Cyber Scurity

Prodi Magister PJJ
Informatika

TATA TERTIB PERKULIAHAN

- Perkuliahan dimulai sesuai jadwal yang ditentukan;
- Kuliah ditiadakan jika dosen terlambat masuk **60 menit** dari jadwal yang telah ditentukan dan dicarikan waktu pengganti dengan kesepakatan antara dosen dan mahasiswa.

untuk dosen:

- Berpakaian rapi dan tidak merokok di dalam kelas;
- Tidak diperbolehkan mengucapkan kata-kata yang menyinggung etnisitas dan agama;
- Harus memberitahukan tempat-tempat mencari bahan atau referensi matakuliah.

untuk mahasiswa:

- Mahasiswa yang terlambat lebih **30 menit** tidak diperkenankan mengikuti perkuliahan;
- Terlambat 10 menit berdiri
- **Jika Tidak Bisa Mengikuti Perkuliahan Dapat Menghubungi melalui WA, Email, Surat Ijin**
- Berpakaian rapi (sepatu serta berkemeja atau kaus berkerah) dan sopan (tidak ketat dan tidak pendek);
- Pertanyaan yang berkenaan topik pembelajaran tidak terbatas hanya di dalam kelas;
- Tidak diperbolehkan merokok;

Materi

1. Ruang lingkup keamanan cyber menurut framework Cyber Security Body of Knowledge (CyBoK)
2. Serangan infrastruktur jaringan
3. Serangan aplikasi desktop dan web
4. Social engineering
5. Solusi pengamanan data dan sistem modern
6. Regulasi dan kebijakan cyber law di Indonesia
7. Implementasi kebijakan keamanan TI
8. Penetration testing
9. Digital Forensic

Ruang lingkup keamanan cyber menurut *framework Cyber Security Body of Knowledge (CyBoK)*

Minggu 1

Outline Pembelajaran

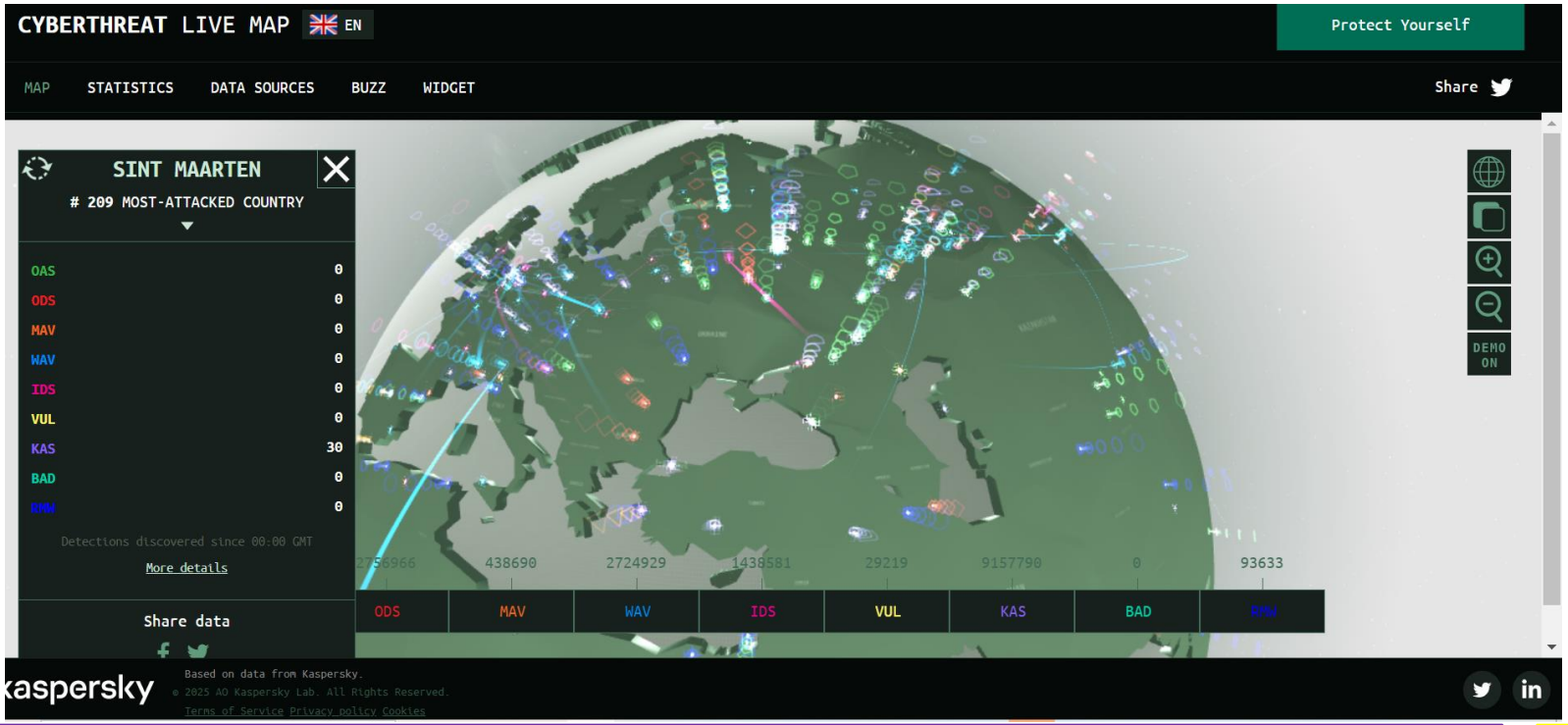
- Perkenalan CyBOK
- *Human, Organisational, & Regulatory Aspects*
- *Attacks & Defences*
- *Software & Platform Security*
- *Systems Security*
- *Infrastructure Security*

Cyber Threat Map

- https://threatmap.checkpoint.com/

Kaspersky

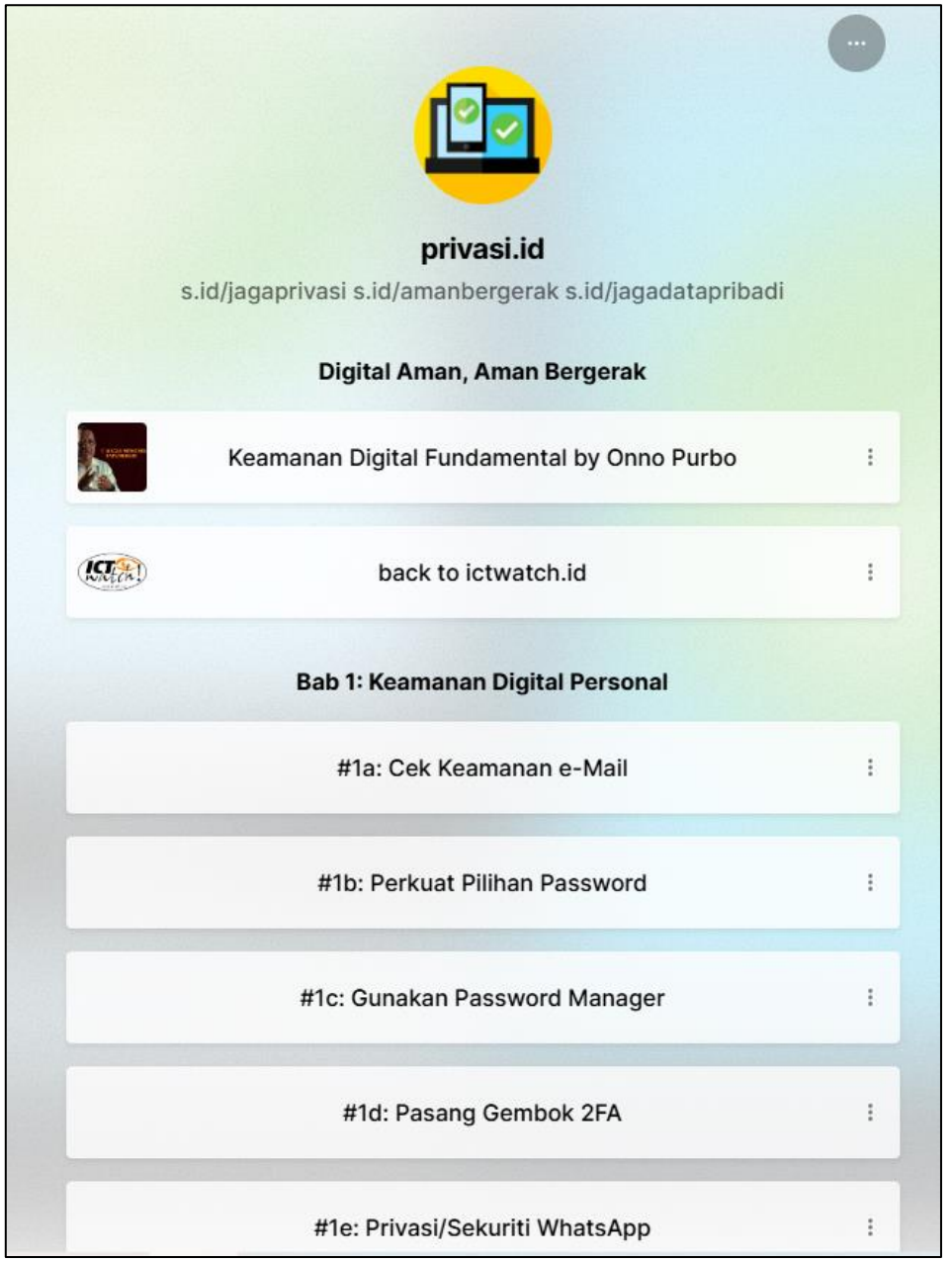
- https://cybermap.kaspersky.com/
- https://threatmap.bitdefender.com/
- https://fortiguard.fortinet.com/threat-map



What is cyber security?

- Cyber security : **perlindungan** terhadap system dan informasi (hardware, software dan infrastruktur), data yang ada di dalamnya, dan layanan yang disediakan, dari penyalahgunaan akses yang tidak sah [UK National Cyber Security Strategy]

- https://linktr.ee/amanbergerak



Why need cyber security?

- Sistem bisa gagal karena berbagai alasan
- Sistem yang handal, dapat mengurangi kegagalan yang tidak disengaja
- **Usabilitas sistem**, dapat mengurangi kesalahan pengoperasian oleh pengguna
- **Keamanan,** mengurangi kegagalan yang disengaja yang dibuat oleh pihak-pihak yang ‘cerdas’

What drives attackers?

- Permusuhan, politik, teror, balas dendam, dll.
- Uang
- Ketenaran, kedengkian, keingintahuan
- Peluang, ada kesempatan
- “The lulz“ lol lucu hiburan dll

Primary Motivation? Money!

Motivasi Utama? Uang!

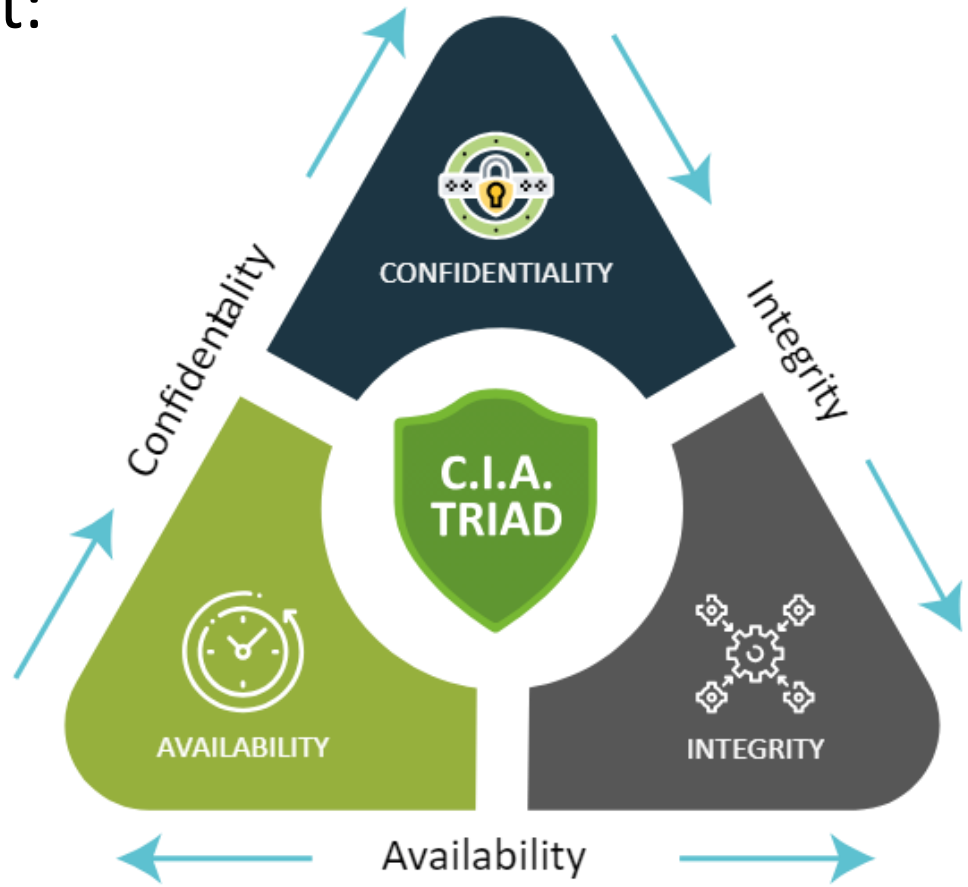
- Denial of service, extortion
- Ransomware
- Ad injection
- Pencurian uang (banking fraud, Bitcoin)
- Pencurian credit card (mall, restaurant, cafe)

Security Threats

- Anda dikatakan mengalami ancaman terhadap serangan jika mengalami salah satu pelanggaran berikut:

CIA TRIAD

- *Confidentiality (Kerahasiaan)*
- *Integrity (Integritas)*
- *Availability (Ketersediaan)*



PETA OKUPASI NASIONAL DALAM KERANGKA KUALIFIKASI NASIONAL INDONESIA PADA AREA FUNGSI KEAMANAN SIBER

KKNI		STRATA JABATAN	
LEVEL	KATEGORI	PEMERINTAH	INDUSTRI
9	AHLI	AHLI UTAMA	DIREKTUR UTAMA, PRESIDEN DIREKTUR, CXO, MANAGING DIRECTOR
8	AHLI	AHLI SENIOR	DIREKTUR; VICE PRESIDENT; GENERAL MANAGER; SCIENTIST
7	AHLI	AHLI PERDANA	MANAGER; EXPERT
6	TEKNISI/ANALIS	TEKNISI/ ANALIS MADYA	ASISTEN MANAGER; DEPUTY MANAGER; ADVISOR
5	TEKNISI/ANALIS	TEKNISI/ ANALIS MUDA	SUPERVISOR; PENYELIA

BEFORE			DURING		AFTER	
100804,07	CHIEF OF INFORMATION SECURITY OFFICER (CISO)					
100805,04	CYBER RISK SPECIALIST				100808,01	CYBER INCIDENT INVESTIGATION MANAGER
100808,04	SECURITY ARCHITECT				100809,01	CYBER FORENSIC SPECIALIST
100807,04	CRYPTOGRAPHIC SPECIALIST					
100723,04	CRYPTOGRAPHIC ENGINEER	100704/ 100704.07	MANAJER CYBERSECURITY/CYBERSECURITY MANAGER			
100724,04	ICT SECURITY PRODUCT LEAD EVALUATOR	100701/ 100701.04	MANAJER KEAMANAN JARINGAN/ NETWORK SECURITY MANAGER		100728,07	DIGITAL FORENSIC ANALYST
		100720,04	CYBERSECURITY AWARENESS LEAD OFFICER			
		100721,07	INCIDENT RESPONSE TEAM MANAGER			
		100722,04	AUDITOR KEAMANAN INFORMASI			
		100725,08	THREAT HUNTER			
		100726,04	PENETRATION TESTER			
		100727,07	CYBERSECURITY GOVERNANCE OFFICER			
100808,04	ICT SECURITY PRODUCT EVALUATOR	100805,04	CYBERSECURITY AWARENESS OFFICER	100801/ 100801.03	CYBERSECURTY ANALYST/ CYBERSECURITY INCIDENT ANALYST	
100810,04	CRYPTOGRAPHIC ANALYST	100806,04	VULNERABILITY ASSESSMENT ANALYST		100612	DIGITAL EVIDENCE FIRST RESPONDER
100811,04	CRYPTOGRAPHIC MODULE ANALYST	100807,04	NETWORK SECURITY ADMINISTRATOR			
		100808,04	CYBERSECURITY ADMINISTRATOR			
		100508,08	CYBERSECURITY OPERATOR			
		100501/ 100501.04	JUNIOR CYBER SECURITY			
		100508,04	TEKNISI PERANGKAT KERAS KRIPTOGRAFI			
		100510,04	CRYPTOGRAPHIC ADMINISTRATOR			

UNIT KOMPETENSI TELAH DILENGKAPI
SEBAGIAN UNIT KOMPETENSI TELAH DILENGKAPI
UNIT KOMPETENSI BELUM DILENGKAPI

LAUNCHING PETA OKUPASI NASIONAL KEAMANAN SIBER

JAKARTA, 12 DESEMBER 2019

Ditandatangani Secara Elektronik Oleh
Kepala Subdirektorat
Fasilitasi Standardisasi dan Pengembangan SDM

Asri Setyowati, S.Si.
NIP. 19700627 199110 2 001

What is CyBOK?

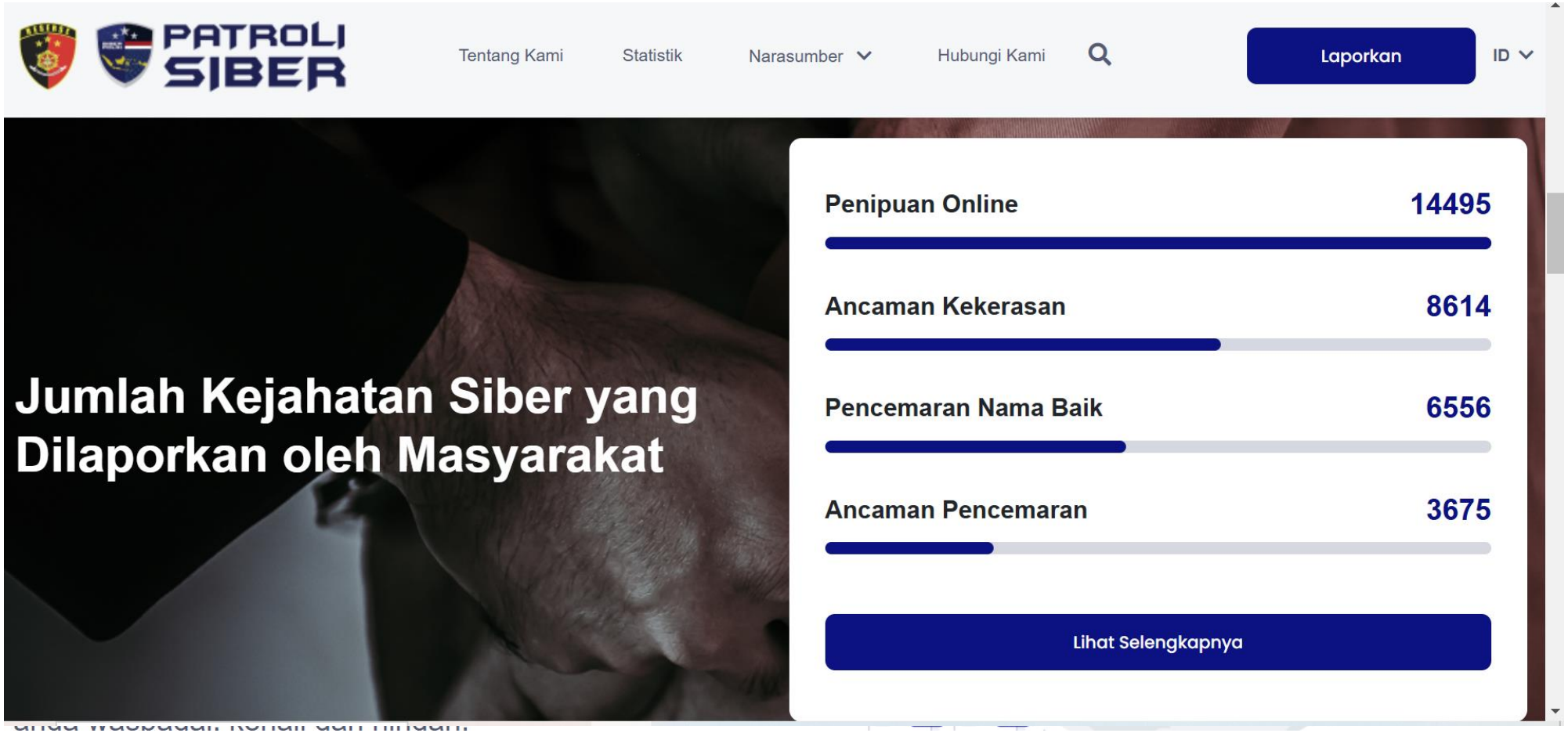
1. **Body of Knowledge**: Rangkaian konsep, istilah, dan aktivitas, yang secara lengkap dan luas (komprehensif) membentuk suatu ranah (domain) professional, mengikuti pendefinisian formal dan sistematik yang ditentukan oleh komunitas pendidikan mapupun asosiasi professional yang relevan.
2. CyBOK: ***Cyber Security Body of Knowledge***
3. CyBOK merupakan Body of Knowledge khusus di bidang keamanan siber dalam mendukung pendidikan dan pelatihan professional.
4. CyBOK disusun berdasarkan referensi yang sudah ada sebelumnya, seperti: textbook, hasil penelitian ilmiah, white paper, standard, dll.
5. Proyek penyusunan dan pengembangan CyBOK disponsori oleh National *Cyber Security Programme*, yang dipimpin oleh University of Bristol, UK, dimulai sejak 1 February 2017.
6. Lebih jauh mengenai CyBOK: https://www.cybok.org

Why CyBOK?

- CyBOK merupakan salah satu pendekatan yang dapat digunakan dalam pengenalan keamanan siber.
- CyBOK bukan merupakan satu-satunya referensi yang ada dan menjadi satusatunya acuan baku (standard) dalam keamanan siber.
- Perkuliahan ini menggunakan CyBOK sebagai salah satu referensi dalam pengenalan keamanan siber, dengan pertimbangan:
- CyBOK merupakan hasil kontribusi praktisi dan komunitas dari berbagai belahan dunia untuk membentuk pondasi bersama dalam keilmuan keamanan siber.
- Materi-materi CyBOK tersedia di website resmi CyBOK secara rinci.
- Siapapun dapat menggunakan CyBOK tanpa dipungut bayaran, baiku untuk tujuan komersial maupun non-komersial. CyBOK lisensi Open Government License (http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/)

Patroli Siber

- https://patrolisiber.id/



Beberapa definisi Keamanan yang dirangkum CyBOK

- Keamanan Siber
- Perlindungan sistem informasi (hardware, software, dan infrastruktur terkait),berikut juga perlindungan terhadap:

1. data yang terdapat didalamnya
2. layanan yang disediakannya

- dari akses yang tidak berwenang (unauthorized access), kerusakan, maupun penyalahgunaan.
- Kerusakan ini juga meliputi segala ketidaksengajaan dan kelalaian dalam pelaksanaan prosedur keamanan.

Keamanan Informasi

Menjaga:

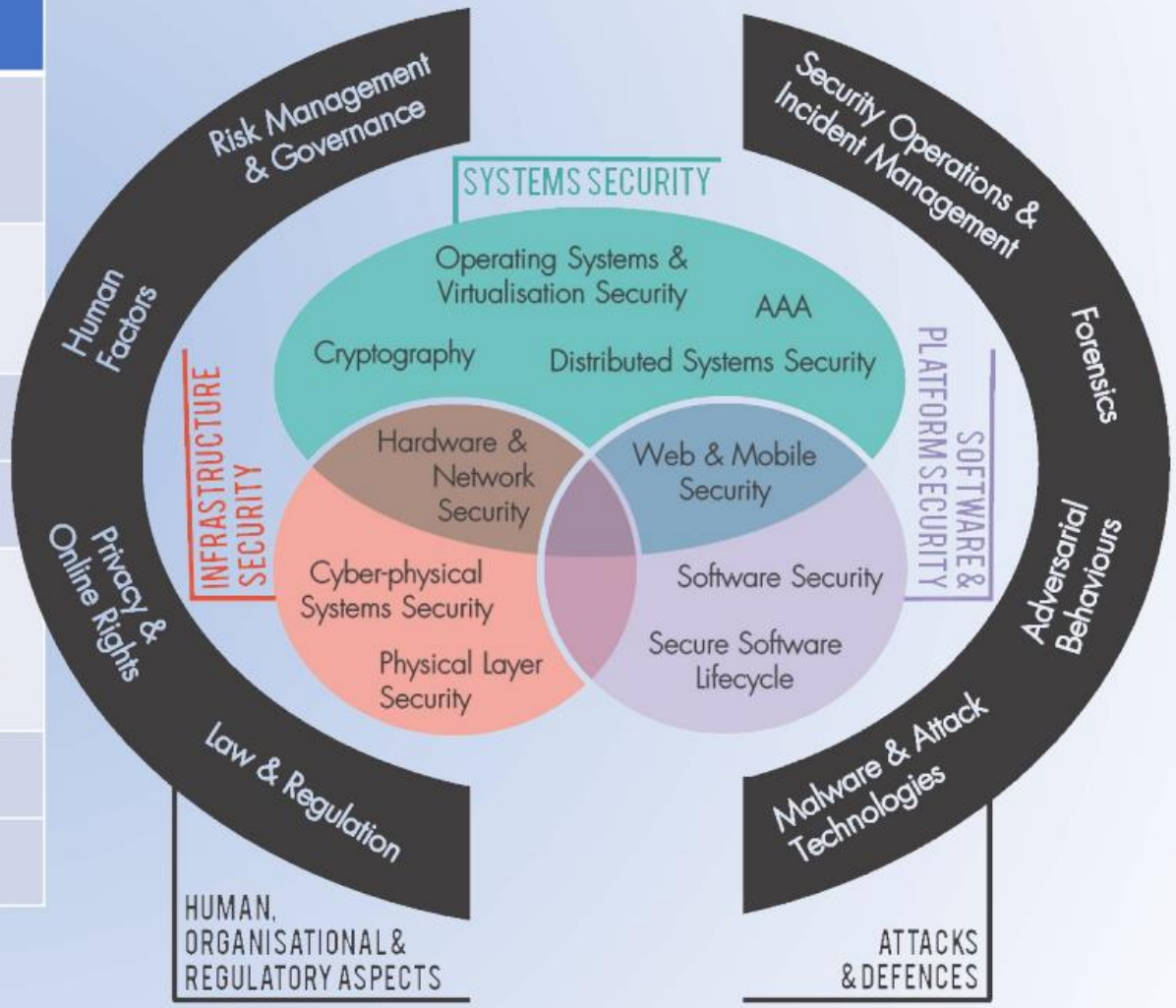
- *confidentiality,*
- *integrity, dan*
- *availability pada suatu informasi.*

Sebagai tambahan, juga termasuk menjaga:

- *authenticity,*
- *accountability,*
- *non-repudiation*, dan
- *reliability.* (Definisi pada ISO 27000)

Bidang Keilmuan (Knowledge Area) pada CyBOK

Category	Knowledge Area (KA)
1. Human, Organisational, & Regulatory Aspects	1. Risk Management & Governance 2. Law & Regulations 3. Human Factors 4. Privacy & Online Rights
2. Attacks & Defences	5. Malware & Attack Technologies 6. Adversarial Behaviours 7. Security Operations & Incident Management 8. Forensics
3. Software & Platform Security	9. Software Security 10. Secure Software Lifecycle
	11. Web & Mobile Security
4. Systems Security	12. Cryptography 13. Operating Systems & Virtualisation Security 14. Distributed Systems Security 15. Authentication, Authorization, & Accountability (AAA)
	16. Network Security 17. Hardware Security
5. Infrastructure Security	18. Cyber-physical Systems Security 19. Physical Layer & Telecomms Security



Human, Organisational, and Regulatory Aspects

Risk Management & Governance	Manajemen keamanan sistem dan pengendalian keamanan di dalam suatu organisasi, penggunaan acuan-acuan baku (*standards*) beserta kaidah-kaidah lazim (*best practice*), termasuk juga pendekatan-pendekatan dalam manajemen resiko keamanan siber beserta mitigasinya.
Law & Regulation	Pemenuhan kewajiban dalam mematuhi undang-undang maupun peraturan nasional dan internasional, etika keamanan, perlindungan data, dan kewaspadaan terhadap perang siber.
Human Factors	Pengaruh perilaku sosial manusia dalam membentuk kesadaran dan kebiasaan mematuhi penerapan keamanan siber, dan sebaliknya pengaruh penerapan keamanan siber terhadap perilaku manusia tersebut.
Privacy & Online Rights	Teknik dalam mengamankan data pribadi , baik dalam transmisi/transfer/komunikasi, pemrosesan dengan aplikasi, maupun penyimpanan (pada basis data ataupun *file system*). Termasuk juga pengamanan privasi dalam layanan digital, seperti pemilu online, sistem pembayaran online, identitas online.

Attacks & Defences

Malware & Attacks Technologies	Rincian teknis mengenai penyebaran dan eksploitasi melalui sistem/*software*/aplikasi yang berbahaya (*malware = malicious software*), bagaimana pendekatan-pendekatan dalam menganalisa dan mendeteksinya.
Adversarial Behaviours	Motif, perilaku, dan metodologi yang digunakan oleh penyerang. Meliputi juga rantai penyebaran *malware*, jalur penyerangan (*attack vectors*), dan segala transfer uang yang terjadi terkait penyerangan.
Security Operations & Incident Management	Pengkonfigurasian, pengoperasian, dan *maintenance* terhadap keamanan sistem. Meliputi juga kemampuan dalam mendeteksi serta memberikan *responses/actions* yang tepat terhadap insiden keamanan yang terjadi, dan penggunaan *threat intelligence* dalam mempersiapkan, mencegah, dan mengidentifikasi ancaman terhadap keamanan siber.
Forensics	Pengumpulan, analisa, dan pelaporan bukti-bukti digital terhadap insiden keamanan siber maupun kejadian kriminal.

System Security

Cryptography	Kaidah-kaidah dasar kriptografi yang umum digunakan saat ini dalam mengamankan sistem, berikut juga analisis terhadap algoritma yang digunakannya, dan protokol-protokol yang menggunakannya.
Operating Systems & Virtualisation Security	Mekanisme perlindungan sistem operasi, penerapan abstraksi keamanan pada perangkat keras, penanganan keamanan pada penggunaan *sharing resources* seperti: isolasi pada sistem multi-user, keamanan pada virtualisasi, dan keamanan basis data yang dipakai Bersama.
Distributed Systems Security	Mekanisme keamanan pada sistem berskala besar yang tersebar dan saling berkoordinasi satu sama lainnya, meliputi pengamanan konsensus dalam sistem, komunikasi *peer-to-peer, cloud*, *multi-tenants data center*.
Authentication, Authorization, & Accountability (AAA)	Segala aspek terkait teknologi pengelolaan identitas dan autentikasi digital. Termasuk juga arsitektur dan perangkat-perangkat (*tools*) pendukung pemberian wewenang (*authorization*) dan akuntabilitas, baik dalam sistem terisolasi maupun dalam sistem terdistribusi.
Formal Methods for Security	Formal specification, modelling and reasoning about the security of systems, software and protocols, covering the fundamental approaches, techniques and tool support.

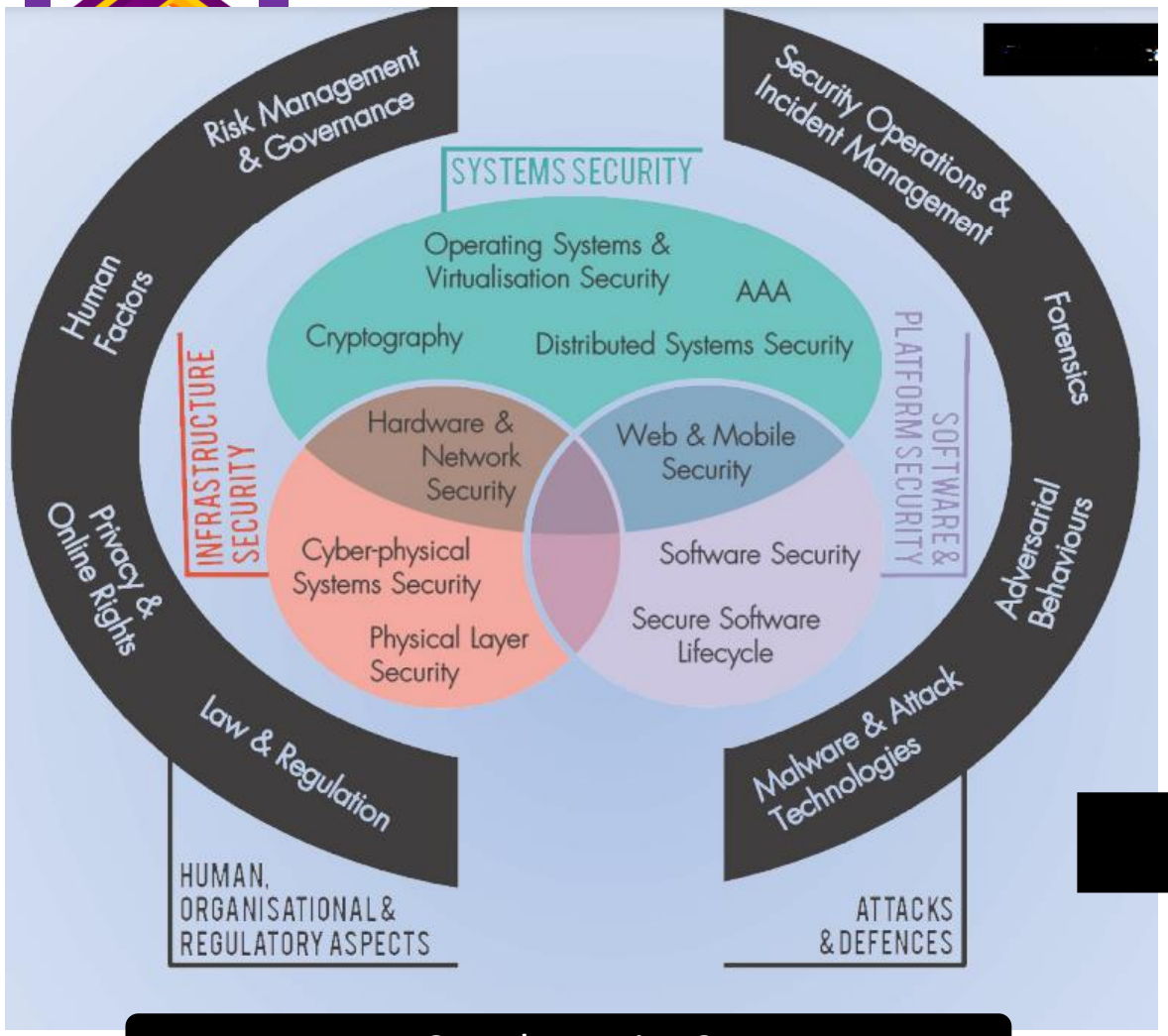
Software & Platform Security

Software Security	Mengenali permasalahan umum dalam pemrograman yang dapat mengakibatkan masalah-masalah keamanan dan bagaimana teknik untuk mencegahnya, baik melalui penerapan kaidah pemrograman yang baik (*coding practice*), memperbaiki perancangan (*design*), ataupun penggunaan alat-alat bantu pemrograman (*tools*). Termasuk juga bagaimana untuk mendeteksi masalah-masalah keamanan pada *software* yang telah ada.
Secure Software Lifecycle	Penerapan teknik rekayasa perangkat lunak (*software*) pada keseluruhan proses perekayasaan sehingga menghasilkan perangkat lunak yang memiliki keamanan yang tangguh sejak dari awal.
Web & Mobile Security	Penangangan permasalahan keamanan pada aplikasi dan layanan berbasis web yang digunakan pada berbagai perangkat yang berbeda-beda.

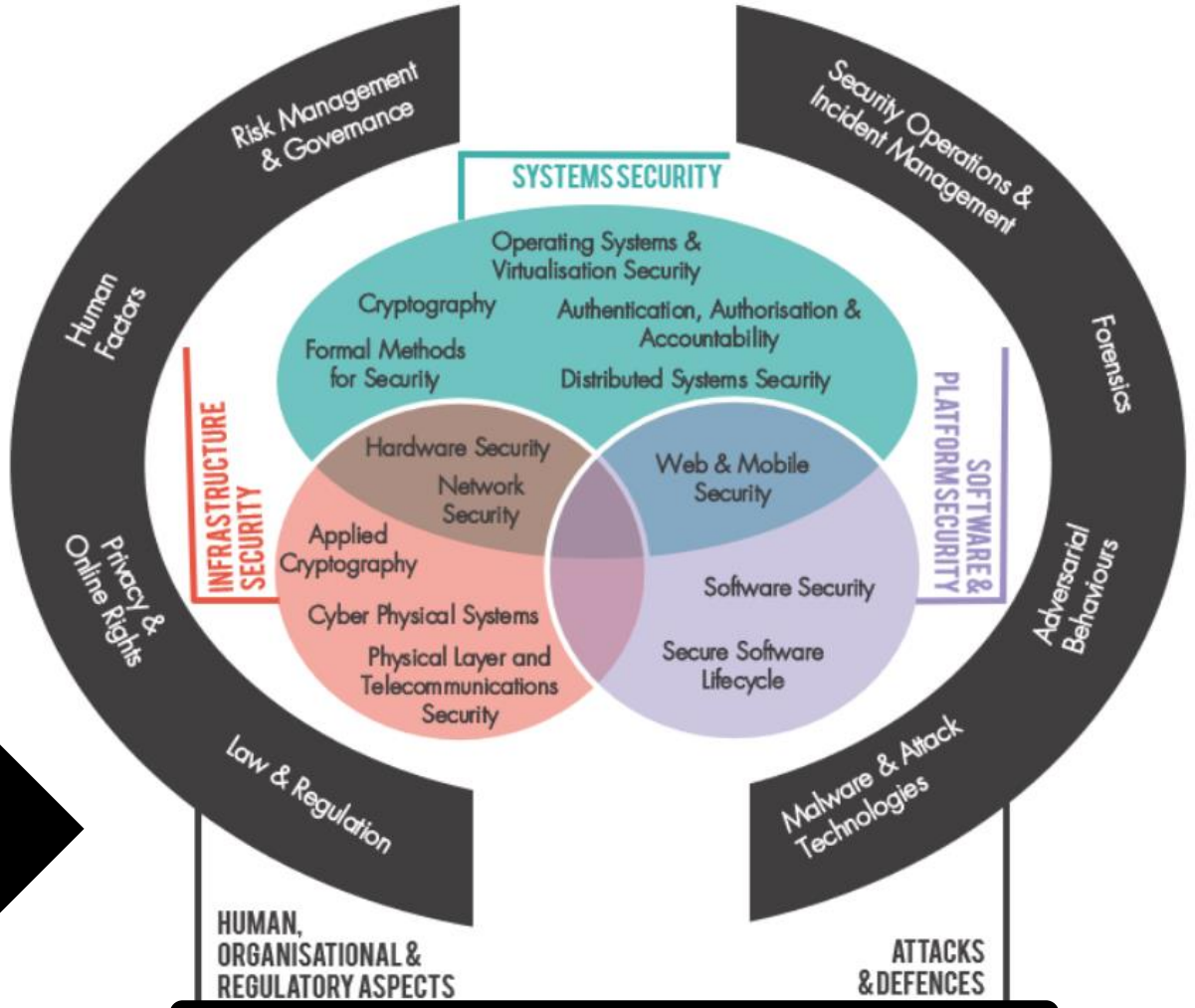
Infrastructure Security

Network Security	Aspek keamanan pada protokol jaringan dan komunikasi, meliputi pengamanan pada *routing*, elemen-elemen jaringan, dan protokol kriptografi tertentu yang dipergunakan untuk mengamankan jaringan.
Hardware Security	Pengamanan pada perancangan, pengimplementasian, dan *deployment* perangkat keras untuk keperluan khusus maupun keperluan umum, termasuk juga pengamanan pada teknologi komputasi terpercaya, dan penanganan randomisasi.
Cyber-physical Systems Security	Tantangan pengamanan *cyber-physical system*, seperti *Internet of Things,* sistem kontrol pada industri, dan pengamanan infrastruktur berskala besar.
Physical Layer & Telecomms Security	Pengamanan pada *physical layer*, meliputi radio frekuensi, teknik pengkodean dan transmisi, radiasi yang tidak diinginkan, dan interferensi.

Applied Cryptography	The application of cryptographic algorithms, schemes, and protocols, including issues around implementation, key management, and their use within protocols and systems.



CyBok Versi 1.0



CyBok Versi 1.1

Bidang keilmuan pada CyBOK merupakan rangkuman cakupan topik yang dipelajari pada keamanan siber.

Tugas I

- **Tugas I** : Membuat review salah satu Chapter dari Buku Cybersecurity Body of Knowledge (CyBOK)
- **Instruksi Tugas**:

1. Pilih Satu Chapter dari Buku Cybersecurity Body of Knowledge (CyBOK) - Link Buku

2. Buat laporan review chapter yang dipilih dengan format:
 - Maksimal 10 halaman
 - Laporan harus mencakup ringkasan inti dari chapter, analisis kritis, serta relevansi dengan perkembangan terbaru di bidang cybersecurity.
3. Presentasi: Buat presentasi PowerPoint berdasarkan chapter yang Anda pilih:
 - Maksimal 10 slide.
 - Presentasi harus berfokus pada poin-poin utama dari chapter yang dibahas dan visualisasi yang mendukung penjelasan.

Any Questions..?