



Expert Consultation: E-resilience, internet security and digital inclusion
14 October 2014

Combating cybercrime: Globally, Regionally, and Nationally

Margaret Akullo
Programme Coordinator



cybercrime@unodc.org

International cybercrime & e-resilience

- Rapid expansion of information and communication technologies (ICT)
- Uninterrupted 24/7 connectivity is becoming the standard
- Interruptions of ICT technologies threaten the entire (e-business continuity)
- Disruptions:
 - Non-intentional incidents vs.
 - Intentional attacks against the confidentiality, integrity and availability of computer systems and data

International cybercrime & e-resilience

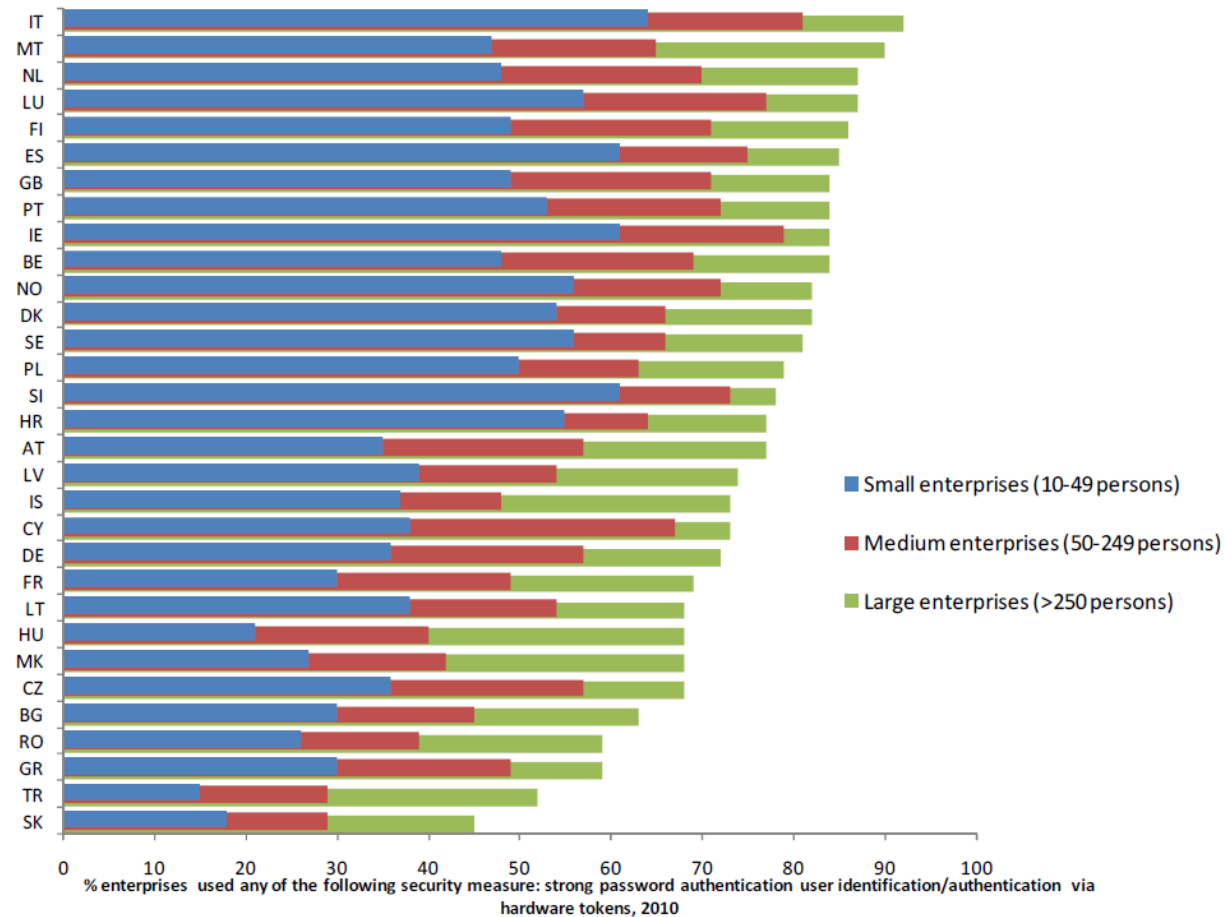
Cybercrime and cybersecurity strategies

National interests and security, trust, resilience, reliability of ICT	Rule of law, human rights, and crime prevention and criminal justice		
Cybersecurity strategies	Cybercrime strategies		
Non-intentional ICT security incidents	Intentional attacks against the confidentiality, integrity and availability of computer systems and data	Computer-related and content-related offences	Any offence involving electronic evidence

Adapted from Seger, A., 2011. *Cybercrime strategies*. Octopus conference 2011.

Public-private partnerships

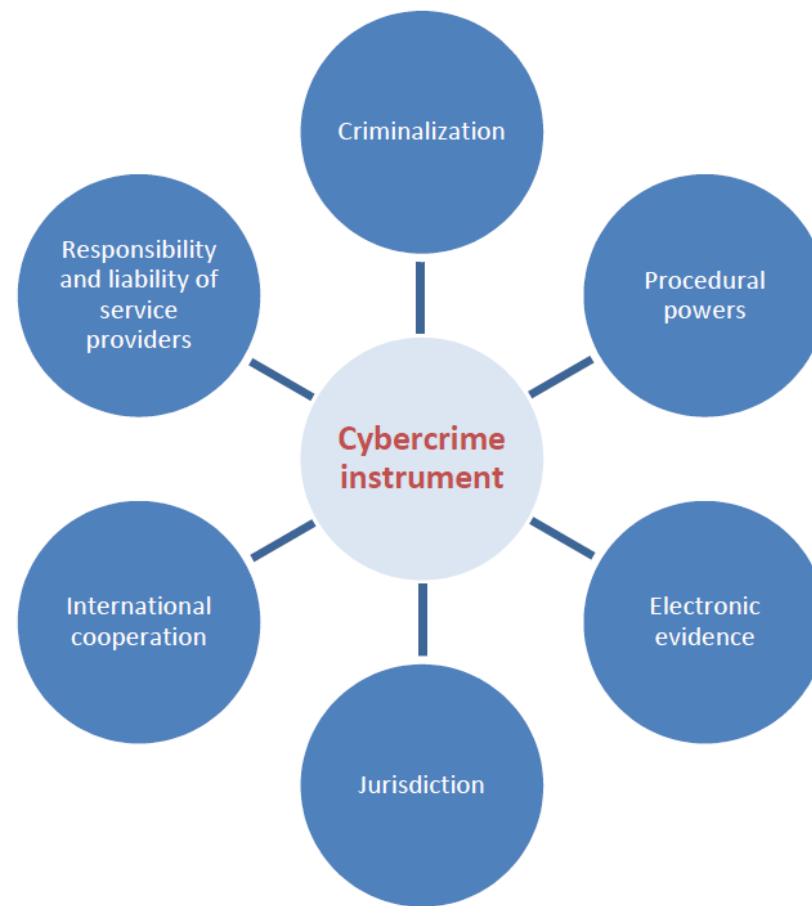
Figure 8.13: Strong password authentication and/or user identification and authentication via hardware tokens by size



Source: Eurostat Community survey on ICT usage and e-commerce in enterprises

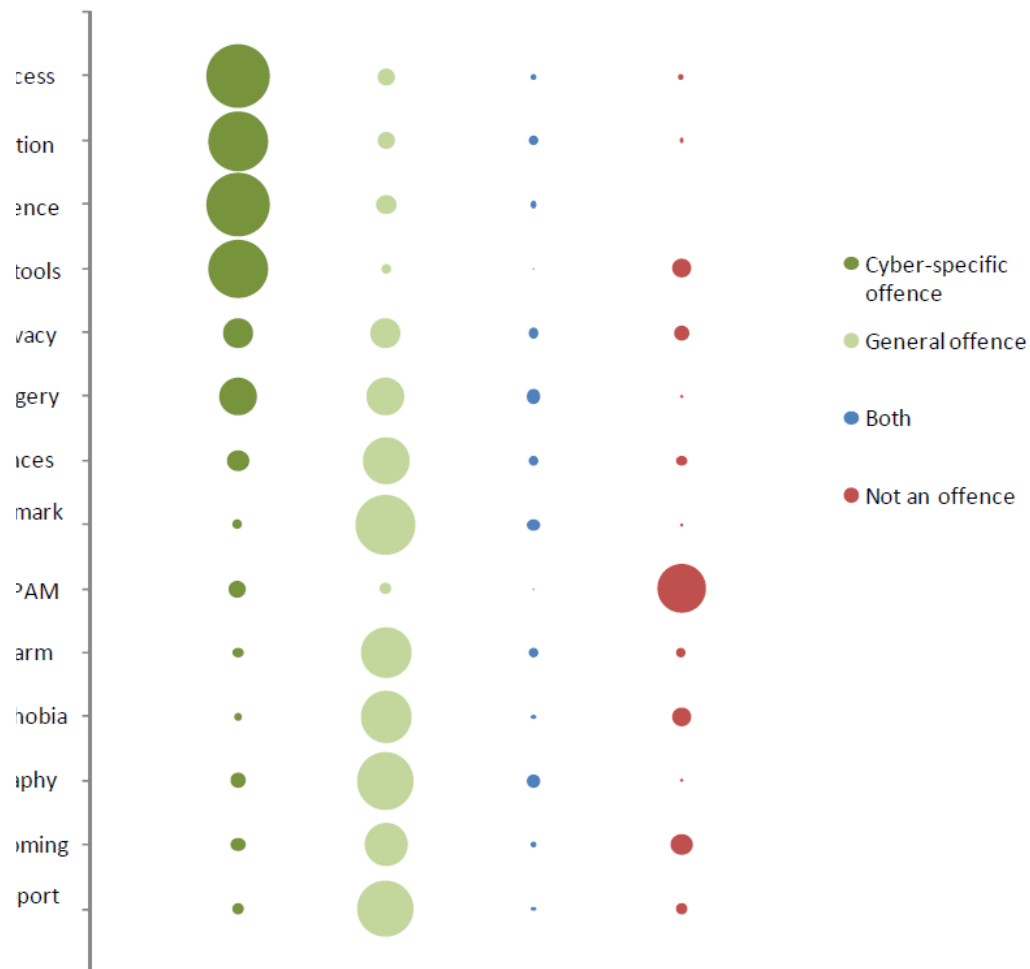
National and international cybercrime instruments

Figure 3.7: Substantive focus of cybercrime instruments



criminalization of cybercrime

ational approaches to criminalization of cybercrime acts



Source: Study cybercrime questionnaire. Q25-38. (n=61)

预览已结束，完整报告链接和二维码如下：

https://www.yunbaogao.cn/report/index/report?reportId=5_4957

