CS2107 Review & Final Exam Tips

Teaching Mode

- **13** Lectures
- **9** Tutorials
- **11** Self-exploration activities (self-exercised mini *labs*)

- Continual Assessment (55%):
  - 2 Assignments (25%): Do submit **A2** before its deadline
  - 1 Mid-term quiz (15%)
  - 1 Group presentation on open-ended topic (5%)
  - Tutorial attendance (5%)
  - 1 **LumiNUS online quiz** assessment (5%)

- **Final E-exam (45%)**: Open-book, ***Thursday* 26 Nov**, 09:00-11:00

  Please *double-check* the timing with CORS again!

Module Description

Objective

This module serves as an introductory module on information security. It ***illustrates*** the ***fundamentals of how systems fail*** due to malicious activities ***and how they can be protected***. The module also places emphasis on the practices of secure programming and implementation. Topics covered include **classical/historical ciphers**, **introduction to modern ciphers** and cryptosystems, ethical, legal and organisational aspects, classic examples of direct attacks on computer systems such as **input validation vulnerability**, examples of other forms of attack such as **social engineering/phishing attacks**, and the **practice of secure programming**.

Outcomes

- Awareness of common and well-known attacks (e.g. phishing, XSS, SQLI, ...)
- Understand basic concepts of security (e.g. confidentiality, availability, ...)
- Understand basic mechanisms & practice of protections (e.g. crypto, PKI, access control, ...)
- Awareness of common pitfalls in implementation (Secure programming)

More Specific Intended Learning Outcome (ILO)

After completing the module, you will be expected to be able to:

1. Explain *the C-I-A security requirements* and recognize their breaches in recent security incident news
2. Describe *key concepts and basic mechanisms* of principal protection mechanisms in information security, such as encryption, authentication, and secure channel
3. Identify the *limitations* of classical cryptographic schemes, and recognize *well-known attacks* on vulnerable hosts, networks, and Web servers

More Specific Intended Learning Outcome (ILO)

4. Utilize some *basic security tools* (e.g. OpenSSL, Wireshark) and security-related *Linux commands* to perform encryption and network traffic analysis
5. Pinpoint flaws in programs due to common *insecure programming practices*, and suggest improvements using more secure practices instead

Some of the Terms Encountered in This Module

Secure channel, Alice, Bob, Eve, Encryption, Decryption, Key-space, Known-plaintext attack, Authenticity, Confidentiality, Availability, Authentication protocol, Man-in-the-middle, Passwords, Dictionary attack, Random IV, Kerckhoffs' principle, RSA, Certificate, Public Key Infrastructure, Digital Signature.

Side-channel attack, Timing attack, ATM skimmer, Social engineering.

SSL, TLS, HTTPS, Secure channel on the Internet.

DDOS, Syn flood, Wireshark, Spoofing, Sniffing, Cache poisoning, Tor.

Input validation, SQL injection, Secure programming, Buffer overflow, Stack smashing, Integer overflow, CVE.

Key-logger, virus*, worm*, rootkit, botnet.

For their differences, see: https://www.kaspersky.com/resource-center/threats/computer-viruses-vs-worms

Completed Lectures

Lecture 1: Encryption *(a big **multi-part** lecture)*

Security requirements, encryption/cryptography (classical ciphers, stream cipher, block ciphers) & attacks, key length, IV, Kerckhoffs' principle

Lecture 2: Authentication (Password/weak)

Password, 2FA, biometrics, confidentiality ⇏ integrity, phishing

Lecture 3: Authenticity (MAC & Signature)

PKC, hash, MAC, signature, birthday paradox

Lecture 4: PKI + Channel Security

PKI, certificate, CA, hierarchical trust relationship

Lecture 5 : Secure Channel, TLS/SSL, Crypto Misc.

Strong authentication, key exchange & authenticated key exchange, SSL/TLS, authenticated encryption

Lecture 6: Network Security

Layering, naming issue (DNS attack), DDoS, firewall

Lecture 7: Access Control

Access control model, Linux/UNIX access control, privilege elevation

Lecture 8 : Software Security

Background on computer architecture, call stack, integer overflow, data representation issue, buffer overflow, security problem with scripting languages, counter measures

Lecture 9: Web Security

Web security issues & threat models, TLS/SSL issues, UI attacks, cookies & SOP, XSS, CSRF

Completed Tutorials

Tutorial 1: Introduction & Encryption

Security requirement, key length requirement, role of IV, tradeoff of usability & security

Tutorial 2: Encryption & Block Cipher

Block size, mode-of-operation, DES insecure usage, 3DES

Tutorial 3: Encryption & Password

Password, security questions, 2FA

Tutorial 4: Data-Origin Authentication

Birthday attack, hash, secure random number generation, implementation issue on secret key generation (which illustrates that hash doesn't produce truly random sequence)

Tutorial 5: PKI, SSL and Birthday Attack Variant

PKI, proxy-re-encryption, limitation of PKI, variant of birthday attack

Mid-term quiz discussion

Tutorial 6: Security Protocol - TLS and Its Renegotiation Attack

SSL/TLS, re-negotiation attack (which illustrates subtlety of protocol design)

Tutorial 7: Network Security + Privilege Escalation

Firewall rules (2-firewall setting, DMZ), setUID, privilege escalation

Tutorial 8: Software Security

Buffer overflow vulnerabilities, safe/unsafe C functions, integer overflow

Group project presentations (2 sessions)

Shared Self-Exploration Activities

Activity 1: Introduction, Classical ciphers

A look at malicious-executable creation difficulty in practice, substitution cipher cracking scripts

Activity 2: Classical ciphers & attacks

Scripts that implement & attack Shift/Caesar cipher, Vigenere cipher, One-Time Pad

Activity 3: Block ciphers, Pseudo-random numbers

OpenSSL for encryptions using block ciphers & modes-of-operation, pseudorandom numbers in Linux/UNIX

Activity 4: Authentication (Password)

Password & shadow files, password cracking using John the Ripper

Activity 5 : Authenticity (MAC & Signature)

OpenSSL for hash & MAC, SHA-1 collision attacks, RSA encryption scheme

Activity 6: PKI

Openssl for public-key pair generation, certificate inspection

Activity 7: TLS/SSL

Openssl for TLS/SSL connection, TLS server configuration & certificate, TLS server & client check

Activity 8 : Network security

Wireshark, Nmap

Activity 9: Access Control

Linux access control

Activity 10: Buffer Overflow Vulnerability & Exploitation

Activity 11: Web Security

OS command injection, SQL Injection, XSS, bypassing anti-XSS input-sanitization

Assignments: CTF Style

- For ***gamification*** of hacking challenges: phased hint releases, possible task-completion dependency, etc.
- For **automated** challenge-submission **marking**: real-time & scalable checking of submission attempts, *mark scoreboard*
- Assignment 1:
  Cryptography, authentication
- Assignment 2:
  Network, software and web security
- Additional **online quiz assessment** via LumiNUS:
  for overall material review and final-exam practice

Ethical Use of Security Information

- We have discussed **vulnerabilities and attacks**
- Most vulnerabilities have been fixed, ***but***:
  - **Do not** assume that all systems are patched/fixed
  - **Some attacks** may still cause harm!
- Purpose of our security modules:
  - Learn to prevent malicious **attacks**
  - Use your knowledge for **good** purposes
- Remember again:
  Computer Misuse and Cybersecurity Act (CMCA)
- Please **observe the prevailing law**

Hacking: It’s Fun, *Do not* Cross the Yellow/Red Line

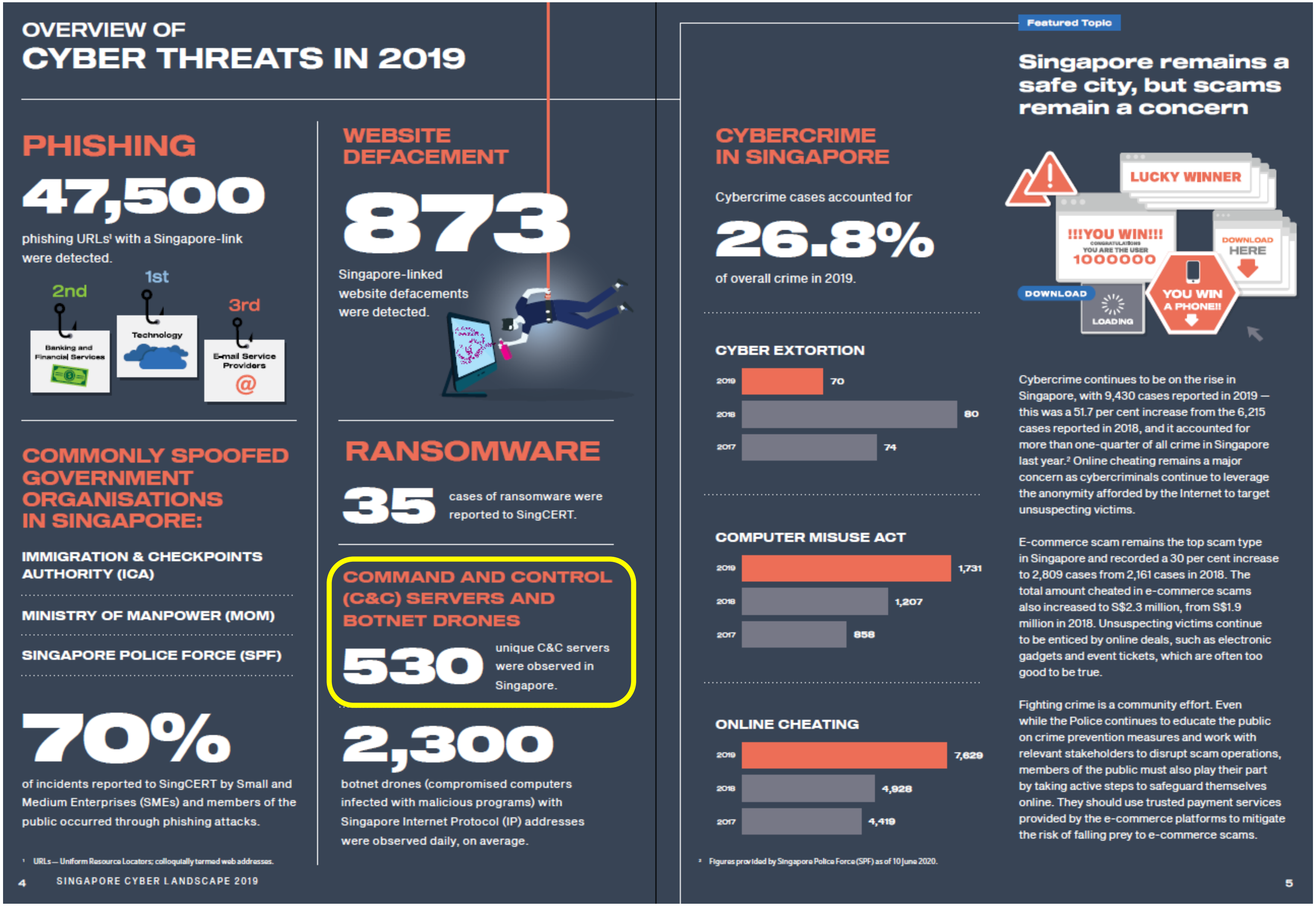
Value Life. Act Responsibly
生命要珍惜.行为要负责
Hargai Nyawa. Bertindak Dengan Tanggungjawab
உயிர் மதிப்புமிக்கது. பொறுப்புடன் நடந்து கொள்ளவும்

Singapore Cyber Landscape

Singapore Cyber Landscape Report

- Annual snapshot of cyber landscape in Singapore
- “***Singapore Cyber Landscape 2019***”,
  by Cyber Security Agency of Singapore, 2020:
  - Global trends & local case studies
  - Upping the game on Singapore’s cybersecurity
  - Looking ahead — Cyber trends to watch:
    including Cybersecurity and COVID-19
- See:
  https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2019

Cyber Threats in 2019



OVERVIEW OF CYBER THREATS IN 2019

PHISHING

47,500

phishing URLs[1] with a Singapore-link were detected.

COMMONLY SPOOFED GOVERNMENT ORGANISATIONS IN SINGAPORE:

IMMIGRATION & CHECKPOINTS AUTHORITY (ICA)

MINISTRY OF MANPOWER (MOM)

SINGAPORE POLICE FORCE (SPF)

70%

of incidents reported to SingCERT by Small and Medium Enterprises (SMEs) and members of the public occurred through phishing attacks.

WEBSITE DEFACEMENT

873

Singapore-linked website defacements were detected.

RANSOMWARE

35 cases of ransomware were reported to SingCERT.

COMMAND AND CONTROL (C&C) SERVERS AND BOTNET DRONES

530 unique C&C servers were observed in Singapore.

2,300

botnet drones (compromised computers infected with malicious programs) with Singapore Internet Protocol (IP) addresses were observed daily, on average.

[1] URLs — Uniform Resource Locators; colloquially termed web addresses.

Featured Topic

CYBERCRIME IN SINGAPORE

Cybercrime cases accounted for

26.8%

of overall crime in 2019.

CYBER EXTORTION

2019	70
2018	80
2017	74

COMPUTER MISUSE ACT

2019	1,731
2018	1,207
2017	858

ONLINE CHEATING

2019	7,629
2018	4,928
2017	4,419

[2] Figures provided by Singapore Police Force (SPF) as of 10 June 2020.

Singapore remains a safe city, but scams remain a concern

Cybercrime continues to be on the rise in Singapore, with 9,430 cases reported in 2019 — this was a 51.7 per cent increase from the 6,215 cases reported in 2018, and it accounted for more than one-quarter of all crime in Singapore last year.[2] Online cheating remains a major concern as cybercriminals continue to leverage the anonymity afforded by the Internet to target unsuspecting victims.

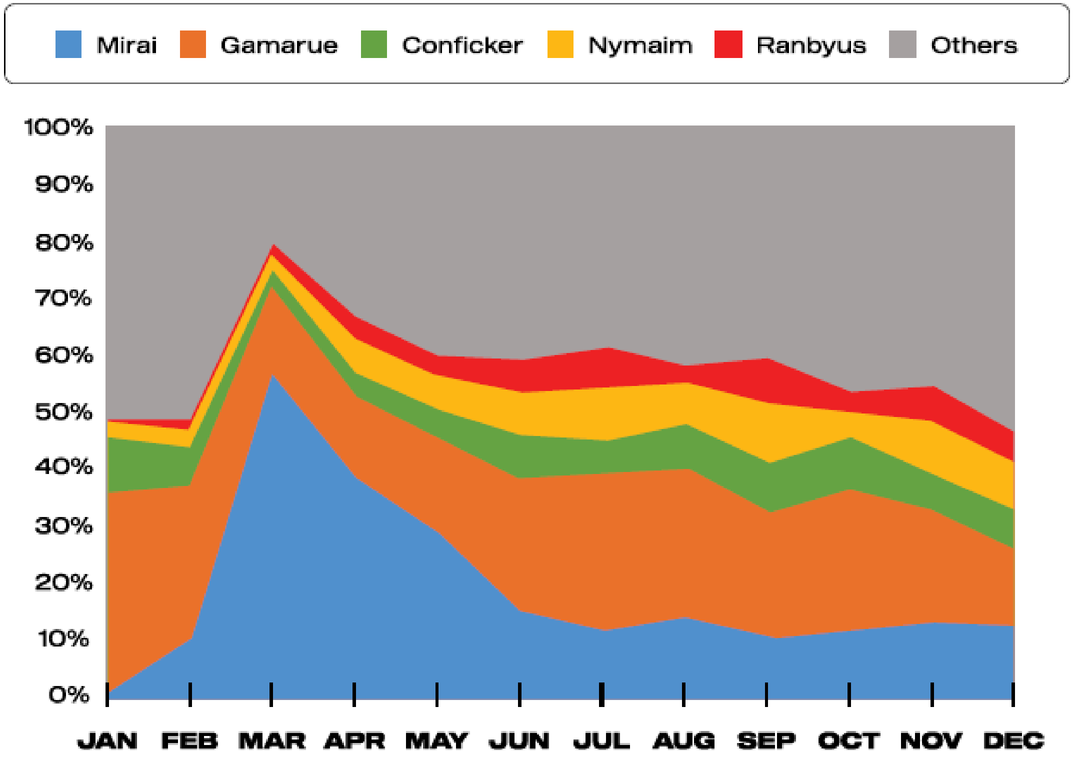
E-commerce scam remains the top scam type in Singapore and recorded a 30 per cent increase to 2,809 cases from 2,161 cases in 2018. The total amount cheated in e-commerce scams also increased to S$2.3 million, from S$1.9 million in 2018. Unsuspecting victims continue to be enticed by online deals, such as electronic gadgets and event tickets, which are often too good to be true.

Fighting crime is a community effort. Even while the Police continues to educate the public on crime prevention measures and work with relevant stakeholders to disrupt scam operations, members of the public must also play their part by taking active steps to safeguard themselves online. They should use trusted payment services provided by the e-commerce platforms to mitigate the risk of falling prey to e-commerce scams.

Spotlight on Cyber Threats: Malware

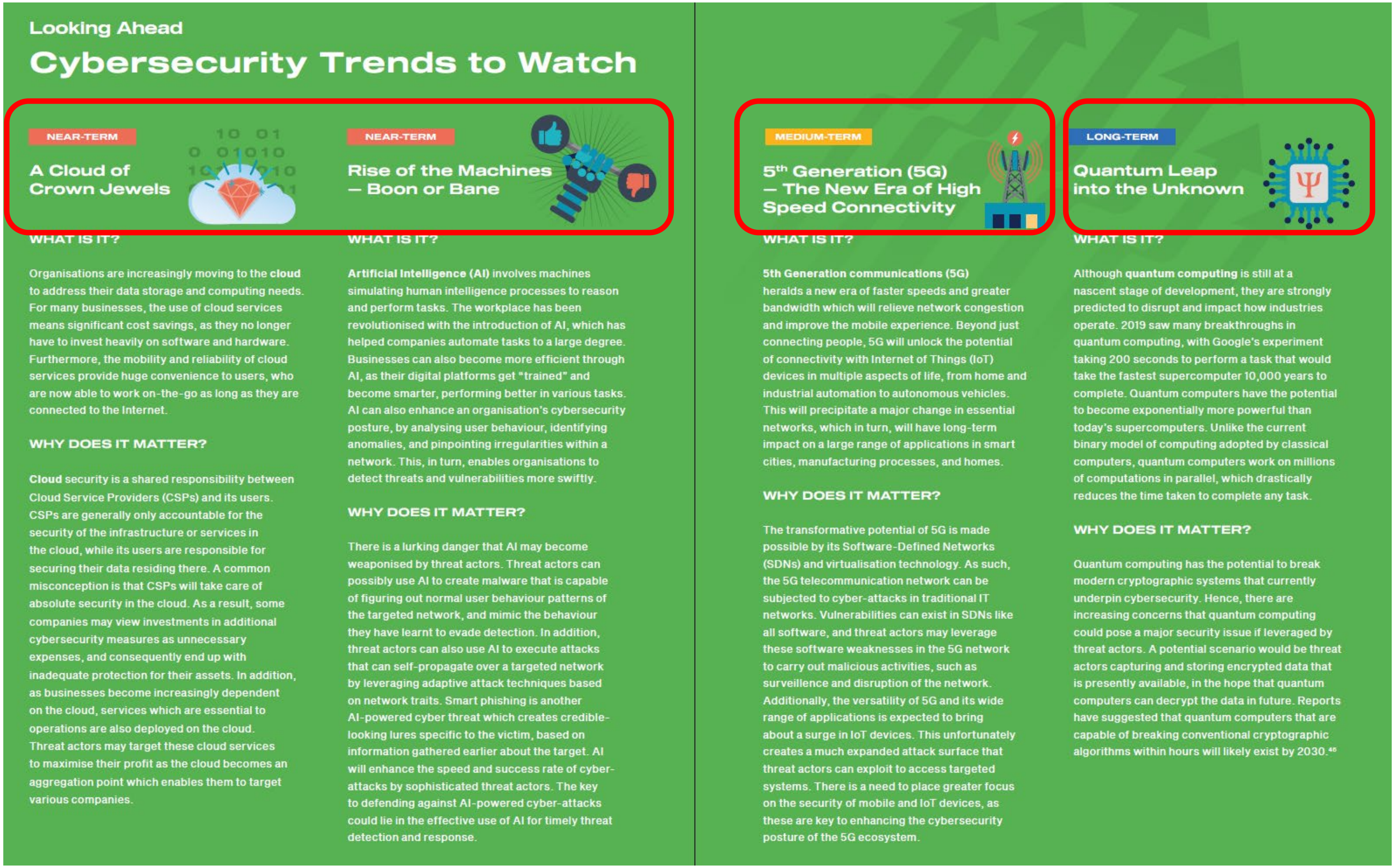
C&C Servers and Botnet Drones

In 2019, CSA detected about 530 unique C&C servers in Singapore, a 73 per cent increase from 2018. On average, about 2,300 botnet drones with Singapore Internet Protocol (IP) addresses were observed daily, a 20 per cent decrease from average daily observations in 2018. Close to 370 malware variants were detected, with the top five malware observed — *Mirai*, *Gamarue*, *Conficker*, *Nymaim*, and *Ranbyus* — accounting for over half of all observed infections. These malware are not new, with *Ranbyus* and *Nymaim* first detected in 2011 and 2013, respectively.



On average, five common malware accounted for over half the daily infections of computing devices in 2019.

Cyber Trends to Watch



Looking Ahead

Cybersecurity Trends to Watch

NEAR-TERM

A Cloud of Crown Jewels

WHAT IS IT?

Organisations are increasingly moving to the **cloud** to address their data storage and computing needs. For many businesses, the use of cloud services means significant cost savings, as they no longer have to invest heavily on software and hardware. Furthermore, the mobility and reliability of cloud services provide huge convenience to users, who are now able to work on-the-go as long as they are connected to the Internet.

WHY DOES IT MATTER?

Cloud security is a shared responsibility between Cloud Service Providers (CSPs) and its users. CSPs are generally only accountable for the security of the infrastructure or services in the cloud, while its users are responsible for securing their data residing there. A common misconception is that CSPs will take care of absolute security in the cloud. As a result, some companies may view investments in additional cybersecurity measures as unnecessary expenses, and consequently end up with inadequate protection for their assets. In addition, as businesses become increasingly dependent on the cloud, services which are essential to operations are also deployed on the cloud. Threat actors may target these cloud services to maximise their profit as the cloud becomes an aggregation point which enables them to target various companies.

NEAR-TERM

Rise of the Machines — Boon or Bane

WHAT IS IT?

Artificial Intelligence (AI) involves machines simulating human intelligence processes to reason and perform tasks. The workplace has been revolutionised with the introduction of AI, which has helped companies automate tasks to a large degree. Businesses can also become more efficient through AI, as their digital platforms get "trained" and become smarter, performing better in various tasks. AI can also enhance an organisation's cybersecurity posture, by analysing user behaviour, identifying anomalies, and pinpointing irregularities within a network. This, in turn, enables organisations to detect threats and vulnerabilities more swiftly.

WHY DOES IT MATTER?

There is a lurking danger that AI may become weaponised by threat actors. Threat actors can possibly use AI to create malware that is capable of figuring out normal user behaviour patterns of the targeted network, and mimic the behaviour they have learnt to evade detection. In addition, threat actors can also use AI to execute attacks that can self-propagate over a targeted network by leveraging adaptive attack techniques based on network traits. Smart phishing is another AI-powered cyber threat which creates credible-looking lures specific to the victim, based on information gathered earlier about the target. AI will enhance the speed and success rate of cyber-attacks by sophisticated threat actors. The key to defending against AI-powered cyber-attacks could lie in the effective use of AI for timely threat detection and response.

MEDIUM-TERM

5th Generation (5G) — The New Era of High Speed Connectivity

WHAT IS IT?

5th Generation communications (5G) heralds a new era of faster speeds and greater bandwidth which will relieve network congestion and improve the mobile experience. Beyond just connecting people, 5G will unlock the potential of connectivity with Internet of Things (IoT) devices in multiple aspects of life, from home and industrial automation to autonomous vehicles. This will precipitate a major change in essential networks, which in turn, will have long-term impact on a large range of applications in smart cities, manufacturing processes, and homes.

WHY DOES IT MATTER?

The transformative potential of 5G is made possible by its Software-Defined Networks (SDNs) and virtualisation technology. As such, the 5G telecommunication network can be subjected to cyber-attacks in traditional IT networks. Vulnerabilities can exist in SDNs like all software, and threat actors may leverage these software weaknesses in the 5G network to carry out malicious activities, such as surveillence and disruption of the network. Additionally, the versatility of 5G and its wide range of applications is expected to bring about a surge in IoT devices. This unfortunately creates a much expanded attack surface that threat actors can exploit to access targeted systems. There is a need to place greater focus on the security of mobile and IoT devices, as these are key to enhancing the cybersecurity posture of the 5G ecosystem.

LONG-TERM

Quantum Leap into the Unknown

WHAT IS IT?

Although **quantum computing** is still at a nascent stage of development, they are strongly predicted to disrupt and impact how industries operate. 2019 saw many breakthroughs in quantum computing, with Google's experiment taking 200 seconds to perform a task that would take the fastest supercomputer 10,000 years to complete. Quantum computers have the potential to become exponentially more powerful than today's supercomputers. Unlike the current binary model of computing adopted by classical computers, quantum computers work on millions of computations in parallel, which drastically reduces the time taken to complete any task.

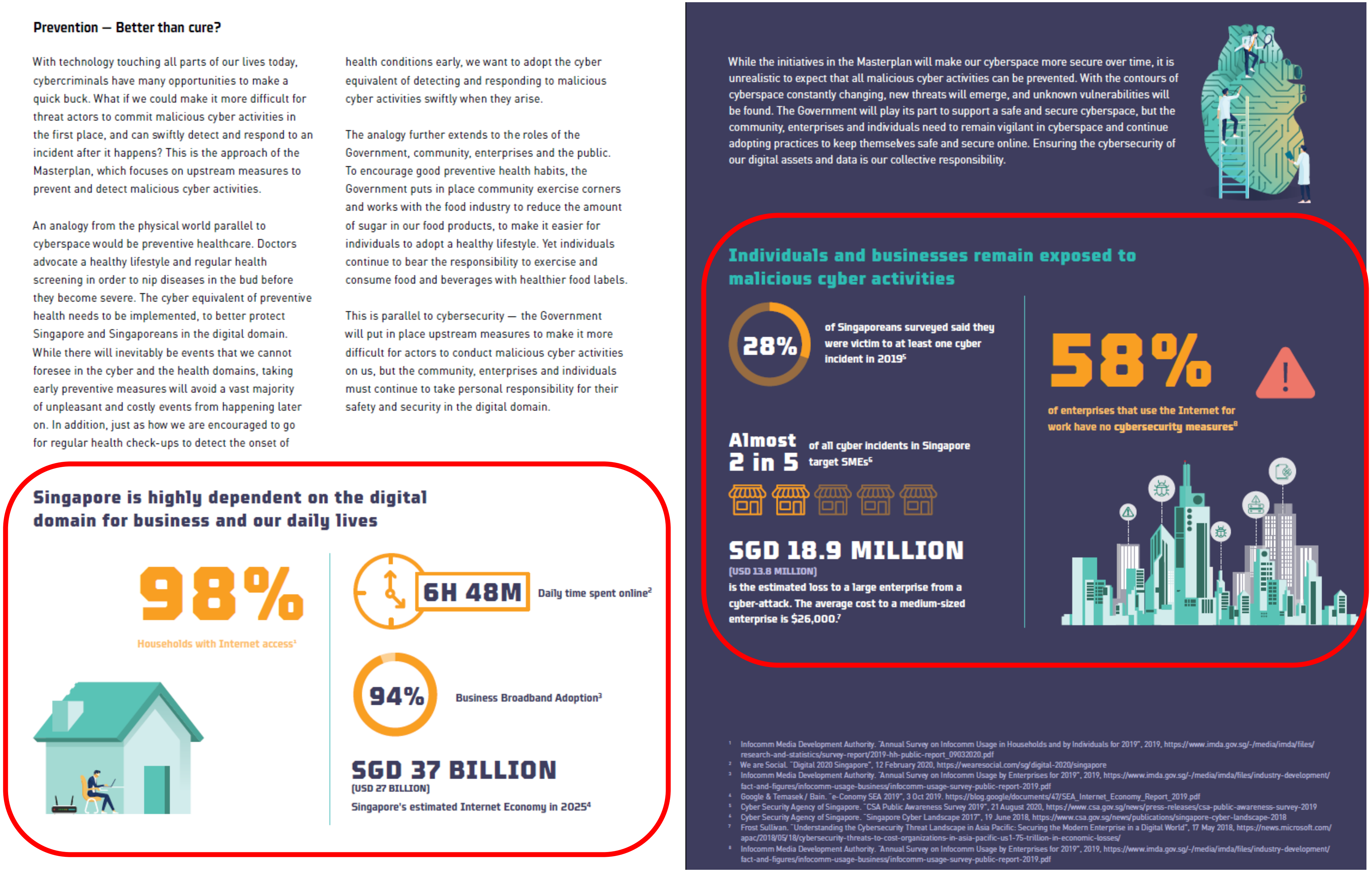
WHY DOES IT MATTER?

Quantum computing has the potential to break modern cryptographic systems that currently underpin cybersecurity. Hence, there are increasing concerns that quantum computing could pose a major security issue if leveraged by threat actors. A potential scenario would be threat actors capturing and storing encrypted data that is presently available, in the hope that quantum computers can decrypt the data in future. Reports have suggested that quantum computers that are capable of breaking conventional cryptographic algorithms within hours will likely exist by 2030.[40]

Singapore’s Safer Cyberspace Masterplan 2020

- “***Singapore’s Safer Cyberspace Masterplan***”,
  Cyber Security Agency of Singapore, 2020,
  https://www.csa.gov.sg/news/press-releases/safer-cyberspace-masterplan-launch
- From its **executive summary**:
  “As Singapore embarks on its digital transformation toward a **Smart Nation and Digital Economy**, Singaporeans and our enterprises will also face **increasing cyber threats** as more of our citizens and businesses go online. **Cybersecurity** will be a **critical enabler** of our push toward digitalisation. Without **robust cybersecurity** in place, our systems and networks remain open and vulnerable for malicious threat actors to exploit our digital assets and data.”
- It comprises the following ***three thrusts***:
  - Securing our core digital **infrastructure**
  - Safeguarding our cyberspace **activities**
  - Empowering our **cyber-savvy population**

Safer Cyberspace Masterplan 2020: Why?



Prevention — Better than cure?

With technology touching all parts of our lives today, cybercriminals have many opportunities to make a quick buck. What if we could make it more difficult for threat actors to commit malicious cyber activities in the first place, and can swiftly detect and respond to an incident after it happens? This is the approach of the Masterplan, which focuses on upstream measures to prevent and detect malicious cyber activities.

An analogy from the physical world parallel to cyberspace would be preventive healthcare. Doctors advocate a healthy lifestyle and regular health screening in order to nip diseases in the bud before they become severe. The cyber equivalent of preventive health needs to be implemented, to better protect Singapore and Singaporeans in the digital domain. While there will inevitably be events that we cannot foresee in the cyber and the health domains, taking early preventive measures will avoid a vast majority of unpleasant and costly events from happening later on. In addition, just as how we are encouraged to go for regular health check-ups to detect the onset of health conditions early, we want to adopt the cyber equivalent of detecting and responding to malicious cyber activities swiftly when they arise.

The analogy further extends to the roles of the Government, community, enterprises and the public. To encourage good preventive health habits, the Government puts in place community exercise corners and works with the food industry to reduce the amount of sugar in our food products, to make it easier for individuals to adopt a healthy lifestyle. Yet individuals continue to bear the responsibility to exercise and consume food and beverages with healthier food labels.

This is parallel to cybersecurity — the Government will put in place upstream measures to make it more difficult for actors to conduct malicious cyber activities on us, but the community, enterprises and individuals must continue to take personal responsibility for their safety and security in the digital domain.

Singapore is highly dependent on the digital domain for business and our daily lives

98% Households with Internet access[1]

6H 48M Daily time spent online[2]

94% Business Broadband Adoption[3]

SGD 37 BILLION (USD 27 BILLION) Singapore's estimated Internet Economy in 2025[4]

While the initiatives in the Masterplan will make our cyberspace more secure over time, it is unrealistic to expect that all malicious cyber activities can be prevented. With the contours of cyberspace constantly changing, new threats will emerge, and unknown vulnerabilities will be found. The Government will play its part to support a safe and secure cyberspace, but the community, enterprises and individuals need to remain vigilant in cyberspace and continue adopting practices to keep themselves safe and secure online. Ensuring the cybersecurity of our digital assets and data is our collective responsibility.

Individuals and businesses remain exposed to malicious cyber activities

28% of Singaporeans surveyed said they were victim to at least one cyber incident in 2019[5]

Almost 2 in 5 of all cyber incidents in Singapore target SMEs[6]

SGD 18.9 MILLION (USD 13.8 MILLION) is the estimated loss to a large enterprise from a cyber-attack. The average cost to a medium-sized enterprise is $26,000.[7]

58% of enterprises that use the Internet for work have no cybersecurity measures[8]

[1] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage in Households and by Individuals for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/research-and-statistics/survey-report/2019-hh-public-report_09032020.pdf

[2] We are Social. "Digital 2020 Singapore", 12 February 2020, https://wearesocial.com/sg/digital-2020/singapore

[3] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf

[4] Google & Temasek / Bain. "e-Conomy SEA 2019", 3 Oct 2019. https://blog.google/documents/47/SEA_Internet_Economy_Report_2019.pdf

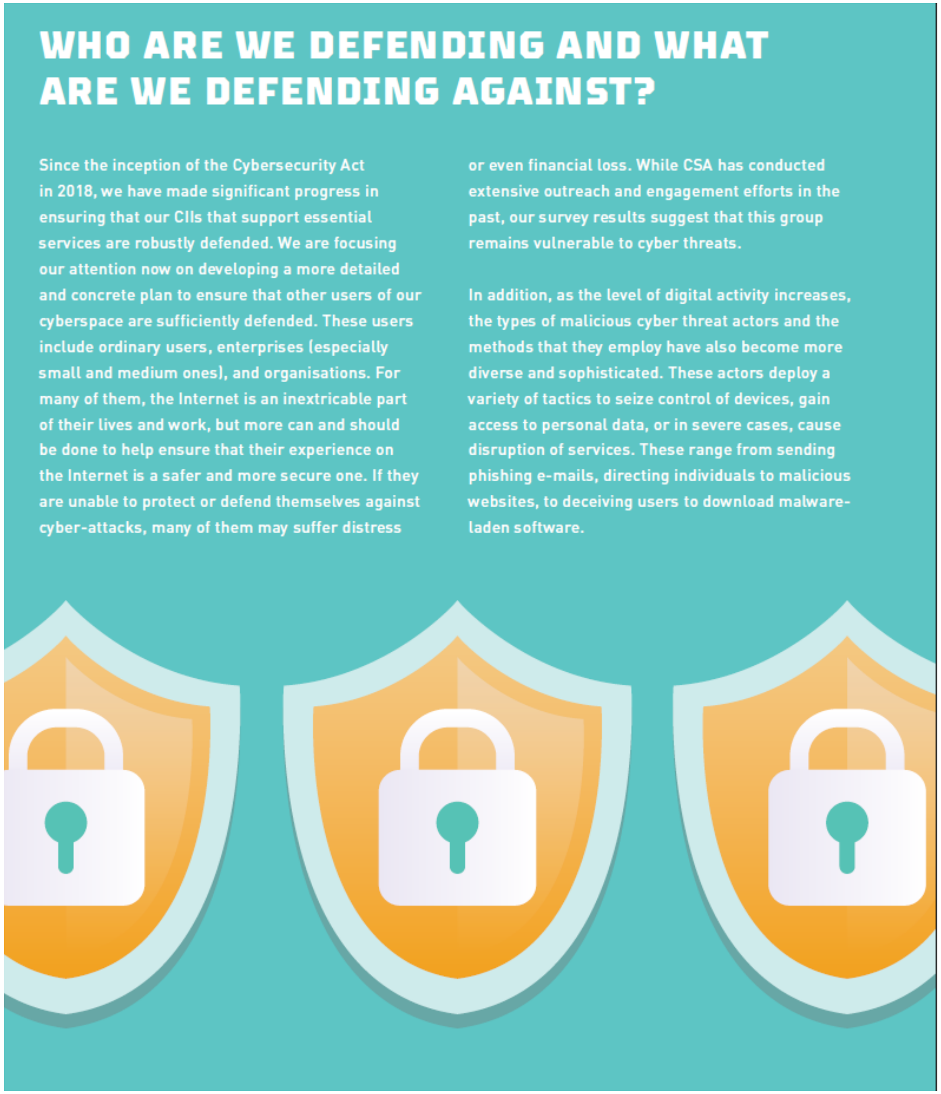
[5] Cyber Security Agency of Singapore. "CSA Public Awareness Survey 2019", 21 August 2020, https://www.csa.gov.sg/news/press-releases/csa-public-awareness-survey-2019

[6] Cyber Security Agency of Singapore. "Singapore Cyber Landscape 2017", 19 June 2018, https://www.csa.gov.sg/news/publications/singapore-cyber-landscape-2018

[7] Frost Sullivan. "Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World", 17 May 2018, https://news.microsoft.com/apac/2018/05/18/cybersecurity-threats-to-cost-organizations-in-asia-pacific-us1-75-trillion-in-economic-losses/

[8] Infocomm Media Development Authority. "Annual Survey on Infocomm Usage by Enterprises for 2019", 2019, https://www.imda.gov.sg/-/media/imda/files/industry-development/fact-and-figures/infocomm-usage-business/infocomm-usage-survey-public-report-2019.pdf

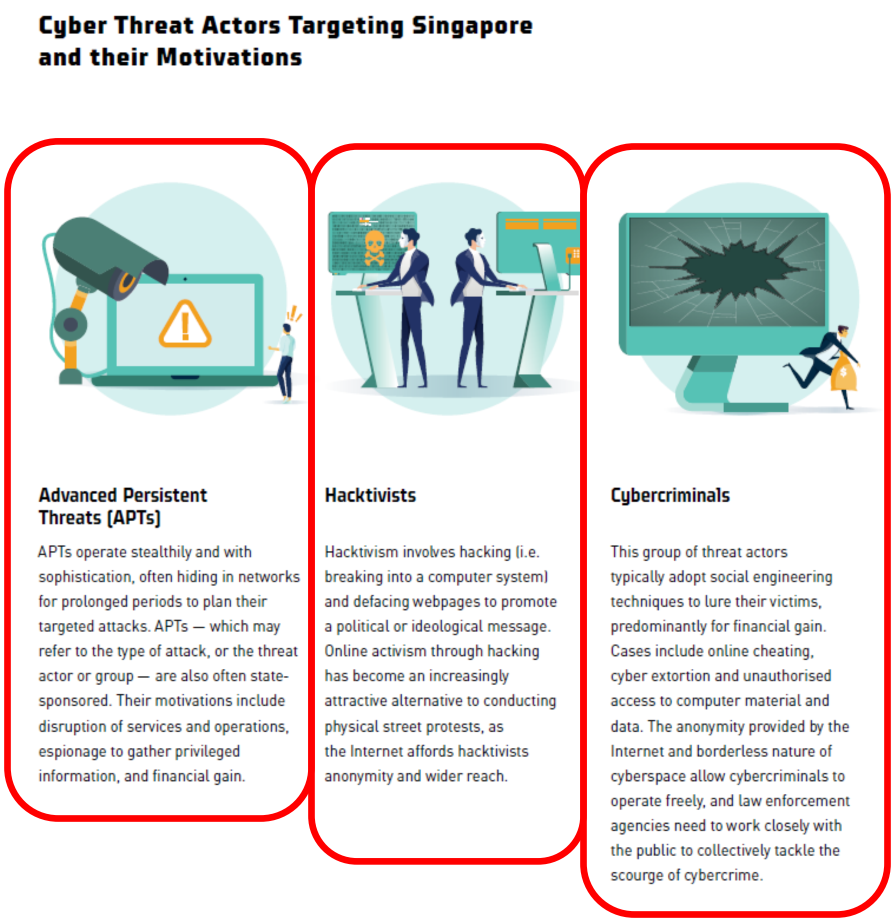
Safer Cyberspace Masterplan 2020: Threat Actors



WHO ARE WE DEFENDING AND WHAT ARE WE DEFENDING AGAINST?

Since the inception of the Cybersecurity Act in 2018, we have made significant progress in ensuring that our CIIs that support essential services are robustly defended. We are focusing our attention now on developing a more detailed and concrete plan to ensure that other users of our cyberspace are sufficiently defended. These users include ordinary users, enterprises (especially small and medium ones), and organisations. For many of them, the Internet is an inextricable part of their lives and work, but more can and should be done to help ensure that their experience on the Internet is a safer and more secure one. If they are unable to protect or defend themselves against cyber-attacks, many of them may suffer distress or even financial loss. While CSA has conducted extensive outreach and engagement efforts in the past, our survey results suggest that this group remains vulnerable to cyber threats.

In addition, as the level of digital activity increases, the types of malicious cyber threat actors and the methods that they employ have also become more diverse and sophisticated. These actors deploy a variety of tactics to seize control of devices, gain access to personal data, or in severe cases, cause disruption of services. These range from sending phishing e-mails, directing individuals to malicious websites, to deceiving users to download malware-laden software.



Cyber Threat Actors Targeting Singapore and their Motivations

Advanced Persistent Threats (APTs)

APTs operate stealthily and with sophistication, often hiding in networks for prolonged periods to plan their targeted attacks. APTs — which may refer to the type of attack, or the threat actor or group — are also often state-sponsored. Their motivations include disruption of services and operations, espionage to gather privileged information, and financial gain.

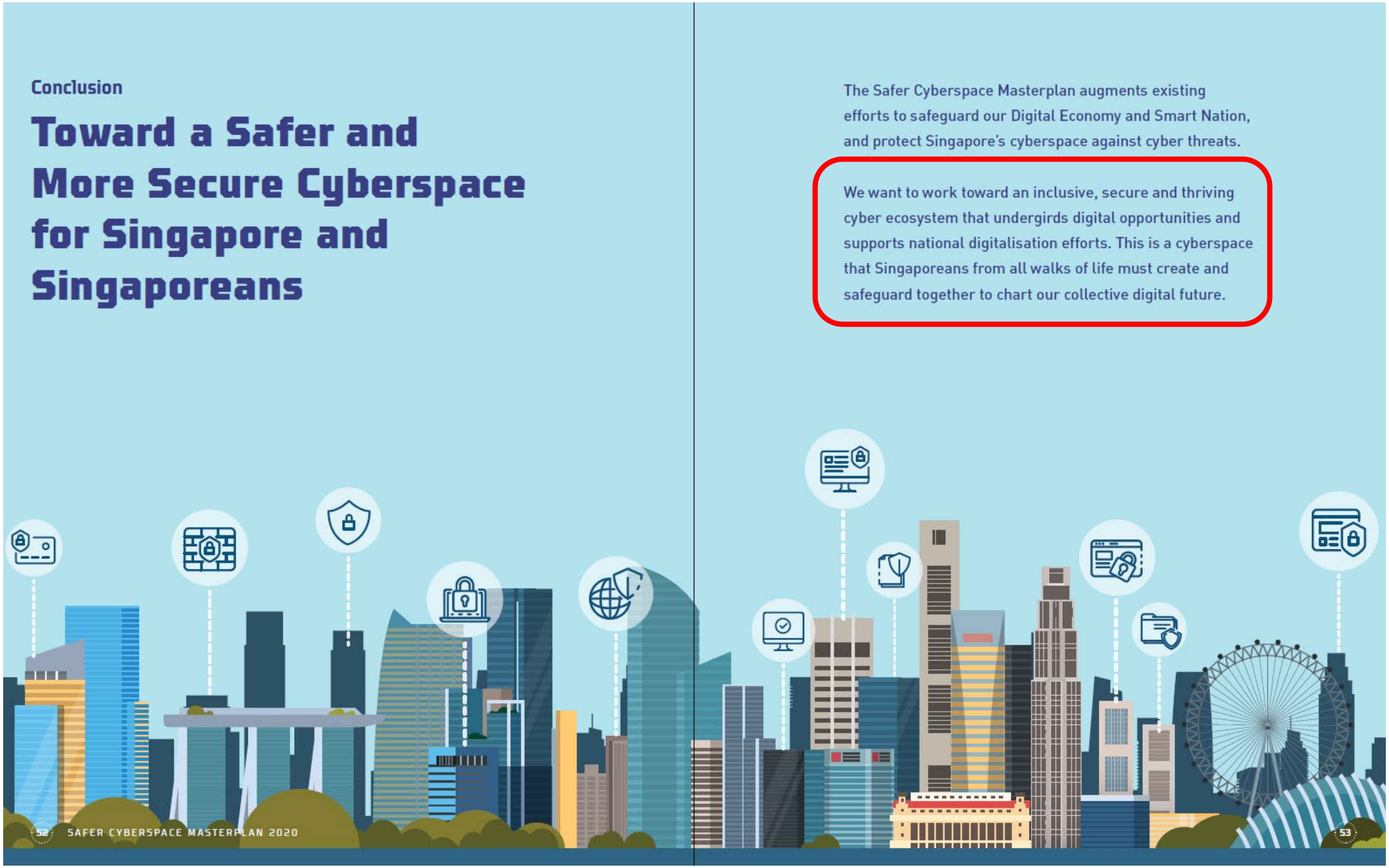
Hacktivists

Hacktivism involves hacking (i.e. breaking into a computer system) and defacing webpages to promote a political or ideological message. Online activism through hacking has become an increasingly attractive alternative to conducting physical street protests, as the Internet affords hacktivists anonymity and wider reach.

Cybercriminals

This group of threat actors typically adopt social engineering techniques to lure their victims, predominantly for financial gain. Cases include online cheating, cyber extortion and unauthorised access to computer material and data. The anonymity provided by the Internet and borderless nature of cyberspace allow cybercriminals to operate freely, and law enforcement agencies need to work closely with the public to collectively tackle the scourge of cybercrime.

Safer Cyberspace Masterplan 2020: Conclusion



Conclusion

Toward a Safer and More Secure Cyberspace for Singapore and Singaporeans

The Safer Cyberspace Masterplan augments existing efforts to safeguard our Digital Economy and Smart Nation, and protect Singapore's cyberspace against cyber threats.

We want to work toward an inclusive, secure and thriving cyber ecosystem that undergirds digital opportunities and supports national digitalisation efforts. This is a cyberspace that Singaporeans from all walks of life must create and safeguard together to chart our collective digital future.

52 SAFER CYBERSPACE MASTERPLAN 2020

53

Your Next Steps

Security-Related Modules in SOC

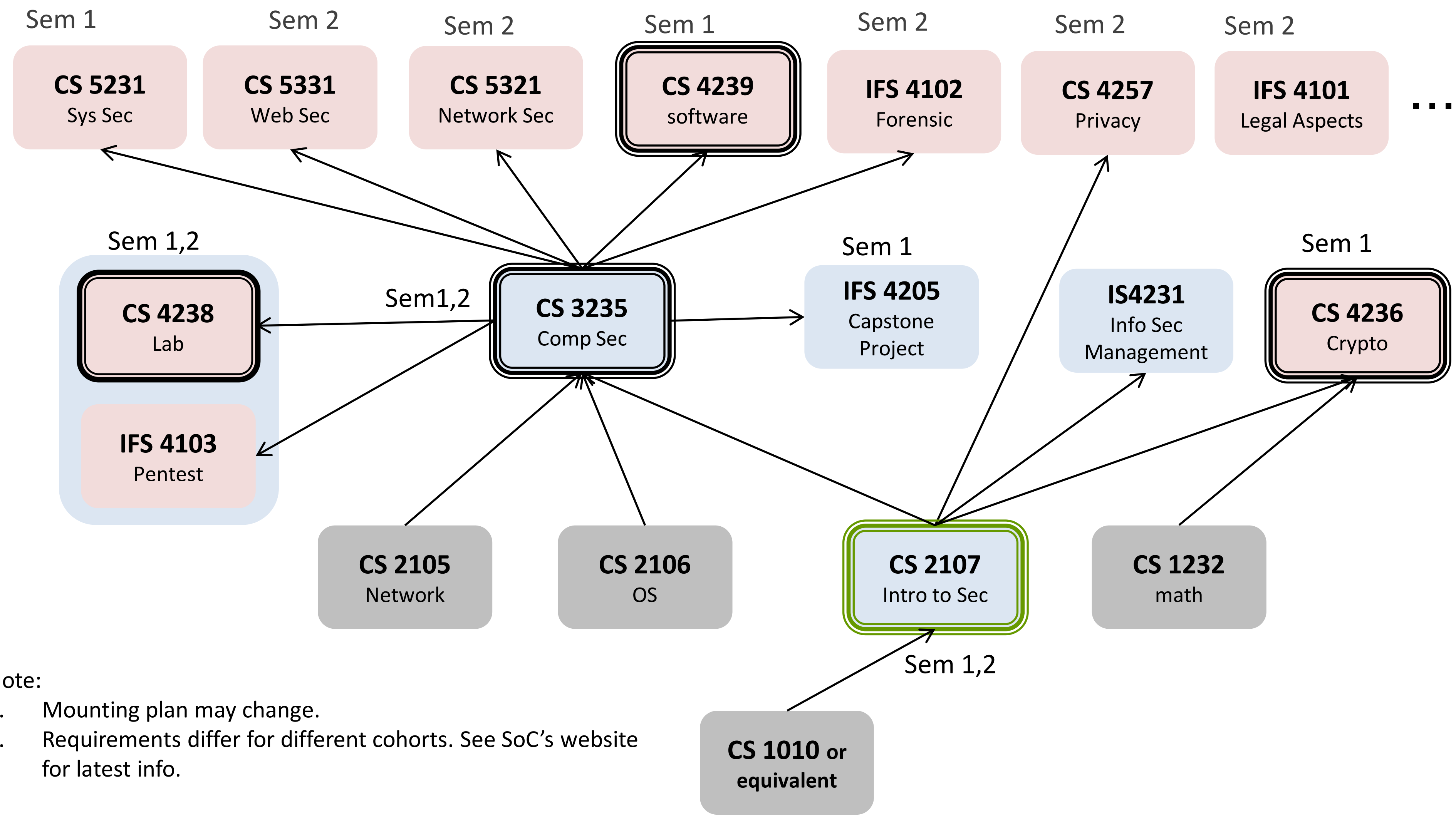
🟦 cores in InfoSec degree

🟥 Electives in InfoSec degree (choose 3)

□ Security Area Focus (choose 3)

CS6230
info sec

CS6231
sys sec



Sem 1
CS 5231
Sys Sec

Sem 2
CS 5331
Web Sec

Sem 2
CS 5321
Network Sec

Sem 1
CS 4239
software

Sem 2
IFS 4102
Forensic

Sem 2
CS 4257
Privacy

Sem 2
IFS 4101
Legal Aspects

…

Sem 1,2
CS 4238
Lab

IFS 4103
Pentest

Sem1,2
CS 3235
Comp Sec

Sem 1
IFS 4205
Capstone Project

IS4231
Info Sec Management

Sem 1
CS 4236
Crypto

CS 2105
Network

CS 2106
OS

CS 2107
Intro to Sec

CS 1232
math

Sem 1,2

CS 1010 or equivalent

Note:

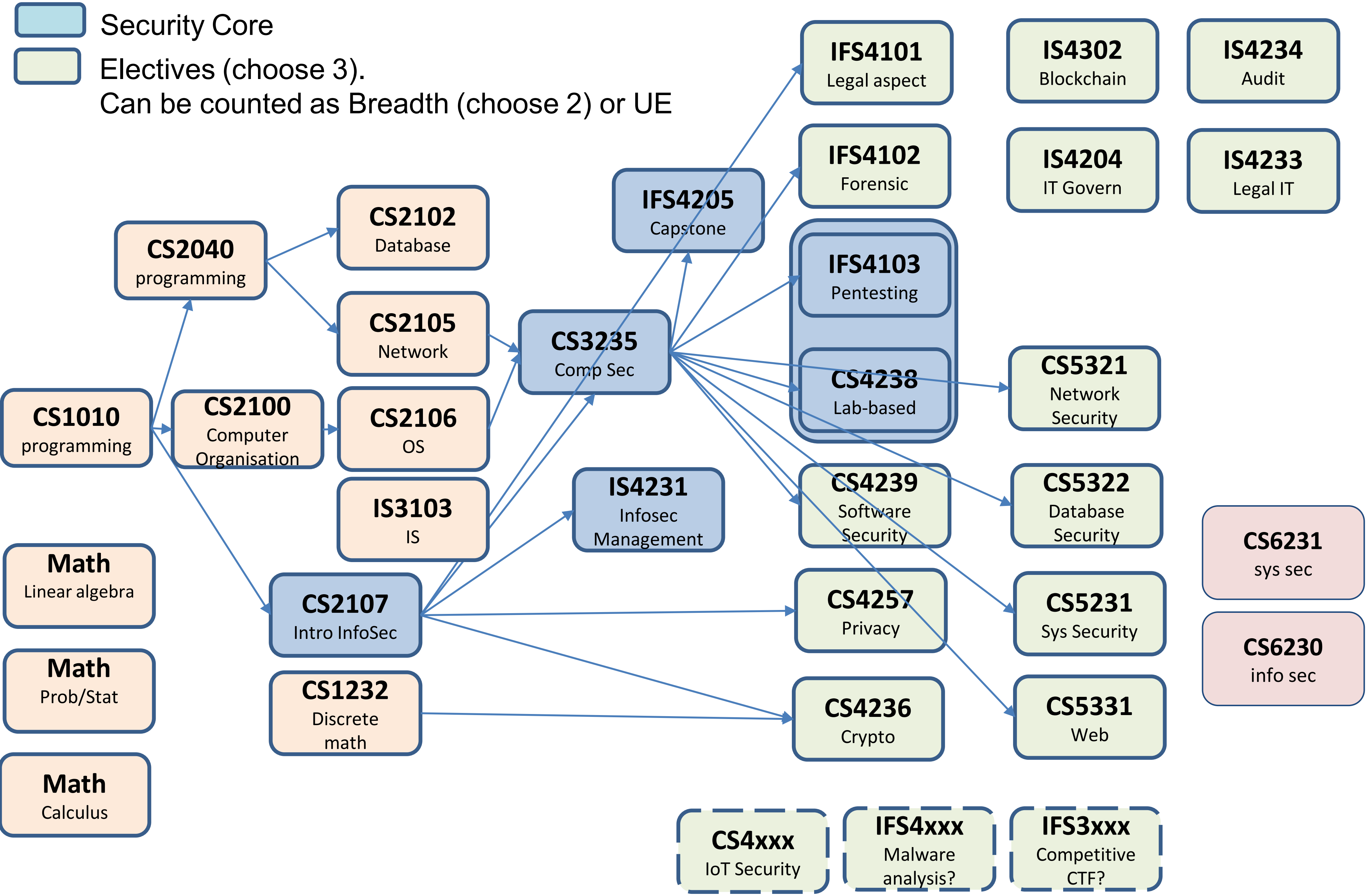
1. Mounting plan may change.
2. Requirements differ for different cohorts. See SoC's website for latest info.

Security-Related Modules and BCOMP InfoSec Requirements

🟧 Foundation

🟦 Security Core

🟩 Electives (choose 3).
Can be counted as Breadth (choose 2) or UE



CS1010 programming

CS2040 programming

CS2100 Computer Organisation

CS2102 Database

CS2105 Network

CS2106 OS

IS3103 IS

CS2107 Intro InfoSec

CS1232 Discrete math

Math Linear algebra

Math Prob/Stat

Math Calculus

CS3235 Comp Sec

IS4231 Infosec Management

IFS4205 Capstone

IFS4101 Legal aspect

IFS4102 Forensic

IFS4103 Pentesting

CS4238 Lab-based

CS4239 Software Security

CS4257 Privacy

CS4236 Crypto

IS4302 Blockchain

IS4204 IT Govern

IS4234 Audit

IS4233 Legal IT

CS5321 Network Security

CS5322 Database Security

CS5231 Sys Security

CS5331 Web

CS6231 sys sec

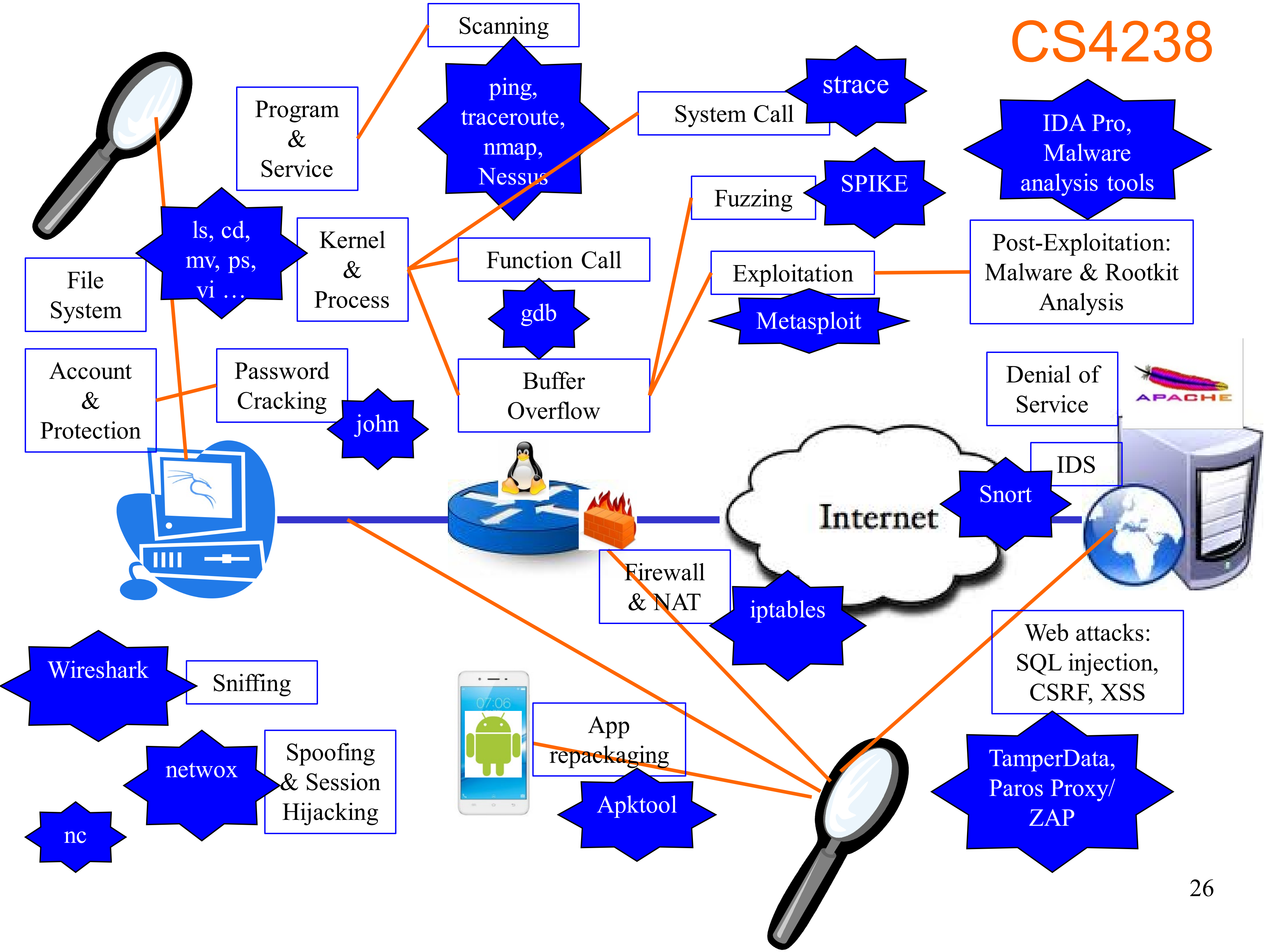
CS6230 info sec

CS4xxx IoT Security

IFS4xxx Malware analysis?

IFS3xxx Competitive CTF?

CS4238



Scanning

ping, traceroute, nmap, Nessus

Program & Service

System Call

strace

IDA Pro, Malware analysis tools

ls, cd, mv, ps, vi …

Kernel & Process

Fuzzing

SPIKE

File System

Function Call

gdb

Exploitation

Metasploit

Post-Exploitation: Malware & Rootkit Analysis

Account & Protection

Password Cracking

john

Buffer Overflow

Denial of Service

IDS

Snort

Internet

Firewall & NAT

iptables

Web attacks: SQL injection, CSRF, XSS

TamperData, Paros Proxy/ ZAP

Wireshark

Sniffing

App repackaging

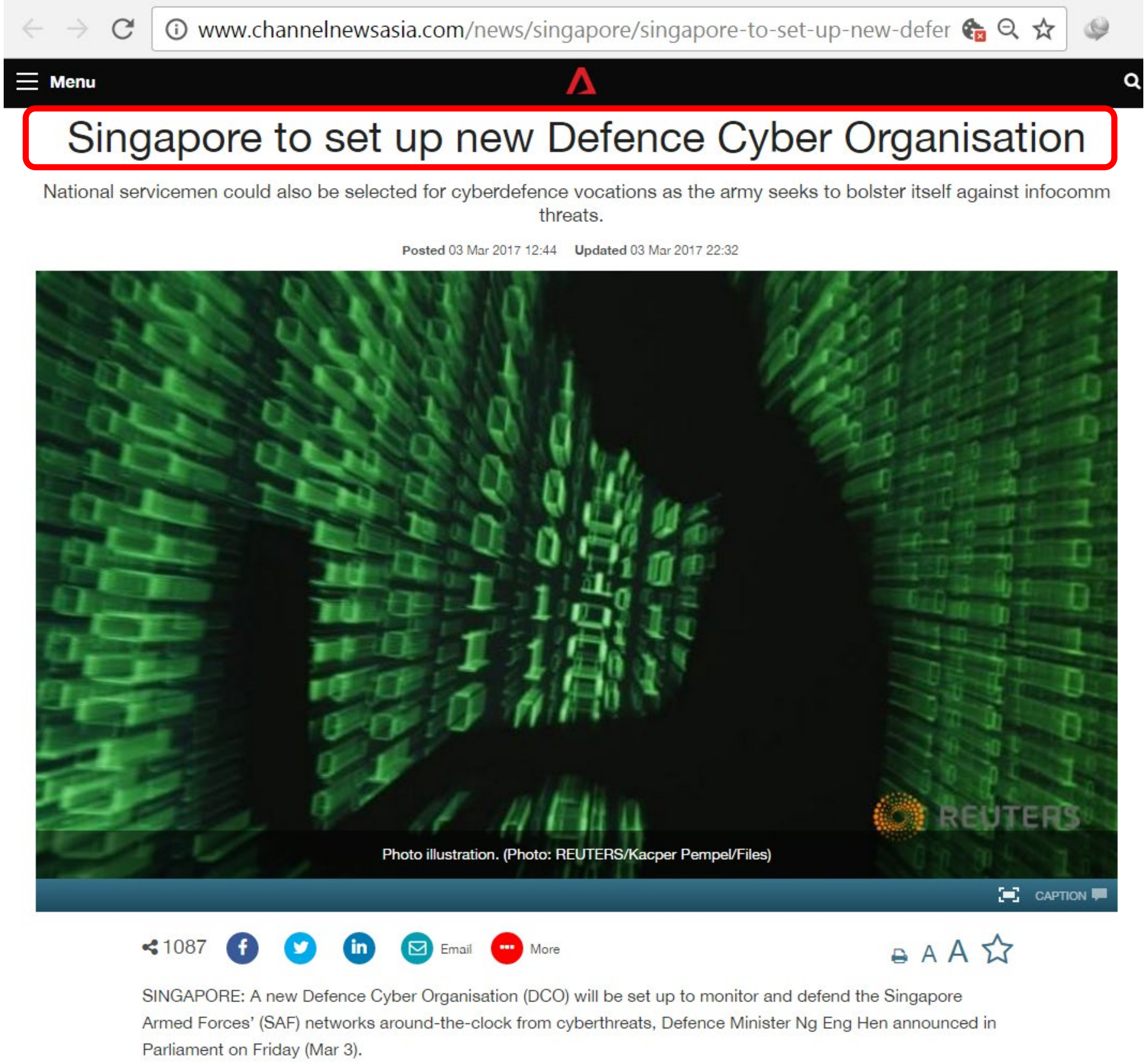
Apktool

netwox

Spoofing & Session Hijacking

nc

Recent News Items (2017)



www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defer
Menu
REUTERS
CAPTION
1087
Email
More
A A

Singapore to set up new Defence Cyber Organisation

National servicemen could also be selected for cyberdefence vocations as the army seeks to bolster itself against infocomm threats.

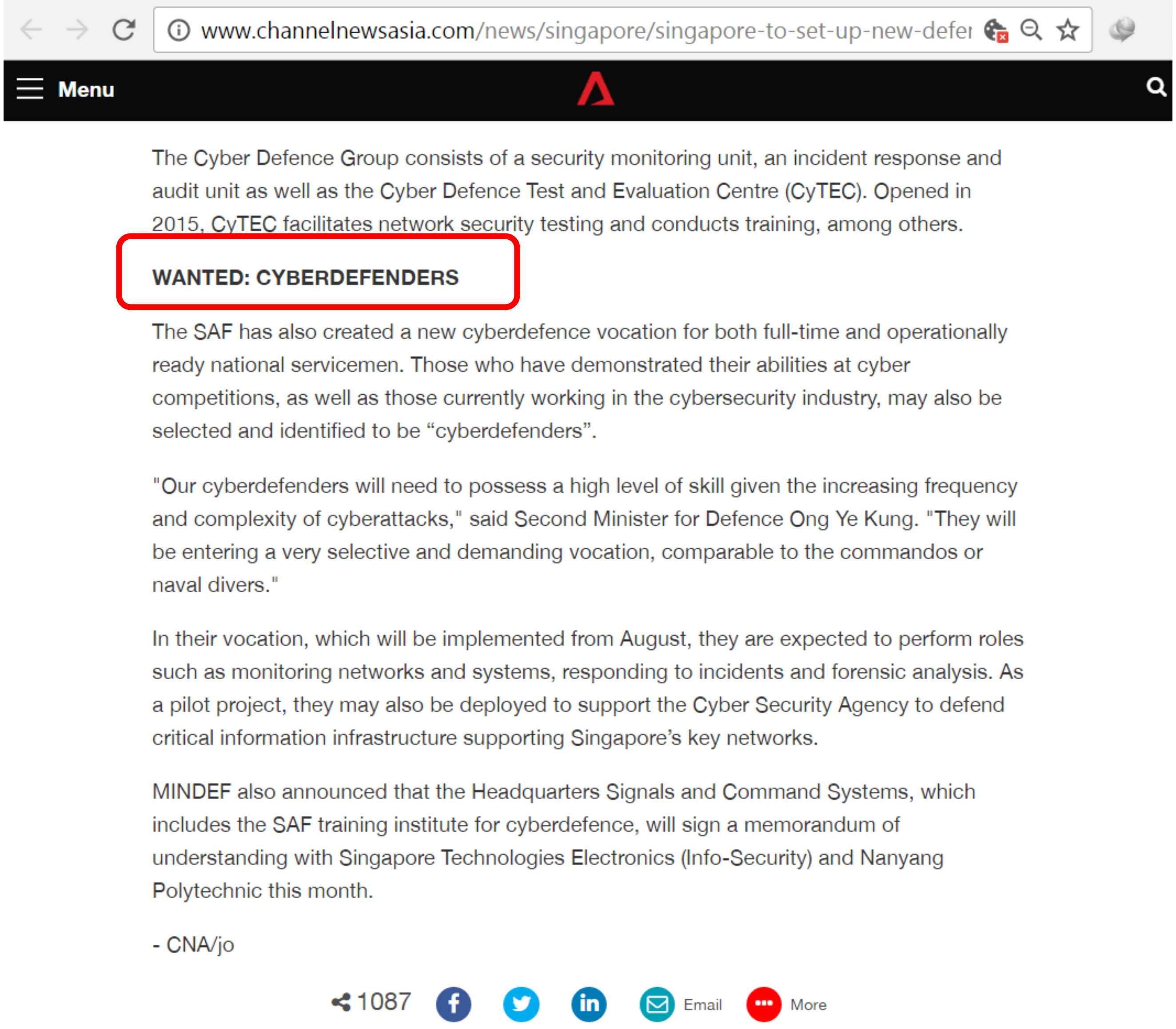
Posted 03 Mar 2017 12:44 **Updated** 03 Mar 2017 22:32

Photo illustration. (Photo: REUTERS/Kacper Pempel/Files)

SINGAPORE: A new Defence Cyber Organisation (DCO) will be set up to monitor and defend the Singapore Armed Forces' (SAF) networks around-the-clock from cyberthreats, Defence Minister Ng Eng Hen announced in Parliament on Friday (Mar 3).

Channel News Asia, Mar 3, 2017

Recent News Items (2017)


www.channelnewsasia.com/news/singapore/singapore-to-set-up-new-defer
Menu

The Cyber Defence Group consists of a security monitoring unit, an incident response and audit unit as well as the Cyber Defence Test and Evaluation Centre (CyTEC). Opened in 2015, CyTEC facilitates network security testing and conducts training, among others.

WANTED: CYBERDEFENDERS

The SAF has also created a new cyberdefence vocation for both full-time and operationally ready national servicemen. Those who have demonstrated their abilities at cyber competitions, as well as those currently working in the cybersecurity industry, may also be selected and identified to be "cyberdefenders".

"Our cyberdefenders will need to possess a high level of skill given the increasing frequency and complexity of cyberattacks," said Second Minister for Defence Ong Ye Kung. "They will be entering a very selective and demanding vocation, comparable to the commandos or naval divers."

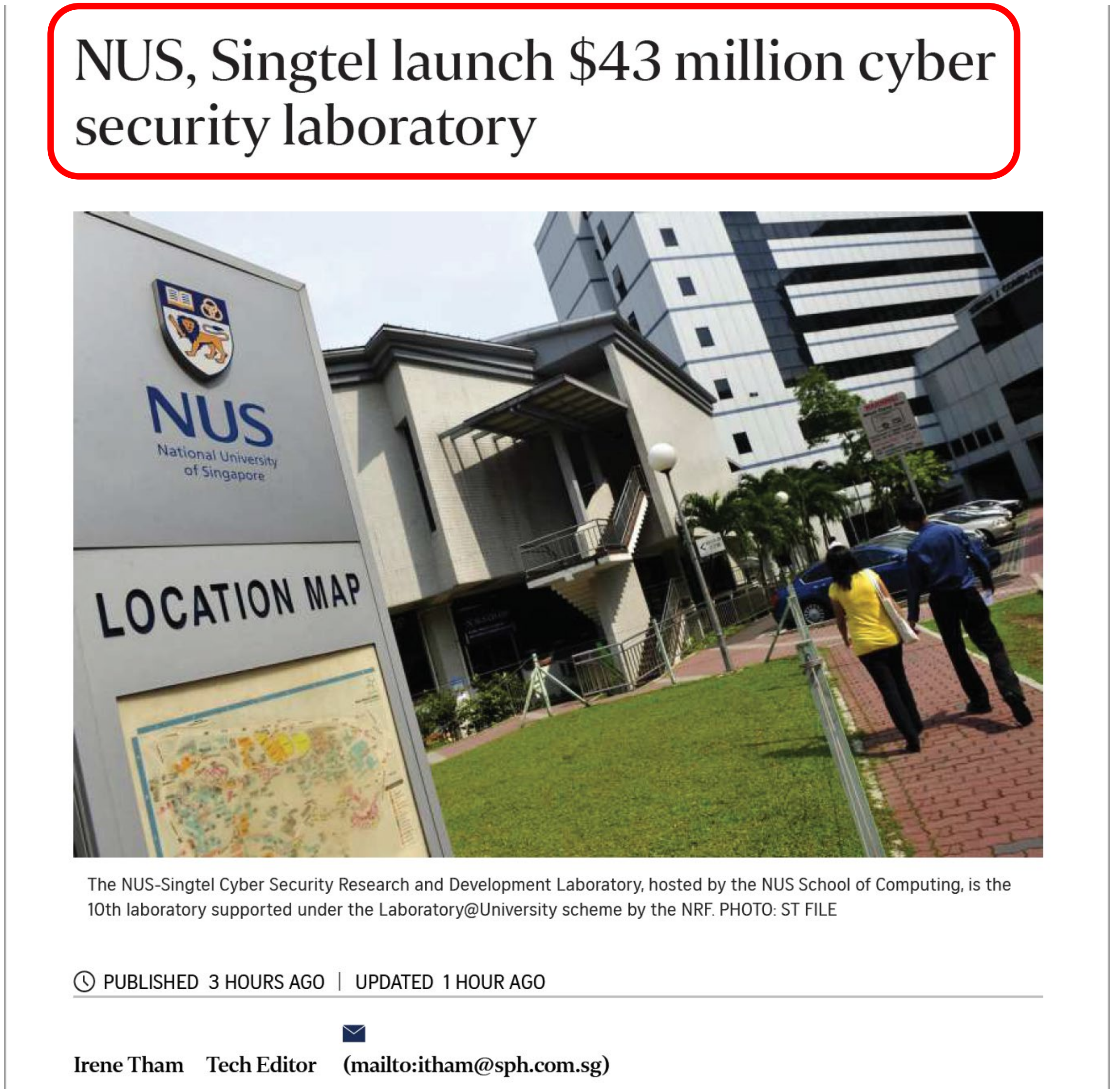
In their vocation, which will be implemented from August, they are expected to perform roles such as monitoring networks and systems, responding to incidents and forensic analysis. As a pilot project, they may also be deployed to support the Cyber Security Agency to defend critical information infrastructure supporting Singapore's key networks.

MINDEF also announced that the Headquarters Signals and Command Systems, which includes the SAF training institute for cyberdefence, will sign a memorandum of understanding with Singapore Technologies Electronics (Info-Security) and Nanyang Polytechnic this month.

- CNA/jo

Channel
News Asia,
Mar 3, 2017

Recent News Items (Oct 2016)



NUS, Singtel launch $43 million cyber security laboratory

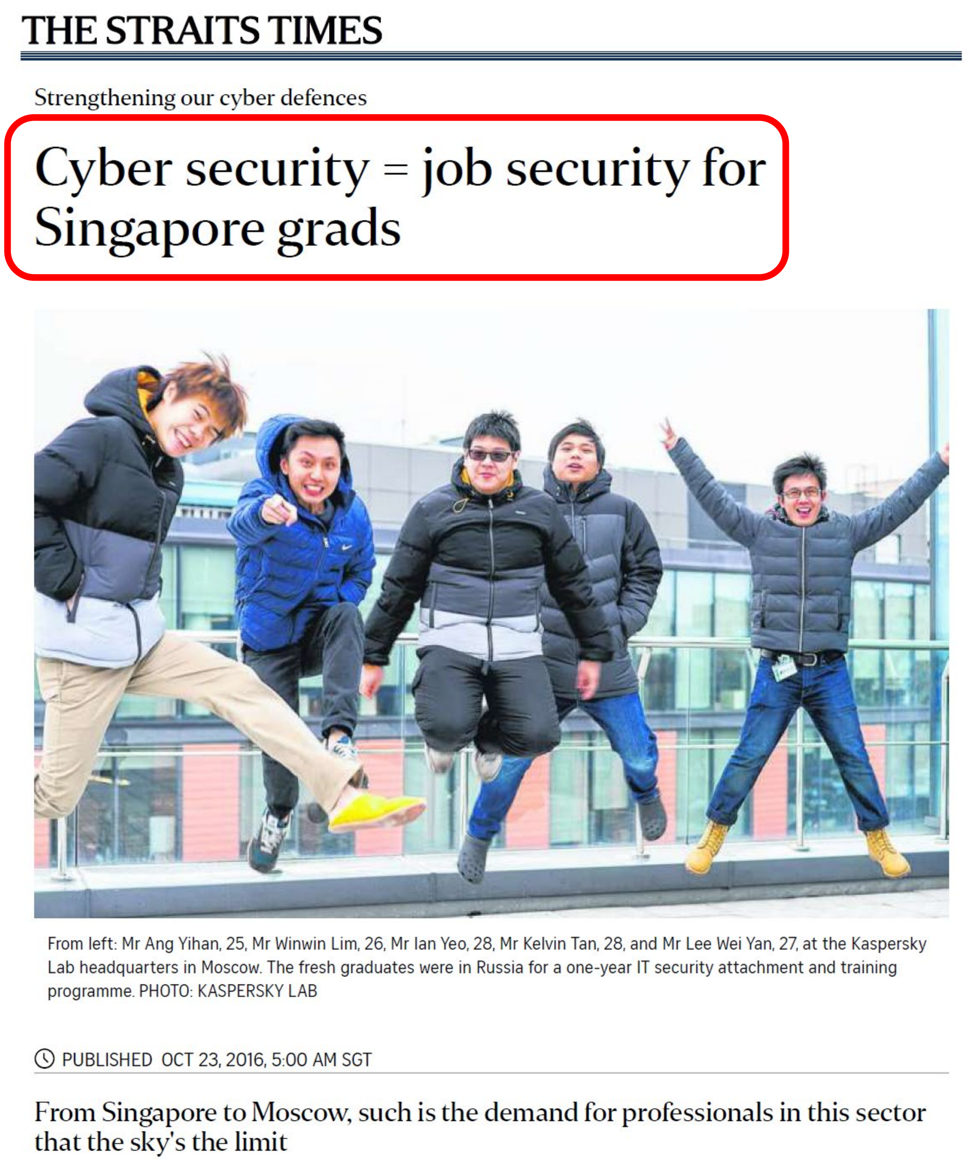
The NUS-Singtel Cyber Security Research and Development Laboratory, hosted by the NUS School of Computing, is the 10th laboratory supported under the Laboratory@University scheme by the NRF. PHOTO: ST FILE

PUBLISHED 3 HOURS AGO | UPDATED 1 HOUR AGO

Irene Tham Tech Editor (mailto:itham@sph.com.sg)

The Straits Times,
Oct 24, 2016

Recent News Items (Oct 2016)



THE STRAITS TIMES

Strengthening our cyber defences

Cyber security = job security for Singapore grads

From left: Mr Ang Yihan, 25, Mr Winwin Lim, 26, Mr Ian Yeo, 28, Mr Kelvin Tan, 28, and Mr Lee Wei Yan, 27, at the Kaspersky Lab headquarters in Moscow. The fresh graduates were in Russia for a one-year IT security attachment and training programme. PHOTO: KASPERSKY LAB

PUBLISHED OCT 23, 2016, 5:00 AM SGT

From Singapore to Moscow, such is the demand for professionals in this sector that the sky's the limit

The Straits Times, Oct 23, 2016

The Rest of the Semester:
Final Exam

Examination Matters

From SoC UG Office

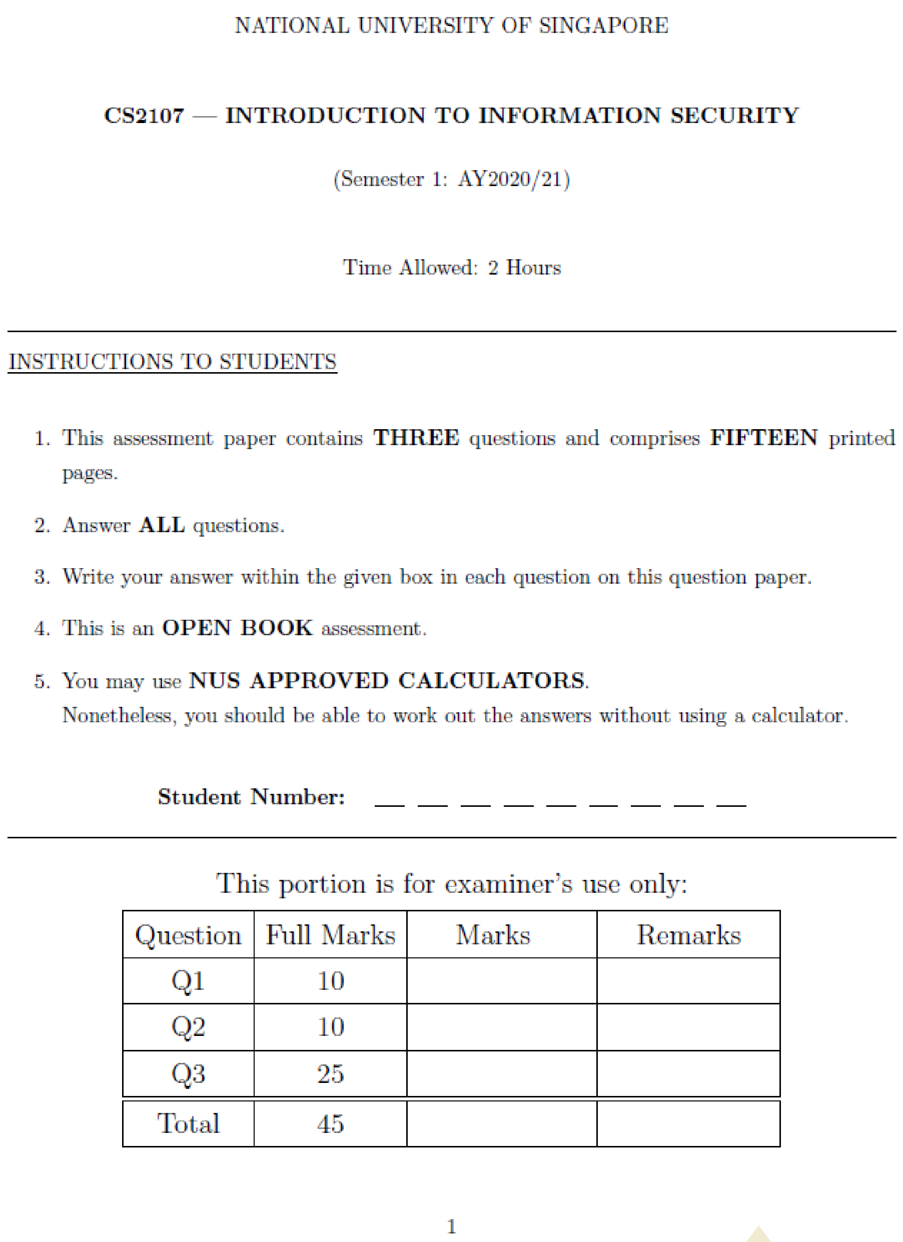
1. SoC has prepared **E-exam SOPs** for students, please refer to the guide: https://mysoc.nus.edu.sg/academic/e-exam-sop-for-students/

   Please ensure that you read thru and set up what you need before the exam date.

2. You should sit for the exam in insolation in a quiet environment with all the required hardware and software. If there's any extenuating circumstances that require you to **attempt your exams in campus**, please email your request to socexams@comp.nus.edu.sg by **09 November 2020, Monday** latest.

Final Exam

- Open book, **2** hours, NUS approved calculators, total: **45** marks
- **Thursday 26 Nov, 09:00-11:00 morning** (*please double-check time again!*)
- **Format**:
  - Q1: Security Terminology (10 marks)
  - Q2: MCQs (10 marks)
  - Q3: Structured-based questions (25 marks)
- **Covered materials**: **all lectures and tutorials**, which also include:
  - Cryptography
  - Authentication & authentication protocol
  - Network security
  - Firewall rules
  - Access control
  - Secure programming
  - Web security



NATIONAL UNIVERSITY OF SINGAPORE

CS2107 — INTRODUCTION TO INFORMATION SECURITY

(Semester 1: AY2020/21)

Time Allowed: 2 Hours

INSTRUCTIONS TO STUDENTS

1. This assessment paper contains **THREE** questions and comprises **FIFTEEN** printed pages.
2. Answer **ALL** questions.
3. Write your answer within the given box in each question on this question paper.
4. This is an **OPEN BOOK** assessment.
5. You may use **NUS APPROVED CALCULATORS**.
   Nonetheless, you should be able to work out the answers without using a calculator.

Student Number: __ __ __ __ __ __ __ __ __

This portion is for examiner's use only:

Question	Full Marks	Marks	Remarks
Q1	10		
Q2	10		
Q3	25		
Total	45		

1

Thanks!
(And Please Congratulate Yourself Too!)

Extra:

Video on Careers in Cybersecurity - Advice