Executive Summary

The purpose of this study is to gather and analyse a primary dataset as the first step towards an EU-wide dataset on cybersecurity exercises, and to create a model for continued reporting on such exercises. The study is the first step towards the larger goal of using the dataset as a resource for planning and collaboration between nations and agencies interested in cybersecurity exercises.

A dataset consisting of over 200 cybersecurity exercises and specialised literature such as after-action reports and previous studies have contributed to the analysis.

The findings show a continuous and accelerated increase in the total amount of exercises held after 2012, as well as an increase in the number of cooperative exercises involving private and public actors. This indicates that it is not just a matter of public agencies running more exercises, but also of more actors benefitting from these exercises.

The study also reveals that many cybersecurity exercises focus on exploring new structures and collaborations, rather than consolidating or building on established ones. Even though this exploration is an important step towards reaching consolidation, it might be in the best interest of the participants to take the next step of establishing procedures.

Finally, the public-affairs aspect, and in particular the explicit goal of educating both the public and decision-makers, is left relatively unexplored in much of the exercise design and planning. While there are undoubtedly links between an increased awareness of cybersecurity issues and an increased number of exercises, this exact nature of this link requires closer inquiry and requires a rather different analytical lens. Nevertheless, as an understanding of cybersecurity issues becomes more and more relevant for an increasingly larger audience, the opportunity to reach such an audience is often missed.

Based on our analysis, this report provides four main recommendations that would help to increase the quality of future cybersecurity exercises.

1. **ENISA should establish a common ground for the exchange of best-practices regarding cybersecurity exercise development**

The dataset developed in parallel to this analysis report has the potential to become a common ground for information and knowledge sharing regarding cyber exercises. ENISA should further develop this dataset by setting a clear focus on experience sharing, knowledge and lessons learned from exercise activities.

2. **Member States should contribute to the cybersecurity exercises community**

In order for the ENISA Cyber Security Exercises Dataset to be a source of valuable information regarding exercises, best practices and methodology, it requires input from the community. We urge all actors involved in exercise activity to contribute to the ENISA Cyber Security Exercise Dataset by providing input during the planning and the evaluation phase of future exercises.

3. **ENISA should produce an Analysis report bi-annually**

The 2012 and the 2015 Analysis report teaches us a lot about the developments within the field of cybersecurity exercises and what the trends have been and where trends are heading. By making this Analysis report a bi-annual publication, it allows for further knowledge spreading, but also, better follow-up

on what the impacts are from the developments within the field. We recommend that the Analysis report becomes a bi-annual publication and that the dataset is updated in accordance with the Analysis report drafting including input from experts in the community.

4. The MS and ENISA should co-develop a European exercise calendar

There is an increased number of cybersecurity exercises, an exercise calendar would help in visualising the exercises being held and would increase awareness amongst stakeholders in Europe and beyond. ENISA should develop the exercise calendar and attach it to the exercise dataset.