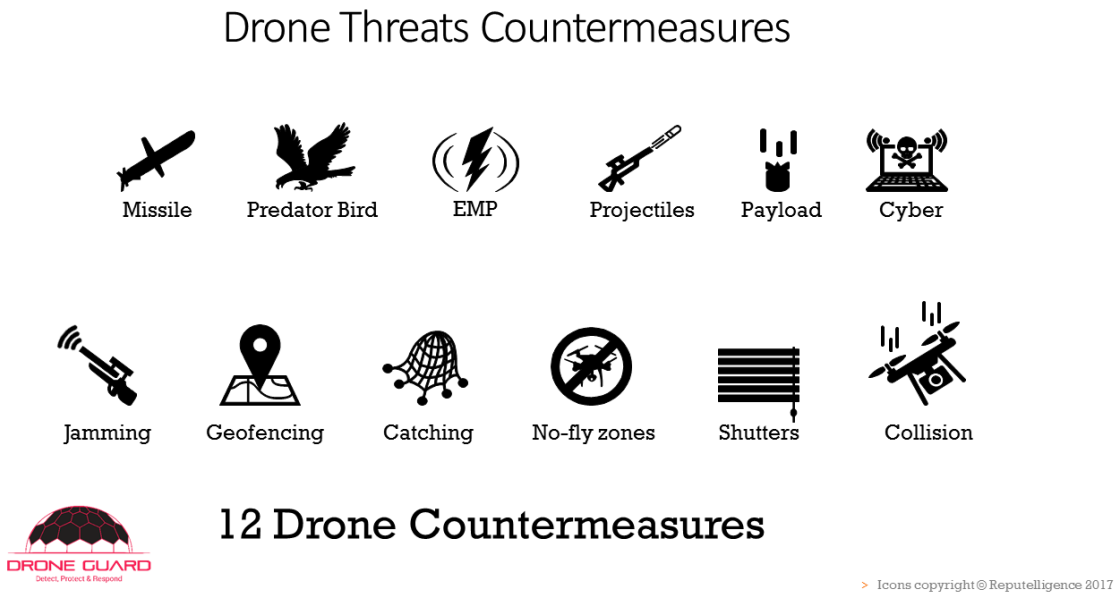
4 Drone Threat Countermeasures

What can you actually do against drones? There are active and there are passive measures. A missile, for instance, works perfectly, is 100% accurate, but a bit expensive and will be considered a disproportionate response and most likely cause collateral damage. It's more something for the military. Other countermeasures include birds. France started very early to explore this avenue. After a while, they had enough and are exhausted. You cannot train brids to catch 50 drones a day. It's a nice way of catching drones and it's ecological, but it's not very efficient. If you keep 20 birds, say, in a sports stadium, you have to feed them; you need a trained animal keeper and keeping birds for this task would be controversial.

Electromagnetic Pulse (EMP)is another possible countermeasure. With an EMP (short burst of electromagnetic energy) you can take out the electronics of a drone. Projectiles are another possible way of taking a drone down. In my view this is very difficult. It's a small target, but the problem is the collateral damage you cause around it. Because a drone so small and the energy of bullets is so high, they will penetrate the drone and continue to fly into objects nearby. The bullet might land in the next building, or the bullet might overshoot and goes astray. Yeah, you can maybe use rubber bullets, but it's not really an efficient defense technology.

Then we have payload. You drop something on the drone itself. You can try to hack into the communication between the remote control and the drone. If there is a remote control and if the drone is going over the mobile network for instance, or if it's just programmed by way points, then hacking into the communication won't work. Jamming, that's actually a perfect way to ground a drone, but it's regulated by the FCC, and only police and military can do it. There are three teams with different jamming technologies, which are part of the World Economic Forum (WEF). Looks like a rifle, but it sends out broadband signals or signals just targeted to the communication band of the drone, and will take it down. The safety function of the drone will either safely land a drone or cause it to fly back to the pilot in case of a signal disturbance. It's a nice way to handle drone threats, but civilians are not allowed to use it. So it's not an option available to a critical infrastructure operator for a nuclear plant, or whatever you have to protect from a private sector perspective.

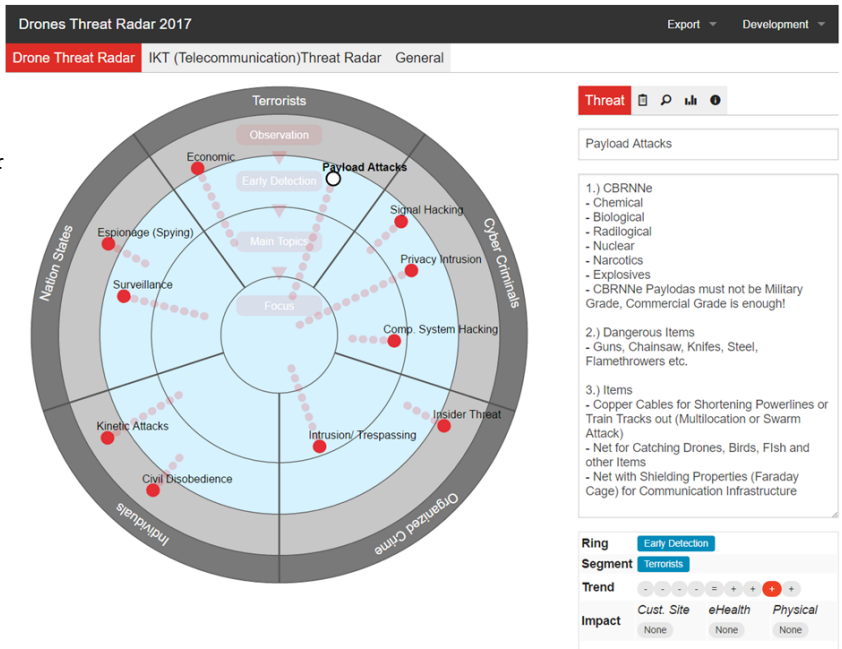
Geofencing is built-in in some drones. Some of them can't start if they're within a certain area of an airport, but you can disable or override this function. There's a lot of drone countermeasures consisting of catching drones with nets. Drones flying around themselves with a net, or you have little guns shooting up a net. Distance is a problem when it comes to this type of countermeasures. It works up to maybe 50 meters or a bit more, but as we mentioned before, a drone can fly up to 180 kilometers per hour - and you want to shoot a net at it. You can try, but it might work as efficient as you think. No-fly zones are more of an administrative measure. This means you try to establish a registered no-fly zone over your facilities. More in the Middle East, shutters as a drone defense system linked with building management has also been used as a measure against drone threats. So, when a drone approaches, it closes at least the shutters of your building and you have no insight into the rooms. Of course, you can also create a collision as a countermeasure. That's something you can do as a civilian as well. You just use another drone to crash it into the attacker drone.



5 Threat Radar

The drone threat radar is more of a consulting management tool to convey where we actually place the different kind of drone risks. This one you can use straight off like it's pictured here. You have drone threats, the development of those threats, how they are likely to develop in the future, if it's a topic you need to look into quickly, or if it's a topic you can have a look at later on. It's about risk over time. The threat radar is general, and usually you create one either for an event, a big festival for example, or you can build a threat radar for a specific location, like, for instance, a critical infrastructure location. This is what we did. We took a critical infrastructure and made this assessment based on the risks we've mentioned before.

- Drone Guard Threat Radar 07-2017
- 11 Identified threat groups (detailed description available)
- 5 defined sectors (actors)
- Presentation for selected groups possible
- Strictly internal



6 Payload Examples from Testing

This is my test fight drone. It's a Phantom 2 Vision+, or, at least, that's how it started out ... I've added remote dropping capability and other features. Please see the payload example video on YouTube: https://youtu.be/6_aPvdv87XM

Some Payload Examples

7 More information

Website: http://droneguard.ch/
Rotorblades testing: https://youtu.be/xdKgeCvZ-f4
Video with payload: https://youtu.be/6_aPvdv87XM

8 About the Author

Dominique C. Brack is a recognized expert in information security, including identity theft, social media exposure, data breach, cyber security, human manipulation and online reputation management. He is a highly qualified, top-performing professional with outstanding experience and achievements within key IT security, risk and project management roles, confirming expertise in delivering innovative, customer-responsive projects and services in highly sensitive environments on an international scale. Mr. Brack is accessible, real, professional, and provides topical, timely and cutting edge information. Dominique's direct and to-the-point tone of voice can be counted on to capture attention, and – most importantly - inspire and empower action.