Chapter 7
Information Age Warfare

Table of Contents

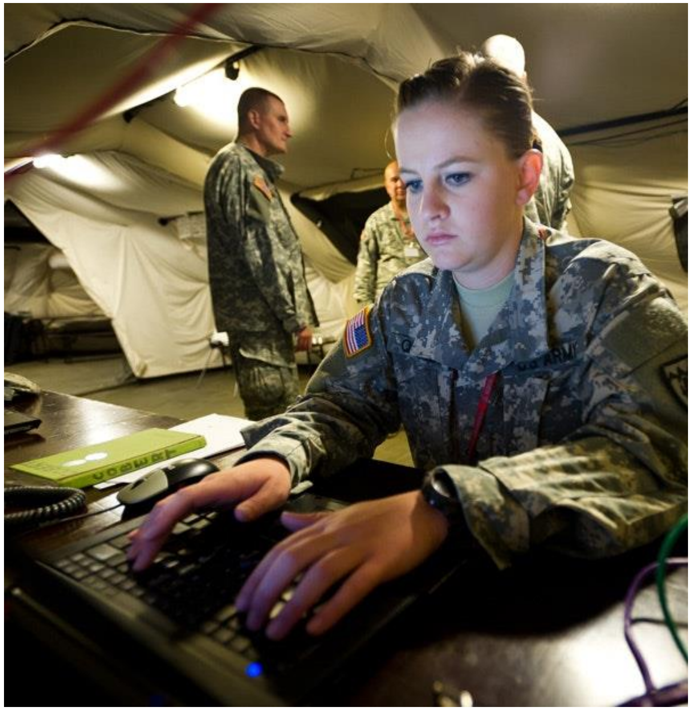
History of warfare
The technology of war

Introduction

Information Age Warfare refers to the use of information and communication technologies (ICTs) in military operations, where information and the ability to control and manipulate it become strategic assets.

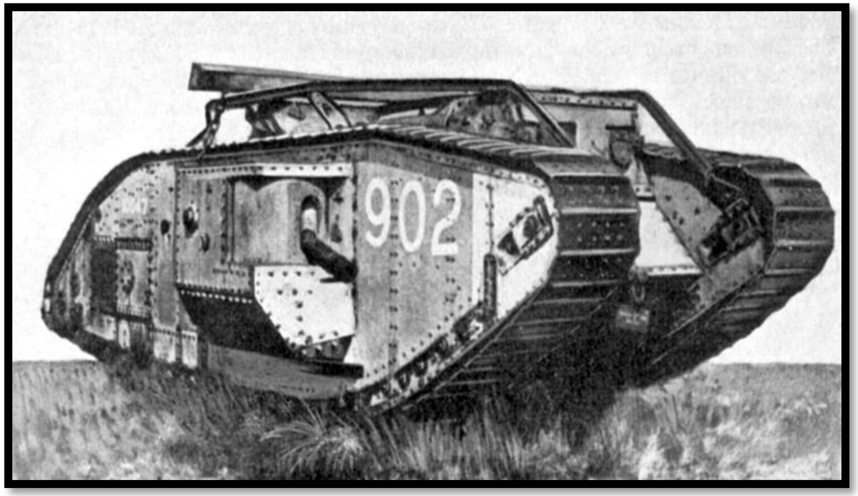
In this era, the focus is on leveraging technological advancements, networked systems, and intelligence capabilities to gain an advantage over adversaries. Information Age Warfare encompasses various elements, including cyber warfare, electronic warfare, command and control systems, information operations, and intelligence and surveillance.

It recognizes the importance of information superiority and the impact of ICTs on modern warfare, allowing for enhanced situational awareness, coordination, and the ability to disrupt or deceive adversaries.



HISTORY OF WARFARE

History of Warfare: World War I



History of Warfare: World War II

THE TECHNOLOGY OF WAR

The Technology of War

Weapons Development: Technological advancements have led to the development of more sophisticated and lethal weapons throughout history.

From the invention of gunpowder and firearms to the development of tanks, aircraft, and nuclear weapons, new technologies have revolutionized warfare, increasing its destructive power and altering tactics and strategies.

The Technology of War

Military Equipment and Logistics: Technology has greatly impacted military equipment, transportation, and logistics.

The introduction of improved communication systems, advanced vehicles, and transportation methods have enhanced the ability to mobilize and supply troops, leading to changes in the scale and duration of military campaigns.

The Technology of War

Intelligence and Surveillance: Technological advancements have greatly enhanced intelligence gathering and surveillance capabilities in warfare.

From aerial reconnaissance to satellite imagery, unmanned aerial vehicles (UAVs), and advanced sensors, technology has provided military forces with increased situational awareness and the ability to monitor and collect information about enemy activities.

The Technology of War

Communication and Command and Control: Advances in communication technology have revolutionized command and control systems in warfare.

From the use of telegraphs and radios to modern-day secure communication networks, real-time communication has facilitated coordination, decision-making, and the dissemination of orders on the battlefield.

The Technology of War

Cyber Warfare and Information Operations: The emergence of the digital age has introduced new dimensions of warfare.

Cyber warfare involves the use of computer networks, hacking, and information technology to disrupt, disable, or gain unauthorized access to enemy systems.

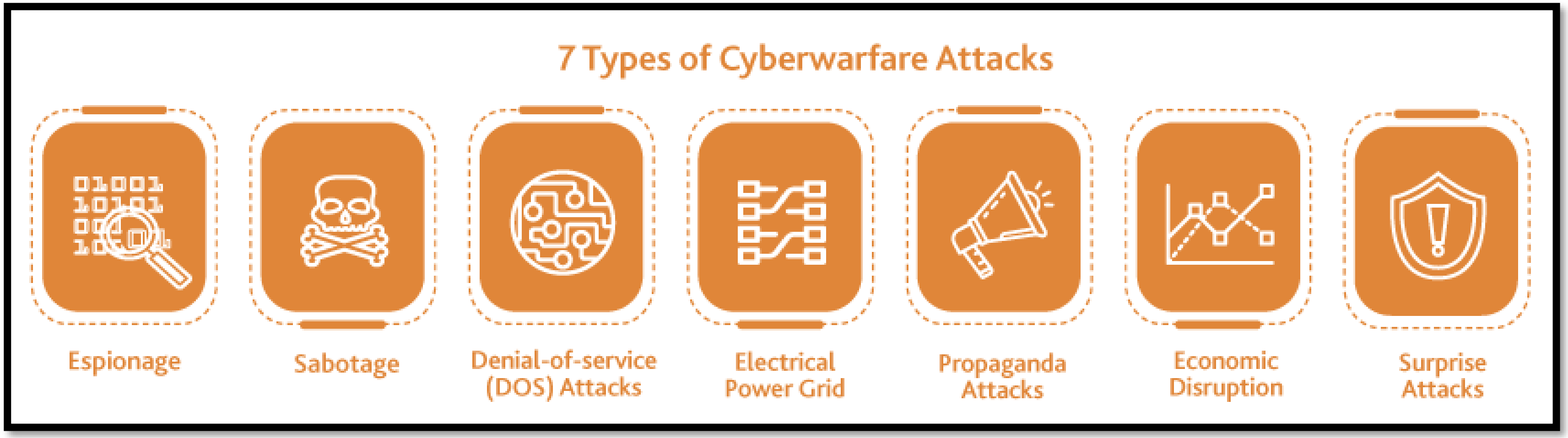
Information operations encompass the use of propaganda, psychological tactics, and the manipulation of information to shape public opinion, influence decision-making, and gain an advantage in conflicts.

The Technology of War

Biological Weapons: Biological weapons are a type of warfare agent that uses harmful biological organisms or toxins to intentionally cause harm or death to humans, animals, or plants.

Some examples of potential biological agents that could be considered "medical weapons" include pathogens, such as bacteria or viruses, that are specifically engineered or manipulated to target certain populations or have specific effects.

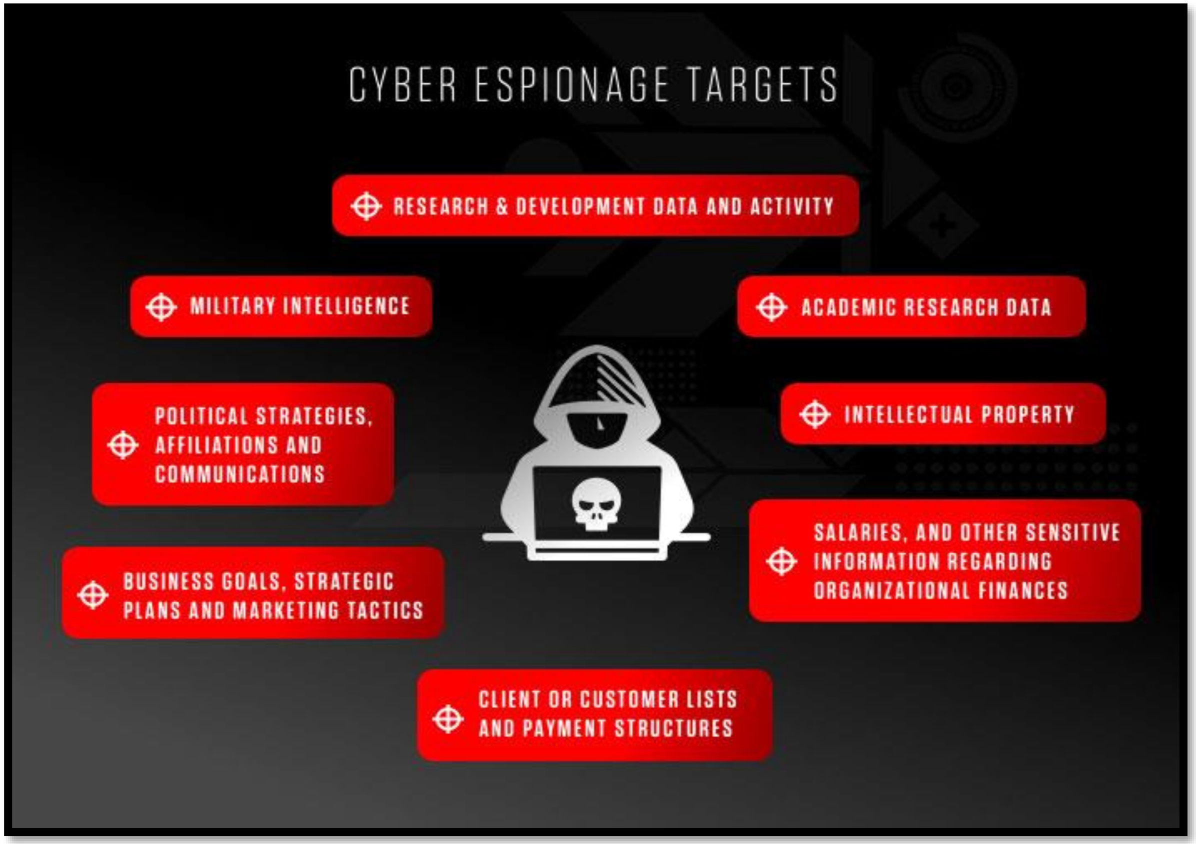
Cyberwarfare



Cyber warfare, also known as cyber warfare or cyber conflict, refers to the use of cyber capabilities and information technology for offensive or defensive purposes in the context of warfare. It involves the deliberate targeting and exploitation of computer systems, networks, and electronic infrastructures to achieve strategic or military objectives.

In cyber warfare, nation-states, state-sponsored groups, or non-state actors employ various techniques, tools, and tactics to conduct cyber attacks and exploit vulnerabilities in digital systems. These attacks can range from simple phishing and malware attacks to more sophisticated operations that involve data breaches, disruption of critical infrastructure, or even sabotage.

Cyberwarfare


CYBER ESPIONAGE TARGETS

RESEARCH & DEVELOPMENT DATA AND ACTIVITY

MILITARY INTELLIGENCE

ACADEMIC RESEARCH DATA

POLITICAL STRATEGIES, AFFILIATIONS AND COMMUNICATIONS

INTELLECTUAL PROPERTY

SALARIES, AND OTHER SENSITIVE INFORMATION REGARDING ORGANIZATIONAL FINANCES

BUSINESS GOALS, STRATEGIC PLANS AND MARKETING TACTICS

CLIENT OR CUSTOMER LISTS AND PAYMENT STRUCTURES

Espionage
It is generally an act of monitoring other countries with the intention to steal secrets. In cyber warfare, it involved sophisticated methods of botnets or spear phishing attacks to compromise sensitive computer systems before exfiltrating sensitive information.

Cyberwarfare

Sabotage
Compromising of military systems such as command and control (C4ISTAR) systems that are responsible for orders and communications could lead to their interception or malicious replacement. Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

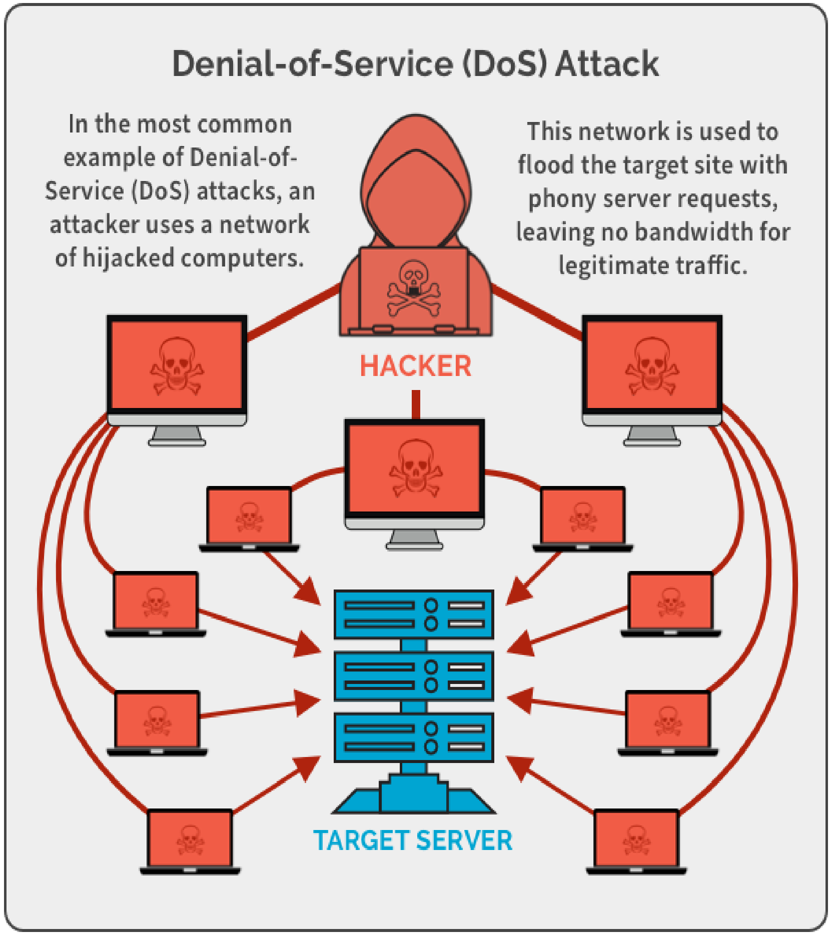
Cyberwarfare

Denial-of-service (DOS) Attacks

DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

DoS attacks can be used to disrupt critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.


Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

Hackers

Black Hat Hacker: A black hat hacker is an individual who engages in hacking activities with malicious intent or for personal gain. They exploit vulnerabilities in computer systems, networks, or software to carry out illegal activities, such as stealing sensitive information, spreading malware, or causing damage to systems. Black hat hackers are generally associated with cybercrime and unauthorized access to systems.

White Hat Hacker: A white hat hacker, also known as an ethical hacker, is an individual who uses their hacking skills to identify vulnerabilities and secure computer systems. They are employed by organizations to conduct authorized penetration testing or vulnerability assessments. White hat hackers work within legal and ethical boundaries to help organizations strengthen their security defenses and protect against potential threats. They play a crucial role in improving cybersecurity.

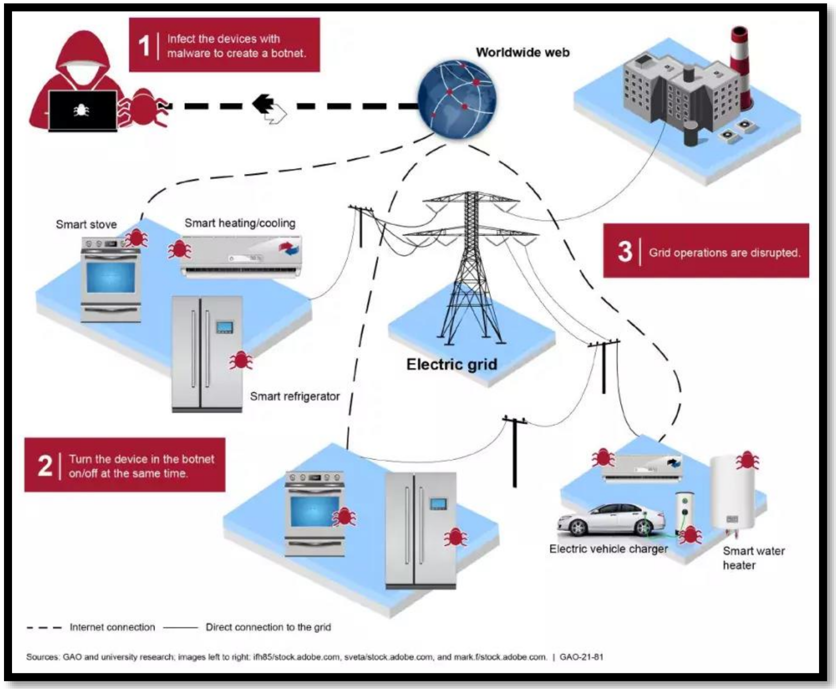
Grey Hat Hacker: A grey hat hacker falls somewhere between a black hat and a white hat hacker. They do not have explicit authorization to access or manipulate computer systems, but they may identify vulnerabilities and disclose them to the affected organization without malicious intent. While their actions may be aimed at exposing weaknesses and promoting security, grey hat hackers still operate in a legally ambiguous area since they perform unauthorized activities. Their motivations can vary, and their actions may be met with both appreciation and legal consequences depending on the circumstances.

Cyberwarfare

Electrical Power Grid

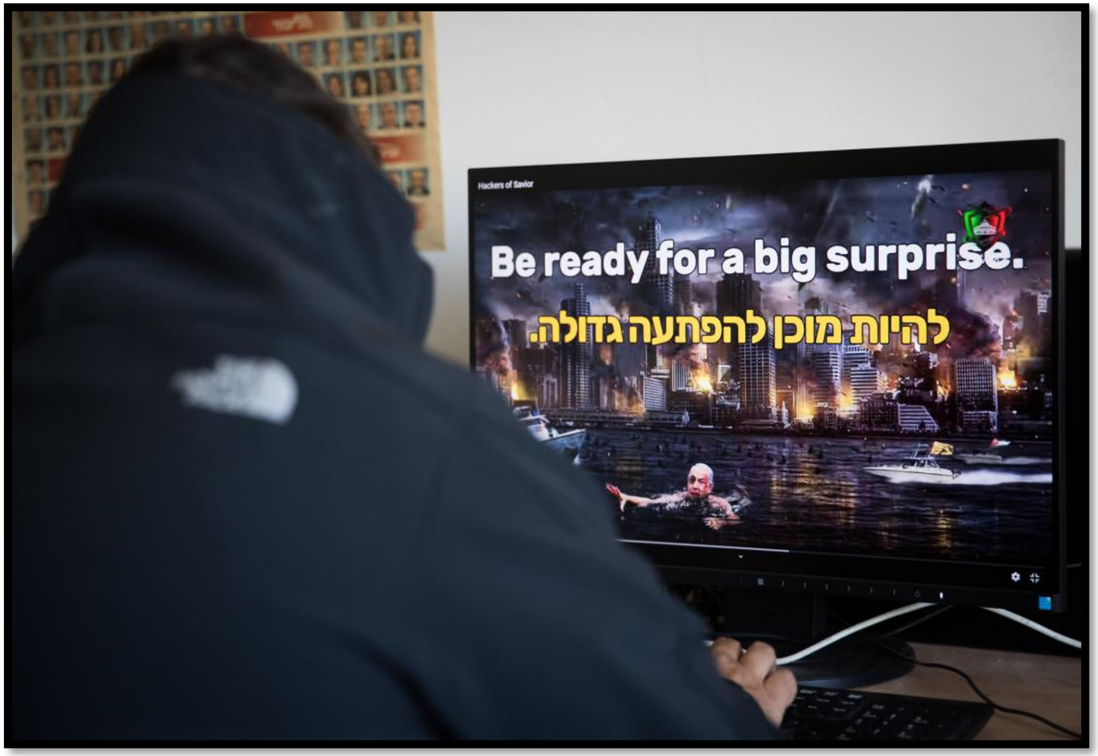
Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm.

Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.


1 Infect the devices with malware to create a botnet.
Worldwide web
Smart stove
Smart heating/cooling
3 Grid operations are disrupted.
Electric grid
Smart refrigerator
2 Turn the device in the botnet on/off at the same time.
Electric vehicle charger
Smart water heater
Internet connection
Direct connection to the grid

Sources: GAO and university research; images left to right: ifh85/stock.adobe.com, sveta/stock.adobe.com, and mark.f/stock.adobe.com. | GAO-21-81

Cyberwarfare



Propaganda Attacks

Cyber propaganda is an effort to control information in whatever form it takes and influence public opinion. It is a psychological attempt to manipulate the minds and thoughts of people living in or fighting for a target country.

Propaganda can be used to expose embarrassing truths, spread lies to make people sway their opinions in a particular direction, or side with their enemies.

Cyberwarfare

Economic Disruption
Most modern economic systems leverage on sophistication of technology. Like cybercrimes, attackers target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

Information Security Spending

Global spending on cybersecurity products and services is predicted to exceed **$1 trillion cumulatively** over the five-year period from 2017 to 2021. This is a 12-15% year-over-year cybersecurity market growth through 2021.

2017
2018
2019
2020
2021
71%

expect cybersecurity budgets to increase **in the next three years**.

Cyberwarfare

Surprise Attacks
These are the cyber equivalent of attacks like Pearl Harbour and 9/11. The point is to carry out a massive cyberattack when the target is least expected, enabling the attacker to breach their defences.

Network-centric Warfare

Network-centric warfare (NCW) is a military concept that emphasizes the use of interconnected systems, information sharing, and real-time communication to enhance military operations. It focuses on creating a shared awareness of the battlefield among military units and platforms through a robust information network. The concept relies on the rapid exchange of information, collaboration, and the exploitation of networked capabilities to achieve a competitive advantage on the battlefield.

INTRODUCTION TO ONLINE CRIME

Phishing: Phishing involves tricking individuals into revealing sensitive information, such as passwords, credit card details, or personal data, by masquerading as a trustworthy entity in electronic communication.

Malware Attacks: Malicious software, or malware, is used to gain unauthorized access, disrupt or damage computer systems, or steal information. Examples include viruses, worms, ransomware, and spyware.

Hacking: Hacking involves unauthorized access to computer systems or networks to exploit vulnerabilities, steal data, disrupt operations, or gain control over targeted systems.

Identity Theft: Identity theft occurs when someone uses another person's personal information, such as their name, Social Security number, or financial details, without authorization to commit fraud or other criminal activities.

Cyber Fraud: Cyber fraud encompasses a wide range of fraudulent activities conducted online, such as online scams, financial fraud, credit card fraud, or online auction fraud.

Online Harassment and Cyberbullying: This includes the use of electronic communication to harass, intimidate, or threaten individuals, often through social media platforms, emails, or messaging apps.

Data Breaches: Data breaches involve the unauthorized access and theft of sensitive information from organizations or databases. This can lead to the exposure of personal data, financial information, or trade secrets.

Denial-of-Service (DoS) Attacks: In a DoS attack, a perpetrator overwhelms a target's computer system, network, or website with an excessive volume of traffic or requests, rendering it unavailable to legitimate users.

Online Scams: Online scams encompass various fraudulent schemes, such as advance fee fraud (e.g., "419 scams"), pyramid schemes, online dating scams, or lottery scams, where individuals are deceived into providing money or personal information.

Cyberstalking: Cyberstalking involves using the internet or electronic means to harass, monitor, or intimidate someone persistently, causing fear or distress.

Maybank Awareness: ONLINE CRIME

End