jims
Sector - 5, Rohini, Delhi

IT KALEIDOSCOPE
STUDENT IT PRESS
EXPLORE • LEARN • INNOVATE • SECURE

MAY-JUNE EDITION
2026

CYBERWARFARE

THE INVISIBLE BATTLEFIELD

Newsletter Overview

War is no longer fought only with guns, missiles, and soldiers. In today's digital world, countries can attack each other through computer networks, using malicious software, hacking, and cyber espionage instead of traditional weapons. These invisible attacks can disrupt power grids, banking systems, hospitals, transportation, communication networks, and even military operations without a single shot being fired. Unlike conventional warfare, cyberattacks often happen silently, making them difficult to detect until serious damage has already occurred. As technology becomes increasingly connected, cybersecurity has become essenntiglly fror protecting national security, businesses, and everyday life. This newsletter explores the rise of cyberwarfare, how cyberattacks are carried out, real-world case studies, and why digital security is one of the greatest challenges of the 21st century.

DEAN & PRINCIPAL
DR. PRAVEEN ARORA

FACULTY INCHARGE
DR. PRIYANKA GANDHI

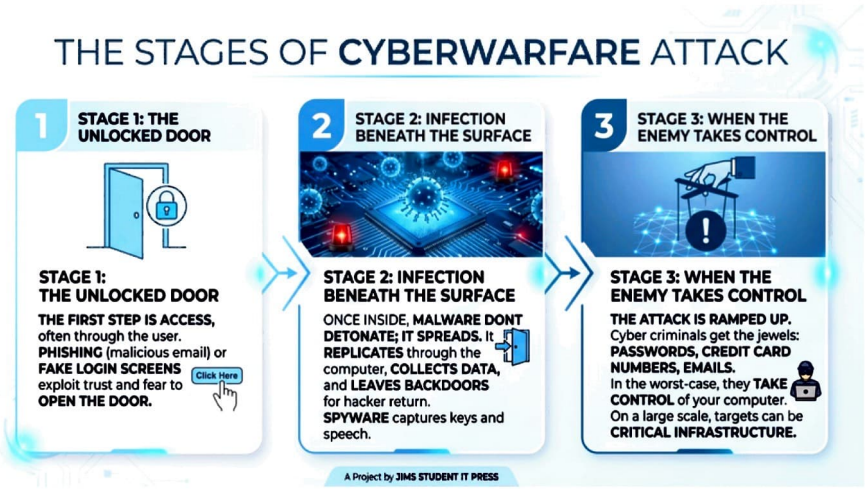
STUDENT INCHARGE
Anushree
(2nd Year, 1st Shift)

OUR DESIGNERS
Manya Agarwal
(1st Year, 2nd Shift)

Introduction

Wars are no longer fought with guns, bombs and tanks. Some of the most dangerous wars are being fought without a sound, without bullets and even without a visible enemy. This is the case with cyber warfare, because the battlefield is invisible and the weapons are lines of code.

With every click you make to read your emails, every time you click on a link and every time you open your Facebook, you are then unintentionally a part of this invisible war. Even more disturbing is that to participate in this invisible war, you don't have to be a soldier; you just have to be connected to the Internet.
Let's take a look at the stages of attack together.



Stage 1: The Unlocked Door
The first step to any attack is access - and most often, it's not access through the computer, but access through the user. A harmless email. A "Click Here" button. A fake login screen that looks exactly the same as the real screen down to the last pixel. This is known as phishing, and it takes advantage of the elements of trust and fear in humans. While in traditional wars we have to blast through the walls to get in, in cyber wars we open the door to our enemies ourselves.

Stage 2: Infection Beneath the Surface
Once the malware breaks into the computer, it doesn't detonate. Instead, it spreads. Like a virus, this stage involves the malware replicating through the computer and collecting data, and sometimes leaving other access points (typically called backdoors) that will allow the hacker to return to the infected computer at a later date. Other types (spyware) operate discreetly for weeks, capturing everything you type and speak

Stage 3: When the Enemy Takes Control
This is where the attack is ramped up to a higher level. The cyber criminals will get access to the jewels - the passwords, credit card numbers, emails and in the worst-case scenario, they will take control over your computer

On a large scale, this could result in critical infrastructure systems being targeted - such as electricity, water and telecommunications - resulting in unprecedented disruption that could potentially impact millions.
When it comes to cyberattack, there is always a purpose - damage. This damage can be in many forms, whether it be the loss of money (due to scams and ransoms), a person's identity, data misuse, the freezing of their computer system or even the theft of secret information. For the individual, it can be devastating and personal.

ANUSHKA SRIVASTAVA
BBA 2ND YEAR SHIFT -1

How Cyber Attacks are Changing Modern Warfare

In today's era, warfare has evolved from its ancient form to a new technological approach by taking place in cyberspace. Earlier, it was all about missiles, tanks and guns but now countries use highly advanced systems to target their rivals. This type of warfare is known as cyberwarfare. This is a kind of invisible battlefield that occurs quietly, with soldiers neither crossing the border nor dropping any bombs.

The term Cyber war refers to the use of technological equipment by one nation in order to cause damage or destruction to another one. It may include computer hacking, security breaches and spreading computer viruses. The most prominent effect that can result from cyber-attacks is on the country's vital infrastructure.

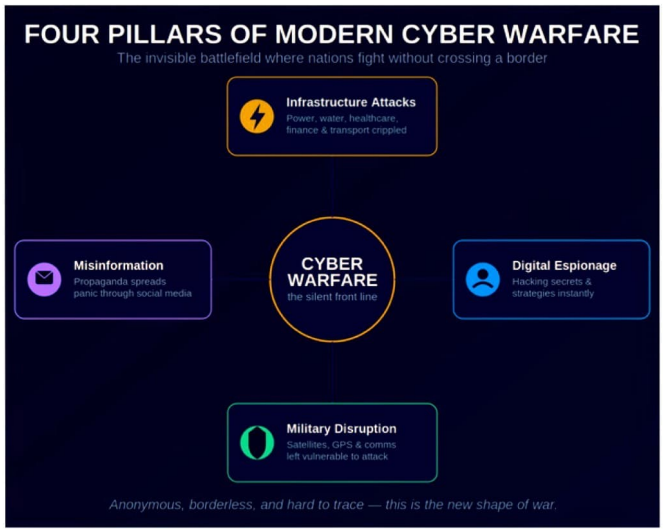
In today's world, nations rely heavily on computerized systems for their power, water supplies, healthcare facilities, finance sector, and transportation network. Should hackers succeed in penetrating such crucial infrastructures, normal life could grind to a standstill. Can you imagine an entire city experiencing a power outage, banks suspending transactions, or hospitals being unable to access patient information?

The next essential element in the area of cyber warfare is hacking into sensitive information. Earlier countries used to spy on each other to fetch essential information but now hackers can easily gain secrets and strategies in no time.

Cyber-attacks have begun to influence the military operations as well. Currently, armies rely on satellites, communication technology, and GPS and unfortunately all of these are extremely vulnerable to any kind of attack or hacking. This can impact the military's mission on a next level

Social media also plays an important role in this cyber-warfare. The spread of misleading information and propaganda through social media platforms can lead to chaos and panic among civilians. Sometimes, manipulating people mentally is just as effective as invading them physically.

The most crucial fact related to this Cyber warfare issue is that, it's hard to guess the course of action and location. Hackers could potentially mask themselves and launch attacks from other countries. This is why many governments have been putting significant effort into the world of cybersecurity and protection against any potential threats from other parties.



It should be said that cyberwarfare has dramatically changed the concept of modern-day war. It is fast, silent, and extremely damaging while not leaving traces like an ancient war. In today's world, it feels like locks are made up of wood and attackers have chainsaw. So as everything becomes increasingly interconnected, digital security plays as big a role as physical security.

ANSHITA
BCA 2ND YEAR SHIFT -2

IT KALEIDOSCOPE
STUDENT IT PRESS

The Colonial Attack

INTRODUCTION (CASE STUDY)

The colonial pipeline attack is the most dangerous Cyber attack in modern history in America on 7th may 2021.It shows how hackers can disrupt critcal national infrastructure without using any physical weapon. This Cyber attack shows that cyberwarfare is not limited to stealing data. It can also affect the digital infrastructure, transportation, businesses as well as every day life. This incidence became global warning about the growing dangerous ransom ware attack and weak Cybersecurity system.

THE CYBERATTACK

The Darkside hacking group launched a ransomware attack on colonial pipeline company. They gained access of the company computer network through a compromised password link to VPN account. Because the multifactor authentication (MFA) is not enabled. There is only single password security between hacker and company data. They stole 100GB company data within 2 hour and then they deployed ransomware to encrypt the company IT system. After this they demand for ransom of 75 Bitcoin (4.4 million USD) in exchange for a digital Decryption key to unlock frozen system. This pipeline was shut down for 6 days (may 7-12).

WHAT IS RANSOMWARE?

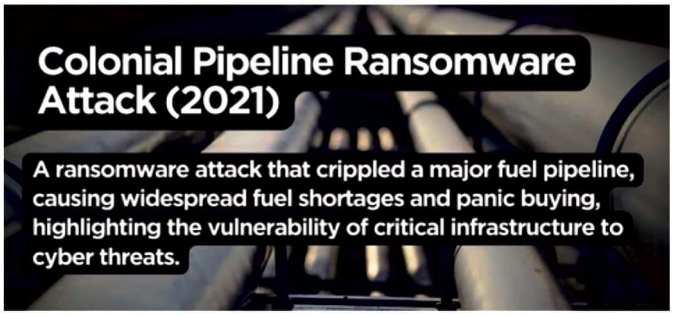
Ransomware is a type of malicious soware (malware) designed to block the access of computer system or network and ask for money (called a ransom) to restore the access by ge ng digital key.

THE BUSINESS DECISION

The business decision The CEO of colonial pipeline, Joseph Blount. Decided to pay within hours of the a ack and authorized a ransom payment of 75 bitcoin. Because it would take much me to get access without decryp on key. And this caused a shortage of fuel supply in the country. Recovery and jus ce

RECOVERY AND INJUSTICE

After the payment to hacker the company shutdown its opera on to stop further damage. Cyber security expert and government agencies help to restore the system. In FBI inves ga on they iden fied the Darkside group and recover (2.3 million USD) of ransom payment from the hacker group.



PRASHANT KUMAR
BBA 1ST YEAR SHIFT -2