Read Chapter 11: Inside the Digital Underground in the Future Crimes book. Prepare responses to the following questions.

1. What is the Silk Road in the context of cybersecurity. Research this network and present notable findings.

In the context of cybersecurity Silk Road is like the Dark Web. It was a massive online criminal marketplace that was hidden from public view where any and all manner of illicit goods were for sale in a secret Web: “If you can smoke it, inject it, or snort it, there’s a good chance Silk Road has it.”

Named after the ancient Asian trading route, Silk Road was a place where buyer and seller could anonymously come together to exchange goods and services in a dizzyingly large emporium of contraband. Known as the “eBay of drugs and vice,” Silk Road offered every possible illicit product imaginable, neatly organized by category such as drugs or weapons, each with accompanying photographs and descriptions. Other items included stolen bank accounts, stolen credit cards, counterfeit currency, computer viruses, keystroke loggers, compromised Facebook accounts, tutorials on hacking ATMs, child pornography, and even hit men for hire. Under the category of forgeries, there were more than two hundred listings for fake driver’s licenses, passports, Social Security cards, utility bills, credit card statements, diplomas, and other identity documents. However, the core of silk road was drugs and controlled substances including crack cocaine, LSD, ecstasy, Molly, marijuana, crystal meth, ’shrooms, syringes, precursors, steroids, stimulants, and a panoply of prescription pills,

Silk road was mastered by Dread Pirate Roberts (DPR) was the most wanted man in the digital underground.

2. What is TOR? How does it work? Prepare a thorough response to the workings of TOR, including origin, operation, statistics and use cases.

TOR (The onion router) is an encryption and obfuscation software that allows all parties buying and selling illicit goods could remain anonymous, only identifying themselves via a chosen made-up screen name.

Tor works by routing your Web connections through a worldwide array of five thousand computer servers in order to hide the source and destination of your connection. Without Tor, your online activities are easy to trace, and every time you visit sites like CNN or ESPN.com, you reveal your location and home network. Bad guys don’t like this; it makes them easy to catch. So instead, they obfuscate and route their traffic through services like Tor.

Tor’s hidden services have their own domain names, which end in an “onion” suffix. This system of dual anonymity allows both buyer and seller on Silk Road to transact by visiting a unique hidden domain (in the case of Silk Road, silkroadvb5piz3r.onion) without ever revealing their true identities to each other.

Tor was originally created and funded as a project of the U.S. Naval Research Laboratory in 2004, with backing from the Electronic Frontier Foundation and the State Department as a means of helping overseas political dissidents and democracy activists safely organize and communicate with one another. There are any number of completely legitimate uses for Tor, and those behind the Great Firewalls of China, Iran, and elsewhere routinely depend on it to access everything from Facebook to the New York Times. Tor is also increasingly being used by journalists to securely communicate with sources and whistleblowers, such as those within the WikiLeaks community.

A 2013 study of forty thousand hidden Tor sites found that nearly 50 percent were involved in illicit activities such as selling stolen credit cards, hacked accounts, weapons, drugs, and child pornography. Some security and law enforcement experts privately estimate that as much as 85 percent of Tor’s hidden services may be unlawful, with the rate of criminal adoption far outpacing that of privacy activists. As of early 2014, the Tor software has been downloaded nearly 150 million times and is used by two million people daily. Assuming the more conservative figure of 50 percent illicit use, that means every day 300,000 criminals are getting up and going to work on the digital underground using Tor’s hidden services.

3. What is Metcalfe's law? As per the law, how valuable are the following: LinkedIn, Instagram, Etsy and TikTok?

According to Metcalfe’s law, the value of a telecommunications network is proportional to the square of the number of users connected to the system; as such, the threat from a fully networked and anonymous criminal workforce is great.

They are very valuable as they have a great number of users.

4. Research statistics on the Deep Web and present notable findings.

Shockingly, the Deep Web is a massive five hundred times larger than the surface Web you use and search every day. While the Deep Web contains seventy-five hundred terabytes of information, the Googleable universe contains a paltry nineteen terabytes. According to a study published in Nature, Google captures no more than 16 percent of the surface Web and misses all of the Deep Web. As a result, when you search Google, you are only seeing 0.03 percent (one in three thousand pages) of the information that actually exists and would be available online if you knew how to get it. In other words, a Google search misses 99 percent of the World Wide Web’s data.

– The Deep Web contains 7500 Terabytes of information. The Surface Web, in comparison, contains 19 terabytes of content.

– The Deep Web has between 400 and 550 times more public information than the Surface Web.

– More than 200,000 Deep Web sites currently exist.

– Together, the 60 largest Deep Web sites contain around 750 terabytes of data, surpassing the size of the entire Surface Web 40 times.

– The total quality of the Deep Web is 1,000 to 2,000 times greater than the quality of the Surface Web.

– 550 billion individual documents can be found on the Deep Web compared to the Surface Web’s 1 billion individual documents.

– 95% of the Deep Web is publically accessible, meaning no fees or subscriptions.

The Deep Web is only getting bigger – it is the largest growing category of new information on the Internet.

5. What are the categories of content on the Deep Web? The chapter presents an excellent summary of categories that you may use.

* The content of your personal email accounts
* The content of your social media accounts
* The content of your online banking accounts
* Data that companies store on their private databases
* Content contained within scientific and academic databases
* Medical records
* Legal documents

6. Credit card theft is a burgeoning form of cyber attack. What are recent statistics on credit card theft?

<https://shiftprocessing.com/credit-card-fraud-statistics/>

7. How does Bitcoin work? Prepare a thorough response highlighting origin, operations, and scope.

Bitcoin, a decentralized peer-to-peer digital form of money. Bitcoins were invented in 2009 by a mysterious person (or group of people) using the alias Satoshi Nakamoto. The coins are created or “mined” by solving increasingly difficult mathematical equations, requiring extensive computing power. The system is designed to ensure no more than twenty-one million Bitcoins are ever generated, thereby preventing a central authority from flooding the market with new Bitcoins. Most people purchase Bitcoins on third-party exchanges with traditional currencies, such as dollars or euros, or with credit cards.

People can send Bitcoins to each other using computers or mobile apps, where coins are stored in “digital wallets.” Bitcoins can be directly exchanged between users anywhere in the world using unique alphanumeric identifiers, akin to e-mail addresses, and there are no transaction fees. Anytime a purchase takes place, it is recorded in a public ledger known as the “blockchain,” which ensures no duplicate transactions are permitted. Bitcoin is the world’s largest crypto currency, so-called because it uses “cryptography to regulate the creation and transfer of money, rather than relying on central authorities.”

Bitcoin acceptance is growing rapidly, and it is possible to use Bitcoins to buy cupcakes in San Francisco, cocktails in Manhattan, and a Subway sandwich in Allentown. They can also be used to purchase a new Tesla Model S, to pay your DIRECTV bill, to sign up with OkCupid, or even to book a ticket on Richard Branson’s upcoming Virgin Galactic space flight.

8. The chapter talks about Crime-as-a-Service. What kinds of criminal activities are available for service online?

Crime as a Service (CaaS) is the new business model and allows all or part of an offense to be carried out by others, while the crime entrepreneur who organized and invested in the scheme is ensured the profit. Just as large corporations are increasingly using Software as a Service to carry out their enterprise operations beyond their core competencies, so too are criminals.

Criminal activities available online include drugs, DDoS Kits, phishing kits, malware, ransomware, fake driver license, pirated content and so on.

9. What is a Remote Access Trojan (RAT)? How is it different from a regular Trojan? Where are RATs being used?

Remote Access Trojans are programs that provide the capability to allow covert surveillance or the ability to gain unauthorized access to a victim PC. RAT is different from a regular Trojan b/c it gives a complete anonymous access. This Trojan can give an attacker full control over your computer via a remote network connection. Its uses include stealing your information or spying on you. This is different from a regular Trojan, a type of malicious code or software that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general inflict some other harmful action on your data or network.

RAT gave its developers complete and total control of an infected machine’s functions. As a result, one could capture keystrokes, steal passwords, launch denial-of-service attacks, hijack Facebook accounts, and install additional malware on the affected system. Worse, it was the tool of choice for would-be stalkers because it allowed its masters to remotely turn on any computer’s microphone and camera to capture any audio and video in its field of view, without giving any notice

10. Research Advanced Persistent Threats. Mention any three.

As the name "advanced" suggests, an advanced persistent attack (APT) uses continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences. They are also designed in a custom way and can use zero-day exploits making them hard to detect.

Examples: <https://www.cybereason.com/blog/advanced-persistent-threat-apt>