Current Trends in Cyber Security

Course on Cyber Attack Detection & Mitigation Techniques (NIT-K)

S. K. Pal

Defence Research & Development Organization (DRDO)
SAG, Metcalfe House, Delhi

What is Cyberspace?

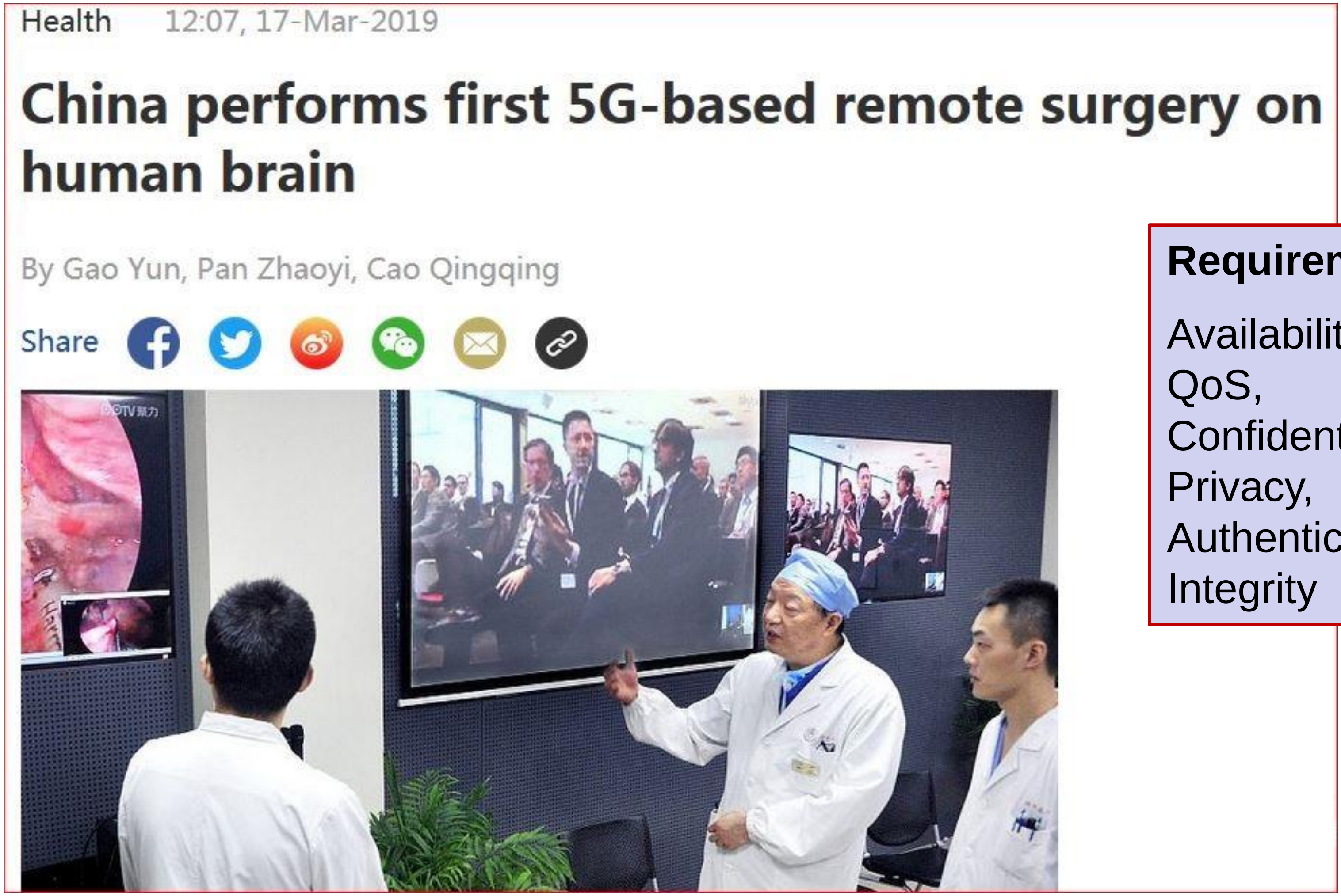
- Refers to the **digital world of computer networks**

- **Components of cyberspace:** Hardware (communication, networking, IT), software (OS, browser, antivirus, apps) & data (in the memory, disk, cloud).
- **Other components:** Cognitive users & cyber personas.

- **Gadgets, sensors & data:** Huge amount of data is generated – 2.5 exabytes / day.

- **Negative impact:** psychological, physiological.
- Browsing habits & psychographic profiling.

Useful Applications



Health 12:07, 17-Mar-2019

China performs first 5G-based remote surgery on human brain

By Gao Yun, Pan Zhaoyi, Cao Qingqing

Requirements:

Availability,
QoS,
Confidentiality,
Privacy,
Authenticity,
Integrity

Data – a Valuable Resource

- **Data** – the most valuable resource.

- **Sensitive & personal data.**
- What is your personal data?

- **Legal implications:** GDPR, Data Protection Bill, IT Act 2000.
- Surveillance state & privacy index.

- **Data breaches & information leakage:** Who is responsible?

Research Problem:
Protection of sensitive & personal data using technology and policies

Research Problem:
Identifying the technical reasons (attack surface, attack vectors) for recent data breaches & development of mitigation strategies

The Human Factor

Human aspect of cybercrime

- Focusing only on the **technical side** won’t help to curb cybercrimes.
- Smart hackers & cybercriminals first **measure victimization** by **online engagement** (email or social media) and by studying **online behaviour** e.g. impulse online shopping, playing online games, downloading music, visiting specific websites etc.
- People who show signs of **low self-control** are found **more susceptible to malware attacks.**

The Human Factor

- Phishing, spear phishing, pharming, smishing, vishing.
- Mobile phones and app permissions.
- Personal information sharing on social media.
- Free WiFi, free downloads, free malware!

Reasons for Cyber Breaches

- Using old OS, browsers, antivirus, **unpatched IT resources** and **application software**.
- Responding to **unknown emails** (links, attachments).
- Visiting unknown / **suspicious websites**.
- Storing classified / personal information on **Internet PCs**, **laptops & smartphones**.
- Unauthorized use of **USB-drives** / removable storage.
- Irresponsible use of **smart phones** & **social media**.

Cyber Crimes in India

- **Website hacks** & **defacements.**
- **Data & information thefts.**
- **Phishing attacks** on **E-commerce** & **financial websites**.
- Cybercriminals targeting **social** & professional **networks**.
- Cybercrimes targeting **mobile platforms** (smartphones & tablets).

Other Cyber Crimes

- Identity theft.
- Data exfiltration, company secrets, IPR.
- DoS, DDoS.
- Ransomware infection.
- Crypto-mining.
- Supply-chain infection.

Misuse of Information

- Surface web
- Dark web
- Deep web

- TOR encrypted sites & traffic

Research Problem:

Cyber security recommender system for web browsers & mobile devices

Research Problem:

Identification & analysis of TOR traffic (in the organization)

Information & Cyber Warfare

- Concept involves the **battlespace use** & **management of ICT** in pursuit of a **competitive advantage over an opponent**.

- Involves **collection of tactical information**, **spreading of propaganda or disinformation** to demoralize or manipulate the enemy, **disrupting/denying victim's ability to gather & distribute information.**

- Makes use of **technology**.
  Also focuses on **human-related aspects** of information use.
  e.g. misinformation & fake news.

Cyber Attacks

- Home devices - Web cameras, climate control devices, door locks, refrigerators
- Medical devices – Insulin pump, paceamaker
- Car electronics
- Hospital, bank servers (ransomware)
- Critical systems – energy grid, nuclear power plant

Cyber Warfare

- **Cyberspace** is now considered as the **fifth domain / dimension of warfare.**
- Nature of cyber warfare is **asymmetric.** Incoming attacks are **not predictable.**
- **State actors** have become active in the cyberspace (Stuxnet, Flame, Gauss, Duqu...).
- Like nuclear weapons & missiles, **new cyber-weapons** (anonymous, zero-day) are being developed by many countries.

The Road Ahead

- **Large volumes of data are generated every moment. Its' proper use & protection is crucial.**
- **Apart from technology, human factor plays a vital role in cyber security.**

- **Cyberspace is the new dimension of warfare.**
- **Machine Learning** is a lucrative tool both for **cyber defence** and **cyber attacks.**

- The **present crisis** has widened the horizon of **cyber threat landscape**. Organizations should quickly **adapt to these changes** and **pay more attention** to **cyber security**.

Thanks for your attention

?

skptech@yahoo.com