D.2.3. Detailed appendixes on cyber crime inventory and networks in non-ICT sectors

Dr Rain Ottis
Tiia Sõmer
Tallinn Technical University

Rome, 19 january 2015

19 January, 2015

Objectives

- analyse the structures of cyber crime networks, their economies and criminal revenue streams that support these networks;
- develop perpetrator and victim “journey maps”.

“Journey mapping”

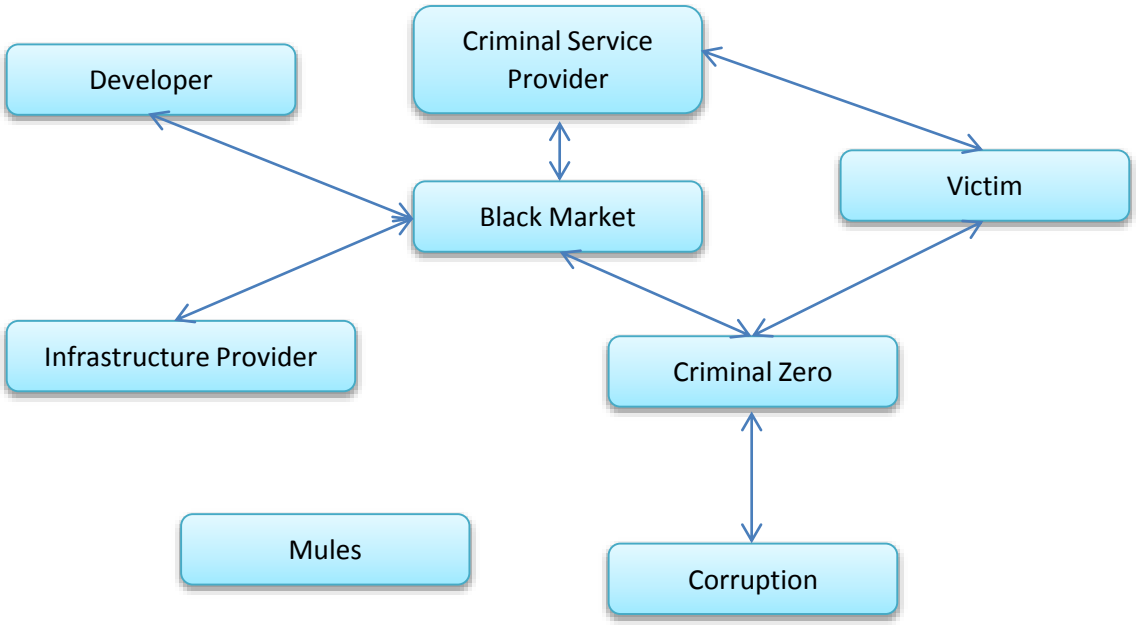
- identify the cyber criminals’ *modus operandi*, or how they operate within a crime cycle from preparation to monetization and exit.
- provide a sense of the processes and practices through which cyber crime occurs, including both technological and organisational pathways.

Methodology

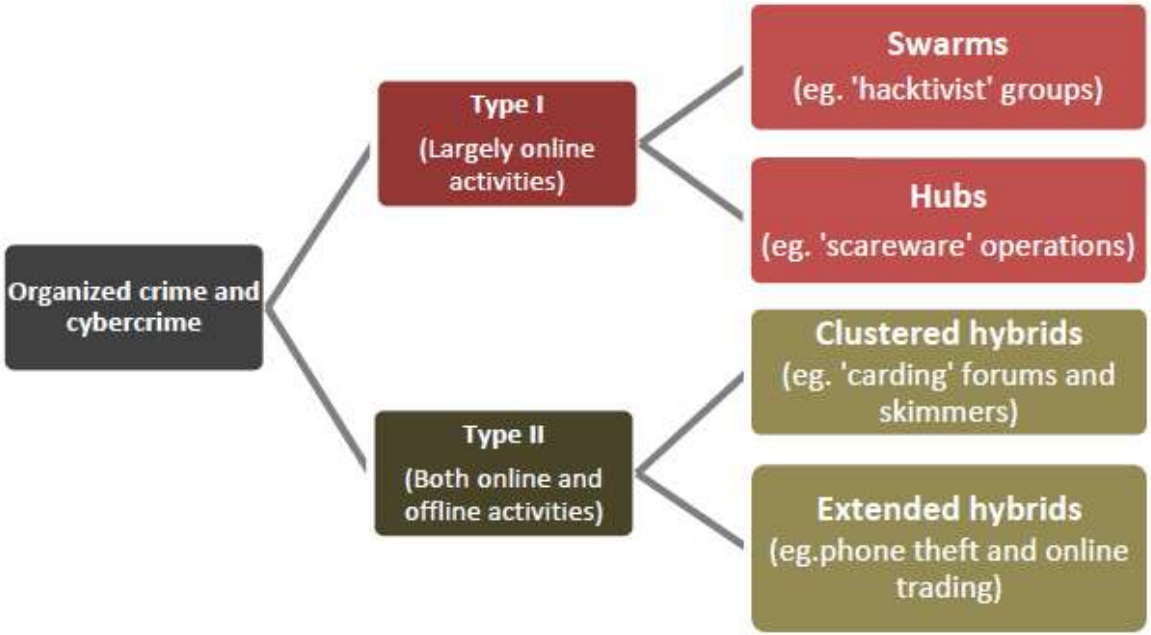
- Literature review
- Expert interviews

- Crime scripting

Cyber crime networks



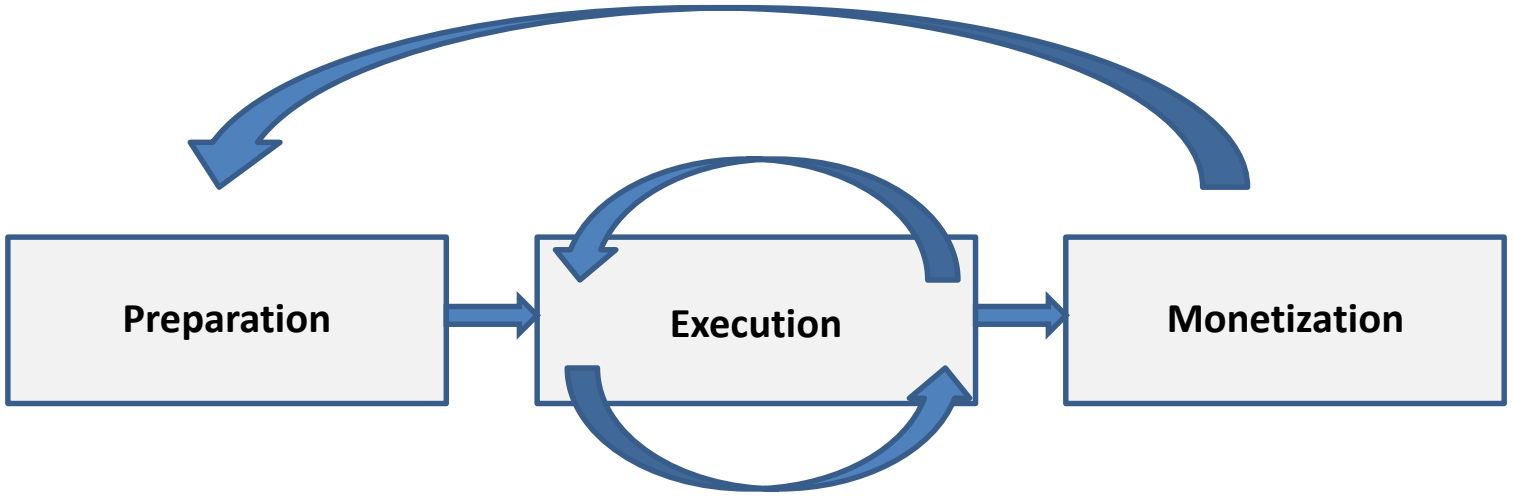
Structures of organised crime groups



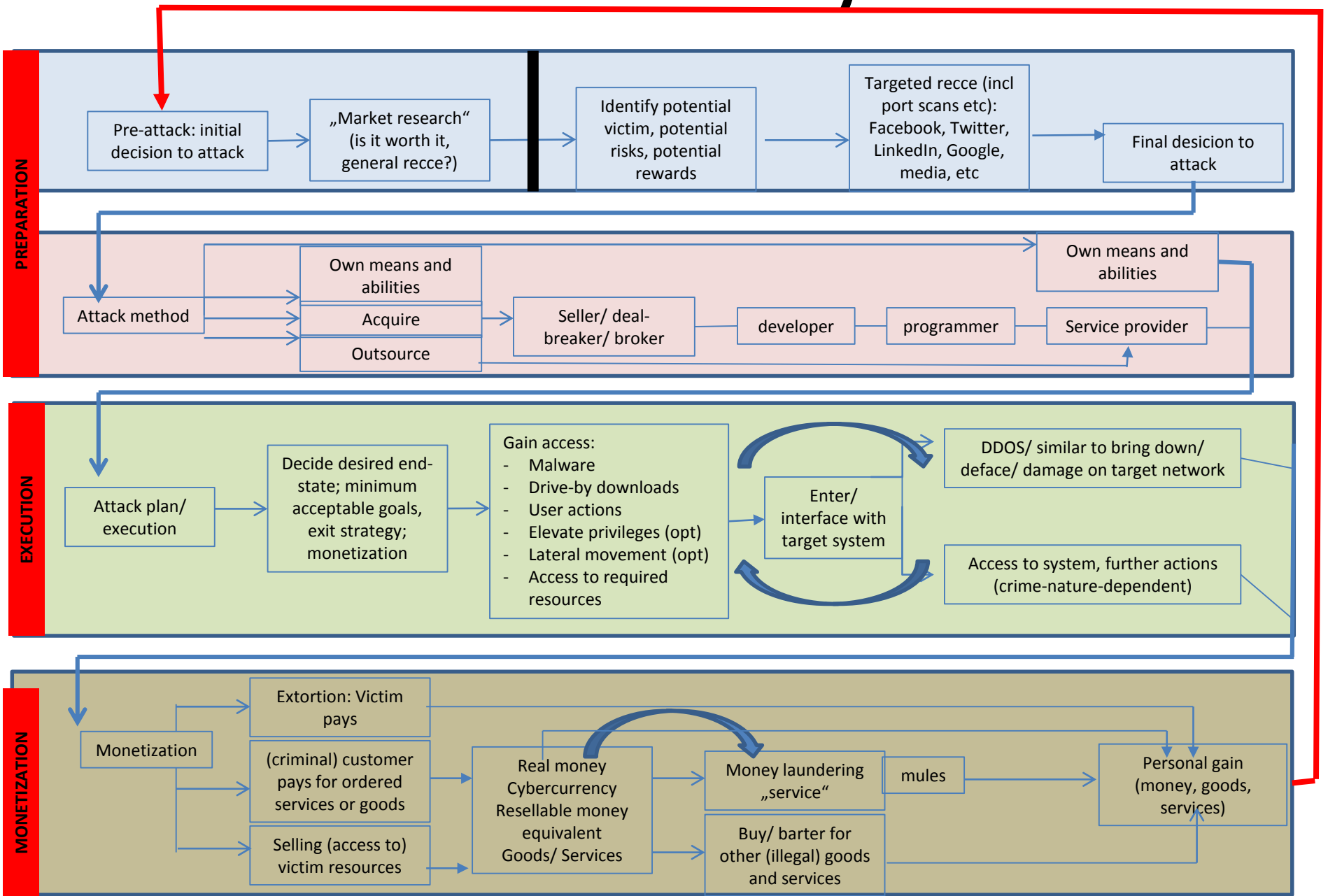
Source: BAE Detica/LMU

Cyber crime cycle

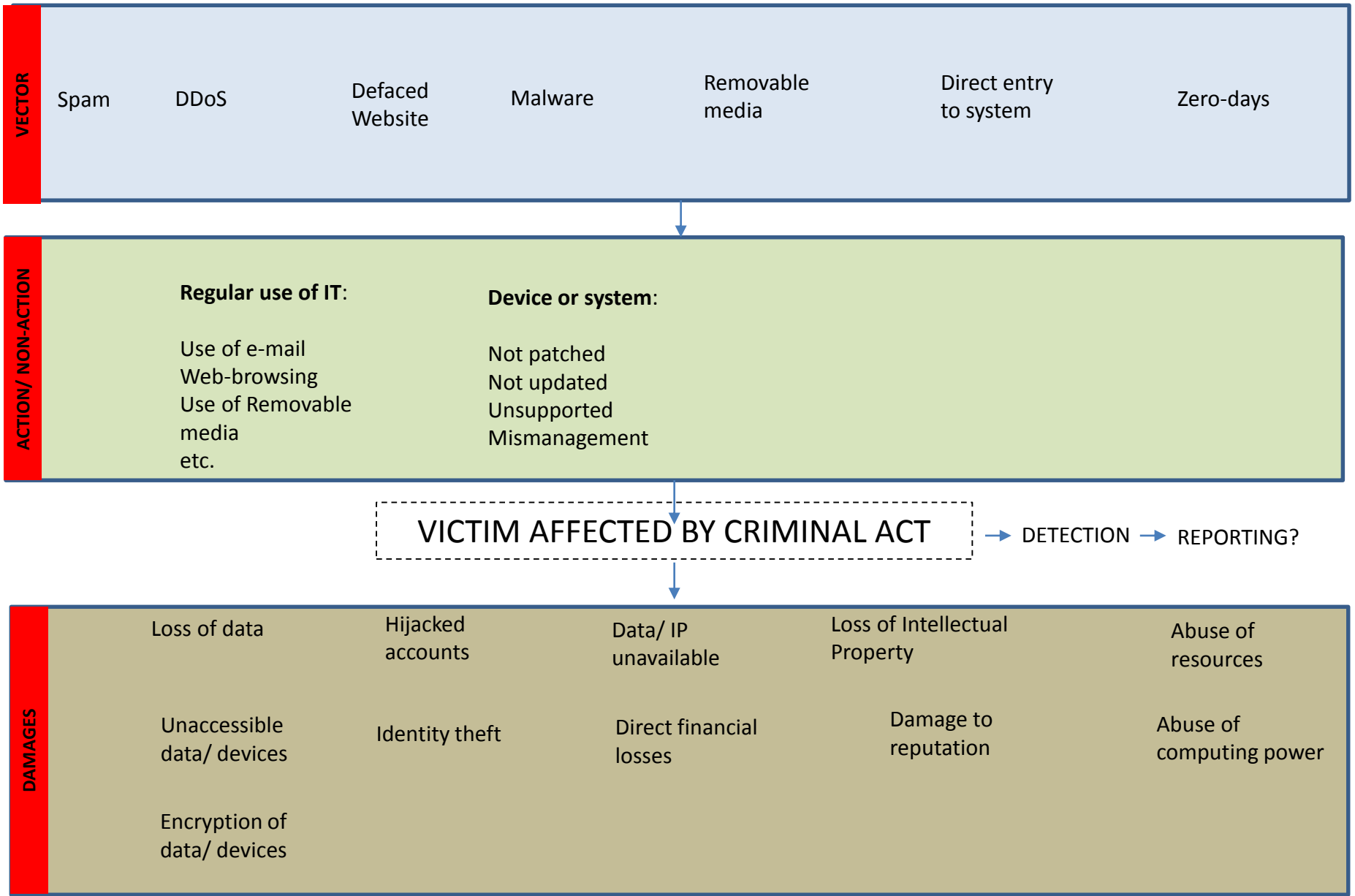
- **Preparation** (recce, prepare attack vector, …)
- **Execution** (establish foothold, move laterally, maintain presence, escalate privilegies, conduct multiple crimes, …)
- **Monetization** (real money, cybercurrency, trade, mules, …)



General crime cycle



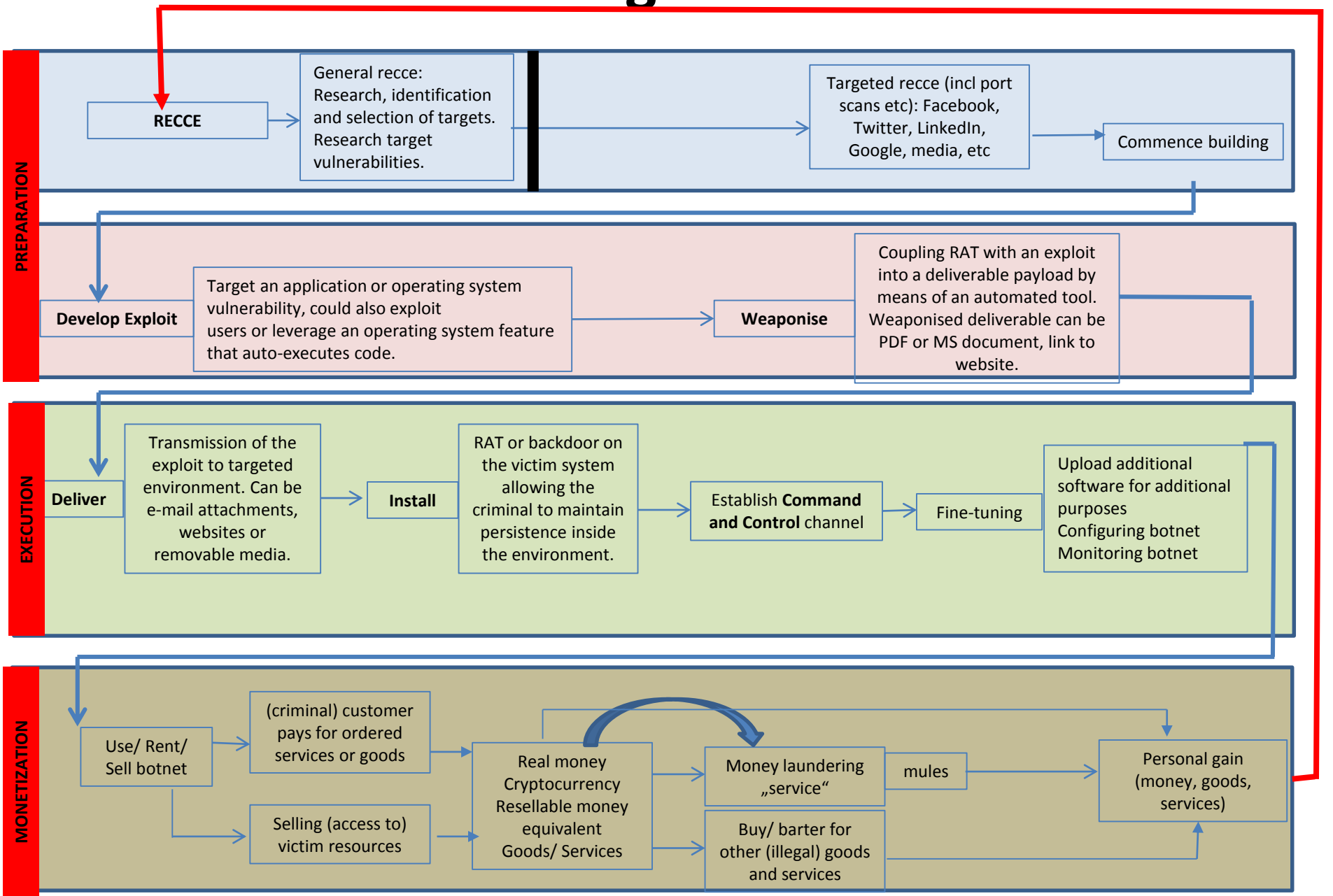
General victim journey



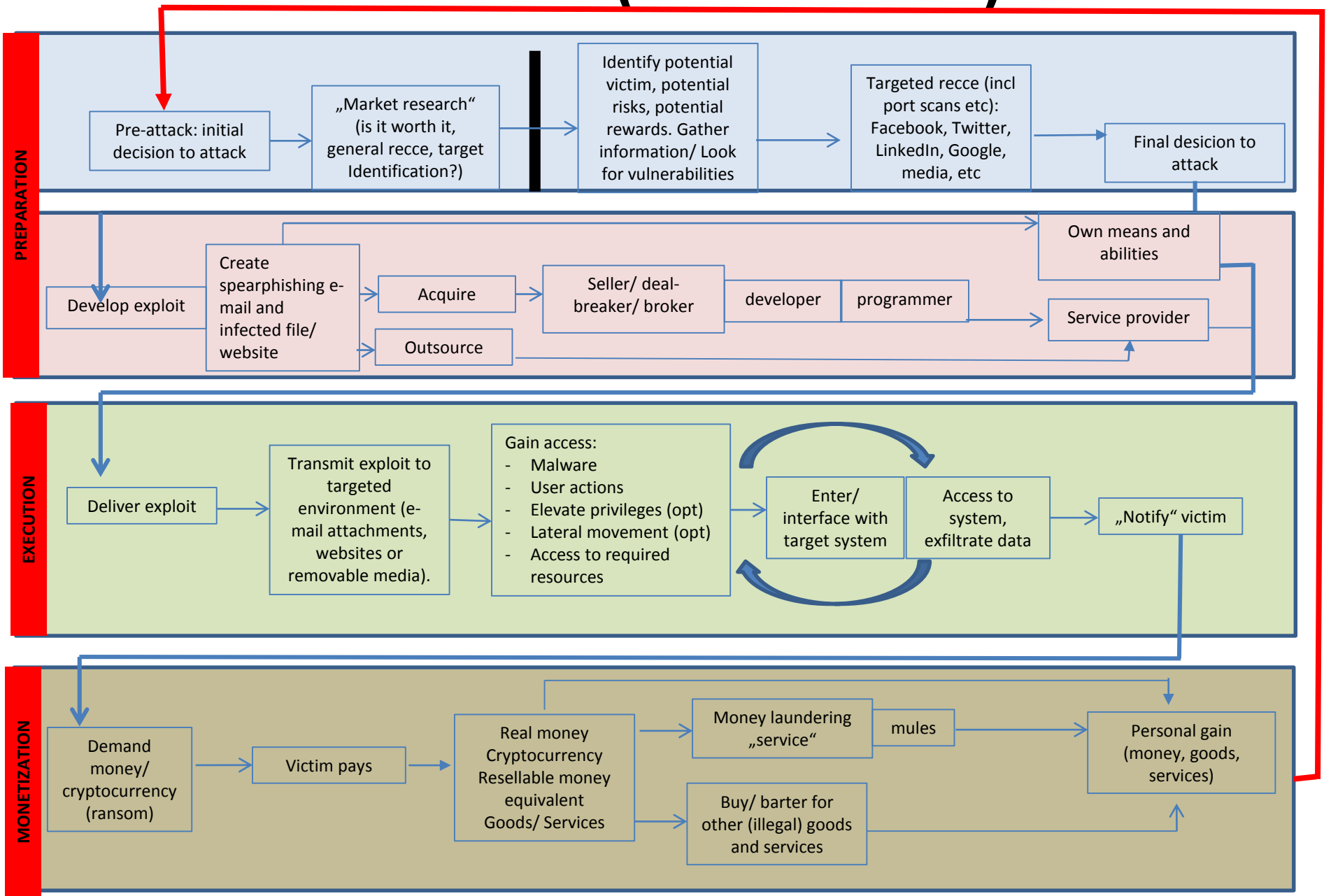
Journeys mapped

- Building a botnet
- Extortion (ransomware)
- Espionage (APT/ APA)
- Malware development/ 0-day exploit development
- VoIP attacks
- Cryptocurrency mining
- Crypto cracking/ DRM cracking
- Click fraud

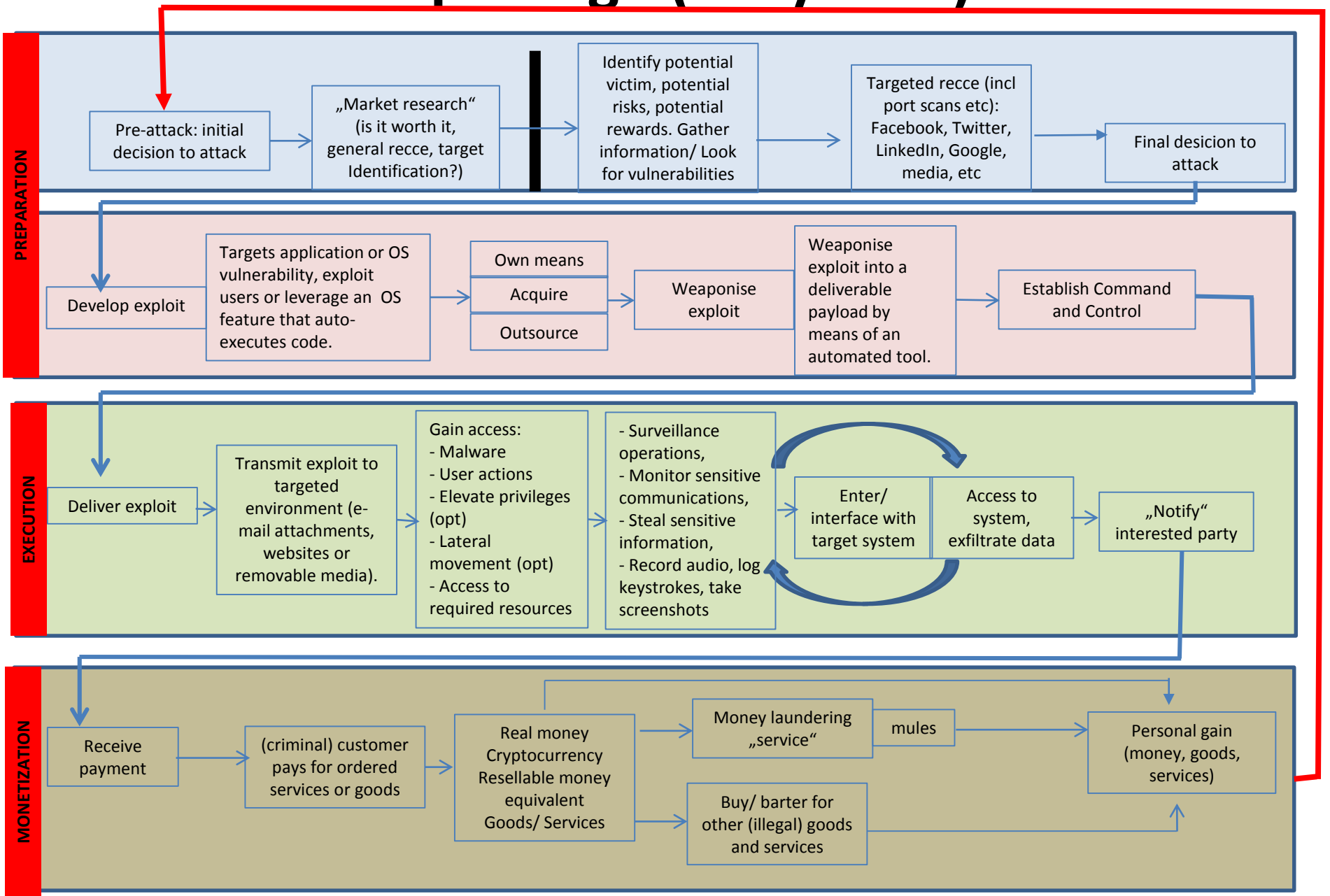
Building a botnet



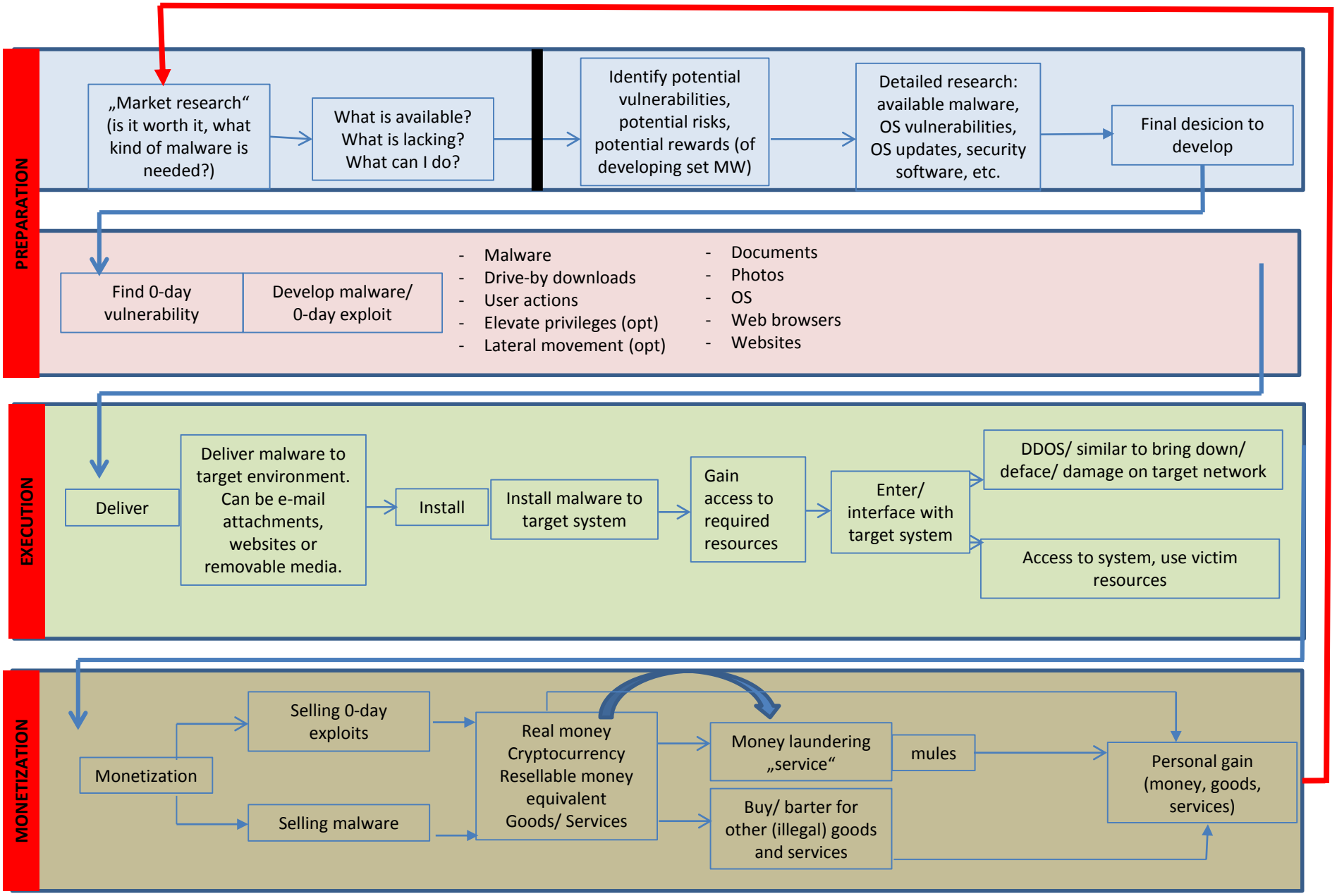
Extortion (ransomware)



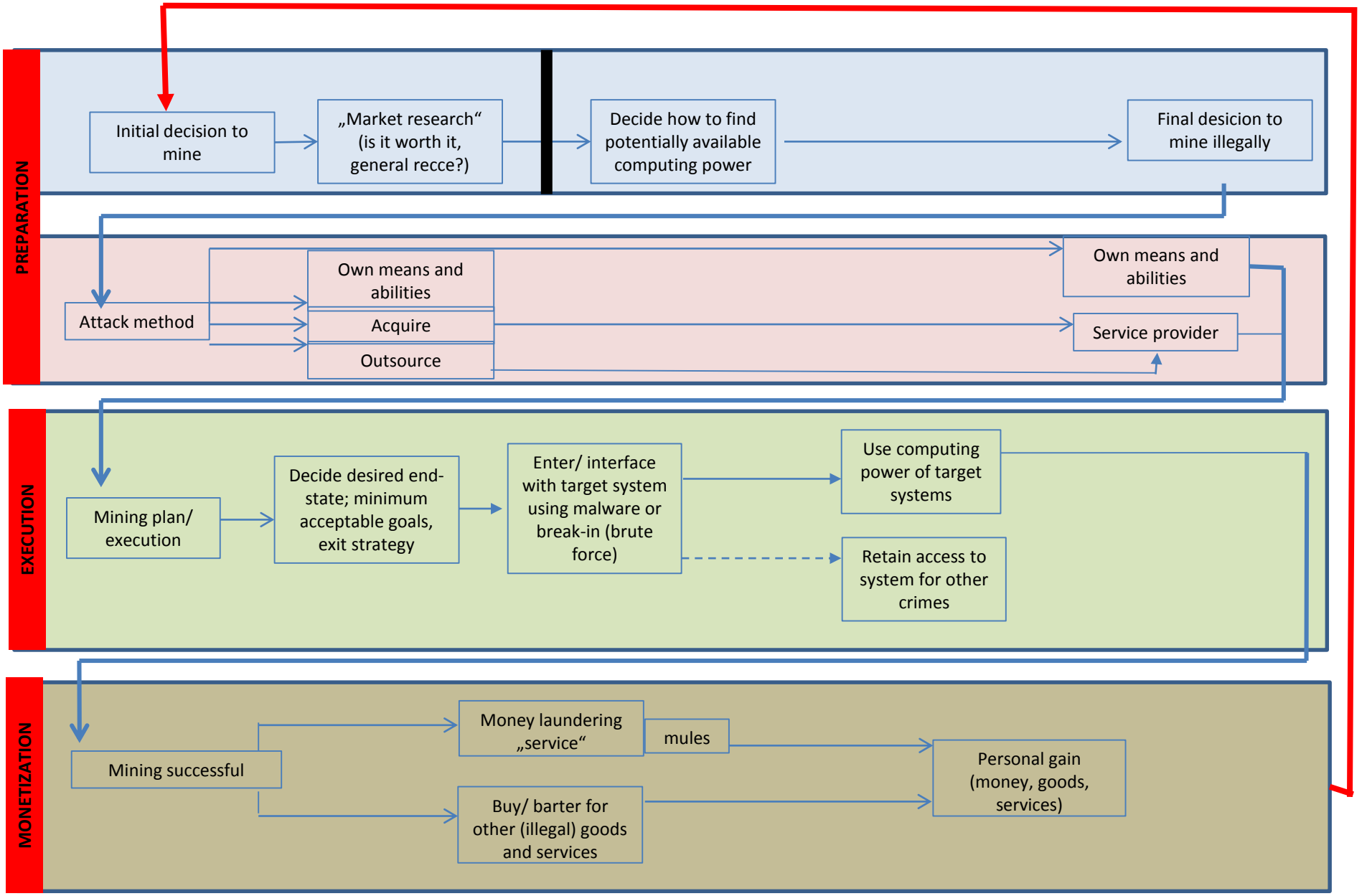
Espionage (APT/ APA)



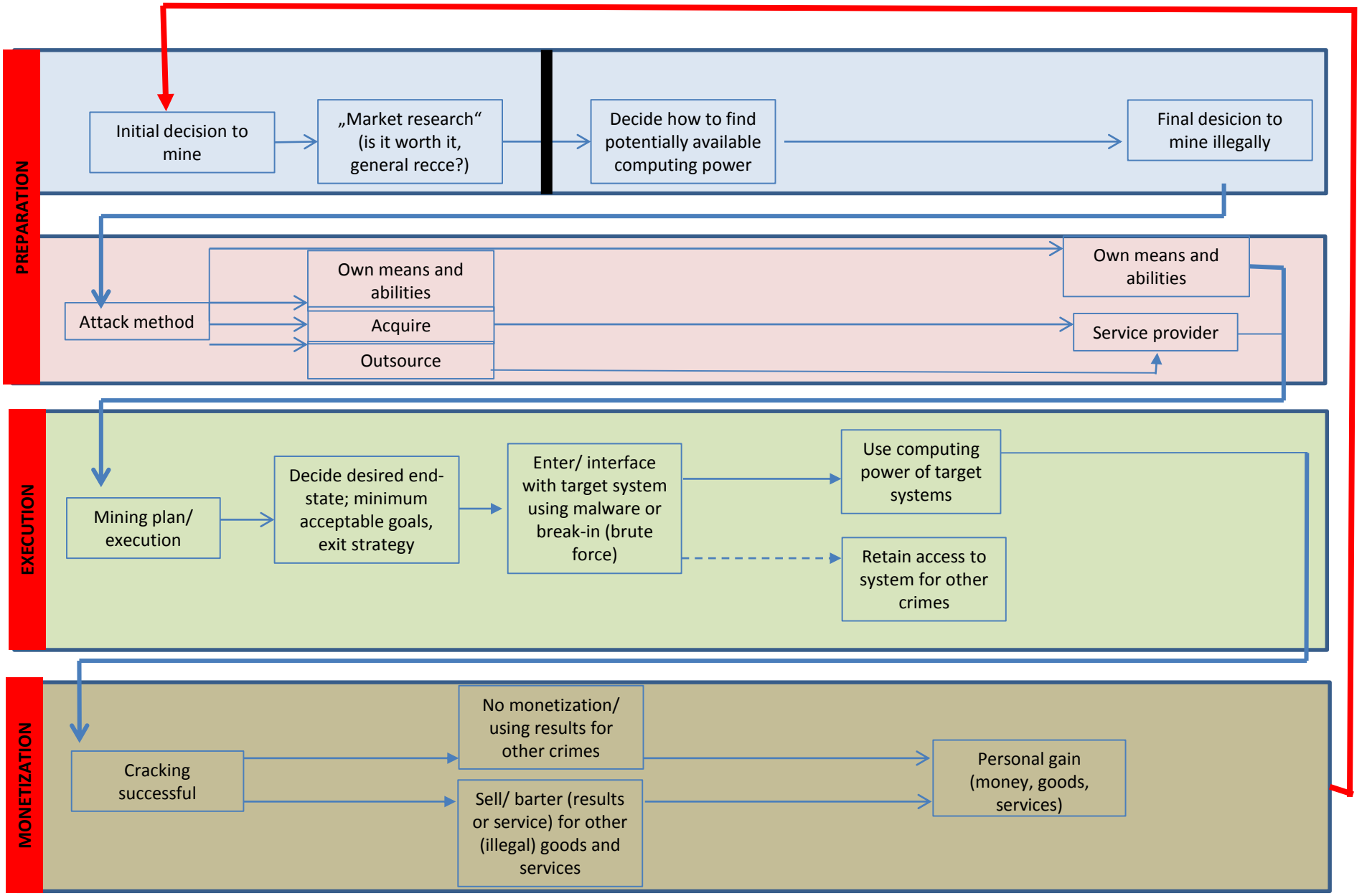
Malware development/ 0-day exploit development



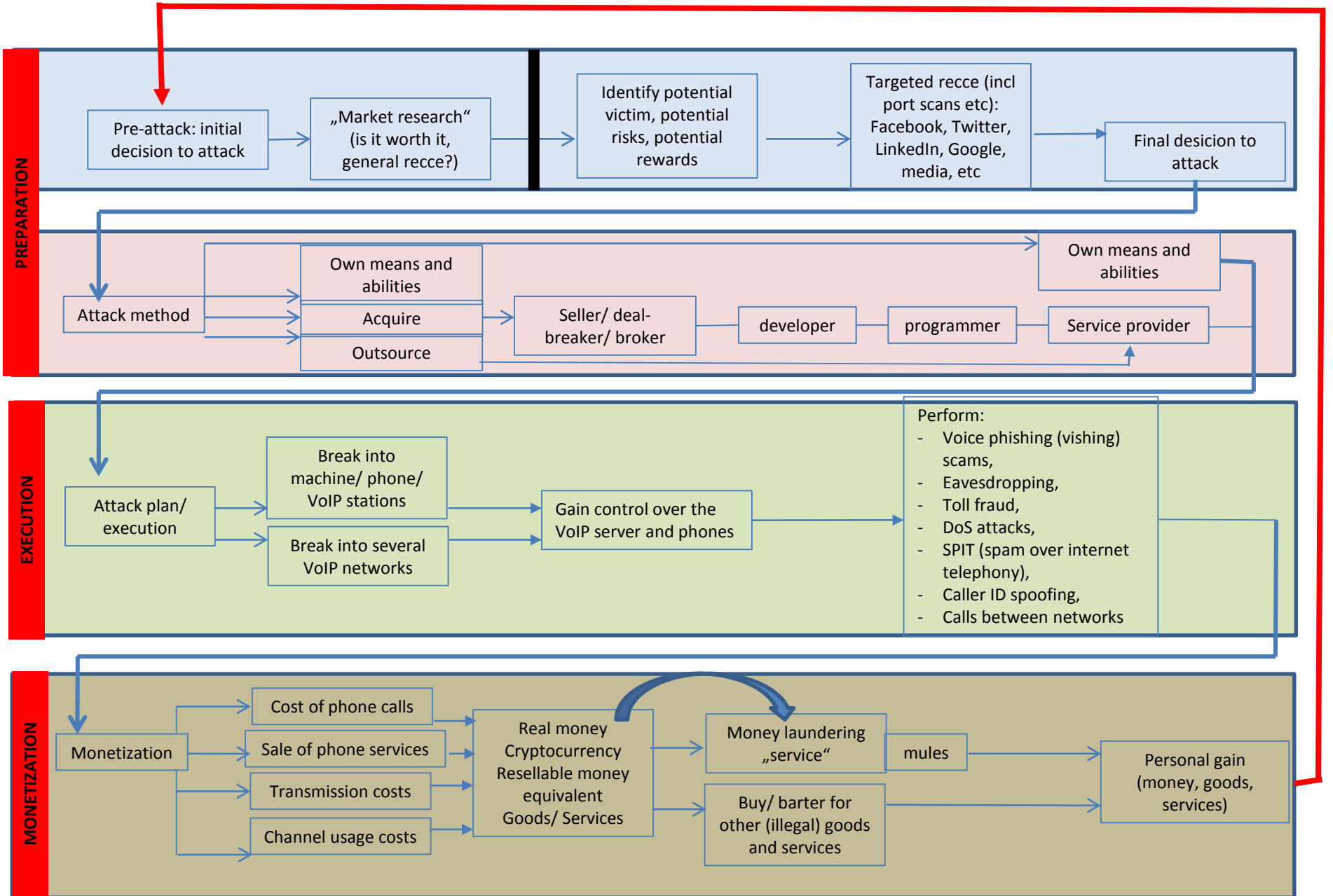
Cryptocurrency mining



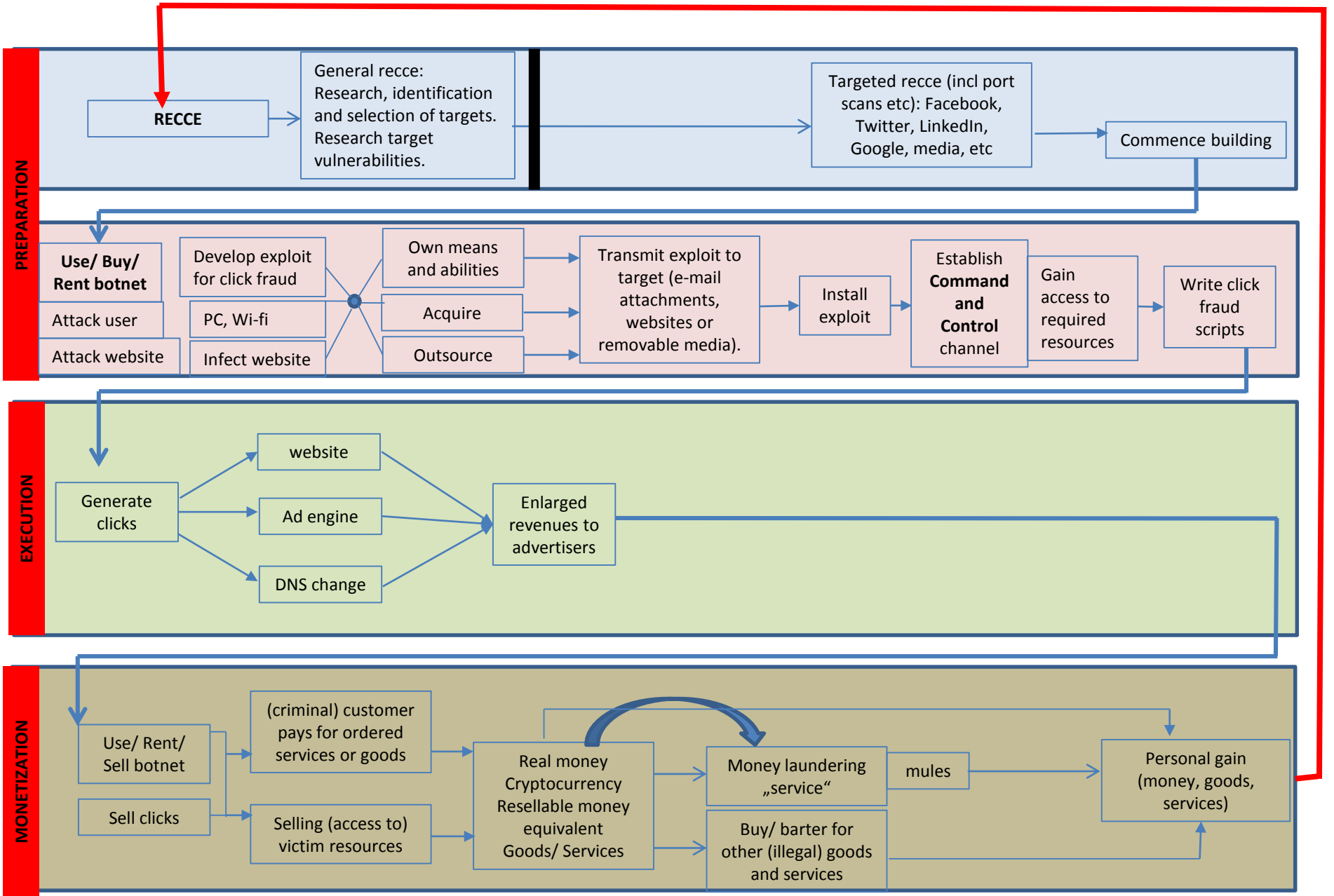
Crypto cracking/ DRM cracking



VoIP attacks



Click fraud


PREPARATION
RECCE
General recce: Research, identification and selection of targets. Research target vulnerabilities.
Targeted recce (incl port scans etc): Facebook, Twitter, LinkedIn, Google, media, etc
Commence building
Use/ Buy/ Rent botnet
Attack user
Attack website
Develop exploit for click fraud
PC, Wi-fi
Infect website
Own means and abilities
Acquire
Outsource
Transmit exploit to target (e-mail attachments, websites or removable media).
Install exploit
Establish Command and Control channel
Gain access to required resources
Write click fraud scripts
EXECUTION
Generate clicks
website
Ad engine
DNS change
Enlarged revenues to advertisers
MONETIZATION
Use/ Rent/ Sell botnet
Sell clicks
(criminal) customer pays for ordered services or goods
Selling (access to) victim resources
Real money
Cryptocurrency
Resellable money equivalent
Goods/ Services
Money laundering „service“
mules
Buy/ barter for other (illegal) goods and services
Personal gain (money, goods, services)

THANK YOU