HOSTILE INTENT

COMBATTING ROGUE DRONE THREATS

An article by
Andrew Staniforth, Director of Innovation,
Saher-Europe

Defence iQ

www.defenceiq.com/events-counteringdrones

INTRODUCTION

The nefarious, criminal and terrorist use of drones raises important questions on the effective responses to rogue drone attacks, and how this once disruptive technology has now become decidedly dangerous. It is clear to see why drones offer a new tactic for operators with hostile intent, as they can be operated anonymously and remotely; they present little or no risk to their operators of detection or prosecution; they can be acquired cheaply and easily; their operation can be mastered simply and safely; and they can be used in isolation or in large numbers as swarms to devastating effect.

Ahead of the Countering Drones conference, taking place on 28-30 July 2020 in London, UK, our Chairman Andrew Staniforth, Director of Innovation, Saher-Europe outlines the threat landscape of rogue drones, and how organisations can prepare to protect themselves against the use of drones by malicious actors.

As well as being the conference Chairman, Andrew Staniforth will also lead a workshop on DENI (Detection, Evaluation, Neutralisation & Investigation) Counter-Unmanned Aerial Vehicle training. You can download the full agenda of the conference **here**.

Andrew Staniforth

Director of Innovation Saher-Europe

Andrew Staniforth is Director of Research and Innovation at Saher (Europe), a security research, training and consultancy operating at a global level, supporting police forces and private sector organisations to identify and implement innovative security technologies to maximise impact. He is a Researcher of Cyber Threats at the Hillary Rodham Clinton School of Law and Criminology, University of Swansea. As a former Special Branch Intelligence Officer and Counter-Terrorism Detective, he has worked across the world and supported missions of the United Nations Terrorism Prevention Branch.

COMBATTING ROGUE DRONE THREATS

THREAT LANDSCAPE

The illegal use of drones is now a pressing security concern across the world as terrorists, activists and criminals are adopting drone technology and developing new, creative and sophisticated ways in which to commit crime and terrorism. The use of drones for hostile reconnaissance in theatres of conflict, and combined with their adaption to carry Improvised Explosive Devices (IEDs), has signalled the use of drones as a deadly and determined terrorist tactic.

Organised Crime Groups (OCGs) profiting from human trafficking and people smuggling into and across Europe, are using drone technologies to monitor security measures at ports and border checkpoints. As a direct result of the criminal use of drones, police officers around the world are having to investigate an acute rise in the number of crime reports involving drones purchased online, direct from stores or from a growing number of home-build enthusiasts. These investigations have included allegations that drones are being used to supply drugs into prisons, by paedophiles hovering over children's playgrounds, and by burglars scoping out properties.

FAULT LINES

Despite counter measures now being put in place to strictly prohibited drone activity in restricted areas, and the clear and present danger posed to aircraft from potential drone-strikes, reports of rogue drone activity at airports across the world continue to occur with alarming regularity. The shutdown and continued disruption of major airports due to rogue drone incursions has exposed fault lines not only in the multi-agency threat and risk assessment prioritisation processes but most critically, has regrettably signalled to would-be terrorist plotters and other hostile actors the effective ways in which to paralyse air travel as part of attack planning intentions to cause mass disruption, damage economic stability and threaten national security.

As drones continue to evolve from novelty items to a ubiquitous business tool, resourceful cyber criminals may also see an opportunity to leverage drones' proximity to homes, businesses, and critical infrastructures to turn them into a jumping-off point to illegally access networks and systems, thus creating a new category of infection vector to amplify cyber security risks. The emergence and persistence of rogue drone activity has created a new dimension and a fundamental shift in the way in which the privacy, safety and security of buildings, personnel, data and other valuable assets must now be protected from the threat of hostile drone incursions.

PROTECT AND PREPARE

All in authority who have professional responsibility for the protection of valuable data and the maintenance of privacy, safety and security of citizens and colleagues, now need to prepare and equip their organisations against all manner of rogue drone hazards. But combatting the threat of drones is largely ineffective without fully understanding the complexity of the UAV threat which forms a key objective of the DENI (Detection, Evaluation, Neutralisation & Investigation) Counter-UAV training.

Building upon joint research and innovation with leading Law Enforcement Agencies and specialists in the defence and security drone detection domain, the new and innovative DENI Counter-UAV training recognises that the formulation of a coherent counter-UAV strategy includes the procurement and deployment of the appropriate equipment, and the integration of that equipment and practical response into the very culture and concept of security operations.

Designed and delivered by leading industry drone and law enforcement experts, the DENI Counter-UAV training is unique and interactive during which attendees will not only gain insights to the contemporary drone threat and related drone and drone detection technologies, but more importantly, how this knowledge can ensure an effective response to rogue drone incidents, putting counter-UAV policy into operational practice.

Given the growing concerns of drone threats, positive steps must now be taken to identify the most effective solutions to safeguard against hostile UAV incursions. By providing professional DENI Counter-UAV training to its personnel, those concerned in preserving safety and security of organisations will be able to effectively respond to the diverse range of threats from rogue drones which are becoming increasingly sophisticated and aggressive.

"Given the growing concerns of drone threats, positive steps must now be taken to identify the most effective solutions to safeguard against hostile UAV incursions"

Picture: DJI

Defence iQ

COUNTERING DRONES

28 - 30 JULY, 2020 | LONDON, UK

www.defenceiq.com/events-counteringdrones

DETER. DETECT. DEFEND.

THE WORLD'S ONLY COUNTERING DRONES CONFERENCE DEDICATED TO THE SECURITY COMMUNITY

The civilian drone market is set to explode, and with it the threat to critical civil infrastructure. In the USA alone, the DOD requested $500 million for counter-UAS funding for civil and military spending in 2020. It is clear therefore that the requirements for counter-drone solutions are still there – and as new regulations come into force, organisations will soon have greater clarity on which solutions they will be able to employ, meaning they will have more freedom to procure new solutions.

Countering Drones 2020 will progress the conversations on drone threat beyond our current understanding, and into the areas of future threats. We will explore how the proliferation of this rapidly developing industry has the power to carry considerable disruptive force, and what we can do now to lay the foundations for future success.

Bringing together experts from law enforcement, airports, critical national infrastructure, subject matter experts, and technology leaders it will provide a platform for meaningful consensus and constructive discussions as to how we can maintain safety and security against the misuse of drones.

Leading the discussions will be:

- **Carissa VanderMey**, Director C-UAS Program Management Office, **U.S. Department of Homeland Security**
- **Chief Inspector Simon Bachelor**, NPCC Counter Drones, Legislation and Policy lead, **UK Counter Drones Unit**
- **Michael Schneider**, Deputy Assistant Director, Critical Incident Response Group, **FBI**
- **Colonel Jean François Morel**, Counter UAS Lead, **Gendarmerie Nationale**
- **Squadron Leader Arnaud Duchene**, Counter-drone Programme Director, **French Civil Aviation Authority**

DOWNLOAD THE AGENDA HERE

A Partner, in and for the Defence Community

Defence iQ Membership

Defence iQ strives to support and strengthen the global defence community by using its events, digital platform and publications to educate and inform, providing insights and analysis on the key issues shaping military doctrine and operations, defence policy, acquisition and technology development.

Our members are given access to a premium collection of publications and content from our global events, including:

- The Defence Digest, our weekly Members' Newsletter
- Defence IQ Market Reports, White Papers and Case Studies
- Monthly Defence IQ Disruptive Technology 'Guide To' Briefs
- All Defence IQ post-show reports, speaker slide decks and video, audio and podcast event highlights

Find out more about our membership benefits and sign up, free of charge, here**.**

Defence iQ Contributors

Defence iQ collaborates with contributors from the military services, defence policy, acquisition, traditional and non-traditional defence inudstry, S&T and academia. Our objective is to provide our members and wider readership with a hub of commentary and analysis on issues covering military operations and doctrine, defence policy, acquisition and technology development.

We recognise that established paradigms in defence are being challenged by new, complex threats and disruptive technologies, and as such public-private sector collaboration and the cross-fertilization of ideas about the present and future defence enterprise has become more important than ever.

As such, Defence iQ welcomes the contributions from thought leaders across the defence community, to help inform, educate and inspire the current and next generation of disruptive thinkers, innovators and smart customers in defence.

Please get in touch with the Editor, Hannah Croft, at hannah.croft@defenceiq.com to discuss submission proposals and dates.

Defence iQ