Defence on Cyber Crimes Against Women and Laws in India-A Survey

BY

R.Krishnaranjani

Cybercrime

- **Cybercrime** or **computer-oriented crime**, criminal activities carried out by means of computers or the Internet.

- **Cybercriminals** may use computer technology to access personal information, business trade secrets or use the internet for exploitative or malicious purposes.

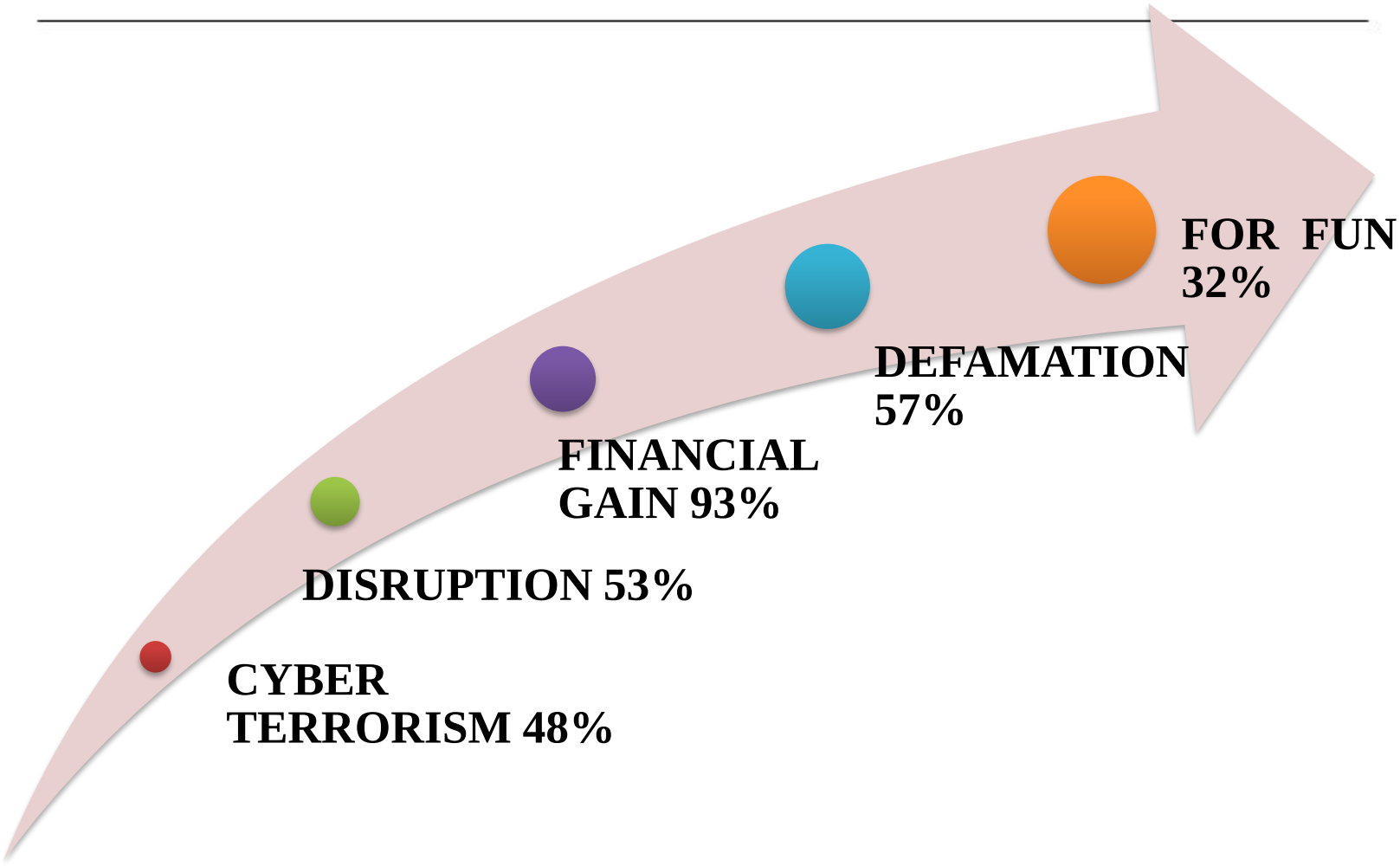
Cyber Crime Cases(2014-2017)

- **44,679** Cyber Crime — **2014**
- **49,455** Cyber Crime — **2015**
- **50,362** Cyber Crime — **2016**
- **53,081** Cyber Crime — **2017**

- **India ranks 3rd in terms of the highest number of internet users in the world**


WHY?

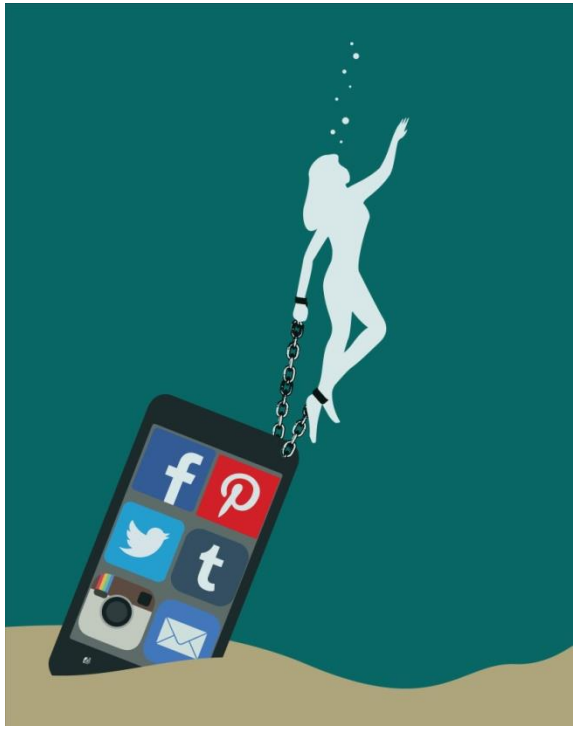
Reasons for Cyber Attacks



‘Are Women Safe On The Internet?’

Major Cyber Crime Areas:

- Cyber stalking
- Defamation
- Morphing
- Cyber Pornography
- E-mail spoofing
- Trolling



Cyber Stalking

- use of the Internet or other electronic means to stalk or harass an individual, group, or organization.

Defamation

- act of making false statements about another which damages his/her reputation. It is a statement that injures someone's reputation.

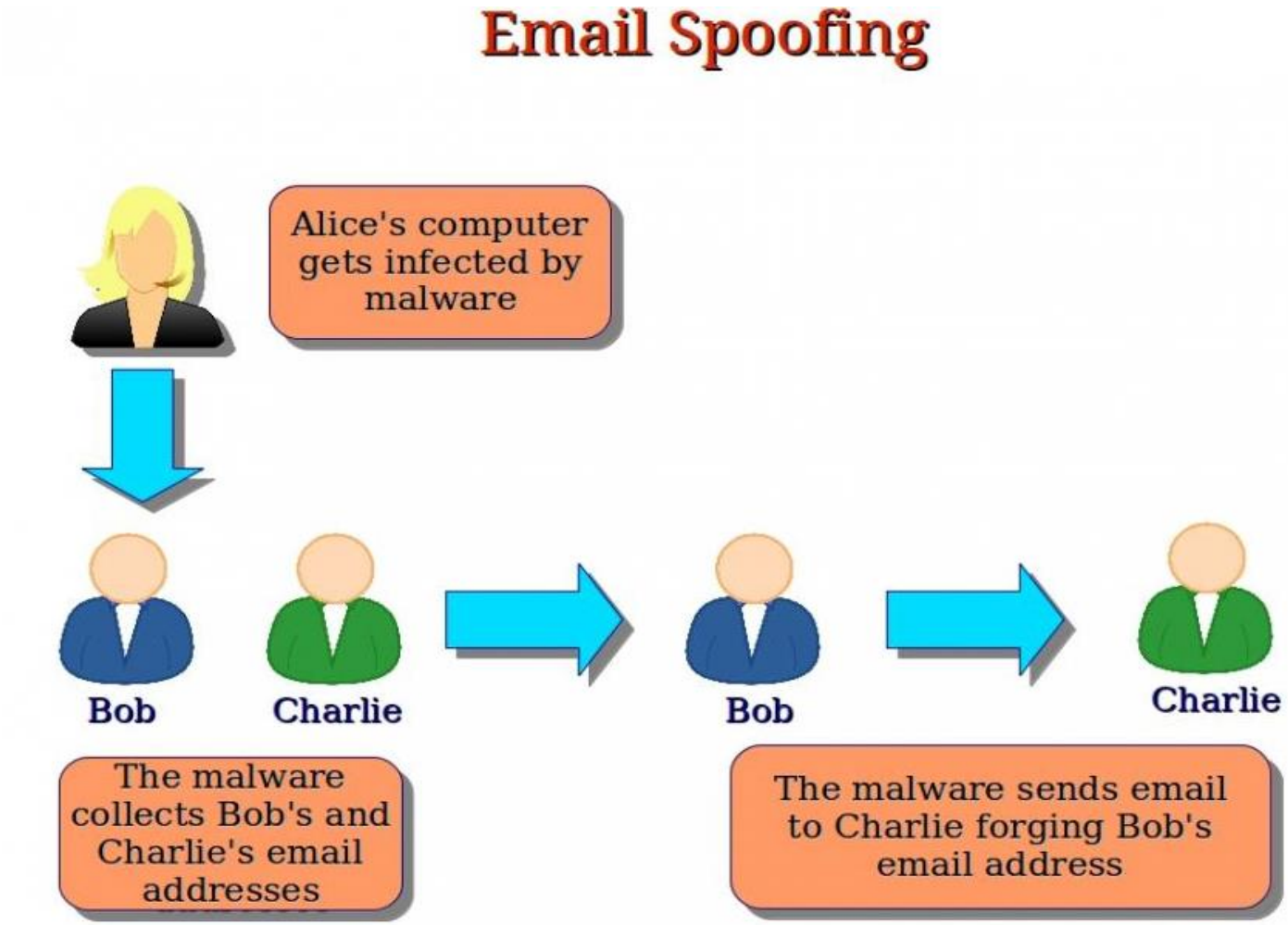
Morphing and Cyber Pornography

Morphing - act of using technology to modify photographs of a person without their consent and using them.

Cyber pornography - act of using cyberspace to create, display, distribute, import, or publish **pornography** or obscene materials.

E-mail spoofing

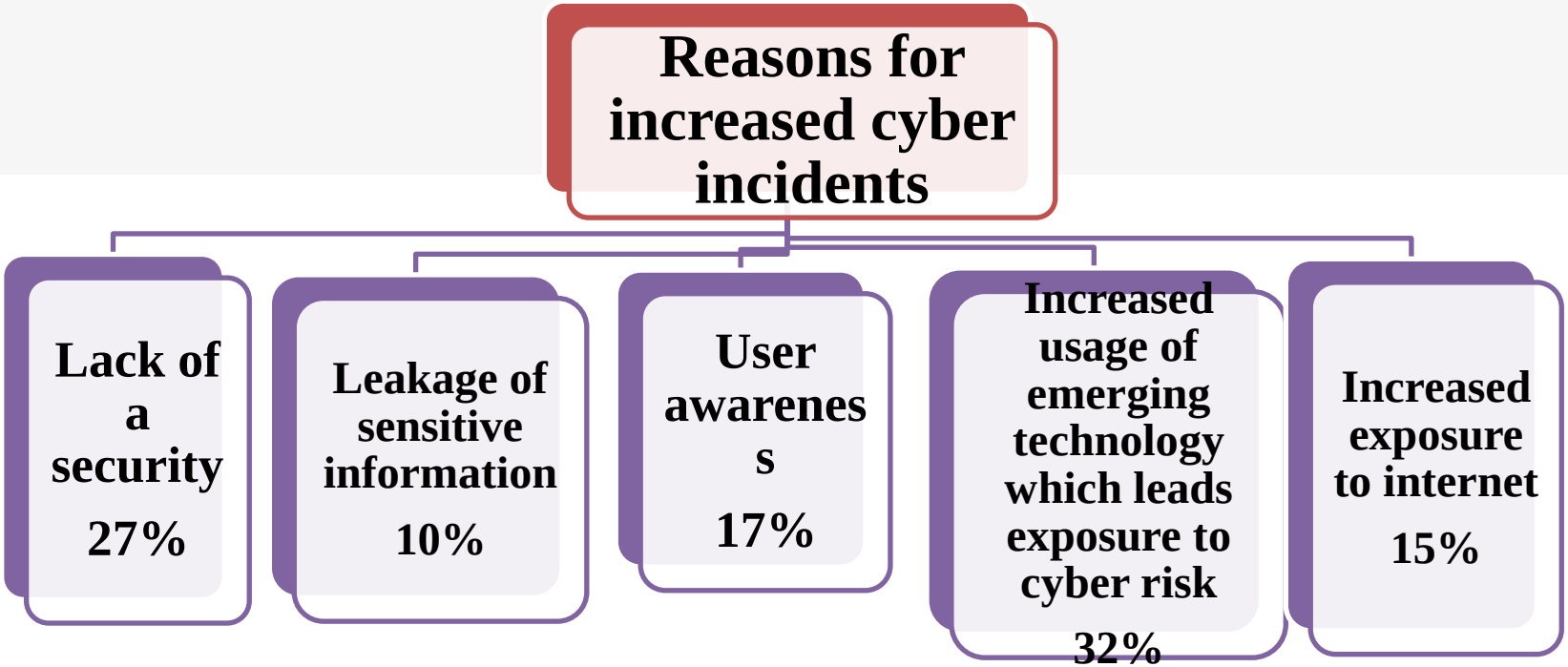
Email spoofing is a fraudulent email activity hiding email origins. eg: **Phishing**



Trolling

Trolling (cyber bullying) - anti-social act of causing personal conflict and controversy online.

Reasons for increased cyber incidents



Cyber Law under the Information and Technology Act, 2000

The stalkers and cybercriminals can be booked under several sections for breaching of privacy.

- **Section 66A** - Sending offensive messages .
- **Section 66B** - Dishonestly receiving taken computer resource.
- **Section 66D** - Cheating by person on victimization compute resource.
- **Section 66E** - Privacy violation.
- **Section 66F** - Cyber terrorism .
- **Section 72** - breaching one's space and confidentiality.
- **Section 72A** - revealing data throughout lawful contract.
- **Section 441 IPC-** criminal misdemeanour.
- **Section 354D** - deals with stalking.

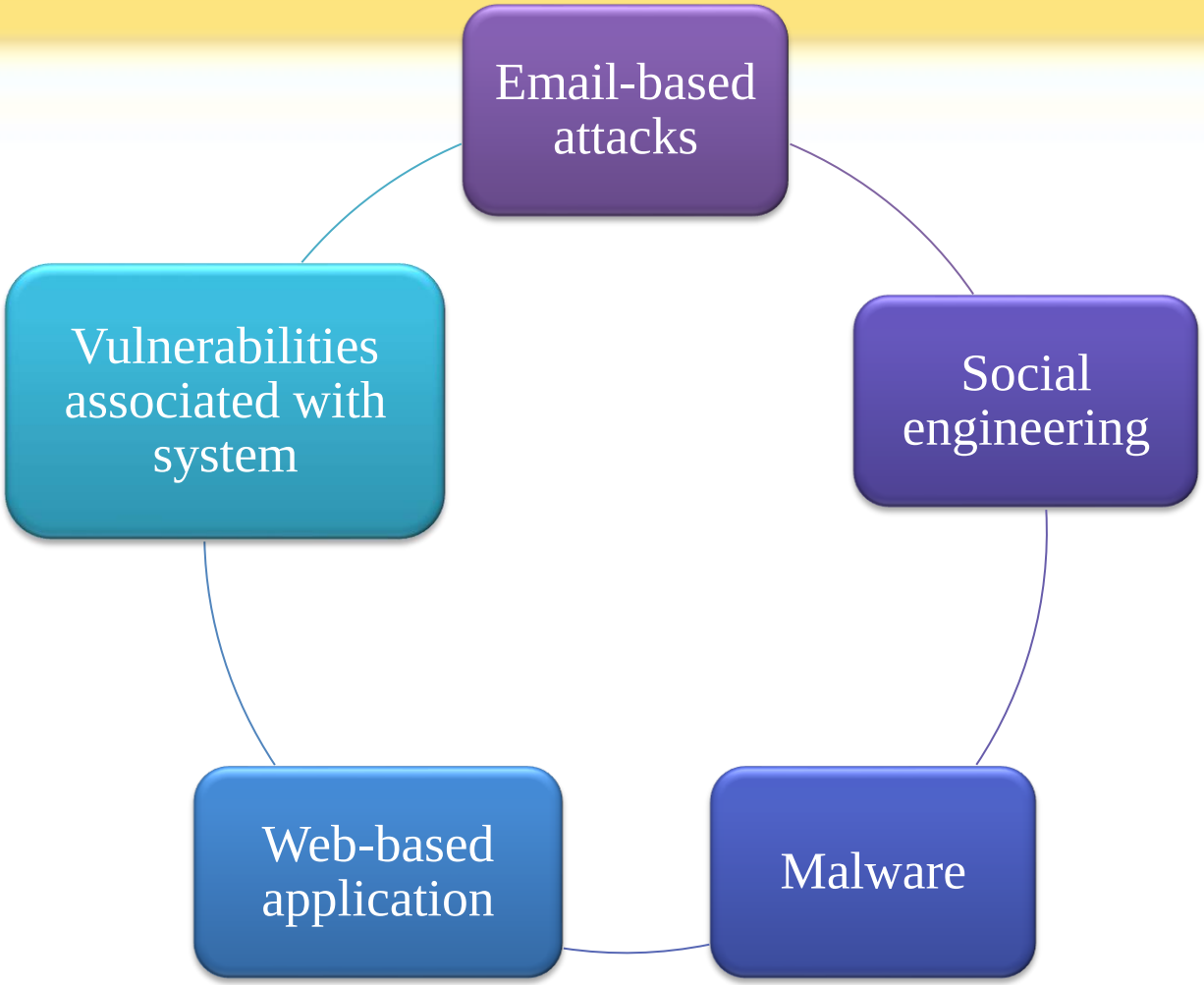
Key to protect cyber crimes

Reporting a cyber crime..

“If There's Cyber Crime, Women Begin Reporting Right Now”

- ✓ Don’t share passwords
- ✓ Don’t leave your webcam connected
- ✓ Don’t share more than necessary
- ✓ Update all operating systems on your devices
- ✓ Secure your devices with anti-virus software
- ✓ There's no such thing as ‘freebies’

Top Five Attacks Faced



Targets for cyber attackers

Targeted Attacks	Percentage(%)
Identity impersonation	**22%**
Phishing attacks	**61%**
E-mail based attack	**75%**
Malware/Ransom ware	**69%**
Web-Based applications	**33%**
Vulnerabilities associated with system	**22%**
Physical theft of computing devices	**22%**

Motives of Cyber attackers

JUNE 2018

AUGUST 2018


Information systems
Protection
Internet attack
Cyber security
Internet
Mobile devices
Computer

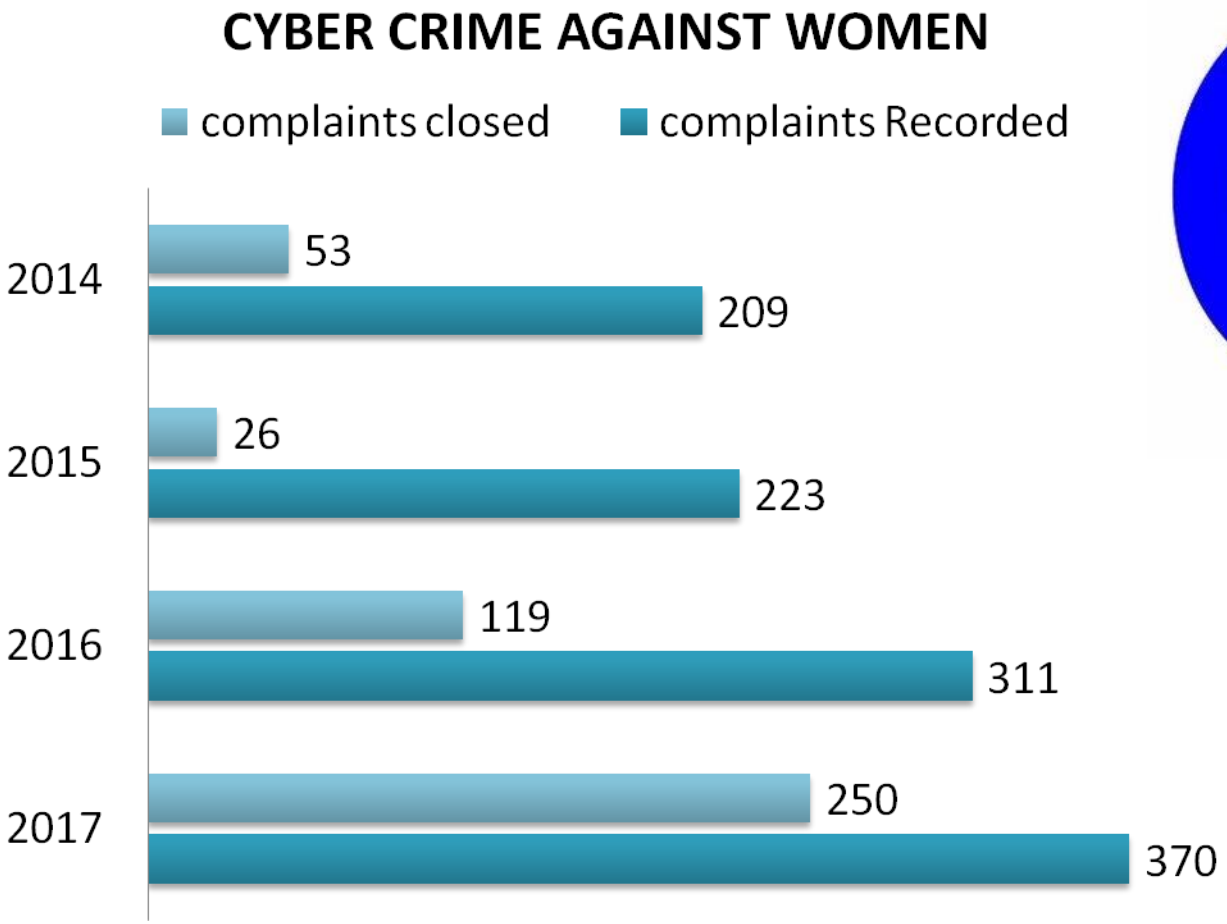
NCRB (National Crime Record Bureau)

NCRB information reveals violations against women and outsiders, cases of sedition have diminished whereas human trafficking, cyber crimes have expanded.

NATIONAL COMMISSION FOR WOMEN

The **National Commission for Women (NCW)** is a statutory body, generally concerned with advising the government on all policy matters affecting women.

NATIONAL COMMISSION FOR WOMEN (NCW)



Projects of NCW

- Cyber Crime Prevention against Women and Children (CCPWC)

- Face book has entered into Partnership with National Commission for Women (NCW) to launch a digital literacy programme aimed at training 60,000 women in universities across India on safe use of the Internet, social media and email in a year.

Cybercrime Tools

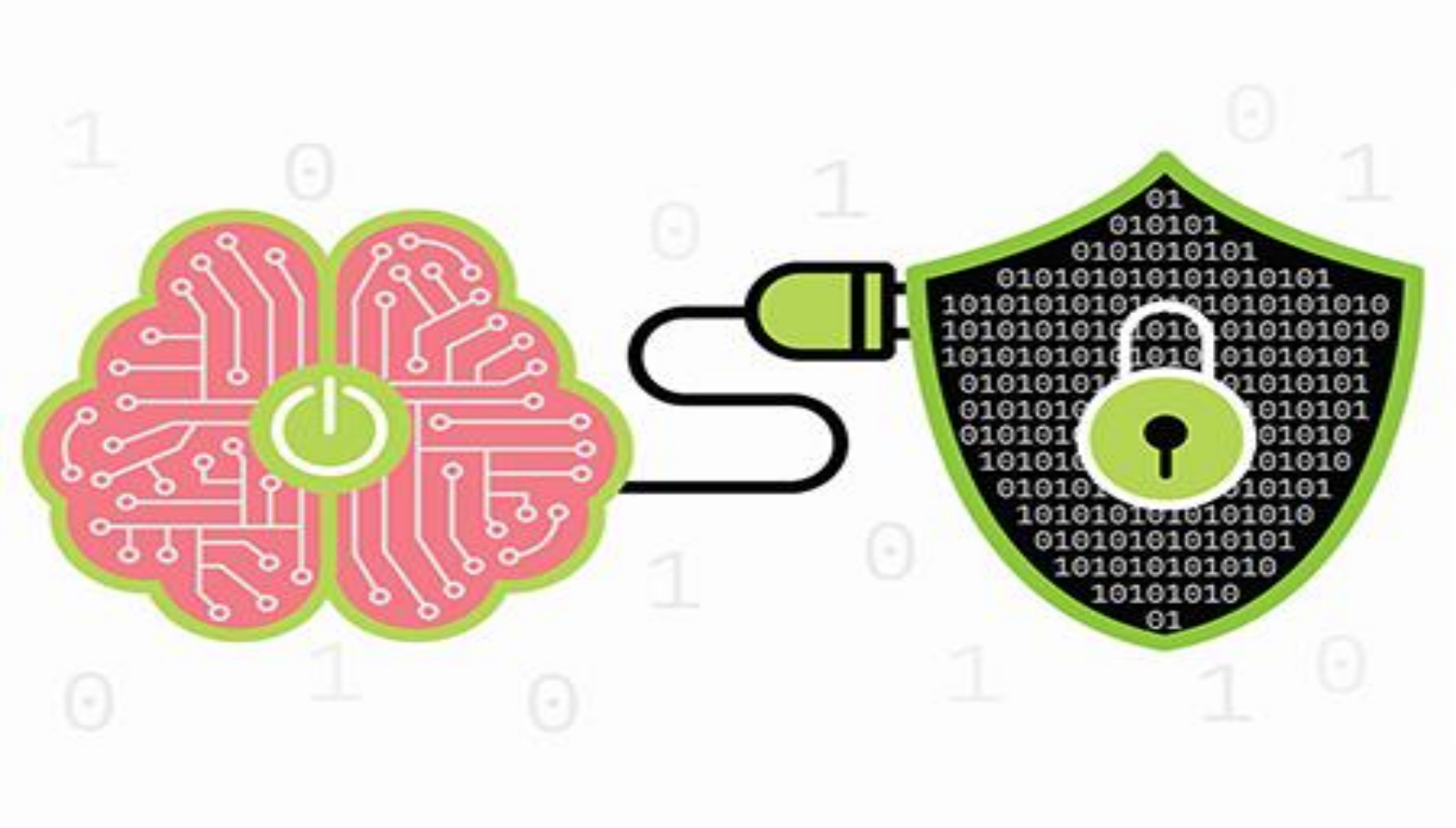
Analysis Tools

Open Source Software Cyber Security Tools

Security at data and network level is greatly enhanced by these software tools which open the door to a more safe and secure cyber world.

- **Wireshark**
- **EnCase**
- **Nmap**
- **Nessus**
- **QualysGuard**
- **Core Impact**

Machine Learning & Deep Learning based Tools



SIEM Tool

Security Information and Event Management

A **SIEM** system provides real-time analysis of security alerts generated by applications and network hardware.

An information security operations centre is a facility where enterprise information systems are

- Monitored
- Assessed
- Defended.

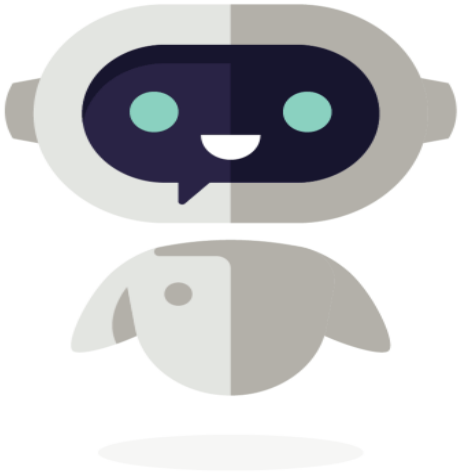
Wearing the Hackers Hat - AI primarily based Sandbox

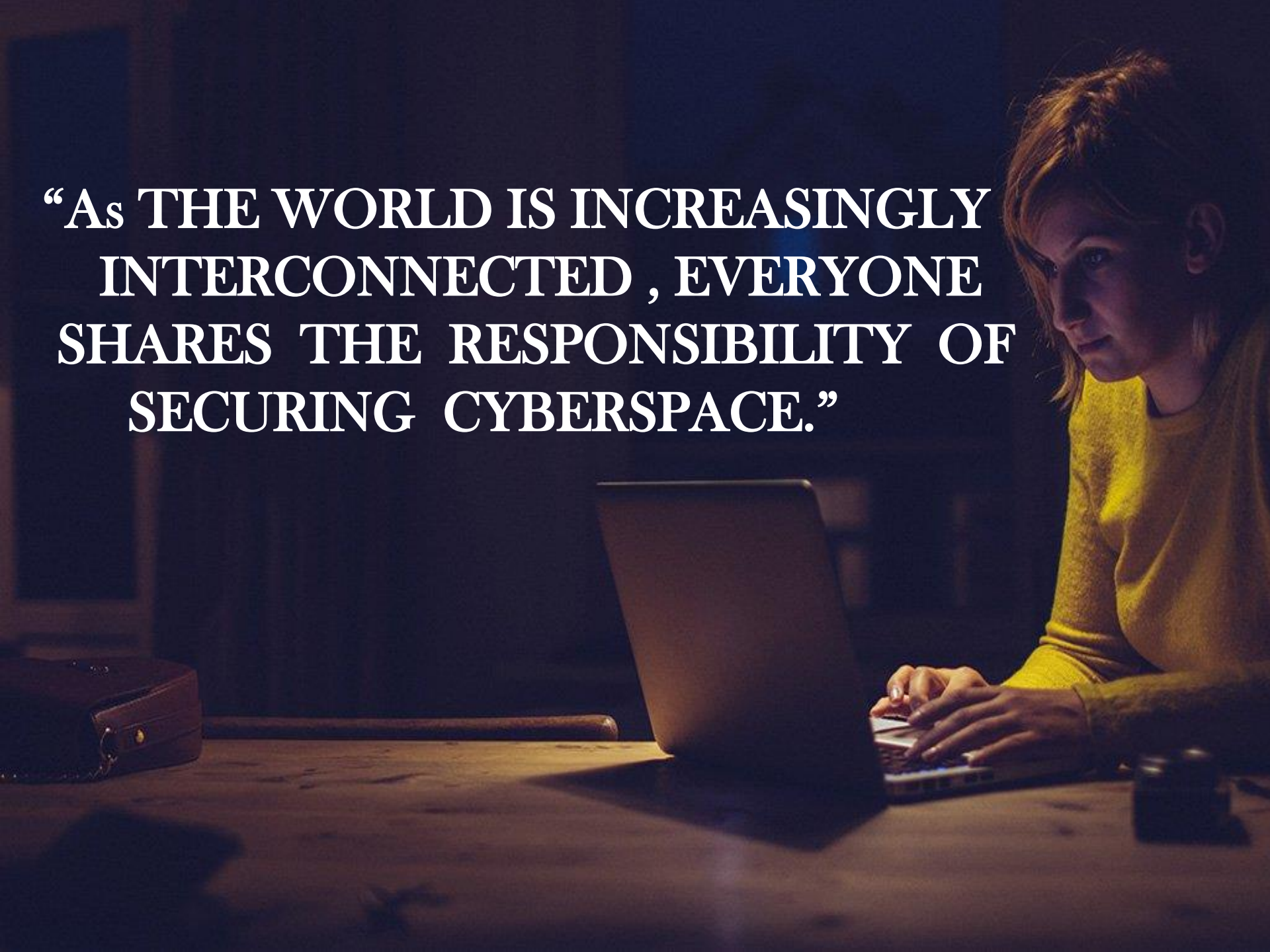
✓ With AI and machine learning we can do inference and pattern-based monitoring and alerting, but the real opportunity is the predictive restoration.

✓Sandbox - used to detect malware offers an additional layer of protection against security threats, such as stealthy attacks and exploits that use zero-day vulnerabilities.

AI and Machine Learning can boost Cyber Defences

The use of artificial intelligence and machine learning is being used to transform cyber security and aid security analysts identity threats more accurately.




“As THE WORLD IS INCREASINGLY INTERCONNECTED , EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE.”