# WP9

**Practical Tools for Capacity Building**

* **Type**: New Task
  + Potential participants: **BUT**, L3CE, IMT, KTU, CINI
  + New deliverables: D9.6: Practical tools implementing cybersecurity skills framework, DEM, PU, M48, BUT
  + New estimated PMs per participant:
    - BUT: 5
    - CINI: 4
    - L3CE: 3
    - IMT: 3
    - KTU: 3
* **Summary**: The new task is focused on the production of practical tools with high impact on users. It will deliver the practical implementations of previous results, in particular the skills framework and good-practice study curricula and open-source cyber ranges.
* **Motivation**: The task will significantly raise the impact and implementation of SPARTA results into the practice, in particular in the area of **Cyber Ranges** and the applications of **EU Cybersecurity Skills Framework**.
* **Impact**: The task is directly linked to the “**Capacity Building (Demand and Supply)**” axis proposed by the Commission. In particular, it aims at these targets:
  + Agreement on EU-wide Cybersecurity Skills Framework (EU CSF) and contribution to related ENISA activities.
  + Development of practical software tools that apply the EU Skills Framework and help educational institutions to build cybersecurity curricula in practice.
  + Creation and first deployment of open-source cyber range tools.
  + Pilots for open-source cyber-range infrastructures at universities.
  + Full-fledged open-source cyber ranges for higher-education institutions that cannot adopt commercial products due to costs and closed environment.
  + Creation of training scenarios.
  + Production of practical tools supporting creation of new training scenarios at users' premises.
  + Creation of domain-specific cyber range infrastructures, e.g. for critical infrastructures, industrial networks, IoT, etc.
  + Creation of hybrid cyber range infrastructures that includes both software and physical hardware scenarios

**Cybersecurity Training Pilots and Awareness Activities**

* **Type**: New Task
  + Potential participants: **SMILE,** BUT, IMT, CESNET, KTU, PPBW, **CINI**
  + New deliverables: D9.7: Summary of piloting and awareness activities, R, PU, M48, SMILE
  + New estimated PMs per participant:
    - * CINI: 4
      * SMILE: 4
      * BUT: 4
      * IMT: 1
      * CESNET: 3
      * KTU: 3
      * PPBW: 1
* **Summary**: In SPARTA, the good-practice curricula for cybersecurity training and education have been designed and evaluated on a small sample. This task aims and larger-scale piloting and evaluation in specific settings, like elderly people, children, outermost regions, industry, etc.
* **Motivation**: The existing results will be evaluated on a large scale and in more variable environment. The dissemination of results will be stronger and wider.
* **Impact**: More institutions will be involved in piloting activities and the results of SPARTA will have impact on wider audience.
* **Strategic Planning**: The task is directly linked to the “**Cybersecurity Awareness**” axis proposed by the Commission. In particular, it aims at these targets:
  + Coordination of training, education and awareness activities with CCN Education Focus Group
  + Large-scale awareness campaigns including EU's outermost regions, on high-schools, SMEs, social media, specific media such as EU's cybersecurity and digital privacy newsletter, ECSO, CYBERWISER, etc.
  + Alignment of awareness campaigns with the EU CSF.
  + Integration of specific focus groups, such as elderly people, children, people with specific needs, SMEs.
  + Deployment of larger pilots for cybersecurity study programs and support of education providers in creating new cybersecurity study programs using the EU CSF.
  + Support continuous education and specialized courses for specific groups, such as kids, elderly people, persons with specific needs.
  + Develop an online methodology to rise cyber awareness
  + Creation of cyber range scenario dedicated to cyber awareness
  + Creation of an intercollegiate cybersecurity championship *CyberChampions.EU* that aims to raise awareness in European universities students and cybersecurity practical knowledge.