

# CYBERCRIME DEPENDENCIES MAP

## EXPLANATORY NOTES

### CRIME-AS-A-SERVICE

Cybercrime covers a myriad of crimes, each of which often requires specialist skills, knowledge or tools. As such, few if any individuals can efficiently carry out a wide range of activities, and will instead specialise in a particular area in which they have specific expertise. When that individual requires access to a skill or tool that he lacks, he must then buy access to that service from another who is similarly specialised within that area.

It is this division of labour which drives the “crime-as-a-service” business model of the digital underground, promoting innovation and nurturing the development of greater skill and productivity. As a consequence, each actor within the digital underground, in order to carry out their own criminality, is dependant to some degree on the services provided by others.

It is accepted that in reality, multiple functions may be carried out by a single individual in which case there would be fewer interdependencies, however the **Cybercrime Dependencies Map (CDM)** reduces each product or service to its basic function, examines which other products and services that activity is dependent on and makes an assessment as to the level of that dependency. A service may have a high dependency on another, unable to function without it, or it may have a moderate dependency on another, able to function without it but at reduced capacity. Lastly access to another service may be

optional and merely facilitates or adds extra value. The CDM uses a traffic light system (red/amber/green) to depict the level of dependency (high/moderate/optional).

The CDM highlights several areas useful to law enforcement. Firstly it identifies which services or products an individual may be using thereby potentially identifying alternative investigative approaches or possible associates. Furthermore it identifies which services have either the highest amount of dependencies or which are highly depended on by other service thereby suggesting investigative priorities.

### EXAMPLE – COUNTER ANTI-VIRUS

In the example to the right, we see **Counter Anti-Virus** services. Both **Crypting** and **Coding** have a medium (Amber) level of dependency on **Counter Anti-Virus** services meaning that they are able to function without access to these services, but are less effective without them.

All three services have some dependency on one or more **Cross Crime Factors** – products or services that are used ubiquitously. Where such a dependency is medium/high, its icon is displayed in the bottom section. Both **Crypting** and **Coding** have a dependency on **Forums** in order to conduct their business whereas **Counter Anti-Virus** has a dependency on **Hosting** and **Domain** services.

