Darknet

> ***‘We must step up cooperation and the sharing of expertise and reinforce our cyber forensics and ability to monitor the Darknet – which enables crimes such as payment fraud, the sale of firearms and counterfeit documents, human trafficking, illegal immigration, dissemination of the worst kind of images and content and more.’***
>
> European Commissioner Julian King, Security Union, 14 May 2018

Online Module: Executive Summary

The darknet is the set of darknets used for illicit activities. These darknets exist in a part of the internet that is intentionally hidden, known as the dark web. They can be accessed only by using software designed for the purpose, such as Tor, I2P and Freenet, which enable users to access the cryptographically hidden sites.

Darknets are increasingly being used to conduct criminal activities because of the anonymity that they provide to their users. In particular, sites called markets or marketplaces are used to trade in almost every kind of criminal product and service. These include illicit goods (such as drugs and firearms), stolen items (such as credit cards, passports and other documents), fake documents (such as passports), illicit content (such as underage sexual content and illegally copied software) and cybercrime enablers (such as cracking tools, hacking services, malware and ransomware).

The darknet is vast – Tor alone has about two million users daily. Although law enforcement agencies have successfully taken down many major markets in recent years, such as Silk Road, AlphaBay, Wall Street Market and Valhalla, the darknet continues to host many others. As of June 2019, these markets listed between 10,000 and 40,000 drug offers.

The Darknet module is intended for people new to the darknet, or with a small amount of knowledge and who want to know more. It is designed to provide a general understanding of the darknet, the way criminals use it and how technology supports them. After completing the module the user should be able to explain the darknet to others, to recognise how someone might be involved in darknet crime, and to know some of the investigation tools needed to manage the threats.

The module consists of an introduction, eight topic chapters and a glossary of darknet-related terms and abbreviations. In the My Progress section, users can assess their levels of understanding of each of the topics by considering a selection of questions and true/false statements.

The individual chapters are:

1. **Introduction**
2. **Criminal Methodology:** This chapter describes how a darknet criminal might operate by presenting a fictional case that ties together elements from the following chapters.
3. **Introduction to the Internet:** The darknet relies on some key concepts of the internet. This chapter discusses how the internet has been constructed and how information is shared.
4. **Concepts:** The many terms used to describe the darknet and related areas are detailed in this chapter.
5. **Encryption Tools:** Encryption is a key part of all darknet crime. This chapter provides the main terms and tools used by darknet criminals to conceal their activities, communicate with other criminals, and describe how they buy and sell items anonymously.
6. **Tor Network:** This chapter provides an overview of 'onion routing' as well as the key parts of setting up and running a Tor Browser and how to manage Tor from your mobile device.
7. **Searching the Dark Web:** Navigating your way around hidden services and understanding the criminal environment are hugely challenging. This chapter provides the tools necessary to manage intelligence investigations and the additional elements to look for.
8. **Cryptocurrencies:** This chapter covers the basics of what a cryptocurrency is, how it works, how it can be used to pay for goods and services and how it can be laundered. It includes Bitcoin and various alternative cryptocurrencies.
9. **International Cooperation:** Darknet crime has international reach. Even simple drug investigations can turn into multinational cross-border situations. In this final chapter some guidance is offered on what to expect and how to manage these scenarios.