CC0002 Navigating The Digital World Notes

Hankertrix

April 29, 2025

Contents

1 Definitions

1.1 Computational

Involving the calculation of answers, amounts, results (e.g. calculation, order).

1.2 Thinking

The activity of using your mind to consider something (e.g. reasoning, questioning).

1.3 Competencies

Important skills that are needed to do a job (e.g. managerial competencies).

1.4 Bioinformatics

Combines different fields of study, including computer sciences, molecular biology, biotechnology, statistics and engineering.

1.5 Pseudocode

An informal description of the steps involved in executing a computer program, often written in something similar to plain language (plain English for example).

1.6 Computational thinking

A problem-solving process that anyone can use in various areas in our daily lives.

1.6.1 How?

By breaking down a problem

- Look for similarities
- Identify relevant information and opportunities
- Create a plan for the solution

1.7 Pangaea

A supercontinent made up of the current 7 continents.

1.8 Geology

The study of structure, evolution, and dynamics of the Earth and its natural mineral and energy resources.

1.9 Quantitative reasoning

Reasoning about things in a quantitative manner, such as asking questions that relate to an amount of something. These questions are usually testable.
Quantitative reasoning tells you:

- how to **frame** concrete numerical questions

- how to **identify** tools and data for analysis

- how to **build** models to analyse the data

- how to **analyse** the results you obtain

1.9.1 Examples

1. How much arsenic in water may still be safe?

2. Does smoking cigarettes really cause cancer?

3. Is renting better than buying your own property?

4. How long should the traffic lights stay red?

Data-driven quantitative questions:

1. How does the app know what I want to buy?

2. How does the World Bank allocate the aids?

3. Which country is the "happiest" in the world?

4. Will blue whales survive of face extinction?

1.9.2 Example of arsenic in water

How much arsenic is in the swimming pool?
   To answer the question, we will need to have a clear idea about:

- Quantities and units in relative terms

- Volumetric measures, given the dimensions

- Proportions and conversion techniques

All that is in addition to the basic knowledge of:

- Global regulations for safe arsenic levels

- Sampling techniques and basic statistics

1.9.3 Example of renting vs buying a house

Will you rent or buy a given flat?
   To answer the question, we will need to have a clear idea about:

- Financial quantities and their relationship

- Rates, periods and compounding effects

- Proportions and comparison techniques

All that is in addition to the basic knowledge of:

- Real estate valuation and appreciation

- Forecasting and the market volatility

1.9.4 Example of the app knowing what you want to buy

The app has a clear idea about:

- Purchasing habits of several individuals

- Effects of pricing on sales over the years

- Placement strategies for improving sales

All this is in additional to the basic knowledge of:

- Who and where you are and what you like

- Market behaviour and the competition

1.10   Cybersecurity

- Cybersecurity refers to the practices, processes and technologies implemented by an organisation to protect its cyber assets from damage, malicious attack and unauthorised access.

- Cybersecurity maintains the confidentiality, integrity and availability of **systems**.

1.11   CIA acronym

An acronym to help keep ourselves cyber safe.

1.11.1   Confidentiality (C)

Ensuring data or information cannot be read by unauthorised personnel.

- Protect your personal information

- Share only what is necessary

1.11.2   Integrity (I)

Ensuring data or information held by an individual or organisation remains accurate and unmodified by unauthorised personnel.

- Practice good cyber hygiene

- Beware of fake sources of information

1.11.3   Availability (A)

Ensuring data or services remains usable or accessible with sufficient capability and capacity.

- Prevent getting locked out of your devices

- Your actions can affect others

1.12   Data

- Data can be in both physical and digital formats.

- It can belong to an individual or an organisation.

1.13 Data security

Data security is the process of protecting and maintaining the confidentiality, integrity and availability of **data**.

1.14 Phishing

- The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information such as passwords and credit card numbers.

- Phishing is a cyberattack in which criminals pose as legitimate institutions to lure individuals into providing sensitive data such as:

  - Personal information
  - Passwords
  - Credit card details

1.15 Falsehoods

A statement is false if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears.

1.16 Misinformation

The inadvertent dissemination of false information.

1.17 Disinformation

The intentional dissemination of false information.

1.18 Fake news

A specific type of falsehood intentionally packaged to look like news to deceive others.

1.19 Confirmation bias

Confirmation bias is the human tendency to seek and believe in information that confirms our existing beliefs.

1.20 Informational apathy

Informational apathy refers to people not bothering to take an action to correct fake news that they see on social media sites.

1.21 Verification

The process of evaluating the veracity of a story before it becomes the news.

1.22 Fact-checking

A process that occurs post publication and compares an explicit claim made publicly against trusted sources of facts.

1.23 Morality

Morality is a subject that pertains to right and wrong action.

- In all human societies on the ethnographic record, people make distinctions between right and wrong.

- I take it that you have your own views about what is right and wrong.

- In the branch of ethics called normative ethics, we try to arrive at well-founded views about morality.

1.24 Ethics

Ethics is the study of morality.

1.25 Normative ethics

- Normative ethics is a branch of ethics.

- It tries to arrive at well-founded views about morality.

- It tries to support our views about right and wrong in the most rational way possible.

- Normative ethics relates to using, applying, and developing digital and online tools.

- It has multiple branches, two of which are data ethics and digital ethics.

1.25.1   Moral theories

In normative ethics, moral theories are developed to achieve two aims:

- Theoretical aim: To explain what features of actions make them morally right or wrong.

- Practical aim: To offer practical guidance in making morally correct decisions.

There are three moral theories that are the most influential in normative ethics.

1. Utilitarianism (Jeremy Bentham, John Stuart Mill, Peter Singer, etc.): An action is morally right when it would likely produce at least as much well-being (welfare) as would any other action one would perform instead. Otherwise, the action is wrong.

    - The classical utilitarians, such as Bentham and Mill, took well-being to consist of pleasure and the absence of pain.
    - Peter Singer, a contemporary utilitarian, takes well-being to consist of the satisfaction of one's preferences or desires.

2. Virtue ethics (Confucius, Aristotle, etc.): An action is morally right when it is what a virtuous person would do in the circumstances. Otherwise, the action is wrong.

    - Commonly recognised virtues include honesty, courage, justice, temperance, beneficence, humility, loyalty, and gratitude.
    - A truly virtuous person is one who has all the virtues. A virtuous person may only be a hypothetical ideal that we can strive to be.

3. Immanuel Kant's deontological ethics: An action is morally right when it treats persons (including oneself) as ends in themselves and not merely as a means. Otherwise, the action is wrong.

    - Kant's theory says that all persons are unconditionally valuable insofar as they are rational and autonomous.
    - It also says that we should respect the value of persons, and not use them in a way that disrespects their value.

1.26　Cyberbullying

Cyberbullying is the use of the internet or digital devices to inflict psychological harm on a person or group.

1.26.1　Examples

- Repeatedly texting or emailing hurtful messages to another person.

- Spreading derogatory lies about another person.

- Tricking someone into revealing highly personal information.

- "Outing" or revealing someone's secrets online.

- Posting embarrassing photographs or videos of other people without their consent.

- Impersonating someone else online in order to damage that person's reputation.

- Threatening or creating significant fear in another person.

1.26.2　Prevalence

- According to the 2020 Child Online Safety Index (Cosi) report, which includes data on 145,000 children across 30 countries, 45% of 8 to 12-year-olds experienced cyberbullying, either as the bullies or as the victims.

- Within Singapore, 40% of 8 to 12-year-olds and 52% of 13 to 19-year-olds were exposed to cyberbullying.

1.26.3　Effects

- Depression and anxiety

- Low self-esteem

- Difficulty sleeping

- Headaches, stomachaches

- Suicidal thoughts

- Suicide attempts

- Eating disorders

1.26.4 What to do if you are cyberbullied

- Don't blame yourself.

- Don't retaliate.

- Save the evidence. Take screenshots of text, record audio, screen record videos etc.

- Talk to someone you trust.

- Block the bully.

- Report the bully.

- Keep social media passwords private.

- Restrict others' access to your social media pages.

- Change your social media accounts. If you're harassed, delete the account and create a new one.

1.26.5 How to know if someone you are around is being cyberbullied

- Changes in mood or personality.

- Work or school performance declines.

- Lack of desire to do things they normally enjoy.

- Upset after using phone or going online.

- Secretive about what they are doing online.

- Unusual online behaviour, like not using the phone or computer at all, using the phone or computer all the time, and receiving lots of notifications.

- Deleting social media accounts.

1.27 Informational privacy

Informational privacy is the confidentiality, anonymity, data protection, and secrecy of facts about persons.

1.28 Whistleblower

A whistleblower is someone who breaks ranks with an organisation in order to make an unauthorised disclosure of information about a harmful situation after attempts to report the concerns through authorised organisational channels have be ignored or rebuffed.

- Whether to "blow the whistle" can arise in any organisation, not just in government agencies and private businesses.

- NTU has its own dedicated whistleblowing channel, which is taken very seriously.

1.29 Intellectual property (IP)

- Creations resulting from the exercise of the human brain.

    - Examples include inventions, designs, ideas, plant hybrids, music, poems, paintings, photographs, logos, books, films, cartoon characters, and trade secrets.

- Bundle of legal rights protecting such creations, i.e. intellectual property rights (IPRs).

- IP law recognises that creators have the right to protect their work.

    - IP law gives legal rights to IP creators, allowing them to control and exploit the use of their IP for a specific period of time.

1.30 Copyright

- Copyright is the right to prevent the unauthorised copying of the tangible form in which a person has chosen to express his ideas, for example in a short story, musical composition, theatre script, painting, computer program, photograph, movie or video game.

- It can be described as a **bundle of exclusive rights belonging to the copyright owner**.

- It allows owners to enforce their rights against infringement.

- Singapore's copyright law is governed by the Copyright Act.

1.31 Contract

- An agreement giving rise to obligations which are enforced or recognised by law.

- It is a voluntary agreement between two or more parties.

- The law exists to govern and regulate the parties' relationship in such agreements.

- It can be verbal or written, simple or complicated.

1.32 Licence

- A licence is a type of contract that gives permission to the holder or recipient to carry out a certain act, which would be infringing in nature otherwise.

- A licence gives the owner the ability to use or exploit intellectual property commercially, most commonly requiring a fee in return for the grant of the licence.

1.32.1 Non-exclusive licence

Non-exclusive licences are granted to more than one person.

1.32.2 Exclusive licence

Exclusive licences are granted to one person only.

1.32.3 Where are licences used?

- All social media platforms

- All software as a service (SaaS) platforms.

- All media aggregation platforms where works can be assessed for use.

1.32.4   Licensing vs assignment

Licensing	Assignment
Grants someone else (other than the IP owner) the right to use the IP	Transfers the entire title and interest in someone's IP to another
Less costly	More costly
IP owner remains in control	IP owner gives up control

- Consider the situation where you want to own or license ("hire").

- If someone is creating something new for you, and you wish to have complete control over it, you may want to take an assignment of the IP rights in the thing created.

- If there is an IP already created by someone else that you wish to use for a specific reason, you may want to just license the IP.

- There will be a cost difference.

1.32.5   Licence of rights

"In consideration of the Publisher paying the Advance Payment and the Royalty to the Author, the Author grants to the Publisher for a period of __ years, beginning on __ or date of this Agreement until __, the sole and exclusive right to publish, use, and licence the Work and any parts of it in all media now known and yet to be invented, including but not limited to all methods of publication and reproduction including hardback, paperback, e-book/digital, serialization, translations, anthologies, quotations, mechanical reproduction, television, radio, theatre, film, media merchandising and the Internet in the Territory for the entirety of the Licence Period."

1.32.6   Strength of licences

- The way a licence is worded can make it almost as strong or effective as an assignment.

- Thus, it is important to understand the language used in licences and assignment agreements.

1.33 Assignment

An assignment is another type of contract. An assignment must be in writing and signed by or on behalf of the assigner.

1.33.1 Legal meaning of "assign"

To regard as belonging to.

1.33.2 Legal effect

- Under the assignment, the assigner (person making the assignment) transfers all entitlement and ownership rights that are the subject of the assignment to the assignee (the person receiving the rights).

- The assignee is not the new owner of the property.

1.33.3 Licensing vs assignment

Licensing	Assignment
Grants someone else (other than the IP owner) the right to use the IP	Transfers the entire title and interest in someone's IP to another
Less costly	More costly
IP owner remains in control	IP owner gives up control

- Consider the situation where you want to own or license ("hire").

- If someone is creating something new for you, and you wish to have complete control over it, you may want to take an assignment of the IP rights in the thing created.

- If there is an IP already created by someone else that you wish to use for a specific reason, you may want to just license the IP.

- There will be a cost difference.

1.33.4 Assignment of rights

"The Writer hereby assigns to the Company all copyright, title, interest and all other rights (including all vested future and contingent interests and rights) concerning the Story, the characters depicted in it and all other output of the Writer's Services conferred under the laws of any country throughout the world (whether now in force or which may be enacted, promulgated or come into effect in the future) for the use and benefit of the Company fully for the entire period or periods of copyright protection including all reversions, renewals and extensions, provided by the laws of any country throughout the world."

1.34 Artificial intelligence (AI)

- Artificial intelligence refers to machines that are capable of performing tasks that typically require human intelligence.

- The focus of artificial intelligence was on the engineering of making intelligent machines and programs.

- It was implemented using rule-based expert systems and fuzzy logic.

- This means that machines are just programs with specific rules for them to exhibit, which are programmed in by the programmer who is a domain expert.

1.35 Machine learning

- Machine learning is the ability of machines to learn without being programmed.

- Large amounts of data is needed to train the machines.

1.35.1 Supervised learning

Supervised learning is machine learning that is supervised with **labels**, such as for regression and classification.

1.35.2 Unsupervised learning

Unsupervised learning is machine learning that doesn't have any supervision from **label**. In other words, the machine is fed **unlabelled data**. An example of this approach is the clustering technique.

1.35.3 Reinforcement learning

Reinforcement learning is machine learning with the use of an "agent" that learns to maximise the "reward" in an environment.

1.36 Hidden layer

- The hidden layer consists of parameters that can be trained when the model is fed with a large amount of data.

- It is the layer that contains the "algorithm" that can learn and improve by itself.

1.37 Deep neural network

A deep neural network is a neural network that consists of multiple hidden layers.

1.38 Deep learning

- Deep learning is just machine learning using a deep neural network that mimics human brains and is a branch of machine learning.

- It is the "algorithm" of deep neural networks.

1.38.1 Artificial neural network (ANN)

Artificial neural networks are usually used for classifying **numbers-based data**.

1.38.2 Convolution neural network (CNN)

Convolution neural networks are usually used for classifying **images**.

1.38.3 Recurrent neural network (RNN)

Recurrent Neural Networks are usually used for time series data, such as audio and video.

1.38.4 Deep reinforcement learning

Deep reinforcement learning is just regular reinforcement learning but with neural networks.

1.38.5 Transfer learning

Transfer learning is a technique where a model trained on one task is repurposed for another related task.

1.39 Big data

Big data just means a massive amount of data.

1.40 Inference process

Inference process is a training process that a machine goes through where it is fed with huge amounts of data for it to recognise and learn from a pattern to deal with similar data in the future.

2 Computational thinking competencies

2.1 Abstraction

- Identifying and utilising the structure of concepts and main ideas.

- Simplifies things

    - Identifies what is important without worrying too much about the detail

- Allows us to manage the complexity of the context or content

- Helps to filter out unnecessary details and highlight important ones

- Involves the induction of ideas or the synthesis of particular facts into one general theory

2.1.1 How to abstract?

- Provide labelling

- Make use of numbers, colours, shapes to simplify information

2.1.2 Examples

- Abstract art, such as cave drawings of dots and symbols, which is a form of communication between the past and the present as we can at least figure out what ancient lifestyles and costumes are like.

- Providing a book synopsis, as you would have to sieve out the main plot line of the book and omit small details describing the appearance of characters.

2.2 Algorithm

- Following, identifying, using, and creating an ordered set of instructions

- Ordering things in either ascending order (e.g. from 1 to 5) or in descending order (e.g. from 5 to 1)

- Allows us to order the complexity of the context or content

2.2.1 An example

The legislative process is a form of algorithm. The judicial system assists in maintaining consistency and reducing bias.

The process of creating a law can be broken down in the these steps:

1. Introducing the bill in Parliament

2. Debating

3. Voting in Parliament

4. Presenting for the President's approval

2.2.2 Other examples

- Traditional poetry, which is defined due to its regular rhythm, verse structure and rhyme scheme.

2.3 Decomposition

- Breaking down data, processes or problems into smaller and more manageable components to solve a problem.

- Each sub problem can then be examined or solved individually, as they are simpler to work with

- Natural way to solve problems

- Also known as to divide and conquer

- Solves complex problems

  - If a complex problem is not decomposed, it is much harder to solve at once. Sub problems are usually easy to tackle.

- Each sub problem can be solved by different parties of analysis

- Decomposition forces you to analyse your problem from different aspects

2.3.1 Examples

- Counting up the coins in a piggy bank, as we would normally separate the coins into bundles of the same type and then count them up separately, before adding their totals together.

- Organisational structure in an organisation, where it would have different departments and teams that hold different sets of responsibilities and powers to ensure a sustained and effective working environment. Each department will then have to submit reports on the work that they have done, which allows organisations to operate efficiently.

- Essay writing in school, as the essay is usually broken down into parts like the introduction, body, and the conclusion. Then, we can tackle each part of the essay separately.

2.4 Pattern recognition

- Is observing patterns, trends and regularities in data (Google's definition)

- A pattern is a discernible regularity

  - The elements of a pattern repeat predictably

- In computation thinking, a pattern is the spotted similarities and common differences between problems

- It involves finding the similarities or patterns among small, decomposed problems, which can help us solve complex problems more efficiently

- Patterns make problems simpler and easy to solve

- Problems are easier to solve when they share patterns, we can use the same problem-solving solution wherever the pattern exists

- The more patterns we can find, the easier and quicker our problem-solving will be

2.4.1 Examples

- Geologists found that the fossil of plants present in the Svalbard in Norway were not the same hardy plants that survived now, so the plants were part of the tropics. They also found that the continents and the rock layers fit together as well, which allowed them to use pattern recognition to figure out that Pangaea existed in the past and the 7 continents we have today are split from Pangaea.

- Young children learning how to pronounce words use pattern recognition to learn how to pronounce a group of words easily.

3 Testing techniques

Suppose you take the drug for a headache now, and your headache goes away within the next hour. Does this mean the drug is effective?

3.1 Desired insights on the problem

- Does the drug at all reduce your headache in reasonable time?

- Does the drug manage to work better than a placebo?

3.2 Steps to obtain the desired insights

- How to **frame** concrete numerical questions?

- How to **identify** tools and data for analysis?

- How to **build** models to analyse the data?

- How to **analyse** the results you obtain?

3.3 Identifying your data

3.3.1 What type of data is relevant?

- Binary: Did your headache subside?

- Continuous: How long did it take to subside?

3.3.2 How much data do you need?

- Is it sufficient to have a single data point?

- Is it required to have a million data points?

3.3.3 Do you want a comparison?

- Which base case would you compare with?

- Is it possible to get data for both the cases?

3.4 Formulating your question

3.4.1 Which case seems to be better?

- Will better in any one of the trials suffice?

- Does it have to be better in all the trials?

- Is it fine if one is better on average?

3.4.2 Is average behaviour sufficient?

- What if the drug seems better on average?

- Do you know if the drug will always be better?

- How about being better most of the time?

3.5   Comparing distributions

- A line plot is for plotting data-points connected by lines

- A histogram is for counting frequency across specific bins (a value that is representative of an interval, which is usually the central value like the mean or median)

3.6   Comparing likelihoods

3.6.1   Idealise the distribution

Assume a normal or Gaussian distribution for the placebo data and find the mean and standard deviation.

3.6.2   Recreate the distribution

Recreate the distribution of the **mean** of the drug trials data set using the idealised distribution of the placebo data obtained earlier. This just means dividing the standard deviation of the placebo data set by the square root of the number of drug trials, which in this case is 30.

3.6.3   Analyse the distribution

Find the probability (likelihood) that the value of the recreated distribution is the same as the actual mean of the drug trials data set.

3.7   Summary

All the steps are above are the steps of hypothesis testing. Below are the hypothesis testing steps:

1. Start by assuming that the drug is identical to the placebo in efficacy.

2. Data hypothesis: The drug trials are identical to the placebo trials.

3. Statistical hypothesis: Statistics of drug trials are identical as if they are drawn from placebo trials.

4. Test the statistical hypothesis using the actual mean from the data set of the drug trials.

5. Obtain the probability from that test to determine whether the drug is identical to the placebo, which is usually checking whether the probability is less than a specific value, usually 1%, 2%, 5% or 10%.

4 Cybersecurity

4.1 Phishing

In 2018 alone, there were more than 16,100 phishing cases.

4.2 Strong passwords

- The password is at least 8 - 12 characters long.

- The password consists of a mixture of numbers, symbols, upper and lowercase letters.

- Use uncommon words for the password.

- The password should be long and random.

- The password should also be easy to remember.

- Create a password from a sentence or a phrase that makes sense to you.

- Do not use personal information in your passwords, such as your name, NRIC, or birthdate as such information can be easily guessed by cyber criminals if they obtain your personal information through other means.

- Always activate two-factor authentication if possible. This can be done by enrolling your mobile number or email address to receive a one-time password (OTP), or through an authentication app.

- Use different passwords for different accounts, especially for more important accounts such as your banking and payment accounts.

- Change your passwords regularly.

- Never share your password with anyone else.

4.2.1 Examples of 2-factor authentication (2FA)

- One-time passwords (OTP) through SMS or an authenticator app

- Biometrics like fingerprints or iris data

4.3 Data classification

4.3.1 Level 1 - Open

This classification applies to data that can be distributed to the public or published on the internet.

4.3.2 Level 2 - Restricted

This classification applies to any data that is generally made accessible to members of an organisation but not to the public. Some examples in a university context are internal meeting minutes, presentation files and project reports.

4.3.3 Level 3 - Confidential

- This classification applies to any data that is contractually defined as confidential, or is by nature confidential. Examples of such data includes personal identifiable information, staff performance reports and audit reports.

- If confidential data is disclosed, the party disclosing the data may be subjected to statutory penalities. The disclosure of confidential data also causes damage to the organisation.

4.3.4 Level 4 - Classified

- This classification applies to any information that is covered under the Official Secrets Act in Singapore.

- Unauthorised disclosure of such information may result in damage to national security.

4.4 Tips on securing data

1. Lock your workstation when leaving your desk.

2. Adopt a clean-desk policy and keep your desk clear.

3. Send and store work information through organisational accounts.

4. Keep your data storage devices securely.

4.5 Safe cyber practices

- Always choose to use trusted Wi-Fi networks and avoid doing sensitive transactions.

- Always choose to use "BCC" instead of "CC".

- Be mindful when connecting an external device to your computer.

- Do remember to install an antivirus software on your devices and always ensure that it is up-to-date.

- Spots the signs of phishing emails.

- Use strong passwords.

- Enable multiple factor authentication (MFA).

- Secure data using encryption.

- Follow the Acceptable IT Usage Policy (AIUP) and conform to security best practices.

4.6 NTU's Acceptable IT Usage Policy (AIUP)

4.6.1 Do's

- Update passwords regularly

- Keep your passwords safe

- Use NTU email for official communications

- Use blind carbon copy (BCC) for mass emails

- Keep your software updated with security patches

4.6.2 Don't's

- Share your passwords

- Forward NTU documents to personal email or storage

- Install software without appropriate licences

- Turn off antivirus or cancel software updates

- Overshare on social media

4.7 Cybersecurity agency (CSA) Singapore

- Established in 2015 as a national agency tasked to protect Singapore's cyberspace.

4.7.1 Mission

- Keep cyberspace safe and secure

- Underpin our national security

- Power a digital economy

- Protect our digital way of life

4.7.2 Vision

A trusted and resilient cyberspace that allows Singapore to capture the benefits of a more connected world.

4.8 Cybersecurity and Singapore

- Cybersecurity is a key enabler for Singapore digital ambitions towards our future economy and society.

- It allows Singapore to leverage the benefits of digitalisation with a peace of mind.

- Cybersecurity is needed to help Singaporeans understand and navigate through cyber risks.

- Individuals also need to take steps to protect our devices and information.

- New technologies such as cloud, 5G, internet of things (IoT), machine learning and AI can give rise to new attack vectors and vulnerabilities.

- The cyberspace environment can be viewed as hostile and contested, with thinking, determined and motivated cyber adversaries such as advanced persistent threat groups, cybercriminal gangs and hacktivists.

- Cybersecurity is known as a wicked problem as cyber threats are asymmetric, borderless, constantly evolving and difficult to attribute.

- Cyber threats do not discriminate when choosing their targets or victims. They can target the young or old, rich or poor, educated or uneducated.

- Cyber threats that Singapore faces mirrors global trends, and some of them include advanced persistent threats, ransomware, phishing and data breaches.

- There has been an up tick in ransomware and supply-chain breaches.

- 89 ransomware cases were reported to the CSA in 2020, which is a sharp rise of about 154% from the 35 cases reported in 2019.

- These ransomware cases mostly affected small and medium enterprises (SMEs) in the manufacturing, retail and healthcare sectors.

- The recent SolarWinds incident showed how supply-chain breaches can compromise many victims at one go. This can cause total loss of trust in the affected products, including for our critical information infrastructure (CII) systems.

- The reliance of digital tools has greatly increased the "attack surface" that malicious actors can target or exploit.

4.9 Cyber trilemma

Because cyberspace is a dynamic environment with evergreen challenges, there is a trilemma among security, usability and cost. Hence, there is no completely secure system as there will always be some trade-offs.

4.10 Good cyber hygiene (PASS)

4.10.1 Password (P)

- Use strong passwords

- Enable two-factor authentication on your accounts

4.10.2 Antivirus (A)

- Keep them installed on your devices

- They help to protect your devices against known malicious software, or malware for short

4.10.3 Spot signs of phishing (S)

- Be aware of urgent or threatening language. Remain vigilant and take a quick moment to think before responding.

- Promises of attractive rewards.

- Requests for confidential information.

- Don't respond to suspicious messages or emails.

- Don't click on any suspicious links or attachments.

- Don't forward those links or attachments to others except when reporting a phishing email or message.

- Always double-check the URL. Cyber criminals often substitute letters in a URL to mislead you.

- Look out for poor English with grammatical errors.

4.10.4 Software applications (S)

- Keep software applications updated and patched in a timely manner.

- Enable auto updates or auto patch because doing so will help protect against known security vulnerabilities and exploits.

4.11   Safe use of public Wi-Fi

4.11.1   Cyber threats

- Cybercriminals can eavesdrop on what you're browsing on the web and sniff sensitive information like usernames and passwords.

- Cybercriminals can also set up bogus Wi-Fi networks to trick you into connecting to what you think is a legitimate network.

4.11.2   Tips

- Do not input sensitive information like banking details and personal information.

- Do not do sensitive transactions.

- Look out for the HTTPS or the padlock icon in the address bar of the browser.

- Use a virtual private network (VPN), which encrypts the data transmitting to and from your devices.

- Disable file sharing to prevent anyone from accessing your files or from sending you malicious files when they are connected to the same Wi-Fi network.

- Disable auto-connect to avoid connecting to bogus networks unknowingly.

4.12 Using e-payment services

4.12.1 Cyber threats

- Online shopping is an increasingly popular option for consumers, especially the young.

- Cybercriminals are exploiting this by creating phishing scams that aim to steal financial information and bogus websites to offer products that don't exist.

- Cybercriminals use spoofed social media accounts to impersonate a victim's friends or followers.

- They will then ask their victims to share their personal information, such as mobile number, internet banking details and one-time password (OTP) on the pretext of helping them to sign up for fake contests or promotions on online shopping platforms.

4.12.2 Tips

- Enable 2-factor authentication (2FA) for all online transactions.

- Do not store your credit card information online.

- Avoid performing financial transactions over unsecured public Wi-Fi networks.

- Be vigilant against phishing or bogus sites.

- Be wary of offers that are too good to be true.

- Be wary of unexpected requests or offers from social media contacts.

- Be wary of URL links provided in unsolicited text messages.

- Always verify the authenticity of the information with official sources, such as official websites.

- Never disclose personal or internet banking information and one-time passwords (OTP).

5   Fake news

A specific type of falsehood intentionally packaged to look like news to deceive others.

5.1   Examples

- Political satire

- Advertising

- News parody

- Manipulation

- Propaganda

- Fabrication

5.2   As true fake news

- A knowingly false headline and story is written and published on a website that is designed to look like a real news site, and is spread via social media.

- News stories that were fabricated and promoted on social media in order to deceive the public for ideological or financial gain.

- News articles that are intentionally and verifiably false, and could mislead readers.

- Fake news takes advantage of what we associate with real news, including language, structure and the layout of a page.

- Fake news has always been around, it is just far more prevalent in the digital age.

- A survey of a thousand Singapore residents in December 2019 showed that higher social media news use resulted in a higher likelihood to believe in fake news.

- Those who actively avoid news about COVID-19 are more likely to believe in misinformation as well.

- 18% - 25% of Singaporeans thought some of the viral false claims in Singapore were true.

5.3   Motivations

5.3.1   Financial

- Attracting clicks

- Advertising revenue

5.3.2   Ideological

- Personal agenda

- Weapons of mass misinformation

5.4   What makes people vulnerable?

5.4.1   Sender

- Credible or familiar?

- Trustworthy or similar?

- Proximate or distal?

5.4.2   Receiver

- Confirmation bias

- Motivations

- Corrections

5.4.3   Message

- Format

- Plausibility

5.4.4   Context

- Information overload

- Instability

5.4.5 Channel

- Trusted or depended on?

- Closed or open?

- Feedback

5.5 Who is the actual source of the message?

5.5.1 Original source

Original source refers to the creator of the message.

5.5.2 Immediate source

Immediate source refers to the source that a person received a message from.

5.5.3 Invisible sources

Invisible sources are sources that are not immediately visible to people who receive the message. It is usually the sources for the message itself, like interviewees, references from other sources, etc. It can also be the original source when the message has been forwarded or shared many times, such that the original source becomes invisible.

5.5.4 Trusted source

Trusted sources are sources that people trust, be it their friends, or a news site.

5.5.5 Disregarded sources

Disregarded sources are sources that people don't trust, and hence dismiss the sources' claims, even if they may be true.

5.6 Message characteristics to take note

- Plausible?

- Mentions experts?

- Conversational tone?

- Stirs emotion?

- Asks you to forward or has call to action?

5.7 Channels where information flows are conducive to fake news

- Popularity cues

- People rely on the channels

- Lack of gatekeeping

- Information overload

5.8 Informational apathy

Informational apathy refers to people not bothering to take an action to correct fake news that they see on social media sites. This is the case for most people.

5.8.1 Reasons for being apathetic

- The issue isn't relevant

- Protecting interpersonal relationships

- Personal inefficacy, people believe that even if they correct the fake news, there's nothing that will come out of it

5.9 The consequences of fake news

5.9.1 Short-term effects

- Fake news affects political decisions

- Businesses are negatively impacted by fake news

- Peace and order are sometimes disrupted by fake news

- Fake news can hurt personal reputation

5.9.2 Long-term effects

- Devaluation of information

- Erosion of trust in institutions

- Larger social divisions

- Chilling effect, where the press or news outlets just report positive news regarding a certain entity when the entity labels them as fake news

5.10 How do we authenticate information?

5.10.1 Internal acts of authentication

- The self: Using one's own intuition to judge if some information is fake.

- The source: Check if the source is reliable, for example, an article from an established media company is generally more factually correct than one from a relatively unknown news site.

- The message: Check the tone of the news article to see if it's polemical or deliberately misleading or false to arouse emotions.

- Message cues: The presence of a lot of likes or dislikes on the message, the number of negative comments versus positive comments, etc.

5.10.2 External acts of authentication

- Incidental and interpersonal: Asking friends or relatives for their opinion on the matter.

- Incidental and institutional: Waiting for a follow-up post to correct the mistakes or to clarify certain things that may have been misunderstood.

- Intentional and interpersonal: Contacting a reliable group of people to verify the information.

- Intentional and institutional: Searching for the title of the report to see if there are similar reports on mainstream news outlets.

5.11 Authentication is a social process

5.11.1 Motivations for authenticating

- Self-image, as we don't want to show our friends and family members that we have questionable beliefs.

- Group cohesion, to maintain good relationships with others.

5.11.2 Strategies of authentication

- Group beliefs, "deep stories"

- Source affiliation

- Sharing as authenticating

5.11.3 Consequences of authentication

- Institutionalisation of interdependence

- Ritualisation of collective authentication

5.12 Gamifying interventions

- "Go viral!" is a 5-minute game that helps protect people from COVID-19 misinformation.

- "Bad News" is another game that helps people identify fake news.

5.13 Singapore's Protection from Online Falsehoods and Manipulation Act (POFMA)

An Act to prevent the electronic communication in Singapore of false statement of fact, to suppress support for and counteract the effects of such communication, to safeguard against the use of online accounts for such communication and for information manipulation, to enable measure to be taken to enhance transparency of online political advertisements, and for related matters.

5.13.1 What is true and what is false?

- A statement of fact is a statement which a reasonable person seeing, hearing or otherwise perceiving it would consider to be a representation of fact.

- A statement is false if it is false or misleading, whether wholly or in part, and whether on its own or in the context in which it appears.

5.13.2 What constitutes communicating?

A statement or material is communicated in Singapore if it is made available to one or more end-users in Singapore on or through the internet, MMS or SMS.

5.13.3 What is "in the public interest"?

- It is in the interest of the security of Singapore or any part of Singapore.

- It is to protect public health or public finances, or to secure public safety or public tranquillity.

- It is in the interest of friendly relations of Singapore with other countries.

- It is to prevent any influence of the outcome of an election to the office of President, a general election of Member of Parliament, a by-election of a Member of Parliament, or a referendum.

- It is to prevent incitement of feelings of enmity, hatred or ill-will between different groups of persons

- It is to prevent a diminution of public confidence in the performance of any duty or function of, or in the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of state or a statutory board.

5.14 Tech companies' interventions

- Supporting third-party fact-checkers and journalists

- Promoting media literacy among users

- Reducing financial incentives for content producers

- Implementing new features to flag content

- Deleting posts and removing accounts

5.15 Fact-checking

- A process that occurs post publication and compares an explicit claim made publicly against trusted sources of facts.

- 21% of Singaporeans said that they use fact-checking sites often or very often.

- Younger Singaporeans are using fact-checking sites more often than older Singaporeans.

5.15.1   Fact-checking sites

- Politifact
- Snopes
- AFP
- Blackdot research
- Vera files
- Cofacts
- Social media hoax slayer

5.15.2   Types of fact-checkers

- Affiliated with news organisations
- Government-owned
- Independent organisation
- Volunteer group
- Individual

5.15.3   Fact-checking tools

- Monitor what's trending using software like CrowdTangle
- Verify images using reverse image search or checking image metadata
- Verify sites by checking their registration dates
- Checking the weather
- Using maps to verify a photo

5.15.4   Ways to deliver a fact-checking message

- Videos
- Rating scales
- Mixed accuracy statements
- Truth sandwich

5.15.5 What can the individual do?

1. Reflect on our own information behaviour.

2. Engage, rather than ignore.

3. Strive to understand others.

4. Use and support reliable and legitimate information sources.

5. Maximise available resources.

6. Equip ourselves with the proper tools and resources to fight fake news.

6 Data and digital ethics

6.1 Why do we need them?

There is an intentional consensus that ethics is vital to the development, application, and use of digital and online technologies.

- Technology shapes the way people live.

- While digital and online technologies offer remarkable benefits, like knowledge, communication, efficiency, and personalisation, they also expose risks of significant harms to privacy, security, autonomy, fairness and transparency.

- Lawmakers are often unable to keep up with the speed of technological advancement. Hence, not only expert technologists, but also ordinary users, must learn to develop and use technologies in ways that avoid harms while getting the most from the benefits.

6.2 Principles of data ethics

- Moral theories are meant to provide very general explanations and guidance concerning what we morally ought to do.

- While moral theories have the advantage of comprehensiveness, it can be difficult to deduce what they would prescribe in a particular context.

- Several professional associations and private firms have formulated more specific principles to guide actions with respect to data and information technology.

- The following principles are sampled from the Singapore Computer society's professional Code of Conduct.

6.2.1 Integrity

SCS members will act at all times with integrity.

- They will not lay claim to a level of competence that they do not possess

- They will act with complete discretion when entrusted with confidential information.

- They will be impartial when giving advice and will disclose any relevant personal interests.

- They will give credit for work done by others where credit is due.

6.2.2 Professionalism

SCS members will act with professionalism to enhance the prestige to the profession and the Society.

- They will uphold and improve the professional standards of the society through participation in their formulation, establishment and enforcement.

- They will not seek personal advantage to the detriment of the Society.

- They will not speak on behalf of the Society without proper authority.

- They will not slander the professional reputation of any other person.

- They will use their special knowledge and skill for the advancement of human welfare.

7 Informational privacy

- Digital and online technologies have a major impact on one's ability to secure privacy

- In particular, these technologies affect what the philosopher Anita L. Allen describes as informational privacy: "Confidentiality, anonymity, data protection, and secrecy of facts about persons".

7.1 OkCupid incident

- Some researchers released the personal profile details of 70,000 users on OkCupid, a dating website.

- Critics maintained that the informational privacy of the OkCupid users was violated by the researchers, because the researchers stored and redeployed the personal information of the users without their consent.

7.2 Right to informational privacy

- A right to privacy is recognised in all international and regional human rights instruments, including Article 12 of the Universal Declaration of Human Rights.

- "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

8 Whistleblowing

- In large organisations, it can be difficult to hold people accountable for unethical or illegal acts.

  - Law enforcement and regulators are not able to constantly monitor the internal operations of organisations. Such constant surveillance isn't desirable.
  - Leadership within the organisation may cover up any corrupt activities.

- Sometimes it is up to ordinary, low-level people to "blow the whistle" on unacceptable conduct in their organisations.

8.1 Examples

There are many examples of misconduct in organisations not being brought to light until much damage has already been done, or only after a private citizen reported it at great personal cost.

- The 1986 Challenger Disaster is a memorable case where something catastrophic happened as a result of internal mismanagement.

- A more recent case involving Wirecard, an electronic payment company, was reported in Singapore.

- Data analytics firm Cambridge Analytica crossed many ethical lines.

8.2 When to whistle blow?

Richard T. De George proposed that whistleblowing is **morally permissible** when the three conditions below are fulfilled:

1. The firm will do, or has done, serious and considerable harm to employees or to the public.

2. Once employees identify a serious threat to the user of a product or to the public, they should report it to their immediate superior and make their moral concern known.

3. If one's immediate supervisor does nothing effective about the concern or complaint, the employee should exhaust the internal procedures and possibilities within the firm.

He also suggests that if the two *additional conditions* below are met, then it would be **morally obligatory** for someone to whistle blow.

1. The whistleblower must have, or have accessible, documented evidence that would convince a reasonable, impartial observer that one's view of the situation is correct.

2. The employee must have good reasons to believe that by going public the necessary changes will be brought about. The chance of being successful must be worth the risk one takes and the danger to which one is exposed.

8.2.1 Objections

1. The criteria are too stringent. It can be morally permissible to whistle blow, even when the first three conditions are not met.

   - For instance, it may be morally permissible to whistle blow when you know that serious harm will be done to the public, but there is not enough time to lobby supervisors and exhaust all internal reporting procedures.
   - By itself, the effort to prevent serious harm may be enough to make whistleblowing morally permissible.

2. The criteria are not demanding enough. It can be morally obligatory to whistle blow even when the two additional conditions have not been fulfilled.

   - For instance, a single employee may have satisfied conditions 1 through 3, but still be unable to acquire enough documented evidence to convince an impartial observer that any wrongdoing has been done.
   - However, it may still be morally obligatory to whistle blow, if one is confident that another organisation, such as law enforcement or the media, would be able to persuade an impartial observer of the organisation's wrongdoing.

9   Intellectual property (IP)

- Creations resulting from the exercise of the human brain.

   - Examples include inventions, designs, ideas, plant hybrids, music, poems, paintings, photographs, logos, books, films, cartoon characters, and trade secrets.

- Bundle of legal rights protecting such creations, i.e. intellectual property rights (IPRs).

- IP law recognises that creators have the right to protect their work.

   - IP law gives legal rights to IP creators, allowing them to control and exploit the use of their IP for a specific period of time.

9.1 Types of intellectual property

- Copyright for original and related works.

- Patents for inventions.

- Trademarks, which are signs used in business.

- Confidential information, which is non-public and valuable information.

- Other types of intellectual property like:

  - Registered designs
  - Plant varieties
  - Geographical indications
  - Layout design of an integrated circuit

9.2 Why protect intellectual property?

- Provides motivation for creators

- Encourages constant creation and innovation.

- Allows creators to exploit their works for commercial gain.

- Allows creators to defend the works from infringement.

9.3 Dealing with intellectual property

- The law regards intellectual property as a type of personal or movable property.

- Intellectual property is capable of being owned and dealt with as other types of personal property.

- In other words, you can buy, sell, lease or hire out or give away intellectual property as intellectual property has commercial value.

9.4 Intellectual property (IP) categories

9.4.1 Copyright (Literary works)

Literally anything that includes **words**.

9.4.2 Copyright (Artistic works)

- Anything that has a **graphic**, like drawings, photographs, and renders.

- Drawings don't have to reach the level of fine art, i.e. highly aesthetic, imaginative, or creative, to be protected as artistic works.

9.4.3 Copyright (Cinematic works)

Anything that is has **animation** or **acting**. Basically, most **videos** that isn't just text.

9.4.4 Copyright (Published editions)

Anything that is published, like books, research papers and journals.

9.4.5 Copyright (Sound recordings)

A sound recording is a series of **musical, spoken, or other sounds** fixed in a recording medium. Note that sound recordings are not limited to recordings of musical works. Sound recordings can also be lectures, podcasts, or other audio recordings. The author of a sound recording can be the performer who is being recorded, the record producer who processes and fixes the sounds, both, or even another entity if the work qualifies as a work made for hire.

Common examples of sound recordings include an audio recording of:

- A person singing a song or playing a musical instrument.

- A person reading a book or delivering a lecture.

- A group of persons hosting a podcast or performing a radio play.

- A person speaking, a dog barking, a bird singing, wind chimes ringing, or other sounds from the natural world (assuming the recording contains a sufficient amount of production authorship).

9.4.6 Copyright (Musical works (musical compositions))

- A musical work is a song's **underlying composition** created by a songwriter or composer along with any accompanying lyrics. Musical works include original compositions and original arrangements or other new versions of earlier compositions to which new copyrightable authorship has been added.

- A musical composition and a sound recording are **two separate works**. A registration for a musical composition covers the music and lyrics, if any, embodied in that composition, but it does not cover a recorded performance of that composition.

9.4.7 Patents

Patents only protects **inventions**, and requires money to maintain.

9.4.8 Trademarks

Trademarks protect a **logo only**, like the Apple logo.

9.4.9 Trade secret (Not protectable by IP protection)

Trade secrets are simply things that **cannot be protected** by intellectual property (IP) protection (copyright, patents and trademarks), like recipes, methods or information, but are "protected" by keeping them **secret**.

10 Copyright

- Copyright is the right to prevent the unauthorised copying of the tangible form in which a person has chosen to express his ideas, for example in a short story, musical composition, theatre script, painting, computer program, photograph, move or video game.

- It can be described as a **bundle of exclusive rights belonging to the copyright owner**.

- It allows owners to enforce their rights against infringement.

- Singapore's copyright law is governed by the Copyright Act.

10.1 Criteria for protection

Copyright protection arises automatically be operation of law, so long as certain basic criteria are satisfied:

- Falls within the categories of protection

- Fixed in tangible form

- Original, which means that the work was created independently by the author

- Author or creator is a Singapore citizen or permanent resident (PR)

10.2 How does copyright work?

- Copyright protects the form of expression, and not the idea or information itself.

- The idea or information is protected by different means.

- Many different media or forms of expression can be protected.

- Expression must, as a general rule, be original.

- No need for registration formalities.

- Copyright arises "as soon as the ink dries".

10.3 The idea-expression dichotomy

- Copyright protects the "**form**" of an idea and **NOT the idea itself**.

- No need for novelty so long as there is independent creation.

- Artistic merit is not a requirement for copyright to attach to a work as it is too subjective.

10.4   Things that are not protected by copyright

- Ideas and concepts

- Information in general

- Discoveries (e.g. a research finding)

- Procedures (e.g. steps in applying for a grant, recipes)

- Methods (e.g. solution to a mathematical problem)

- Any subject matter that has not been reduced to a tangible form

- Works in the public domain

10.5   Copyright categories

10.5.1   Literary works

Literally anything that includes **words**.

10.5.2   Artistic works

- Anything that has a **graphic**, like drawings, photographs, and renders.

- Drawings don't have to reach the level of fine art, i.e. highly aesthetic, imaginative, or creative, to be protected as artistic works.

10.5.3   Cinematic works

Anything that is has **animation** or **acting**. Basically, most **videos** that isn't just text.

10.5.4   Published editions

Anything that is published, like books, research papers and journals.

10.5.5 Sound recordings

A sound recording is a series of **musical, spoken, or other sounds** fixed in a recording medium. Note that sound recordings are not limited to recordings of musical works. Sound recordings can also be lectures, podcasts, or other audio recordings. The author of a sound recording can be the performer who is being recorded, the record producer who processes and fixes the sounds, both, or even another entity if the work qualifies as a work made for hire.

Common examples of sound recordings include an audio recording of:

- A person singing a song or playing a musical instrument.

- A person reading a book or delivering a lecture.

- A group of persons hosting a podcast or performing a radio play.

- A person speaking, a dog barking, a bird singing, wind chimes ringing, or other sounds from the natural world (assuming the recording contains a sufficient amount of production authorship).

10.5.6 Musical works (musical compositions)

- A musical work is a song's **underlying composition** created by a songwriter or composer along with any accompanying lyrics. Musical works include original compositions and original arrangements or other new versions of earlier compositions to which new copyrightable authorship has been added.

- A musical composition and a sound recording are **two separate works**. A registration for a musical composition covers the music and lyrics, if any, embodied in that composition, but it does not cover a recorded performance of that composition.

10.6 Exclusive rights in copyright

10.6.1 Literary, dramatic or musical works

- Reproduce the work in a material form.
- Publish the work if the work is unpublished.
- Perform the work in public.
- Communicate the work to the public.
- Make an adaptation of the work.
- Do any of the above in relation to an adaptation of the work.

10.6.2 Sound recordings

- Make a copy of the sound recording.
- Enter into a commercial rental arrangement in respect of the recording.
- Publish the sound recording if it is unpublished.
- Make available to the public a sound recording by means of, or as part of, a digital audio transmission.

10.6.3 Cinematographic films

- Make a copy of the film.
- Cause the film, insofar as it consists of visual images, to be seen in public.
- Communicate the film to the public.

10.6.4 Artistic works

- Reproduce in material form.
- Publish the work if the work is unpublished.
- Communicate the work to the public.

10.6.5   TV and sound broadcasts

- Make a cinematographic film of a TV broadcast or a copy of a TV the film.

- Make a sound recording of a TV or sound broadcast or a copy of the recording.

- Cause it to be seen or heard in public by paying audience.

- Communicate the work to the public.

10.6.6   Cable programmes

- Make a film of visual images, or a copy of such a film.

- Make a sound recording of the work or a copy of such sound recording.

- Cause work to be seen or heard by paying audience.

- Communicate the programme to the public.

10.6.7   Published editions

- Make a reproduction of the edition, including by way of a photographic process.

10.7   Duration of copyright protection

Type of work	Duration of protection
Literary, dramatic, musical and artistic works (e.g. photographs, paintings, drawings, sculptures, etc.)	Life of author plus 70 years from the end of the year in which the author died.
Published editions (editions of a book, like the first edition of a physics textbook)	25 years from the end of the year in which the edition was first published.
Sound recording and films	70 years from the end of the year of release
Broadcasts and cable programmes	50 years from the end of the year of the first broadcast
Performances	70 years from the end of the year of the performance

10.8   Overlapping copyright

- One product may contain a variety of copyright works. For example, a music album with songs contains lyrics, musical works and sound recordings.

- Purchasing a physical product does not give rights to the underlying copyright works (e.g. purchasing an original music CD does not give the right to make copies).

10.9   Who owns the copyright?

The person who creates or authors the work automatically owns it from the moment of creation.

10.9.1   Exceptions

- **Employment**: If the work is created by an employee pursuant to the terms of his employment, the employer owns the copyright in the work.

- **By agreement**: The author can agree to transfer some or all of his rights.

10.9.2   Joint authors

- When work is created jointly by more than one author, the authors are all co-owners of the copyright in the work.

- When more than one author creates inseparable or interdependent parts of a whole work. For example, two trainers involved in creating the training materials for a course.

- Contributions must be original material expression, not just ideas or non-copyrightable materials.

10.10   Creative Commons Licences (CC Licences)

- **The licences and CC0 cannot be revoked.** This means once you apply a CC licence to your material, anyone who receives it may rely on that licence for as long as the material is protected by copyright, even if you later stop distributing it.

- You must own or control copyright in the work. Only the copyright holder or someone with express permission from the copyright holder can apply a CC licence or CC0 to a copyrighted work. If you created a work in the scope of your job, you may not be the holder of the copyright.

10.10.1   CC BY

This licence enables re-users to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The licence allows for commercial use. CC BY includes the following elements:

- BY: Credit must be given to the creator.

10.10.2   CC BY-SA

This licence enables re-users to distribute, remix, adapt, and build upon the material in any medium or format, so long as attribution is given to the creator. The licence allows for commercial use. If you remix, adapt, or build upon the material, you must license the modified material under identical terms. CC BY-SA includes the following elements:

- BY: Credit must be given to the creator.

- SA: Adaptations must be shared under the same terms.

10.10.3 CC BY-NC

This licence enables re-users to distribute, remix, adapt, and build upon the material in any medium or format for non-commercial purposes only, and only so long as attribution is given to the creator. CC BY-NC includes the following elements:

- BY: Credit must be given to the creator.

- NC: Only non-commercial uses of the work are permitted.

10.10.4 CC BY-NC-SA

This licence enables re-users to distribute, remix, adapt, and build upon the material in any medium or format for non-commercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms. CC BY-NC-SA includes the following elements:

- BY: Credit must be given to the creator.

- NC: Only non-commercial uses of the work are permitted.

- SA: Adaptations must be shared under the same terms.

10.10.5 CC BY-ND

This licence enables re-users to copy and distribute the material in any medium or format in unadapted form only, and only so long as attribution is given to the creator. The licence allows for commercial use. CC BY-ND includes the following elements:

- BY: Credit must be given to the creator.

- ND: No derivatives or adaptations of the work are permitted.

10.10.6 CC BY-NC-ND

This licence enables re-users to copy and distribute the material in any medium or format in unadapted form only, for non-commercial purposes only, and only so long as attribution is given to the creator. CC BY-NC-ND includes the following elements:

- BY: Credit must be given to the creator.

- NC: Only non-commercial uses of the work are permitted.

- ND: No derivatives or adaptations of the work are permitted.

10.10.7 CC0 (CC Zero)

CC0 is a public dedication tool, which enables creators to give up their copyright and put their works into the worldwide public domain. CC0 enables re-users to distribute, remix, adapt, and build upon the material in any medium or format, with no conditions.

11 Contract

- An agreement giving rise to obligations which are enforced or recognised by law.

- It is a voluntary agreement between two or more parties.

- The law exists to govern and regulate the parties' relationship in such agreements.

- It can be verbal or written, simple or complicated.

11.1 Function of contracts

- Set out the extent of the agreement

- Identify and clarify rights and obligations

- Allocate risk

- Provide certain guarantees

- Set performance standards

- Provide how non-fulfilment of obligations should be dealt with

11.2 What the law of contract covers

- Formation of contracts, which are the elements required for a contract to exist.

- Contents (terms) of a contract.

- Performance of terms of the contract by its parties.

- Remedies when there is no-fulfilment of either party's obligations (breach).

11.3   Elements of a contract

Once all the below elements are in place, a contract is deemed to be formed. The absence of any one of these means that no contract is in existence.

11.3.1   Offer

It is an indication by the offerer of the willingness to contract

11.3.2   Acceptance

- The acceptance is absolute and unqualified. It must be communicated to the offerer.

11.3.3   Consideration

It is usually indicated by price or the carrying out of an act in return for the benefit.

11.3.4   Intention to create legal relations

It is reasonable to conclude that the parties involved have the intention to be legally bound from their conduct.

11.3.5   Capacity

- Both parties must have the capability to enter a contract.

- Issue of minors (below the age of 18) and impaired mental capacity.

11.4   Contractual terms and performance

- Set out and determine the rights and obligations of respective parties.

- Provide for how obligations are to be performed.

- Provide for how risks are to be allocated.

- Provide for how the contractual relationship is to be regulated. For example, hot it begins, carries on, ends, or is renewed.

11.5 Common terms in contracts

11.5.1 Purpose of contract or the description of collaboration

What is the aim of the contract?

11.5.2 Payment and fees

How much, and how is payment to be made?

11.5.3 Rights and obligations of each party

What rights and obligations does each party have?

11.5.4 Duration or termination

How long is the contractual relationship going to last? How will the contract end?

11.5.5 Warranties (fundamental promises)

Basic assurance that the contract can be carried out effectively.

11.5.6 Dispute resolution

How will disagreements be resolved?

11.6 Breach and remedies

- A contract is breached when there is non-performance of a term.

- It does not automatically terminate the contract.

- Breach entitles the wronged party to demand cure of the breach from the other party, as well as financial compensation (damages) if there is a loss.

  - The wronged party may also be entitled to terminate the contract.

12   Artificial intelligence (AI)

Artificial intelligence refers to machines that are capable of performing tasks that typically require human intelligence.

12.1   History of AI

12.1.1   1950s

- The term was coined in a proposal in 1955 when scientists applied for funding to study artificial intelligence.

- There was also development of the LISP programming language as well as computers that could run LISP programs.

- The results from such developments did not meet expectations mostly due to the lack of computing power, and the government stopped funding in the 1970s.

- The focus of artificial intelligence was on the engineering of making intelligent machines and programs.

12.1.2   1973: The first winter

From 1973 to the early 1980s, there was very little research interest in AI.

12.1.3   1982: The second spring

- The Fifth Generation Computer Project in Japan reignited AI research in the 1980s.

- The project was to develop a system for computers that can perform knowledge processing instead of information processing.

- However, most of the goals of the project were too ambitious and could not be met, which resulted in funding being cut in the 1980s.

12.1.4   1985: The second winter

From 1973 to the early 1980s, there was very little research interest in AI.

12.1.5 2000 - Present day: The Renaissance

- In the late 1990s and early 2000s, AI had a resurgence and is considered as the Golden Age of AI.

- The ability to learn without being explicitly programmed, or machine learning, was developed.

- In the 2010s, deep learning was discovered, where machines could learn by using a deep neural network.

12.2 Reasons for the recent success of AI

- Powerful computers became widely available and easily accessible through platforms like cloud computing, as well as using graphical processing units (GPUs) to train models.

- The availability of big data, or large amounts of data, due to the internet and smart mobile phones that allow people to share their data to the internet.

- The advancements in software algorithms, especially those used in machine learning and deep learning.

12.3 Neural networks

- Neural networks used in deep learning mimics the human brain to recognise patterns and learn on its own.

- The basic neural network has 3 layers, the input layer, the hidden layer, and the output layer.

12.3.1 Hidden layer

- The hidden layer consists of parameters that can be trained when the model is fed with a large amount of data.

- It is the layer that contains the "algorithm" that can learn and improve by itself.

- In practice, neural networks usually have far more than just one hidden layer.

- Neural networks with multiple hidden layers are called deep neural networks, which are able to learn more sophisticated algorithms.

12.3.2   AlexNet

- An 8-layer deep convolution neural network used in the 2012 ImageNet computer image recognition competition by Alex Krizhevsky to beat handcrafted software written by computer vision domain experts for the first time in history.

- This neural network is considered rudimentary compared to current neural networks that have hundreds of layers.

12.3.3   Convolution Neural Networks (CNN)

- The inputs in a CNN, usually images, go through a mathematical operation called convolution, which transforms the inputs into feature maps.

- The feature maps then undergo subsampling to create smaller feature maps, which then go through another round of convolutions and subsampling to create increasingly smaller feature maps.

- This process continues until the feature maps are fully connected, and the neural network produces an output.

- An example is a convolution neural network built to detect human faces.

  – During the training process, many images of human faces are fed into the deep neural network.
  – This first input layer of the neural network extracts the local low-level features of faces based on the images provided.
  – The middle hidden layer then combines the low-level features to form the features that are found on various parts of the face.
  – The next hidden layer then combines the facial features to form typical human faces.
  – During the face detection process, which is known as inference, the result is obtained by comparing the input image against the features of faces that the neural network has been trained to recognise.

12.4 Applications

- AI-powered robots can learn by themselves to perform more complicated tasks.

- This will enable industries to improve on their efficiency, productivity, and maintain safety.

- Robots are especially suitable for performing repetitive and dangerous tasks.

- Robots today still don't have artificial general intelligence and are only capable of solving problems and thinking in a limited and narrow capacity.

12.4.1 Autonomous automotives

- AI-driven self-driving cars use sensors and images to automatically detect lanes and obstructions on the road, which can provide higher convenience and potentially lower running costs.

- It can also remove potential human errors such as those due to tiredness and hence improve safety.

- AI technology is also used to provide navigation functions, and optimise route planning as it can be used to provide the shortest path, or the fastest path, based on traffic conditions in real time.

- It can also plan routes that avoid fare gates and tolls, such as the ERP gantries in Singapore.

12.4.2 Recommendation algorithms

- AI is also used extensively as a recommender in various social media apps.

- It uses your likes and the accounts you follow to determine what news, posts, or products that you are interested in, and push relevant advertisements and contents to you when you are using these social media apps.

12.4.3   Consumer electronics

- Many consumer electronic devices also implement AI algorithms on the device.

- Most smartphones nowadays consist of AI-driven apps that can respond to your voice commands.

- The Google Pixel 6 even uses an AI chip, known as Tensor, to optimise performance, such as performing real-time translations on the phone itself.

- Many household devices are also incorporated with AI nowadays.

- With the help of object recognition, a smart fridge can detect the quantity of food available and make orders on behalf of the user through the internet.

- A smart oven can detect the type of food that the user has and populate all possible recipes that the user can cook using the items that are already available.

- AI-powered floor vacuum cleaners can learn the environment of the floor area to plan the most optimised way of cleaning the floor.

- Smart security cameras can determine whether an intrusion is caused by a human or just due to other disturbances, such as an animal passing through the area.

12.4.4 Business operations

- AI technologies are also used to manage inventory and to forecast demand more precisely to improve business efficiency and reduce inventory costs.

- AI is also used in personalised merchandising based on the customer online browsing history, preferences, and interests when they are visiting a web store.

- Some e-commerce companies can even ship their products in advance to places near the potential customers while they are browsing the products in the web store in anticipation of potential sales.

- Chatbots are software applications that are used to conduct conversations in real time with a customer.

- They can be used as fully automated self-service tools, or sometimes they assist real people to handle multiple conversations at the same time.

- AI-driven chatbots can be used to find the most appropriate responses during conversations with customers either via text or even using text-to-speech.

- By using AI technologies, businesses can deliver highly targeted and personalised advertisements, which improve customer experience, build relationships, and loyalty.

12.4.5   Banking and finance

- The financial industry relies on accuracy, real-time reporting, and the need to process high volumes of quantitative data to make better decisions, which are the areas that AI excels in.

- In trading, AI robot advisers are used to analyse millions of data points in real time to execute trades at the optimal price.

- It could effectively crunch millions upon millions of data in real time to capture information that the current statistical models can't achieve.

- Financial underwriters use AI to analyse huge amounts of data from credit bureau sources to assess credit risk for consumer and small business loan applicants.

- This system acquires portfolio data and apply machine learning to find patterns to determine good and bad applications.

- In wealth management, AI can be used to recommend sophisticated portfolios and to offer financial advice to high net worth clients to produce high potential returns.

- By considering usage patterns, AI can help to reduce the possibility of credit card fraud taking place.

12.4.6   Healthcare

- Ai is able to analyse large amounts of data stored by healthcare organisations in the form of medical images to identify patterns and insights often undetected by humans.

- It can also be used to detect potential problems earlier, such as in cancer cases where the cancer cells could have been detected at a much earlier stage by using AI.

- AI is also now used by many drug companies to develop more effect new drugs, which have long been a trial and error process that cost drug companies a lot of time and money.

- AI can help to identify which genes have been affected by harmful mutations so that they can be targeted in gene therapy.

12.4.7 Agriculture

- AI can be used to harvest crops at a higher volume and at a faster pace than human labourers can achieve at the moment.

- AI can also be used to detect nutrition levels of farms to provide proper guidance to farmers about nutrition and water management of the farms.

- AI can also be used to detect diseases in plants, and pests on the farms.

- AI sensors can detect and target weeds, and then decide which herbicide to apply within the region.

- By using drones to collect images of the crops, AI can then be used to analyse the crop health and provide appropriate measure for farmers.

- All these will likely help to improve the overall harvest quality and accuracy, which is known as precision agriculture.

12.4.8 Education

- AI e-tutors can provide more precise coaching, automatic grading of written assignments and AI based e-proctoring for online assessments and exams.

- These tools will allow schools and teachers to do more than ever before, freeing up more time to focus on other aspects of education, such as teaching higher-order thinking skills and promoting creativity, which AI is not able to perform as of now.

12.5 Concerns

12.5.1 Job loss

- Many jobs that can be done by AI systems at a lower cost and are more efficient will result in unemployment.

- For example, the arrival of self-driving taxis would remove the need for taxi drivers in the future.

12.5.2 Misuse of AI

Deep fakes can be used to spread false information and create tensions among different groups of people.

12.5.3 AI explainability

- It is difficult or even impossible to understand how AI arrives at certain decisions, which is especially the case for AI that are based on deep learning.

- This is an area that needs more research and studies.

12.5.4 Bias

- There could be bias built into AI algorithms that can lead to discrimination against certain groups of people, such as based on age, gender, race, and culture.

- The bias could be due to the data the model is trained on being biased, which could in turn be the result of a lack of data on those specific groups of people.

- In 2015, it was discovered that hiring algorithms used were biased against hiring females, as the algorithm was trained on resumes from the past 10 years, which were mainly male.

- Hence, the algorithms were less likely to highly rate applications by females.

12.5.5 AI ethics in decision-making

- AI is ultimately programmed by humans, and different people have different upbringing, different cultural backgrounds with diverse ethical and moral values.

- Furthermore, the use of AI in autonomous weapons will remove the human judgements based on moral considerations during battles.

- Hence, the issue of making AI systems fair for everyone in society is an ethical issue that receives a lot of debate and research interest.

12.6 Summary

- AI is rapidly changing the way we live:

    - Helps to make things run more efficiently.
    - Improves safety and work productivity
    - Frees up time for human to do more creative things
    - Enables better quality of life

- Current generation of AI technologies are still considered as Artificial Narrow Intelligence (ANI)

    - The goal is to eventually Artificial General Intelligence (AGI)

- But there are also many concerns about the potential risk that we need to be aware of

    - It is important for us to development appropriate frameworks to promote the responsible use of AI