International Expert Group Meeting on the Protection of Vulnerable Targets and Unmanned Aircraft Systems

UN Office of Counter-Terrorism

6-7 October 2021, 8.45 a.m. – 12.15 p.m. (EDT)

Public address to the UNOCT on

UAS threats against vulnerable targets, including soft targets and critical infrastructure

Bruno Oliveira Martins, *Peace Research Institute Oslo*

Dear ladies and gentlemen,

It is my biggest pleasure to address this International Expert Group Meeting and raise some of the key issues surrounding the threat posed by non-cooperative drones. In brief terms, I will talk about the nature of the threat, the technological means to respond to it, and the societal, human rights and regulatory problems that persist today.

The thoughts that I will bring to the discussion emerge out of the work that we conduct at the Peace Research Institute Oslo, through which we have established a fruitful dialogue with policymakers, technology developers, and civil society organizations that work on this specific issue. Some of my remarks have some direct operational implications, whereas others point to broader debates that remain unresolved. Having a continuous conversation on this topic is fundamental to better identify the contours of the threat, the operational responses to it, and the technological support for that response. As of today, the combination of the nature of the threat with the operational and technological shortcomings make the vulnerability of soft targets a clear reality.

Nature of the threat

When it comes to the nature of the threat, it is important to note that drones have indeed been used by a range of terrorist groups in different scenarios, but also by other politically motivated actors, such as climate activists. Politicians and heads of state have been harassed by drones, the motives for which have never been declared. Whereas the intention to cause harm is certainly different from case to case, from an operational, responsive viewpoint, particularly in some scenarios such as airports, the intention behind the drone operator is less relevant, inasmuch as the mere non-cooperative character of the intruding drone make it a risk and a threat. I would say that, in the field of drones and counter-drone systems in metropolitan areas, the distinction between safety and security has become blurred. Moreover, counter-drone technologies, operating in a regulatory environment that is not fully updated, are unable to provide a clear and immediate distinction between mal-intentioned and mere careless drone users. Considering that, in the case of a drone sighting in, for example, an urban area, the intention of the drone operator is hard to determine, the vulnerability of the soft target comes from the mere presence of the drone. In some cases observed in the past, such as with energy-producing facilities, the sighting of a drone has meant everything from industrial espionage to climate activism and terrorism.

The technological means to respond to it

The growing perception of the threat posed by drones has led to the emergence of an expanding counter-drone technology market. Security practitioners have hundreds of options for systems to both identify non-cooperative drones and engage / mitigate the threat they pose. Yet, contrary to what most vendors would say, these systems face innumerous challenges that result in very substantial difficulties in delivering the security they propose. Some of the problems are technical: detection systems face communication interferences; radars mix birds for drones; weather conditions affect mitigating efforts. Other times, the problems have a regulatory nature. For example, in many countries, radio frequency jammers cannot operate in urban environments due to the risk of interference with other channels of communication also operating with radio frequency, such as police communications. The most kinetic mitigating technologies, by which non-cooperative drones can be shot by a projectile or attacked by microwaves, pose serious risks and in most cases cannot be used in civilian settings, where the soft targets are placed.

From this, it results that both threats and vulnerabilities are real. Yet, like with all cases involving security threats, the real challenge is to strike an acceptable balance between the risk and the response, while ensuring that human rights are respected, and broader societal implications are an integral part of the decision-making processes. Our engagement with regulators, security professionals, and technological developers has revealed that many of these issues are largely disregarded when decisions are made in this field. In the remaining minutes of my address, I will focus on these aspects, hoping that, with time, they can become an integral part of the debates regarding the threat of drones.

Societal implications

The first point I want to make is that the sighting of counter-drone systems increases threat perception and may generate psychological stress. Some of these systems have a distinct military appearance and their deployment in civilian contexts may trigger uneasy feelings. Their deployment needs to be balanced against the risks posed by drones, and it needs to be proportional. The civilian airspace is facing a phase of re-regulation and re-conceptualization in face of the integration of drones, and in this process, we should avoid an over-securitization of airspace in a logic similar to an arms race. As of today, our civilian skies don’t need that, and should not witness that.

The second point I want to make is that counter drone systems are surveillance systems, and should be treated as such. They collect information about drone users, they generate visual data, they provide geolocation information, and therefore their use needs to comply with general data protection rules and should not be granted exceptions.

The third point is a crucial one. Even though most of contemporary drone and counter-drone R&D happens in the civilian and commercial sectors, these fields are still marked by a military logic, testimony to the environment in which drones were first used and for which they were first conceived. The feed of a drone camera over a city resembles the sight of a conflict zone. The visual images of people collected by drones portray a vision devoid of humanity. The jargon involving drones and counter-drone systems is often of a military nature (“target”, “person of interest”, “intruder”, “mitigation”, “kinetic”, “combat-proven”, etc). The growing use of military gear in civilian settings by law enforcement agents and private security companies contributes to a militarization of society that has broad implications that we need to address explicitly.

Additionally, as our societies become “smarter” and more technologically advanced, dual-use technologies become increasingly important. Given that the technological frontier is often in the civilian and commercial sectors (from drones to facial recognition technologies and other AI-powered systems), military technology became dependent on civilian research. Today we witness a proliferation of military-funded research in universities and defence contracts awarded to private companies to conduct R&D. While much of this is not totally new, today we can observe a combination of factors that may lead, and in some cases is indeed leading, to the militarization of basic research, in a movement that does not always abide to the principles of responsible research and innovation. This risks bringing us backwards to a time where much of civilian research was driven by military imperatives.

All these factors make the drone threat much more than a mere security issue that can easily be solved. I am afraid it is not and it cannot. But in the effort to develop responses to it, we should be aware of the broader questions at stake here. I hope that this event provides an opportunity to advance the contours of our discussion and may lead to further international cooperation. Finally, it is crucial that civil society organizations are regularly involved in these debates. As a broad societal issue, dealing with the risks of drones should involve the participation of all society, and not only the end users of either drones or counter-drone technology.

Thank you.