A person wearing a dark hoodie with their face obscured by a black silhouette. The background is a blue-toned digital landscape with binary code (0s and 1s) and various keyboard keys like 'Esc', 'Psc', 'F1', 'Tab', and 'Q' floating around. The overall theme is cybersecurity and technology.

Autonomous Vehicles and Cybersecurity

**Sarah Fall: Associate Dean of
Information Technology**

Cybersecurity Concerns

- I. Cybersecurity threats in hardware and software
- II. Communication gateways in autonomous vehicles, connected and automated
- III. Addressing Security
- IV. Who owns the data?



Cybersecurity Threats

Hack



- Camera
- Contacts
- Radio – Change your station/Delete your music

Control

- Steering
- Vehicle – Brakes
- Increase speed



Cybersecurity Threats

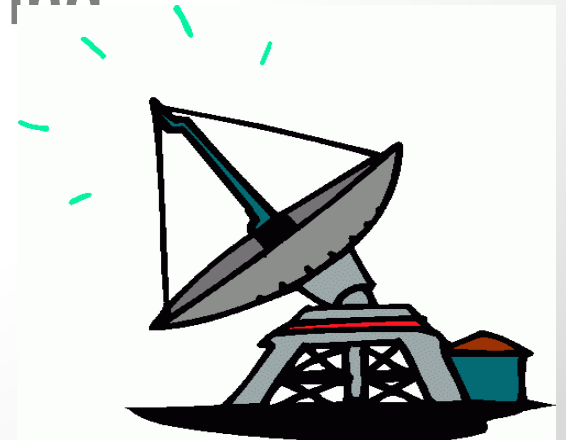
- Unauthorized access
- Lack of awareness
- Remote surveillance through telematics unit in vehicle
- Attacks on Infrastructure
- Data corruption
- System Failure



Communication Gateways

Frequencies and Wireless Technologies

- AM/FM
- Bluetooth
- Cellular Phones
- Digital Audio Broadcasting
- Radar
- Remote Keyless Entry
- Satellite Navigation (GPS)
- Satellite Radio
- Tire Pressure Monitoring
- TV
- WiFi



Communication Gateways

Issues with Autonomous Vehicles

- Hack into vehicle communication safety system
- Hackers Penetrated, modified, corrupted or taken control of vehicles
- OEM services like On-Star
- Cellular services (Sprint/Harman/FCA)
- Prevent the car from moving



Autonomous Vehicles

Issues with Connected, Automated (Autonomous) Vehicles

- **Connected: V2V Vehicle-to-Vehicle,**
- **Automated: (Autonomous), roadside infrastructure (vehicle-to-infrastructure V2I)**



Addressing Security

Automated Threats

- Internal system hacking threats
- Privacy and exposure of sensitive data
- Identity theft



YOU HAVE BEEN
HACKED !

Data

Who owns the data?

- **Companies**
- **Government**
- **Colleges**
- **Employee**

Thank You

www.devil-shop.com

www.google.com