Step 1:

Three main types of cybercrime are present:

Crimes against people

These offenses include child pornography dissemination, credit card fraud, human trafficking, spoofing, identity theft, and cyberstalking and harassment.

Thefts of Property

Some internet crimes target tangible objects like computers or servers. These offenses include copyright infringement, IPR violations, hacking, virus transmission, cyber and typo squatting, computer vandalism, and DDOS attacks.

Defamation of the government

Cybercrime against the government is regarded as an assault on the sovereignty of that country. Hacking, gaining access to private information, cyberwarfare, cyberterrorism, and using unlicensed software are all examples of cybercrimes committed against the government.

Step 2:

Cybercrimes' negative repercussions frequently cause tremendous financial ruin and reputational damage to both organizations and individuals. Additionally, cybercrimes' effects on society might take many different forms. Cybercrime can take many different forms, from online con games for small-time robberies to grave dangers like terrorism.

Sensitive data, such as credit card numbers, passwords, and private information, might be lost as a result of cyberattacks. Cybercriminals can now use their information to harass their clients, demand ransom, or sell it on the dark web. Hackers can use personal data to steal identities or pass it off as someone else.

Businesses that experience a cyberattack also pay more due to operational disruption and modified business procedures. The largest damages resulting from harm to one's reputation. Businesses that are no longer in control of their clients