Actors in cyber conflict

Rain Ottis, PhD

- „Thus it is said that one who knows the enemy and knows himself will not be endangered in a hundred engagements.“
  - Sun Tzu

Agenda

- Know the enemy
- Dave
- “Friendly“ forces
- Activism and hacktivism
- Cyber crime
- Cyber espionage
- Cyber terrorism
- Cyber warfare

Meet Dave

- Dave is in charge of designing, building, integrating, administering and troubleshooting all your systems.
- Dave works with you every day.
- Dave is sometimes lazy or incompetent.
- Dave is sometimes angry at you
- Dave is the most likely cause for a cyber incident in your organization

Friends or enemies?

- Commercial service providers
  - Mistakes
  - Following their own interests
- Government entities
  - Collects data, but why? How is it handled?
  - Surveillance
  - Forced collaboration

Activism and hacktivism

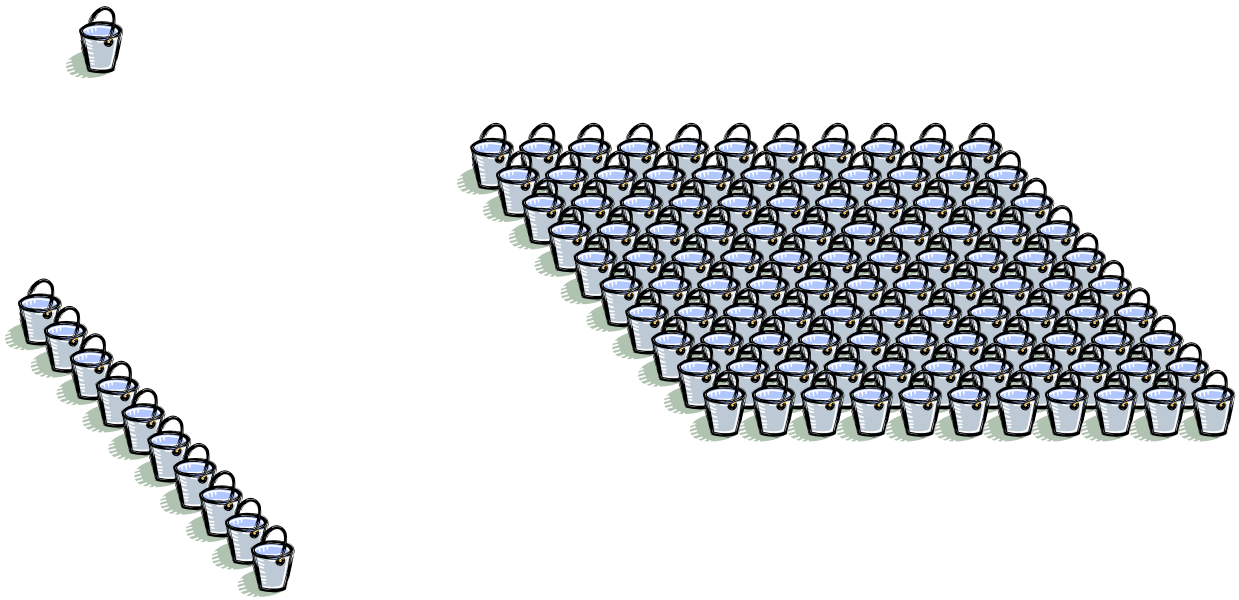
- Hacking + activism => hacktivism
- Ideological rationale, no personal gain
- Related terms
  - Electronic civil disobedience
  - Internet vigilantism
  - Patriotic hacking
  - “Cyber terrorism“?
- Benign or malicious?

Activism and hacktivism

- Cyber conflict and hacktivism
- 1999 – NATO and Kosovo
- 1999 – Chinese embassy bombing
- 2001 – Hainan Island incident
- 2007 – Estonia – Bronze Soldier riots
- 2008 – Russia-Georgia war
- 2009 – Operation Cast Lead
- 2013 – Syrian Electronic Army
- Anonymous & LulzSec

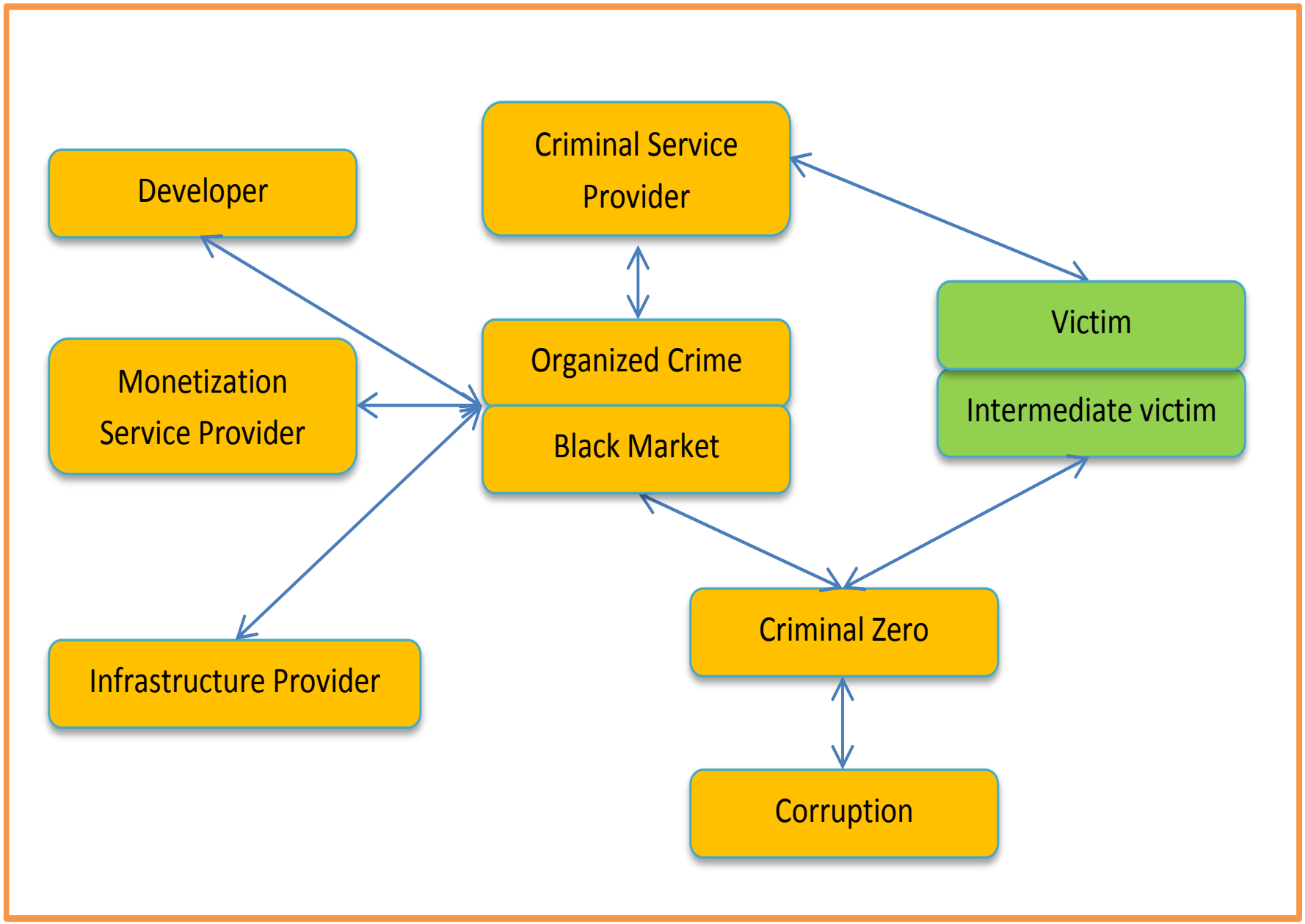
Estonia 2007

- What does a DDoS really mean?

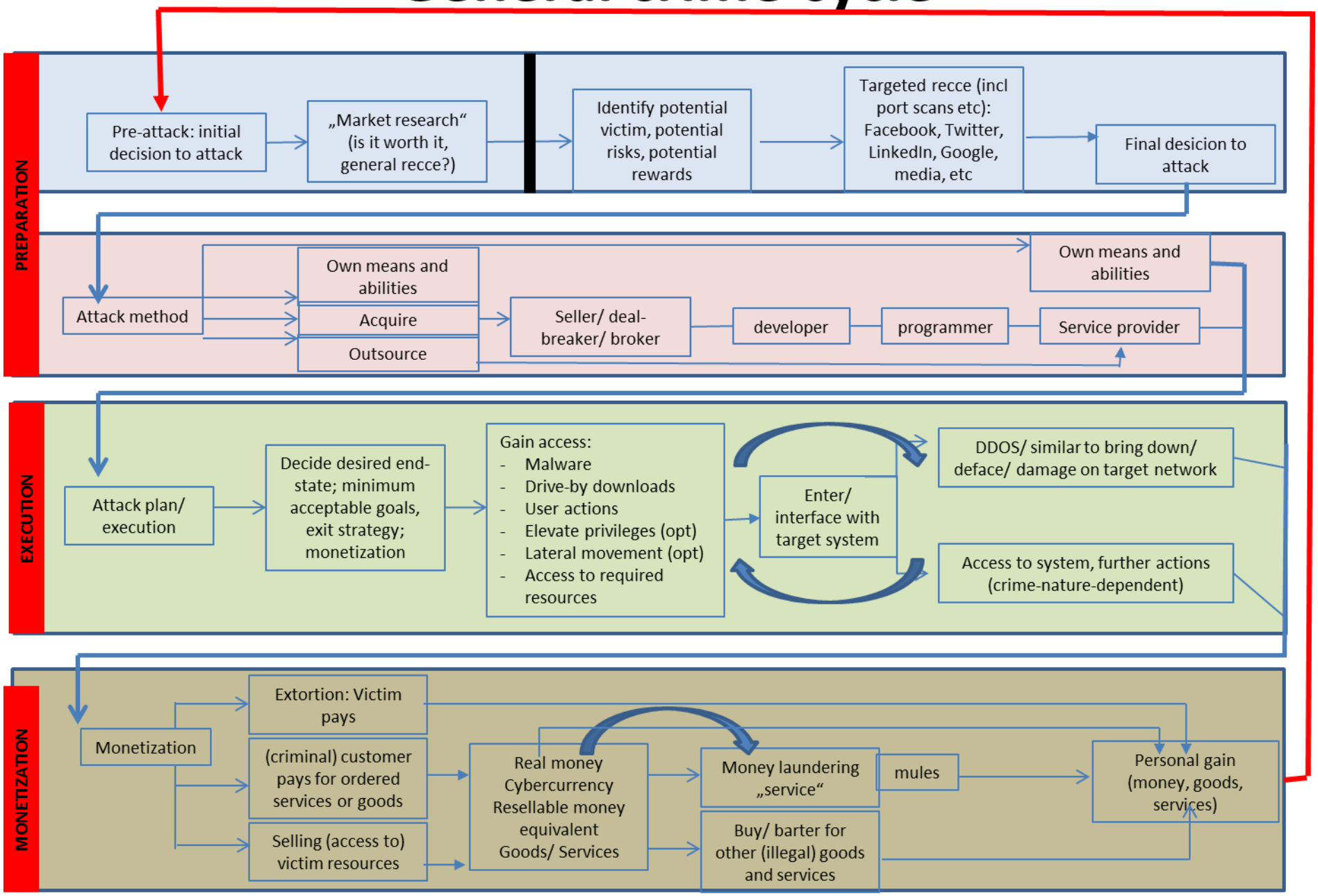


Cyber crime

- Exploiting the (logical) functionality of the Internet/IT in unintended ways that breach the (criminal) law
- Irrational
  - .. includes (most) parts of hacktivism
  - revenge, bullying, stalking, etc.
- Rational
  - Personal/organizational gain
  - Money (or equivalent)


Developer
Criminal Service Provider
Victim
Intermediate victim
Monetization Service Provider
Organized Crime
Black Market
Infrastructure Provider
Criminal Zero
Corruption

General crime cycle



Cyber crime

- Cyber crime vs cyber assisted crime

	Target: cyber	Target: non-cyber
Method: cyber	Defacing a website; DDoS; spreading malware	Remotely manipulating tram/train tracks to derail the vehicle
Method: non-cyber	Setting fire to a server room; stealing a laptop	Hitting someone with a laptop

Cyber crime

- Business models
  - Identity theft
  - Botnet trade
    - Extortion, spam, DDoS as a service, malware distribution, BitCoin mining, etc.
  - Malware trade
    - ZeroDay development, malware (kit) development, etc.
  - Ransomware
  - Etc.

Cyber espionage

- Individual vs organization vs state
- Targeted vs general purpose
  - Anything of interest
  - Key persons
  - Security (military, intel/CI, security forces) capabilities, procedures, equipment, etc.
  - R&D information (designs, data, prototypes, etc.)
  - Economic (resources, infrastructure, etc.)
  - Social and political assessments

Cyber espionage

- Internationally – de facto accepted (no law)
  - … as long as you don't get caught
- Nationally – state laws apply
  - Treason
  - Espionage
- Related topics: insiders, removable media, spear phishing, etc.
- Ghost Net, Unit 61398, PRISM, …

Cyber terrorism

- Theoretical threat, no examples yet.
- Systematic use of cyber attacks ..
- .. in order to cause fear (through death, destruction, etc.) ..
- .. in the civilian population ..
- .. to advance a political/ideological/religious goal.

Terrorist use of Internet/IT

- Propaganda
- Recruitment and fund raising
- Training
- Communication and coordination
- Reconnaissance
- Planning
- Executing attacks
- Recording

Problem?

Cyber warfare

- Sabotage – ? – armed conflict / war
- Legal paradigm
  - UN Charter (use of force, armed attack)
  - Various other international law documents and principles
  - Tallinn Manual
  - War, peace, and the everyday grey area in between

StuxNet

- Discovered 2010
- 4 Zero-days
- 2 stolen certificates
- MS Windows → Siemens PLC via Step-7
- Sensor feed hijack
- Control data corruption
- Physical destruction of the P1 uranium enrichment centrifuge

Military cyber operations?

- 2007 Israeli air strike against Syrian nuclear site (Operation Orchard)
- 2011 Iran hijacks US drone in mid-flight
- Plus all the operations that did not fail
  - … meaning – they are not publicly known

What to take from this?

- Not everyone on this list is going to attack you
- Analyze who your potential adversaries are and what would they want from you (+how?)
- Adjust your defensive profile to mitigate risks
  - Prevent, Detect, Respond, Recover (and Learn!)
- OODA loop – Observe, Orient, Decide, Act
- Velociraptor vs “All for one, one for all“
- Include failure in your plans

Questions