Read Chapter 2: A Gathering Storm and Chapter 3: Moore's outlaws in the Future Crimes book. Prepare your responses to the following questions.

1. In Chapter 2, the author describes three SCADA breach incidents. Be prepared to discuss these.

In 2011, Local water treatment facility, hackers breached the south Houston, Texas water and sewer department, they repeatedly turned of and turned on a pump causing it to fail. Hack was traced back to Russia.

In 1998, Federal aviation administration control tower in Worchester, a local teenager used his knowledge of computing to server communications between inbound aircraft and the tower, and even turned off the runway lights for approaching aircrafts.

In 2001 in Australia, a hacker attacked the sewage treatment plant, he gained control of the facility industrial control systems and cause millions of litres of raw sewage to spill out into the local parks, it destroyed significant amount of marine life and was an environmental threats to local residents.

2. Research three more SCADA breach incidents from online/other sources.

<https://consultingstl.com/recent-industrial-scada-attacks/>

<https://threatpost.com/insecure-scada-systems-blamed-in-rash-of-pipeline-data-network-attacks/130952/>

https://krebsonsecurity.com/tag/scada/

3. Summarize the threats to the US electrical grid from (a) hackers and (b) terrorists. Describe the incidents provided in Chapter 2.

US energy grid is one of the most complex in the world, they are always under attack from terrorist who are trying to carryout waves of cyber-attack against the US network of both govt and critical infrastructures e.g. al Qaeda

Hackers are also trying to exploit and expose the vulnerabilities of SCADA and other critical infrastructure e.g. conference in Germany showing how to take full control of industrial infrastructures in the gas, chemical and energy industries.

4. What is the Shodan database. Research it and provide key findings.

Shodan is the world’s first search engine for internet-connected devices. Use it to discover which of your devices are connected to the internet.

<https://www.csoonline.com/article/3276660/what-is-shodan-the-search-engine-for-everything-on-the-internet.html>

Shodan is the search engine for everything on the internet. while google and other search engines index only the web, Shodan indexes pretty much everything else — web cams, water treatment facilities, yachts, medical devices, traffic lights, wind turbines, license plate readers, smart tvs, refrigerators, anything and everything you could possibly imagine that's plugged into the internet (and often shouldn't be).

Shodan collects data mostly on web servers (http/https - port 80, 8080, 443, 8443), as well as ftp (port 21), SSH (port 22), telnet (port 23), SNMP (port 161), IMAP (ports 143, or (encrypted) 993), SMTP (port 25), sip (port 5060), and real time streaming protocol (rtsp, port 554). the latter can be used to access webcams and their video stream.

it was launched in 2009 by computer programmer john matherly, who, in 2003, conceived the idea of searching devices linked to the internet. The name Shodan is a reference to Shodan, a character from the *system shock* video game series.

5. What are sources of cyber threats? Page 31 includes a cast of characters as sources. Provide examples.

These includes nation states, neighborhood thugs, transnational organized crime groups, foreign intelligence services, hacktivists, military personnel, cyber warriors, script kiddies, state sponsored proxy fighters etc.

6. Why does the author call cyberwarfare asymmetric?

Because the defender must build a perfect wall to keep out all intruders, while the offense needs to find only one chink in the armor through which to attack.

7. Research any one full-service cybercrime organization. What services do they offer?

<https://www.cyberpolicy.com/cybersecurity-education/5-cybercrime-groups-making-organizations-uneasy>

The level seven crew: [https://en.wikipedia.org/wiki/Level\_Seven\_(hacking\_group)](about:blank)

8. The book describes the hacking group, Anonymous, in some detail. How does LulzSec differ and compare to them?

Both hacking groups are hacktivists and they represent one of the most influential and powerful groups in cyberspace. Anonymous views itself as hacking for good and has taken on a wide variety of social causes. They have combated criminal organizations and injustice. LulzSec also go after the social data leaked by government officials. The group even demonstrated its power to go after the FBI.

9. List examples from the book that describe how terrorists are using cyberspace.

Terrorists are using cyberspace to recruit new members, use it to finance their crimes through online fund raising, communicate clandestinely and disseminate propaganda, use it to learn new techniques and skills to make them more effective

10. List examples from the book that describe Chinese activities in cyberspace that are malicious.

F-35 , China steals important technological blueprints from different countries

11. Chapter 3 is called Moore's outlaws. This title is a play on the famous Moore's law. What is Moore's law? What are its implications?

Moore’s law: The number of transistors per square inch on an integrated circuit would double every eight months to two years into the future.

Implications: It is applied more broadly to the power and capabilities of all circuit-based technologies. Hence, increasing spectrum of emerging scientific discovery, everything from biotechnology to robotics is governed by Moore’s law. Moore’s law also has implications ranging from geopolitics to economics.

12. Tabulate the lines of computer code (LOC) for the following: Microsoft Office, Large Hadron Collider, automobile clocks, flight software.

Microsoft Office: 45 million LOC

Large Hadron Collider: About 50 million LOC

Automobile clocks: 100 million LOC

Flight software: 400,000 LOC

13. How might bad software have contributed to the Deepwater Horizon disaster?

The bad software might have contributed to the disaster because of its complexities which led to computer failures. It posed significant safety risk even though it wasn’t exploited by hackers.