



**UNIVERSITAS
NASIONAL**
PIONIR PERUBAHAN

Cyber Security

Dr. Irma Indrayani, M.Si

FISIP

Hubungan Internasional



Latar Belakang *Cyber Security*

► Globalisasi dan hadirnya internet

Hadirnya internet sebagai bentuk teknologi baru menyebabkan manusia tidak mampu terlepas dari arus komunikasi dan informasi. Internet telah menyebabkan terjadinya satu lompatan besar dalam kehidupan.

Terkait dengan internet terdapat sejumlah konsep yang berhubungan yaitu telematika, multimedia dan *cyber space*.

Cyber space didefinisikan sebagai media elektronik dan jaringan komputer di mana komunikasi terjadi secara online. Komunikasi yang terjadi dalam *cyber space* bisa melibatkan siapa saja, kapan saja, dan dari mana saja selama media komunikasi memungkinkan. Karena *cyber space* merupakan ruang virtual yang terbentuk dari hasil penyatuan antara manusia dan teknologi. Teknologi yang dimaksud ialah teknologi informasi dan komunikasi. Maka konsep keamanan *cyber* tidak lagi hanya menyentuh wilayah teknologi tapi telah menjadi ancaman terhadap keamanan nasional.

Salah satu dampak negatif yang muncul dalam *cyber space* adalah terjadinya *cyber crime*. Maraknya *cyber crime* memerlukan perhatian dan keseriusan dalam mengembangkan *cyber security* bagi sebuah negara



Cyber Security

- ▶ Joseph Nye dalam tulisannya yang berjudul Cyber Power, Cyber security dihadapkan kepada empat ancaman utama yaitu, spionase, kejahatan, perang cyber dan terorisme cyber. Kemungkinan ancaman ini di tentukan oleh tiga faktor yaitu kelemahan dalam desain internet, kelemahan dalam perangkat keras dan lunak serta langkah dalam penempatan sistem yang disebutnya “more critical” dalam dunia maya/virtual.

Cyber security = Security of cyberspace

ketersediaan, integritas dan kerahasiaan informasi sistem dan jaringan dalam menghadapi serangan, dan kegagalan dengan tujuan melindungi sistem operasi dan Aset

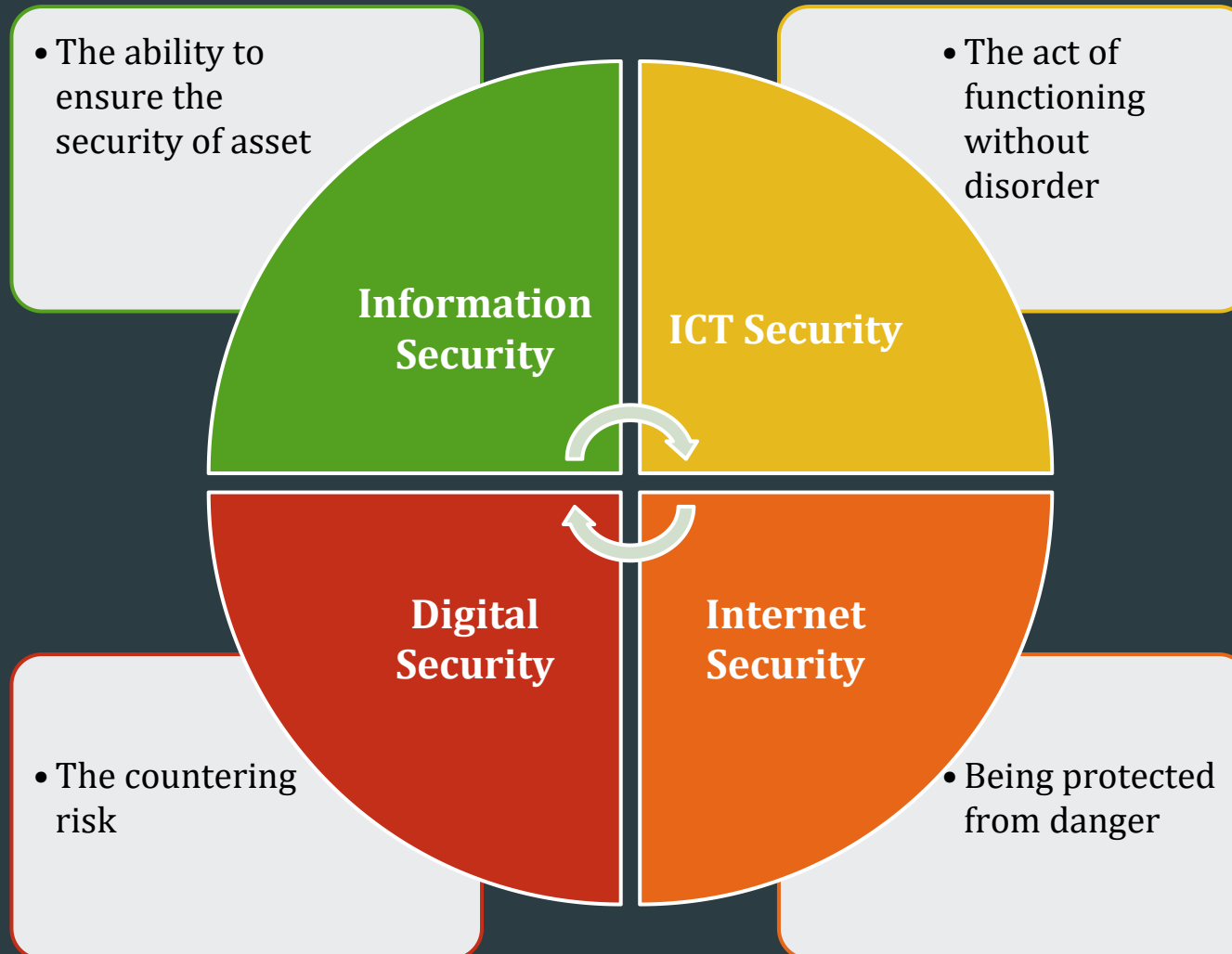
↓
**Information system
and network**



Definisi *Cyber Security*

- ▶ Cyber security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan cyber dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam cyber security termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.
- ▶ Cyber-security merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan cyber. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk di dalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.

Cyber Security





Cyber Security

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun cyber attack.

Cyber-security merupakan upaya untuk melindungi informasi dari adanya cyber attack, adapun elemen pokok cyber-security adalah:

1. Dokumen security policy merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
2. Information infrastructure merupakan media yang berperan dalam kelangsungan operasi informasi meliputi hardware dan software. Contohnya adalah router, switch, server, sistem operasi, database, dan website.



Cyber Security

3. Perimeter Defense merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya IDS, IPS, dan firewall.
4. Network Monitoring System merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan performance infrastruktur informasi.
5. System Information and Event Management merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
6. Network Security Assessment merupakan elemen cyber-security yang berperan sebagai mekanisme kontrol dan memberikan measurement level keamanan informasi.
7. Human resource dan security awareness berkaitan dengan sumber daya manusia dan awareness-nya pada keamanan informasi.



Cyber Security

Usaha untuk meningkatkan komitmen dunia dalam keamanan siber, dilakukan dengan pemeringkatan Global Cybersecurity Index (GCI) oleh Internasional Telecommunication Union (ITU) kepada 193 negara-negara anggotanya.

Global Cybersecurity Index (GCI) merupakan survey yang dilakukan oleh International Telecommunication Union (ITU) untuk mengukur komitmen negaranegara anggota ITU terhadap keamanan siber. Tujuan GCI adalah untuk membantu negara-negara mengidentifikasi area yang harus diperbaiki dalam dunia keamanan siber, sehingga membantu meningkatkan tingkat komitmen keseluruhan terhadap keamanan siber di seluruh dunia.



Cyber Security

Penilaian didasarkan pada lima pilar yaitu:

1. Legal, diukur dari keberadaan institusi legal dan framework keamanan siber
2. Technical, diukur berdasarkan keberadaan institusi teknis dan penerapan teknologi
3. Organizational, diukur berdasarkan koordinasi pembuat kebijakan dan pengembangan strategi keamanan siber
4. Capacity Building, diukur berdasarkan penelitian dan pengembangan, pendidikan dan program pelatihan, profesional dan aparatur yang tersertifikasi.
5. Cooperation, diukur dari adanya partnership, kerangka kerjasama dan information sharing network.

Jenis Keamanan Cyber menurut modus operandi



**UNIVERSITAS
NASIONAL**
PIONIR PERUBAHAN

1. Cyber Crime
2. Cyber Warfare
3. Cyber Terrorism

Kerjasama Internasional



UNIVERSITAS
NASIONAL
PIONIR PERUBAHAN

Pakta pertahanan seperti NATO akan mengedepankan aspek collective defense untuk mengatasi ancaman cyber.

Mekanisme NATO dalam mengatasi ancaman cyber masih tetap berkorelasi dengan militer karena fokus utama organisasi tersebut adalah menjaga pertahanan negara-negara anggotanya baik secara fisik ataupun maya

Kerja sama ASEAN



**UNIVERSITAS
NASIONAL**
PIONIR PERUBAHAN

Berdasarkan ASEAN ICT Masterplan 2012, salah satu tugas pokok negara anggota ASEAN dalam menyambut MEA adalah memperkuat keamanan cyber untuk memperkuat perekonomian kawasan melalui kerja sama.

Negara anggota dapat memanfaatkan kelembagaan ASEAN untuk mempererat kerja sama keamanan cyber dengan cara information sharing serta saling membangun trust di antara sesama anggota

Uni Eropa

Uni Eropa memberlakukan kebijakan data hub yang mana semua data warganya yang tergabung dalam keanggotaannya hanya boleh dikelola di dalam wilayahnya.

EU International Cyberspace Policy

Kebijakan tersebut setidaknya memuat empat aturan utama yaitu

1. freedom and openness,
2. EU's laws, norms and core values,
3. developing cyber security building
4. international cooperation (EU, 2014).

Interpol fokus menangani ancaman cyber dari sisi penegakan hukum

BADAN SIBER dan SANDI NEGARA (BSSN)



UNIVERSITAS
NASIONAL
PIONIR PERUBAHAN

- Latar belakang pembentukan Badan Siber dan Sandi Negara
- Tugas dan Fungsi Pokok Badan Siber dan Sandi Negara

Topik Diskusi

- ▶ Bagaimana pandangan Realis dan Liberalis Institusionalis memandang kerja sama internasional dalam penanggulangan Cyber Crime?
- ▶ Bagaimana kerja sama internasional dalam menangani cyber crime?

Referensi



- ▶ Ghernaouti, Solange. 2013. *Cyber Power :Crime, Conflict and Security in Cyberspace*. Lausanne: EPFL Press
- ▶ Handrini Ardiyanti. (2014). *Cyber-security Dan Tantangan Pengembangannya Di Indonesia*. *Politica* Vol. 5 No. 1 Juni. Diakses melalui <https://dprexternal3.dpr.go.id/index.php/politica/article/view/336/270>
- ▶ Pedoman Pertahanan Siber. (2014). Kementerian Pertahanan Republik Indonesia
- ▶ Global Cybersecurity Indeks. Diakses melalui <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- ▶ Koh, B. (t.t.): Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, HarperCollins Publishers, 2010, 290 pages 3.
- ▶ Brandon Valeriano and Ryan C. Maness. 2018. *International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain*, dalam *The Oxford Handbook of International Political Theory*. Oxford University Press. Diakses melalui <https://www.oxfordhandbooks.com/view/10.1093/oxfordhb/9780198746928.001.0001/oxfordhb-9780198746928-e-19>
- ▶ Arquilla, John dan David Rondfelt. (1993). *Cyberwar is Coming*. *Comparative Strategy* 12
- ▶ Waltz, Kenneth. (1993). *The Emerging Structure of International Politics*. *International Security*