e-mail: paolo@zampolli.com

The Greatest Potential Risk to Global Security

Prepared by: Ambassador Paolo Zampolli

As small Unmanned Aerial Vehicles (sUAVs) become more numerous, smaller, cheaper and widely available in the global supply chain, small drones (sUAVs) represent the most significant prospective risk to national security and privacy. The advances in drone technology is constantly improving making then faster, more efficient and capable of performing ever more tasks all while becoming virtually undetectable. Millions of drones are circulating unrestricted in the airspace with millions more expected in the next year. A number of steps need to be taken to protect against hostile drones before a real life disaster occurs.

Heads of States and members of government most implement strict and overreaching regulations to control the use of drones. These regulations should be stricter for autonomous drones that are guided only by GPS location. For starters, Radio Frequencies used by drones should be standardized. 5.8 GHz and 2.4 GHz are the most common RF used by drones and should be mandated that absolutely all sUAVs operate solely on this signal. This regulation would make it feasible for authorities to intercept any rogue and dangerous drone.

Drones operating on Long-Term Evolution (LTE) and 5G signals are already in the testing stage. Future generation drones will operate on mobile signal rather than Radio Frequency (RF) making it an almost impossible task to mitigate and stop such drones. These drones represent an even greater risk to National Security as they can travel for unlimited distances (battery permitting) for as long as there is mobile signal available. The US is almost in its entirety wired with wireless signal. LTE and 5G drones should not be allowed for distribution in the global market for the public. It should be strictly allow for the use of telecommunications companies solely. Stringent regulations in regards to general market drones operating strictly on 5.8 GHz and 2.4 GHz should be urgently established.

There is currently a lack of regulations to prevent someone from flying heavily armed drones into a crowded city. It is a proven fact that drones are capable of delivering flammable devices, explosives and toxic materials into uncontrolled and unmonitored airspace in the same way sUAVs have done in the past.

Automated drones should have regulated flight plans and Drone Identification Number (DIN). Similar to a car's VIN, the DIN should be registered to the owner of the drone. These can be taken a step further and the mission of the drone should be specified with every flight at any given time.

Drones function through connected technology. This imposes another major risk and make drones vulnerable to being hacked by cybercriminals. A guideline of stringent rules must be imposed for developers vetting the software programming. Rigorous test of the software programming can help expose and resolve any potential inadequacy vulnerable to hackers, limiting security and privacy risks from inception. This will elevate the chances of drones being manage safely and decrease loopholes for hackers.

Drones have the potential to revolutionise various industries, with companies like Amazon rigorously testing drone deliveries, regulations should be a top priority to be address. Quality assurance and strict regulatory compliance must be enforce throughout product development and taken seriously. If the technology continues to developed as it has been doing without guidelines, drones could become a global security threat of unprecedented magnitude.