THE UAS TRIBUNE

Critical Infrastructure Resilience & Counter-Drone Systems
An Opinion on the Situation in Europe

By Dr Oliver Heinrich & Malte Krumm
BHO Legal, Germany

Recent drone attacks on Ukraine's electrical power plants causing blackouts in more than 1,1000 towns and villages, reports about unidentified drone sightings over Norway's offshore platforms days before the attacks on the Nord Stream pipelines, as well as alleged espionage by drone flights near several sensitive areas in Norway and Sweden, have moved the issue of European Union (EU) critical infrastructure resilience, once again, to the top of the current political agenda (cf. Opening remarks by EU Commissioner Johannson at the press conference on EU critical infrastructure resilience on 18.10.2022, SPEECH/22/6265).

Already back in 2020, the EU Security Union Strategy [COM(2020) 605 final] identified, inter alia, a "future proof security environment by enhancing cyber security and protecting critical infrastructure and public places" as one of its four main strands of necessary actions for the period of 2020 to 2025. The Strategy explicitly referred to the hazard potential of drones misused by criminals and terrorists in public spaces and over critical infrastructures. While the European Commission acknowledged the European regulatory framework for drones, laid down in Regulation (EU) 2018/1139, Implementing Regulation (EU) 2019/947, and Delegated Regulation (EU) 2019/945, as an important first step to minimize potential hazards, in particular by careless and reckless drone pilots, it also stressed a need for additional action, including information sharing, guidance and good practice for use by all, including law enforcement, as well as for additional testing of drone countermeasures.

This article provides an overview on the most recent and prospective EU efforts to meet this need for additional action in favour of critical infrastructure resilience by counter-drone systems. In addition, it aims to clarify roles and responsibilities in the multilevel context of the EU and its Member States. In this context, particular attention is paid to a new legislative proposal, the Directive on the resilience of critical entities [CER-Directive, cf. COM(2020) 829 final]. Long after the proposal's publication at the end of 2020, an inter-institutional agreement was finally reached in June 2022. The proposal is expected to be voted on in the European Parliament early in November 2022. A first analysis reveals that it might turn out to be a game-changer for an internal market of critical infrastructure entities, as well as counter-drone systems.

EU Policy & Guidance Material In The Field Of Counter-drone Systems

The willingness of the EU actors to support and engage in the field of critical infrastructure resilience in general, and counter-drone systems in particular, is reflected in several policy actions, published as well as announced over the course of the last two years.

EASA Drone Incident Management At Aerodromes Part I-III

In the aftermath of several incidents, involving drones near or inside the perimeter of airports, as well as in their immediate proximity, and in the arrival and departure paths of runways since 2018, most prominently at London Gatwick and Heathrow airports in December 2018, the European Aviation Safety Agency (EASA) established a Counter Drone Task Force in November 2019 to develop an action plan in order to ensure that aerodrome operators, aircraft operators and air traffic services (ATS) providers are prepared to take preventive action as far upstream as possible, and to react to the misuse of drones with minimum disruption of operations, while still being able to accommodate friendly drone operations [European plan for Aviation Safety (EPAS) 2020-2024, pp. 54 f.]. As one of the five proposed actions to reach this objective, EASA - in collaboration with national law enforcement bodies, aerodrome operators, as well as the European Commission's Directorate for Migration and Home Affaires (DG HOME) - proposed to develop comprehensive guidance material for relevant stakeholders to ensure that counter-drone measures are swiftly considered and implemented from a global safety perspective. A tripartite manual on Drone Incident Management at Aerodromes was published in March 2021. Part 1 of the manual, entitled "The challenge of unauthorized drones in the surroundings of aerodromes", is freely available online. Part 2 ("Guidance and recommendations") and Part 3 ("Resources and practical tools") have been made available only to relevant stakeholders and authorities due to the sensitive nature of the subject matter, but can be accessed in case of a duly motivated request to EASA (aerodromes@easa.europa.eu).

Although the manual itself is technology-neutral and does not recommend any specific counter-drone system, Part 3 provides an overview of available systems and offers some guidance as to the procurement and testing of counter-drone solutions. In line with the distribution of competences described in detail below, in particular the EU principle of subsidiarity, the manual acknowledges that security forces and law enforcement authorities are organised at the national level. It provides that it is the Member States' responsibility to include arrangements to dictate how law enforcement authorities shall respond to drone incidents in their national counter-drone strategies and associated national operational arrangements. For this reason, Part 3 of the manual contains, inter alia, a methodology for a local risk assessment, advice for procurement and testing of technological counter-drone

solutions, an overview of different technological counter-drone solutions, and guidance for the initial response to a drone incident by first responders.

EU JRC Handbook For Counter-drone Protection Of Critical Infrastructures

In addition to EASA's efforts, the European Commission's Joint Research Centre (JRC) announced during the Amsterdam Drone Week 2022, that it will publish an additional "Handbook for counter-drone protection of critical infrastructures" at the end of 2022. According to Paul Hansen, Project Manager at the JRC, the Centre is developing a risk analysis framework for critical infrastructure, and common criteria for aligning counter-drone solutions with the results of an analysis of the specific infrastructure risk. Apart from the handbook, which has not been published at the time of writing, it is worth mentioning that the JRC is also providing a comprehensive overview of international best practices, standards, and technical support regarding counter-drone measures on an ongoing basis, (cf. JRC Technical Report, Karlos/Larcher, A guide to key information on the protection of Public Spaces, 2021, pp. 33 ff.).

Handbook For Securing Urban Areas From Non-cooperative Drones

A third policy document, the "Handbook for securing urban/metropolitan areas from non-cooperative drones", has been announced on several occasions by European Commission officials and was scheduled for publication in late 2021. Advertised as a top-level, non-technical, accessible handbook addressing relevant audiences and stakeholders such as regulatory authorities and law-enforcement agencies in urban contexts, it is based on an extensive study of different metropolitan approaches in countering threats posed by drones. Apart from practical guidance and support by sharing best practices, the study also aims to identify possible needs for further legislative engagement.

EU Drone Strategy 2.0

Finally, the EU Drone Strategy 2.0 is a high-level EU policy initiative aiming to enable drones to contribute, through digitalization and automation, to a new offer of sustainable services and transport, while accounting for possible civil and military technological synergies. The strategy is supposed to provide a forward-looking vision for the future holistic development of the sector with a time horizon of 2030, which can foster the uptake of this innovative technology in Europe, while establishing the right balance between safety, security and other societal concerns, and a sustainable economic environment. The European Commission will present the Strategy to the public on the 29th of November 2022 in collaboration with SESAR JU in Brussels.

According to first insights on the Strategy's content given by EU officials, "increasing system resilience and counter-UAS capabilities" will form one of the ten priorities of the new Strategy under the umbrella of two main objectives:

1) Building a European drone service market; and
2) Strengthening the European civil and defence industry capabilities.

While it remains to be seen, which precise legislative or policy actions will be based on the new Strategy, it is more than likely that new funding and financing opportunities provided under Horizon Europe, the European Defence Fund (EDF), or by the European Investment Bank (EIB) will be available for counter-drone projects, too.

EU Competence In Critical Infrastructure Protection

In order to understand the distribution of competences between the EU and its Member States in the field of critical infrastructure protection, it is essential to start with the EU primary law, notably the Treaty of the European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU).

In line with the principle of conferral, enshrined in Article 5(1) TEU, the EU shall only act within the limits of the competences conferred upon it by the Member States in these treaties to attain the objectives set out therein. In addition, the principle of subsidiarity in Article 5(3) TEU governs the exercise of EU competences in areas in which the EU does not have exclusive competence by safeguarding the ability of Member States to take decisions and action as close to the citizen as possible. It authorizes intervention by the EU when the objectives of the relevant action cannot be sufficiently achieved by the Member States, but can be better achieved at EU level by reason of the scale and effects of the proposed action.

The protection of critical infrastructures against physical threats is not directly addressed in the EU treaties. Closely related activities in the field of counterterrorism and police cooperation however constitute a key plank in making the EU an Area of Freedom, Security and Justice (AFSJ), a domain subject to shared competences between the EU and its Member States, Article 4(2)(j) TFEU. As further specified in Articles 67 to 89 TFEU, this area relates to common policies on border checks, asylum and immigration, judicial cooperation in criminal, as well as civil matters, and police cooperation.

In respect of critical infrastructure protection, as part of the broader field of internal security, this means that the EU has the authority to legislate where security can be improved through coordination and cooperation among the Member States, in particular their security agencies. However, considering the principle of subsidiarity, this does not apply for security issues that are of an entirely regional or local nature. Thus, due to its close ties to national sovereignty, the actual safeguarding of critical infrastructures as part of national public security, is by its very nature a genuine responsibility of the individual Member State. This is confirmed by Article 73 TFEU, which stipulates that any form of action in the context of the EU's objective to create the ASFJ "shall not affect the exercise of the responsibilities incumbent upon Member States with regard to the maintenance of law and order and the safeguarding of internal security".

A New Internal Market For Services Of Critical Entities & Counter-drone Systems?

Notwithstanding these limitations in competence, the EU did not, and does not refrain from acting in the field of critical infrastructure protection and resilience.

The new CER-Directive will be based on Article 114 TFEU, which involves the approximation of laws for the improvement of the internal market. Like the AFSJ, the internal market is subject to the rules of shared competences between the Member States and the EU, cf. Article 4(2)(a) TFEU. A substantial difference however is the circumstance that is subject to significantly more influence of the European institutions regarding the adoption of legislative harmonization measures.

According to the proposal, the new legal basis of the Directive is justified by the shift of its aim, scope and content, increased interdependencies, and the need to establish a more level playing field for critical entities. Instead of protecting a limited set of physical infrastructures from the disruption or destruction, which would have significant cross-border impacts, the proposal aims at enhancing the resilience of entities which are critical for the provision of services, and which are themselves essential for the maintenance of vital societal functions or economic activities in the internal market of the EU.

The new CER-Directive (as negotiated at time of writing) will expand the scope of its predecessor from only two sectors (energy and transport) to cover in total eleven sectors of critical entities (energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, public administration, space, and food). While Member States will be obliged to adopt a national strategy for reinforcing the resilience of critical entities, and to carry out regular national risk assessments to identify critical entities by using a common methodology, critical entities themselves will have to carry out site-specific risk assessments of their own, taking measures to ensure their resilience, and to report disruptive incidents.

In addition, a Critical Entities Resilience Group, bringing Member States and the Commission together, will evaluate national strategies and facilitate cooperation. Member States will have to empower a single or multiple national competent authorities to enforce the relevant rules, in particular to conduct on-site inspections, and to introduce penalties in case of non-compliance.

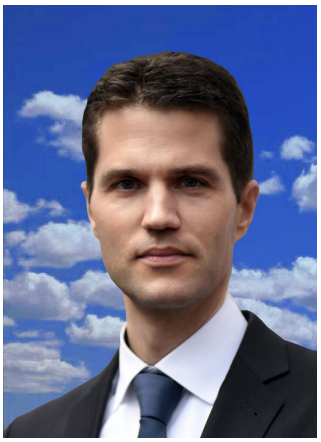
The European Commission will be tasked, inter alia, to support Member States and critical entities in complying with their obligations under the new CER-Directive, in particular by preparing a Union-level overview of cross-border and cross-sectoral risks to the provision of essential services, and by facilitating information exchange among experts. Furthermore, the Commission will complement Member States' activities by developing best practices and methodologies, and by supporting cross-border training activities and exercises to test the resilience of critical entities.

For these reasons, the Commission will be empowered to adopt delegated acts establishing detailed rules specifying some, or all, of the measures to be taken by Member States to ensure that critical entities take appropriate and proportionate technical and organizational measures to ensure their resilience, e.g., adequate physical protection of sensitive areas, including fending, perimeter monitoring tools, or detection equipment. In addition to that, the Commission shall adopt implementing acts in order to set out the necessary technical and methodological specifications.

Particularly noteworthy is the fact that the proposal is not limited to a support function in favour of a resilient internal market itself. In fact, it stipulates new obligations for critical entities, as well as Member States aimed at improving their ability to provide services and their oversight in the internal market, thereby establishing a new internal market for services of critical entities themselves.

It is more than likely that suppliers of counter-drone systems will benefit from these developments, too. On the one hand, Member States will soon have to include threats by illicit drone use in their new national strategies. On the other hand, critical entities will have to evaluate, based on their individual risk assessments, whether or not, to implement counter-drone systems as risk mitigation measures. The fear of penalties imposed by national authorities in case of non-compliance might provide for an additional incentive to perform an in-depth risk assessment.

In the end, harmonized standards for risk assessments and mitigation measures for critical entities, paired with the outlined EU policy efforts and distribution of best practice guidance on counter-drone systems, might flatten the entry-barriers to a formerly fragmented market. They will provide an excellent opportunity to expand counter-drone services on a pan-European level.



Dr Oliver Heinrich Malte Krumm
BHO Legal, Germany
bho-legal.com