Excellence Hubs – experiences from project preparation: Cyber-security Excellence Hub in Estonia and South Moravia (CHESS)

Ladislav Čoček
Masaryk University
17 October 2023

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

https://cordis.europa.eu/project/id/101087529

Initiation

- What are the strengths of our region?
- Can we make connections to all (4) sectors?
- Who can coordinate?

MUNI

Partnership

- Who are our (research) partners?
- Can they reach all (4) sectors?
- Do we have some interesting story?

The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli*

Matus Nemec
Masaryk University,
Ca' Foscari University of Venice
mnemec@mail.muni.cz

Marek Sys†
Masaryk University
syso@fi.muni.cz

Petr Svenda
Masaryk University
svenda@fi.muni.cz

Dusan Klinec
EnigmaBridge, Masaryk University
dusan@enigmabridge.com

Vashek Matyas
Masaryk University
matyas@fi.muni.cz

COMPLETELY BROKEN —

Millions of high-security crypto keys crippled by newly discovered flaw

Factorization weakness lets attackers impersonate key holders and decrypt their data.

DAN GOODIN - 10/16/2017, 1:00 PM

Enlarge / 750,000 Estonian cards that look like this use a 2048-bit RSA key that can be factored in a matter of days.

MUNI

Consortium building

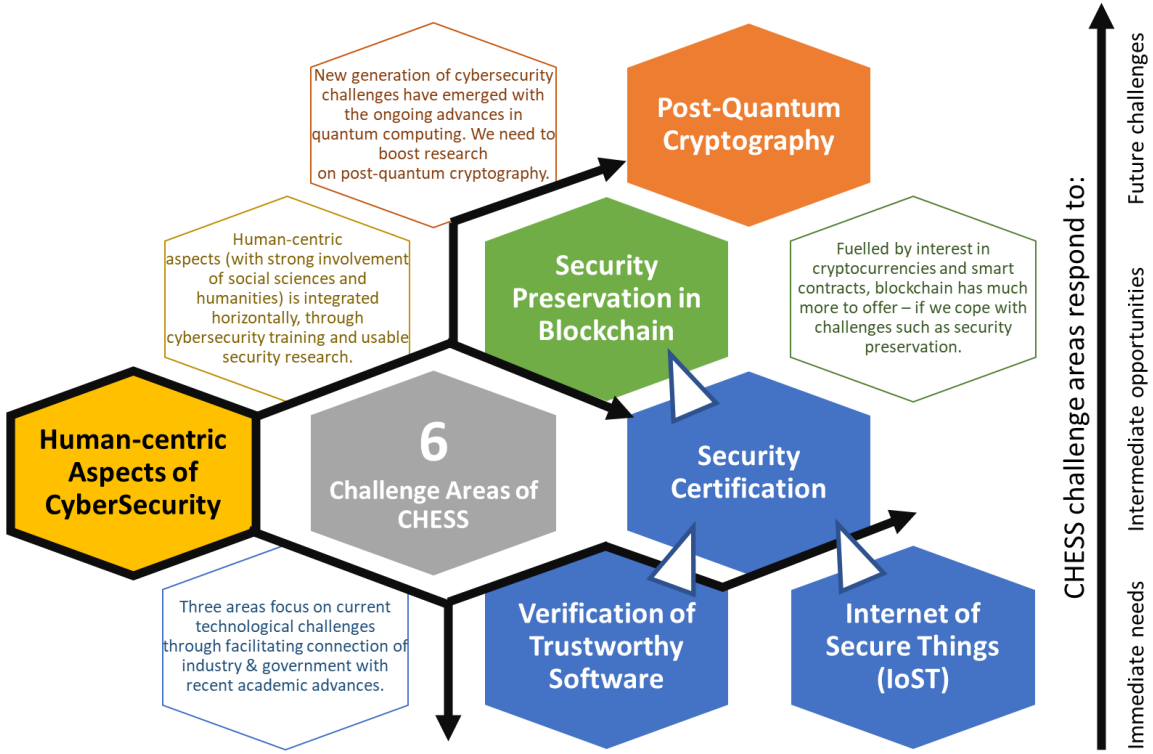
- Contribution to EU

- Academia
- Industry (established!)
- Government / Public
- Society

MUNI

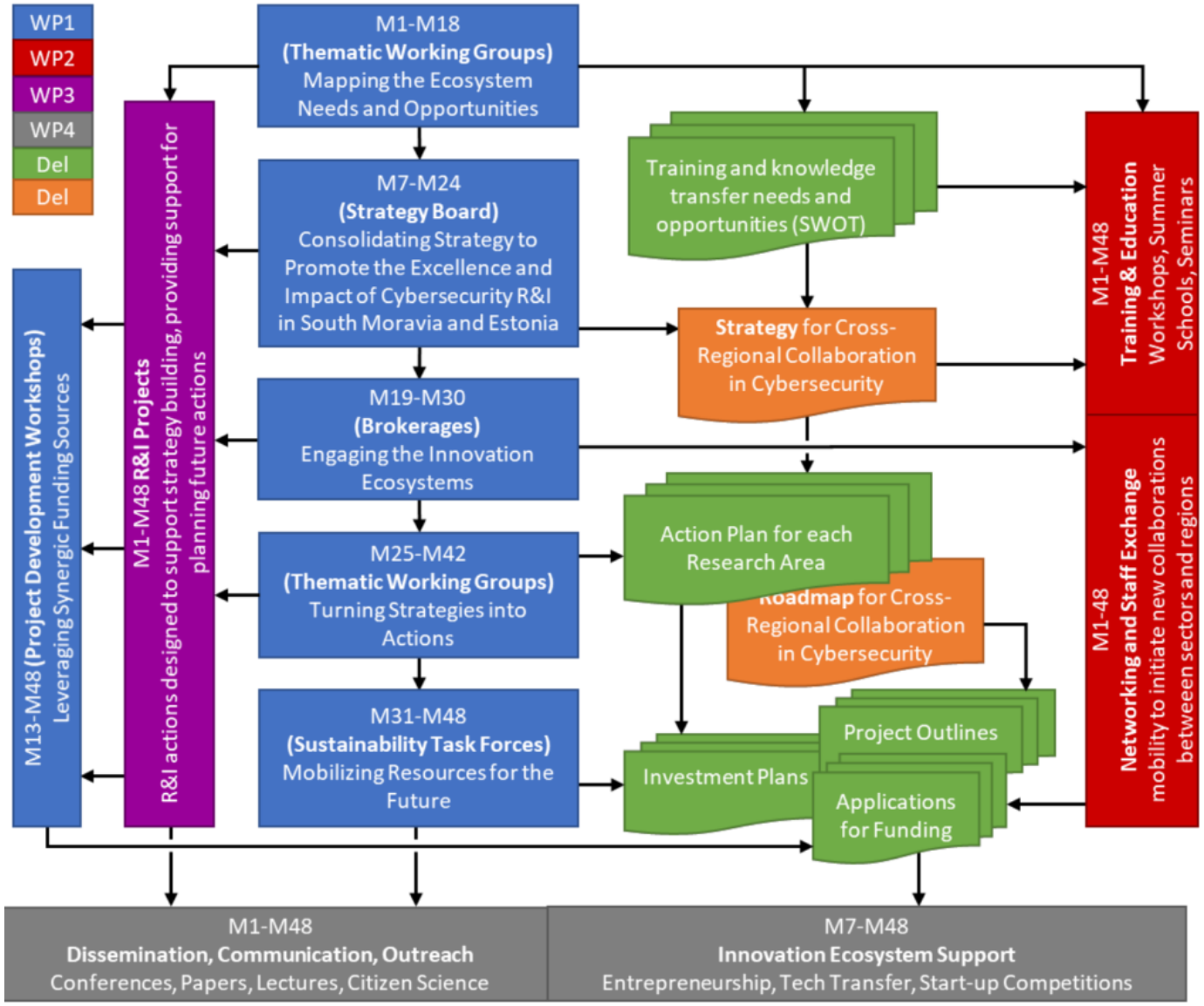
Project design

- Target challenge areas based on common research interests (6)
- Broad areas with high degree of flexibility
- All challenge areas co-led by both regions



Project workplan

- Work plan as simple as possible (5 WPs)
- All WPs co-led by both regions
- Strategy building as the main axis



MUNI