Kewajipan, Maruah, Integriti

Cyber-Electronic Warfare:

Roles and Challenges in IR 4.0

By

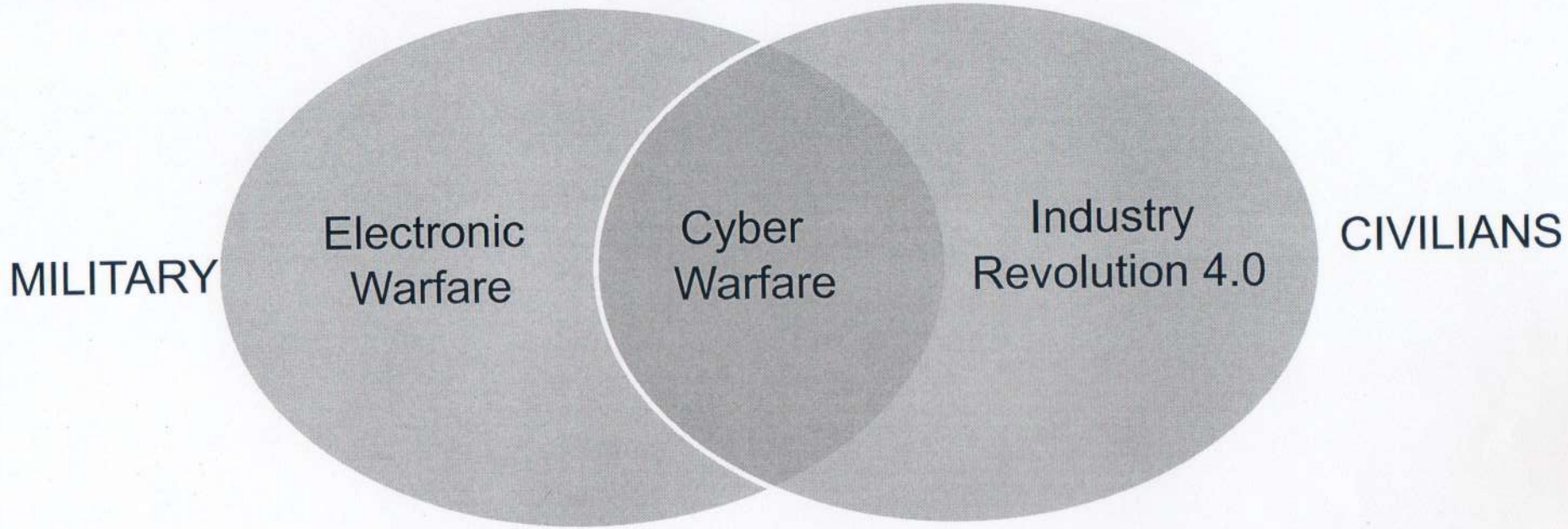
Assoc. Prof Maj Ir Dr Kamaruddin Abdul Ghani (Rtd)

Cyberspace and Electronic Warfare

Niche: Defence & Security

Cyber EW is any military action involving the use of electromagnetic energy to control the domain characterized by the use of electronics and the EM spectrum to use exchange data via networked systems and associated physical infrastructures.

Cyber, Electronic Warfare & IR 4.0



Cyber EW: collect live data, analyze them, and even make decisions based upon them.

IR 4.0

- Cyber-physical systems, the IOT, IOS, cloud computing and cognitive computing.
- Domains are overlapping and interconnecting.
- Role of Electrical Engineers and IT Experts are interdependent and complement each other.

The Need to Have Cyber-EW

- Cyber space is also becoming an operational domain for the military that contributes to improved decision making, increased situation awareness, as well as better command and control.

- There is a need for interdisciplinary center that connect academia and researchers not just in terms of sharing information, but also offering innovative and creative solutions.

Cyberspace and Electronic Warfare: The Similarity

Cyberspace:

A global domain within the information environment whose distinctive and unique character is framed by the

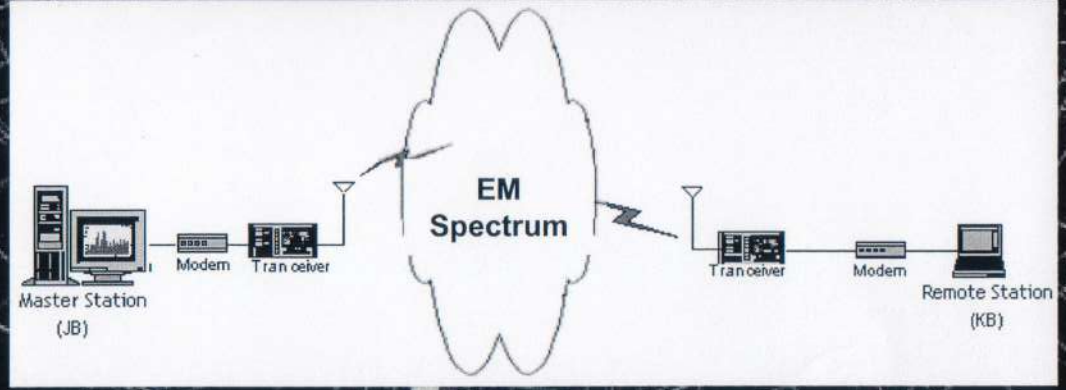
use of electronics and the electromagnetic spectrum

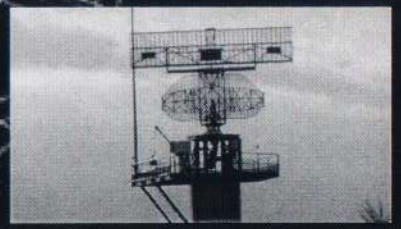
to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information communication technologies.

EW:

Any action involving the **use of the electromagnetic spectrum** or directed energy to control the spectrum, attack an enemy, or impede enemy assaults. The purpose of EW is to deny the opponent the advantage of, and ensure friendly unimpeded access to the electromagnetic spectrum.

Cyberspace and EW: Sharing the Same Spectrum

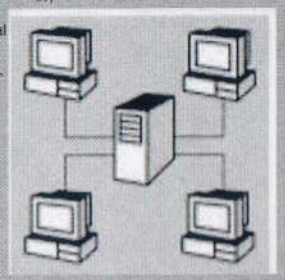




The Threats in Cyber and EW

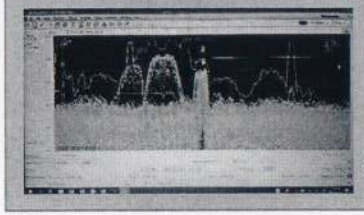
Cyber Threats

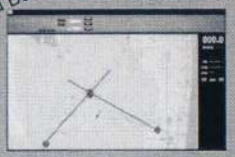
Malware Attack
Cyberattacks
Cyberthreats
LDAP Injection
Web Based Attack
Cyber Sabotage
DDos
Spyware
Port Scanning
Web Exploitation
Command & Code Injection
Directory Traversal
Cross Site Request Forgery
Cyber Espionage
Intrusion
Direct Attack
Wireless Hacking
Cross Site Scripting
Cryptographic Interception
ARP Spoofing
Network Sniffing
Exploiting
Wifi Snooping
Remote Code Execution
Zero Day Attac
Cross Site Scripting
Network Monitoring
Nmap
Bot &
URL Interpretation
Cookie Snooping & Poisoning
IPS & IDS
SQL Injection
Parameter Tampering
Application Hacking
HTTP Parameter Pollution
MITM
Network Hacking



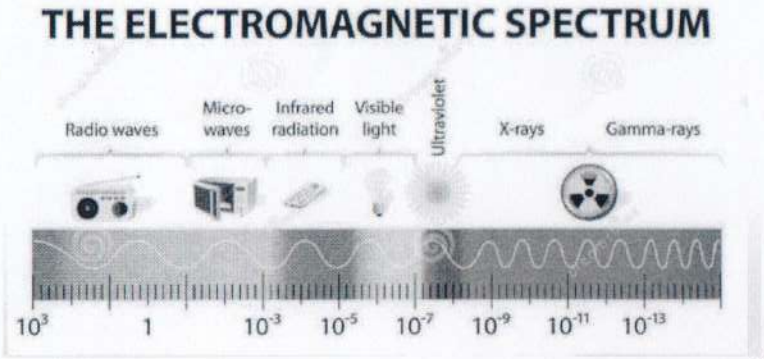
EW Threats

Radar Guided Missile
reconnaissance
Barrage Jammers
Intelligence
Decoy
Tapping
Interception
EMCON
Cyber-Physical System
Signal Analysis
Counter Surveillance
GPS Jammer
ARM
Spectrum Jammers
Decoding
Message Analysis
Deception
Eavesdropping
Bugging
Stealth
Transmission Protocol
Frequency Hopping
Decyphering
Intelligence Gathering
EMP
Missile
DEW
Sidelobes Canceling
Tracking and Beacons
Direction Finding
EOB
Spectrum Analysis
Spot Jammers





Cyber and EW: The Threat



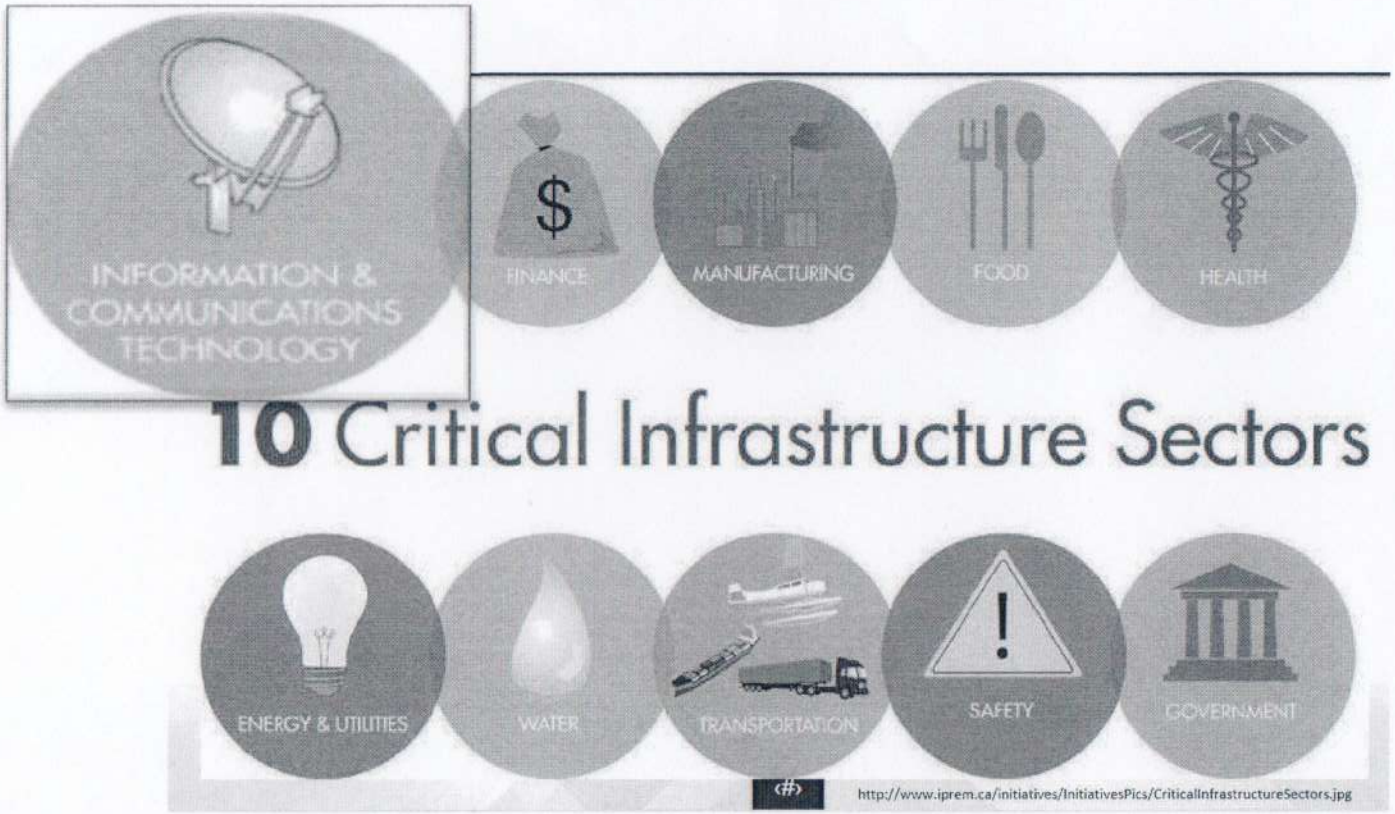
Challenges in Cyber-EW

- Security – ICT security risk is the most challenging
  - Online integration gives room to security breaches and data leaks
- Privacy – interconnected industry
  - Producers need to collect and analyze data
  - Threat to privacy

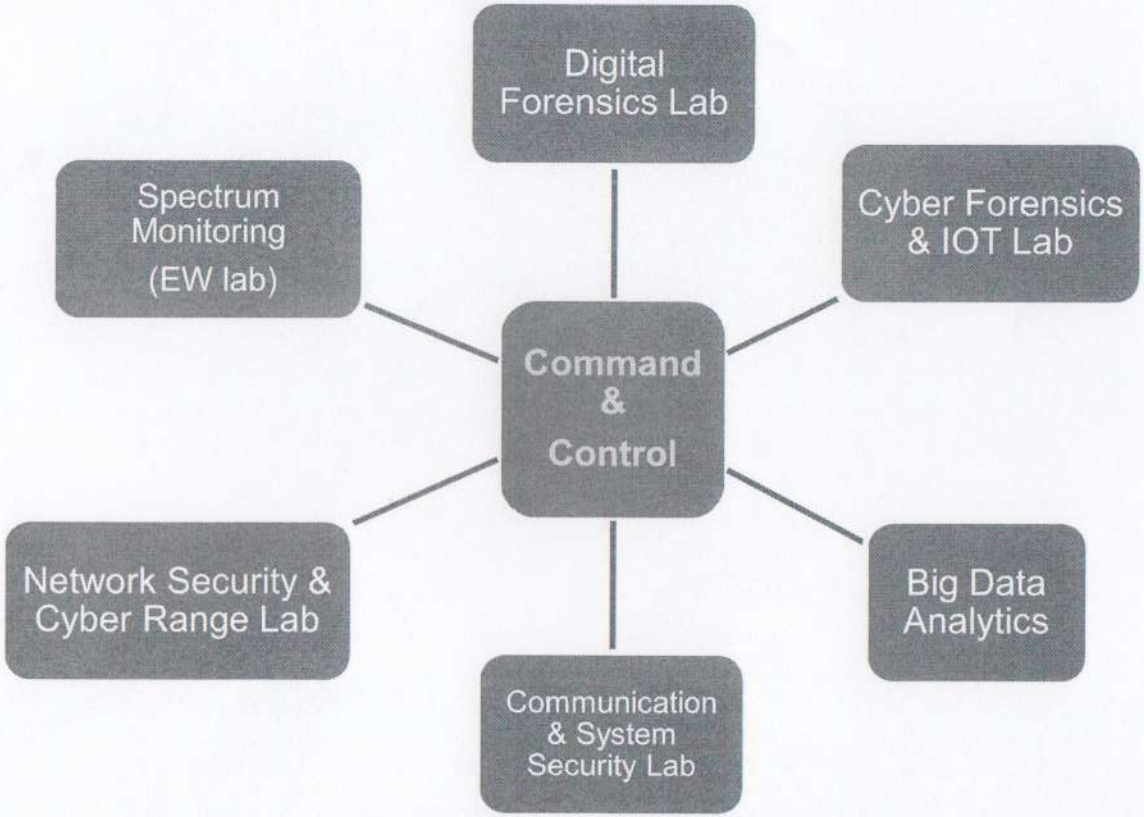
Establishment of Cybersecurity & EW Centre

- UPNM has set up a Centre of Excellence (CoE)
- Cyber Security Centre (CSC) to enhance teaching & learning as well as research in the area of cybersecurity and electronic warfare (EW).
- Joint establishment between Dept. of Electrical Engineering and the Dept. of Computer Science.

Cyber-Physical System



Cyber Security Centre (CSC) – Estb 2014



Roles of Electrical Engineers and IT Experts

- Electrical and Electronic Engineers
  - Focusing on the electronics and electromagnetic spectrum activities in EW
- IT Experts
  - Focus on the ICT and cyber related in Cyberspace.
- Complement each other

Electrical & Electronic Engineering Students

Program	Civilians	Military Cadets	Total
Bachelor of Electrical & Electronics Engineering (Communication)	39 (36%)	72 (64%)	111
Bachelor of Electrical & Electronics Engineering (Power)	46 (30%)	109 (70%)	155
	85	**181**	**266**

Academic and Professional Qualifications: Electrical Engineering

Active efforts for achieving Professional Engineer status from Board of Engineers Malaysia (BEM) .

Academic and Professional Qualifications	Current Percentage	Target (2020)
PhD	48%	60%
Professional Engineers (Ir)	17%	30%

*Based on Academic calendar 2018/2019

Computer Science and IT Students

Program	Civilians	Military Cadets	Total
Bachelor of Computer Science (Intelligence System)	21 (30%)	45 (68%)	66
Bachelor of Computer Science (Computer System Security)	25 (33%)	50 (66%)	75
	46	**95**	**141**

Academic and Professional Qualifications: IT Experts

Collaboration between Dept. of Computer Science and EC-Council: CEH, CHFI

Academic and Professional Qualifications	Current Percentage	Target (2020)
PhD	61.8%	60%
Certified IT Experts	6%	10%

*Based on Academic Calendar 2018/2019

Post Graduate Courses in Cybersecurity

	Post Graduate by Course	Collaboration with	Starting
1	MSc in Cybersecurity & Management	Warwick UK	2016 (2nd batch)
2	MSc in Digital Security	EURECOM France	2022

Collaborations with Gov/Industries

A. Cyber
   i. Cybersecurity Malaysia (CSM)
   ii. Malaysian Communications and Multimedia Commission (MCMC)

B. EW
   i. Malaysian Armed Forces (MAF)
   ii. CSIR South Africa

Conclusion

- We are prepared for the IR 4.0 challenges.
- Electrical Engineering and ICT fields play a very significant roles.
- Enhancing Cyber-Electronic Warfare capabilities.
- Increasing number of PhD, Professional Engineers and Certified IT Experts among the lecturers.

Thank you