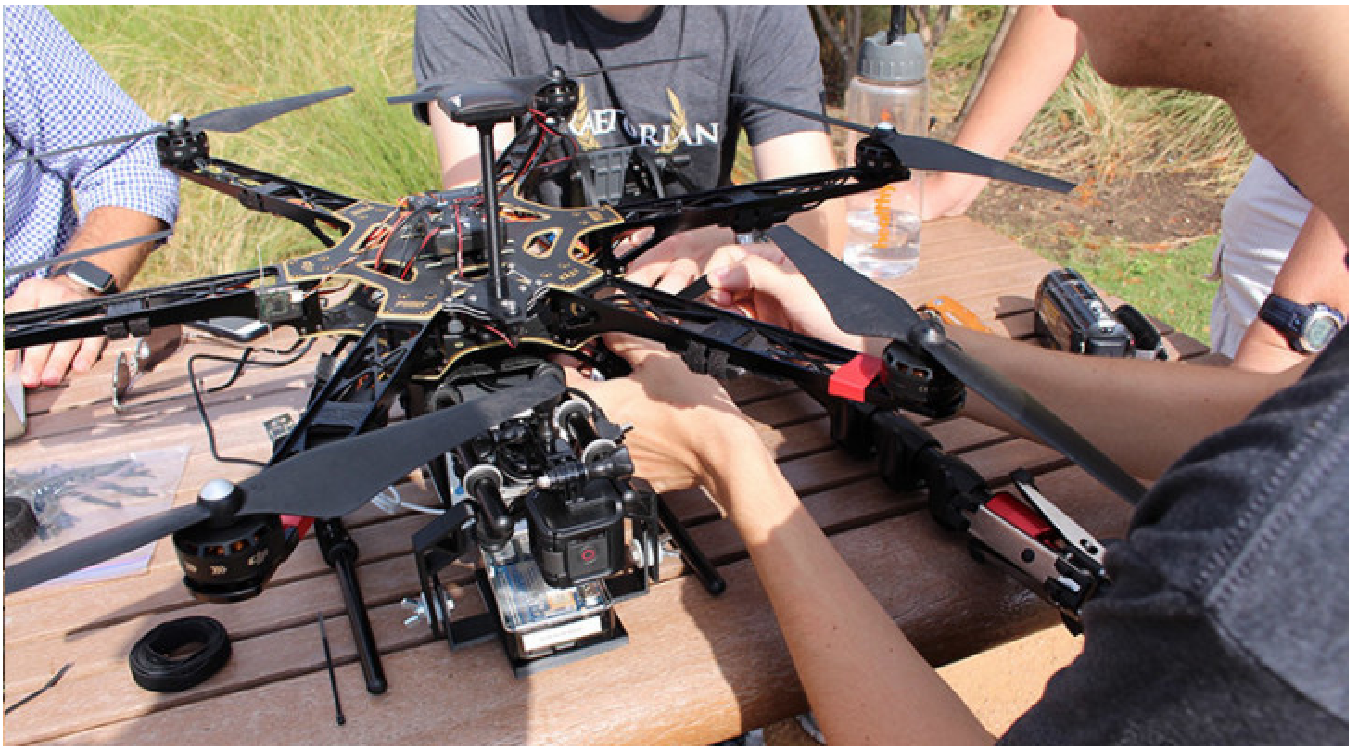


Drone regulation – Keeping the skies safe from commercial drones

November 11, 2015 By Pierluigi Paganini

My participation at the World Insight on CCTV discussing the Federal Aviation Administration regulation for the commercial drones.

Q1 First of all, the Federal Aviation Administration gave a very compressed timeline. They're asking a expert panel task force to make registration guideline recommendations by November 20 and these recommendations implemented by mid-December, so that 1 million done sold during this year's holiday season would all be registered. Do you think it's feasible? And if achieved, do you feel like it's done in too much of a hurry?

It is a great challenge for the US administrations, I think it is difficult to meet deadlines, but the most important thing is the message that the government wants to launch. Any abuse of unmanned vehicles could represent a serious threat to the privacy and the security of citizens.

Q2 These new regulations set new records: there is no precedent for the federal government requiring the registration of consumer electronics; even guns and cars are done at a state level. Some drone hobbyists argue the vast majority of drones are used responsibly and that the few clowns who make the news aren't representative of the whole. Do you feel like these guidelines are necessary?

I understand the position of hobbyists, but we have to consider a number of threat actors (cyber criminals, state-sponsored hackers, hacktivists) could use them. The law enforcement and Intelligence agencies fear that the drones could be intentionally and unintentionally used for illegal activities or cause problems to the collectivity (interference with operations conducted by the law enforcement, public services and so on).

Pl
it

Q3 Let's talk about some details. In your opinion, if implemented, when within the timeline for assemblage to sale should the drones be registered? And how about those Do-It-Yourself drones or 3-D printed drones—both of which are rapidly growing in numbers, should they be registered too?

Home | Cyber Crime | Cyber warfare | Digital ID | Hacking | Intelligence |
Laws and regulations | Malware | Mobile | Data Breach | Security |
Social Networks | Reports | EXTENDED COOKIE POLICY | Contact me |

elligence Laws
XTENDED COOKIE PO

practices and specific path to follow to allow hobbyists to manufacture their DIY drone.

Q4 Some believe these new policies may be the best-case scenario for consumers and manufacturers. Without the current regulations, the drone industry may receive a far more stringent treatment in Congress. How is the business community responding to these changes?

For sure, the policies will have an impact on the business community. Users are empowered to use these tools, they have the legal responsibility for any abuse of the system

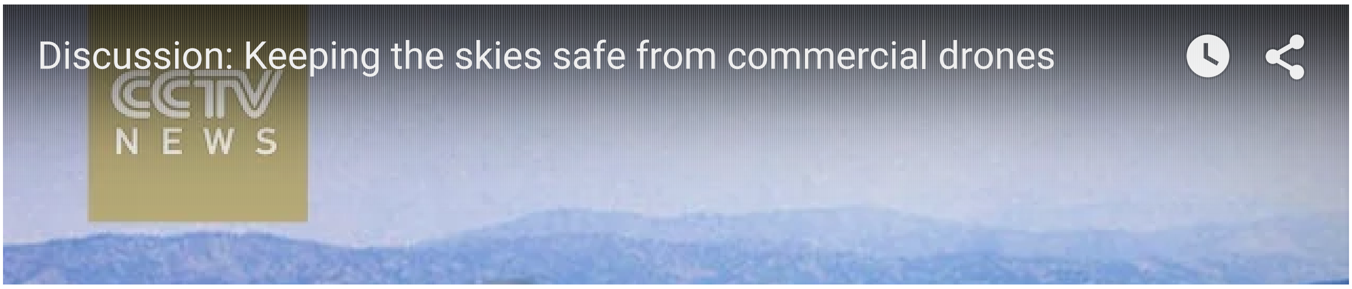
drone. Surely many hobbyists could be deterred with inevitable repercussions on retail sales.

Q5 In your opinion, will this registration process be enough to deal with current risks? Research in Singapore have demonstrated how attackers using a drone plus a mobile phone could easily intercept documents sent to a seemingly inaccessible Wi-Fi printer. What are some other unkno security risks drones bringing?

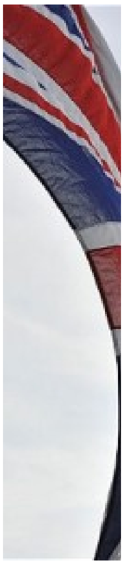
Absolutely no, threat actors will continue to drones for sabotage, espionage and so on. Y use it to

Drones could be equipped with chemical weapons, sensors to spy on targets, hacking tools that could allow breaching the Wireless Lan of an organization by simply landing the drone on the roof of a building. The concept of physical security is changing and has to take in count the threat represented by the drones.

You have also to consider that drone, especially commercial ones could be easily hacked. They could be hacked, infected by malware or jammed causing incidents and data leakage.



MORE S



Ransom
Parliam

A ransom
UK Parlia
hit the in
Parliame

Q6 Do you feel like some negative examples soured the public on the UAV sector and encourage legislators to pass reactionary laws and policies that might inhibit drone innovation?

I don't think legislators are interested hamper the drone innovation. Their use will continue to increase in civil and military environment. I have no doubt. First of all we have to keep in mind that we have protect humans from the abuses of such class of vehicles. It is important to regulate the use of these vehicles for the reason we have explained.

Q7 On a global level, countries are dealing with similar situations. China has established some no-fly zones, and in Japan, the government and the ruling coalition are moving quickly to regulate drones following the discovery of a small remote-controlled aerial vehicle on the roof of the prime minister's office in late April. How can the world learn from the FAA's recent move, and come up with a universal solution to the current problem?

I think that all the major organizations and governments will converge to a single legal framework that will address legislative, security and privacy issues related to the use of drones.

Pierluigi Paganini

(Security Affairs – drone regulations, US Government)

Share it please ...

Drones FAA Hacking Hijacking jamming malware Pierluigi Paganini regulation Security Affairs UAV US Government

Breaking News Laws and regulations Security

SHARE ON

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at "Cyber Defense Magazine", Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to find the security blog "Security Affairs" recently named a Top National Security Resource for US. Pierluigi is a member of the "The Hacker News" team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News Magazine and for many other Security magazines. Author of the Books "The Deep Dark Web" and “Digital Virtual Currency and Bitcoin”.

‹ PREVIOUS ARTICLE

Ransomware infected the UK Parliament's computer networks

NEXT ARTICLE ›

Android Tablets with Pre-loaded Cloudsota malware sold on Amazon

YOU MIGHT ALSO LIKE

Snooping Samsung S6 calls with bogus

base stations

November 12, 2015 By Pierluigi Paganini

Did FBI pay the Carnegie Mellon to hack Tor?

November 12, 2015 By Pierluigi Paganini