THE EDUCATION UNIVERSITY OF HONG KONG

Course Outline

Part I

Programme Title	**:**	All undergraduate programmes
Programme QF Level	**:**	5
Course Title	**:**	Cyber security and daily life: National security and global perspectives
Course Code	**:**	GEK1034
Department	**:**	Mathematics and Information Technology
Credit Points	**:**	3
Contact Hours	**:**	39 hours
Pre-requisite(s)	**:**	Nil
Medium of Instruction	**:**	English
Course Level	**:**	1

Part II

The University's Graduate Attributes and seven Generic Intended Learning Outcomes (GILOs) represent the attributes of ideal EdUHK graduates and their expected qualities respectively. Learning outcomes work coherently at the University (GILOs), programme (Programme Intended Learning Outcomes) and course (Course Intended Learning Outcomes) levels to achieve the goal of nurturing students with important graduate attributes.

In gist, the Graduate Attributes for Undergraduate, Taught Postgraduate and Research Postgraduate students consist of the following three domains (i.e. in short "PEER & I"):

- **P**rofessional **E**xcellence;
- **E**thical **R**esponsibility; **&**
- **I**nnovation.

The descriptors under these three domains are different for the three groups of students in order to reflect the respective level of Graduate Attributes.

The seven GILOs are:

1. Problem Solving Skills
2. Critical Thinking Skills
3. Creative Thinking Skills

4a. Oral Communication Skills

4b. Written Communication Skills

5. Social Interaction Skills
6. Ethical Decision Making
7. Global Perspectives

1. Course Synopsis

Digital technologies permeate all aspects of our everyday life. The use of social media, artificial intelligence (AI), the Internet of Things (IoT) and mobile technologies reshaped the society, economy and education. The reliance of the use of technology in the digital age has led to consideration of the consequences regarding how we use the digital tools and how data privacy is done over the Internet. This course covers the topics of being a good digital citizen to take ownership of their digital lives to media balance and well-being online and consider cyber security technologies, data privacy and national security in global perspectives. The course includes the technology implications of national security education across privacy, cybersecurity, data and trade issues to meet the requirements and regulatory rules on both national and industry-specific levels. As the Greater Bay Area is a highly developed transport hub, it is important to promote the use of security measures to strengthen the protection of communication networks and raise the level of information security protection. Class activities, including case studies, quizzes, role play and online games, are used to deliver the fundamentals of digital safety, cyber security and national security in local and global perspectives. Emerging technology opens the door for new opportunities and possibilities to improve life quality, but it also introduces potential risks and damages. The ethical, legal and social aspects of the proper use of the emerging technologies to safeguard national security will also be discussed with daily life examples.

2. Course Intended Learning Outcomes ($CILO_s$)

Upon completion of this course, students will be able to:

$CILO_1$ identify cyber security measures and common cyber security practices in local, national and global perspectives

$CILO_2$ apply security technologies and skills for threat prevention and safeguarding the online systems from local to national perspectives

$CILO_3$ analyse real-world incidents to understand various types of cyber security attacks

$CILO_4$ develop awareness of ethical and legal issues in cybersecurity and national security

3. Content, CILOs and Teaching & Learning Activities

Course Content	CILOs	Suggested Teaching & Learning Activities
Cyber security Measures and Practice (13 hours) - Cybercrime figures and report - Centralised security policy - IoT security - Multi-factor authentication - Cryptography and firewall - Personal data privacy practice and protection - IT security standards and practices	$CILO_{1,2,3}$	Lectures, group discussions and case studies

Cyber Attacks and National Security Threats in local, national, and global perspectives (13 hours) - Malware - Password Attacks - DOS/ DDOS - Hactivism/ Man in the Middle - National security threats in cyberspace - Cyber Warfare and National Security	$CILO_{2,3}$	Lectures, group discussions, workshops, case studies and presentation
Cybersecurity Laws and National Cyber Security Education (13 hours) - National and international cyber-attacks on government agencies, defense and infrastructure companies - Legal frameworks for combating cybercrime - Measures of safeguarding national security - Cyber security ethics and ethical principles in daily life - Local, national, and global cybersecurity legislation and data security laws - Cyber security education in schools to safeguard national security	$CILO_{1,3,4}$	Lectures, case studies, seminar, class discussions and exercises

4. Assessment

Assessment Tasks	Weighting (%)	CILO
a. Class Exercises Each student needs to work on class exercises to apply different cyber security technologies and measures. Discuss and examine cyber security threats and national security measures.	20%	$CILO_{1,2}$
b. Case Study Students need to work in groups (4 to 6 students) to conduct an oral presentation (20%) to describe a real-world cyber security-attack case with detailed analysis on the reason(s), impacts and solutions. Discuss the impacts on personal, society and national aspects. Each group should create a short digital story to demonstrate the whole scenario with captions/ narrations in slideshow/ video format (20%).	40%	$CILO_{1,2,3,4}$

c. Reflective Essay Each student needs to write a reflective essay (no less than 1,200 English words) to elaborate his/her critical understanding of the recent measures of cyber security, the impact of advancement of technologies on cyber security and national security, and the negative impact of unethical and illegal manipulation by considering code of ethics and laws from local and global perspectives. Suggest the ways to promote and implement cyber security education supported with the implications at schools, workplaces and daily lives.	40%	*CILO1,2,3,4*

5. Required Text(s)

Nil

6. Recommended Readings

ACM Code Task Force (2018). Code of Ethics. The Association for Computing Machinery (ACM). https://www.acm.org/code-of-ethics

Christensen, ProQuest Information Learning Co, & University of California, Los Angeles. Library Information Science 0509. (2018). The Ethics of Social Media Policy : National Principles of Justice, Security, Privacy and Freedom Governing Online Social Platforms in Russia, China and the United States.

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Education and Information Technologies, 27(4), 4729–4752. https://doi.org/10.1007/s10639-021-10806-7

Dakota Cary (2021). China's National Cybersecurity Center - A Base for Military-Civil Fusion in the Cyber Domain, Center for Security and Emerging Technology.

Dawson, ProQuest Information Learning Co, & London Metropolitan University. (2017). Hyper-connectivity : Intricacies of national and international cyber securities.

Duxbury, & Haynie, D. L. (2019). Criminal network security: An agent-based approach to evaluating network resilience. Criminology (Beverly Hills), 57(2), 314–342. https://doi.org/10.1111/1745-9125.12203

England, & Utica College. Cybersecurity. (2020). Internet of Things Device Cybersecurity and National Security.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities. Journal of Physics: Conference Series, 1339(1), 12098. https://doi.org/10.1088/1742-6596/1339/1/012098

Guo, M. (2018). China's cybersecurity legislation, it's relevance to critical infrastructures and the challenges it faces. International Journal of Critical Infrastructure Protection, 22, 139–149. https://doi.org/10.1016/j.ijcip.2018.06.006

Hasheminasab, & Tork Ladani, B. (2018). Security Investment in Contagious Networks. Risk Analysis, 38(8), 1559–1575. https://doi.org/10.1111/risa.12966

Ji, C. (2018). Cybersecurity and Data Protection: A Study on China's New Cybersecurity Legal Regime and How It Affects Inbound Investment in China. The International Lawyer, 51(3), 537–552.
Kharlamov, & Pogrebna, G. (2021). Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity. Regulation & Governance, 15(3), 709–724. https://doi.org/10.1111/rego.12281
Kutylowski, Wang, Y., Xu, S., & Yang, L. T. (2018). Special issue on social network security and privacy. Concurrency and Computation, 30(5), e4414. https://doi.org/10.1002/cpe.4414
Latham & Watkins (2022). China Issues New Rules on Cybersecurity Review for Network Platform Operators Listing Abroad.
Monoscalco, Simeoni, R., Maccioni, G., & Giansanti, D. (2022). Information Security in Medical Robotics: A Survey on the Level of Training, Awareness and Use of the Physiotherapist. Healthcare (Basel), 10(1), 159. https://doi.org/10.3390/healthcare10010159
Morris, ProQuest Information Learning Co, & Utica College. Cybersecurity. (2017). The Misuse of Encryption and the Risks Posed to National Security.
Musa. (2018). Network security and cryptography : a self-teaching introduction. Mercury Learning and Information.
Oncioiu, IGI Global, publisher, & Ideal Group. (2020). Network security and its impact on business strategy. IGI Global.
Özsungur, F. (2022). Cyberbullying and the Importance of Cyber Security Awareness in Preventing Cyberbullying. In Handbook of Research on Cyber Approaches to Public Administration and Social Policy (pp. 365–379). IGI Global. https://doi.org/10.4018/978-1-6684-3380-5.ch015
Peltier. (2017). Managing a network vulnerability assessment (1st edition). CRC Press.
Rahima Aissani. (2022). Anti-Cyber and Information Technology Crimes Laws and Legislation in the GCC Countries: A Comparative Analysis Study of the Laws of the UAE, Saudi Arabia and Kuwait. Journal of Legal, Ethical and Regulatory Issues, 25(1), 1–14.
Romaniuk, & Manjikian, M. (2021). Routledge companion to global cyber-security strategy. Routledge.
Rupesh Kumar, Shreyas Parakh, & CNS Vinoth Kumar. (2021). Detection of Cyberbullying using Machine Learning. Turkish Journal of Computer and Mathematics Education, 12(9), 656–660.
Sabharwal, & Pandey, P. (2020). Pro Google Kubernetes Engine. Apress L. P.
Sadiqui. (2020). Computer network security. ISTE : Wiley.
Timmers. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. Minds and Machines (Dordrecht), 29(4), 635–645. https://doi.org/10.1007/s11023-019-09508-4
Yang, & Xu, J. (2018). Privacy concerns in China's smart city campaign: The deficit of China's Cybersecurity Law. Asia & the Pacific Policy Studies, 5(3), 533–543. https://doi.org/10.1002/app5.246
Zureich, & Graebe, W. (2015). Cybersecurity: the continuing evolution of insurance and ethics. Defense Counsel Journal, 82(2), 192.

7. Related Web Resources

Cybersecurity scenarios

https://www.cisa.gov/publication/cybersecurity-scenarios

https://www.cisa.gov/cyber-storm-i

Gamified Cyber Simulation Platform

https://www.hacktale.com/
Cyber Attack game
https://store.steampowered.com/app/1230560/Cyber_Attack/
Interland (by Google)
https://beinternetawesome.withgoogle.com/en_us/interland
Online tutorial on Cybersecurity
https://www.edureka.co/blog/cybersecurity-firewall/
Best Cybersecurity Practices
https://www.ekransystem.com/en/blog/best-cyber-security-practices
China's Cybersecurity Law and safeguards for national cyberspace sovereignty and security
https://www.protiviti.com/HK-en/insights/china-cybersecurity-law-and-impacts
National Cybersecurity Strategies Repository
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
Local cyber security information portal and network security incident reporting
https://www.ogcio.gov.hk/en/our_work/information_cyber_security/community/

8. Related Journals

Intelligence, Crime and Cybersecurity
Journal of Cybersecurity
Computers & Security
International Journal of Information Security and Cybercrime
Journal of Cybersecurity and Privacy
International Journal of Cyber Criminology

9. Academic Honesty

The University upholds the principles of honesty in all areas of academic work. We expect our students to carry out all academic activities honestly and in good faith. Please refer to the *Policy on Academic Honesty, Responsibility and Integrity* (https://www.eduhk.hk/re/uploads/docs/00000000001633679892454 8BbN5). Students should familiarize themselves with the Policy.

10. Others

Nil

Last update: 21 July 2022