



# Active defence

Cosmin Ciobanu | ISO  
CTI-EU | Rome | 31 Oct 2017

European Union Agency for Network and Information Security



# Agenda



- 1** What is active defence & areas of applicability

---

- 2** Real cases of active defence

---

- 3** Active defence tools

---

- 4** Active defence strategies, methods & frameworks

---

- 5** Potential implications of active defence (legal)

---

- 6** The future of active defence

---

# What is active defence and what is not?



Active defence != hacking back

- Active defense involves the potential victim making things as difficult as possible for attackers, such as with the use of honeypots, false data, or tagged data, which if stolen can be used by investigators to trace the attackers TTPs (Ex. Deception, Beaconing).

The goal is to enhance the detection capabilities, slow & annoy attackers.

- Hacking back, on the other hand, involves accessing an attacker's computer or network in order to identify them, to cause damage or disruption, or to find or destroy stolen data.

# Active Defence tools



## Opensource

### Active defence harbinger distribution

<http://adhdproject.github.io/#!index.md>

### Modern honeypot network.

<https://threatstream.github.io/mhn/>

### Commercial tools:

There are around 10 vendors ( Canarytokens, Symetria, TrapX, CounterCraft, Symantec )...

# Active defence strategies, methods, frameworks



Detection as deception techniques:

<https://github.com/0x4D31/deception-as-detection>

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Application Shimming	Automated Collection	Data Compressed	Communication Through Removable Media
AppInit DLLs	AppInit DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Exploitation of Vulnerability	Command-Line Interface	Clipboard Data	Data Encrypted	Connection Proxy
Application Shimming	Application Shimming	Clear Command History	Create Account	Network Service Scanning	Logon Scripts	Execution through API	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Authentication Package	Bypass User Account Control	Code Signing	Credential Dumping	Network Share Discovery	Pass the Hash	Execution through Module Load	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol

# Legal implications



Engaging in AD is highly dependent on the context (ex. military implies mandate for such operation)

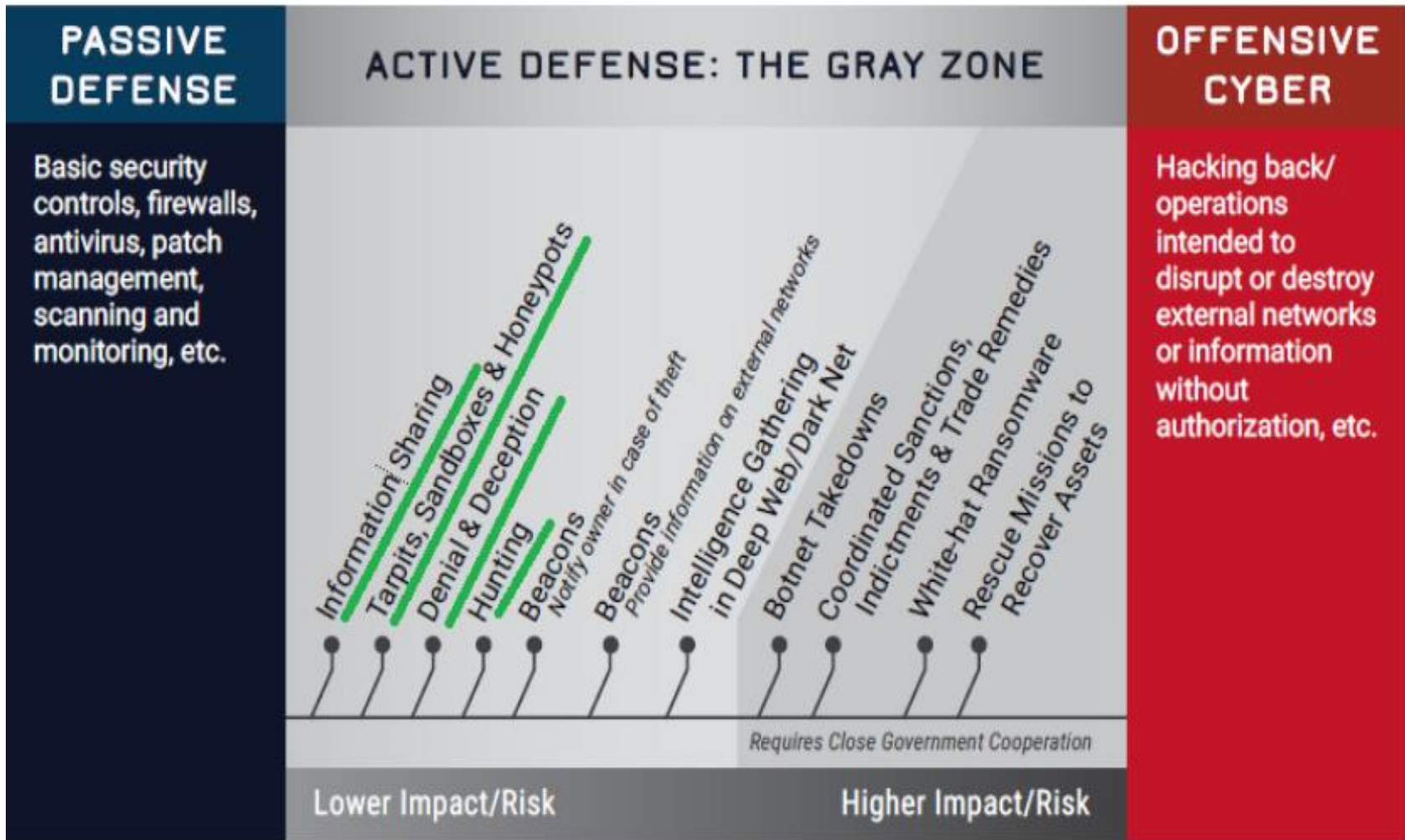
At the moment in the EU there is no legal framework for AD.

Also the terminology differs from sector to sector.

Ex. off US bill:

([Rep. Tom Graves](#)) proposed the "Active Cyber Defense Certainty Act (ACDC)" to amend US law to allow private entities, with mandatory reporting requirements to law enforcement, to conduct certain forms of hack-back to attribute breaches to the responsible individuals and prosecute them

# 50 shades of gray areas



[https://cchs.gwu.edu/gray-zone-active-defense-private-sector-against-cyber-threats&usg=AOvVaw1\\_T0DfdpAvAMvozDlfdSn](https://cchs.gwu.edu/gray-zone-active-defense-private-sector-against-cyber-threats&usg=AOvVaw1_T0DfdpAvAMvozDlfdSn)

# Conclusions



Where is active defence going ?

An unified terminology and definition needs to be established.

A more holistic approach for AD is required.

Concerns:


- Implementations
- Integration & Operationalization
- Costs & resources
- We might see ADaaS or DaaS 😊





# Thank you

 PO Box 1309, 710 01 Heraklion, Greece

 Tel: +30 28 14 40 9710

 [info@enisa.europa.eu](mailto:info@enisa.europa.eu)

 [www.enisa.europa.eu](http://www.enisa.europa.eu)

