Operasi Siber TNI dan Koridor Demokrasi

Latar Belakang

Bagaimana operasi siber dilakukan dalam koridor demokrasi?

TEMPO

Menu Harian Mingguan Tempo Plus

Politik Politik Pendidikan Nusa Sosial Difabel

Politik

Kontroversi Pelibatan Tentara Hadapi Ancaman Siber dalam UU TNI

Kementerian Pertahanan menyatakan tugas TNI di ruang siber dalam UU TNI akan relevan dengan perkembangan zaman. Tidak menyasar pengkritik.

27 Maret 2025 | 12.06 WIB

Aa

Bagikan

Tolak RUU TNI, Tolak Militerisasi Ruang Siber

/ Akses Internet, Keamanan Digital, Kebebasan Berekspresi, Press Release, Publikasi, Rilis Pers, Sorotan / Oleh Safenet Voice

Persepsi Ancaman Siber

Perspektif perang siber

Menko Polhukam Hadi Tjahjanto (4 September 2024)

"Kita sudah pernah mengalami perang siber, misalnya saat konflik dengan Timor Leste. Kita harus berhadapan dengan negara-negara pendukungnya melalui perang siber, dan saat itu kita masih membutuhkan pengalaman lebih untuk menang," kata Hadi.

Menurut dia, perang siber bukan hanya tentang teknologi, tetapi juga perang pikiran. Media dan informasi menjadi senjata utama dalam membentuk opini masyarakat dan mempengaruhi keputusan mereka.

"Perang siber adalah perang pikiran. Kita mempengaruhi pikiran masyarakat untuk melaksanakan kehendak kita. Oleh karena itu, Kementerian Pertahanan sedang membangun kemampuan untuk melaksanakan perang siber dan menangkal serangan balik yang mungkin terjadi," ujar Hadi,

Jubir Kemhan (23 Maret 2025)

Kemenhan: Operasi Informasi di Ruang Siber Targetkan Pihak yang Ancam Kedaulatan Bangsa

TNI akan melakukan operasi informasi dan disinformasi untuk menanggulangi ancaman kedaulatan negara di ruang siber.

26 Maret 2025 | 10.00 WIB

Juru Bicara Kementerian Pertahanan Frega Ferdinand Wenas Inkiriwang memberikan keterangan pers di gedung Kementerian Pertahanan, Jakarta, 23 Januari 2025. Tempo/Hendrik Yaputra

TEMPO.CO, Jakarta - Kepala Biro (Karo) Infohan Setjen **Kementerian Pertahanan** (Kemenhan) Brigjen TNI Frega Ferdinand Wenas Inkiriwang mengatakan, TNI akan melakukan operasi informasi dan disinformasi untuk menanggulangi ancaman kedaulatan negara di ruang siber. Operasi itu menargetkan pihak-pihak yang memiliki motif melemahkan kepercayaan publik terhadap institusi pertahanan dan pemerintah.

"Hingga yang berpotensi memecah belah bangsa," kata Frega saat dihubungi pada Ahad, 23 Maret 2025.

Seperti apa ancaman siber dalam UU sektor pertahanan?

		UU Hanneg 2002	UU TNI 2004	UU PSDN 2019	UU TNI 2025
Jenis Ancaman	Ancaman militer	Masuk dalam kategori spionase dan sabotase	Masuk dalam kategori spionase dan sabotase	- Ancaman siber disebutkan sebagai jenis ancaman - Ancaman hibrida pertama kali disebutkan; TNI menjadi komponen utama	- Masuk dalam kategori spionase dan sabotase - Ancaman Pertahanan Siber sebagai bagian dari OMSP
	Ancaman nonmiliter	Membahas tetapi tidak menjelaskan lebih jauh	Tidak membahas ancaman nonmiliter		Tidak membahas ancaman nonmiliter
	Ancaman hibrida	Tidak membahas ancaman hibrida	Tidak membahas ancaman hibrida		Tidak membahas ancaman hibrida

Sebelum masuk revisi UU TNI 2025, 'Siber' sebagai ancaman baru masuk dalam UU di PSDN 2019. 'Ancaman pertahanan siber' seharusnya membuat koridor operasi siber TNI terbatas...

Seperti apa otoritas operasi siber TNI terhadap aktor ancaman?

		Sasaran			
		Jaringan Militer	Jaringan Pemerintahan Sipil	Infrastruktur Kritis	Kepercayaan Publik (melalui peperangan informasi)
Aktor/ Pelaku	Militer negara lain	Ya	Ancaman Hibrida	Ancaman Hibrida	Ancaman Hibrida
	Terafiliasi negara atau instansi intelijen sipil	Ya	Tidak	Tidak	Tidak
	Lainnya	Ya	Tidak	Tidak	Tidak

...tapi, definisi 'ancaman hibrida' mengaburkan operasi TNI menghadapi ancaman siber.

Siber sudah masuk dalam dokumen strategis sektor pertahanan di era 2014-2016...

Buku Putih Pertahanan 2015 (hal. 93)

dan bersifat proxy war. Tren menguasai suatu negara dengan menggunakan 'senjata' asimetris yang dibangun secara sistematis, seperti konflik Suriah dan perang di Ukraina semakin meningkat. Penciptaan kondisi lewat propaganda dilakukan dengan memanfaatkan kemajuan teknologi informasi dan ruang siber seperti media sosial.

Permasalahan serius terkait konflik kontemporer adalah meningkatnya konflik internal, yaitu konflik yang dapat memicu gerakan separatis karena kepentingan politik dan wilayah, termasuk konflik sosial yang terjadi di beberapa negara dengan dilatarbelakangi dinamika sosial, budaya, primordialisme, suku, ras, dan agama.

Pola devide et impera atau memecah-belah komponen-komponen bangsa dalam negeri merupakan cara yang efektif untuk menghancurkan suatu negara. seperti yang terjadi pada fenomena Arab Spring, kekacauan politik dan keamanan di Mesir, serta perang saudara di Irak, Afghanistan, Libya, dan Suriah membuktikan adanya pola konflik tersebut.

Pedoman Strategis Pertahanan Nirmiliter 2016 (hal. 23)

dengan alasan mengurangi risiko kehancuran fatal. Pihak ketiga biasanya merupakan negara kecil, tetapi bisa juga *nonstate actors* yang berupa LSM, ormas, kelompok masyarakat, atau perorangan, dengan melakukan propaganda dan memanfaatkan kemajuan teknologi informasi dan ruang siber seperti jejaring sosial. Sehingga dengan cara ini tidak dapat dikenali dengan jelas siapa kawan dan siapa lawan karena musuh mengendalikan *nonstate actors* dari jauh. Peluang terjadinya *Proxy War* ini sangat dimungkinkan terjadi seiring semakin pesatnya populasi penduduk dunia yang tidak diimbangi dengan ketersediaan pangan dan energi, sehingga dapat menjadi pemicu munculnya konflik-konflik baru. Kondisi demikian menunjukkan bahwa keamanan energi dan

...dengan fokus pada ruang siber digunakan untuk memecah belah bangsa.

Dalam dokumen yang lebih anyar..

Kebijakan Umum Pertahanan Negara 2020-2024 (hal. 40, 42-43)
Ancaman Nonmiliter berdimensi teknologi:

5.	Teknologi	kejahatan siber, khususnya terhadap objek vital nasional	penyalahgunaan teknologi informasi melalui berbagai media internet untuk tujuan propaganda, intimidasi, menyesatkan	yang dapat mendorong gerakan sosial yang mengancam kedaulatan negara

..juga memberikan fokus pada ruang siber berpotensi membawa ancaman perpecahan.

Sebenarnya, Jakgara Hanneg 2020-2024 telah mencoba menempatkan siber dalam kerangka perang modern..

Pembangunan Postur Pertahanan Militer (hal. 12)

Mengintegrasikan jaringan sistem Trimatra terpadu (tiga matra secara terpusat)/*network centric warfare* (NCW) dalam rangka meningkatkan interoperabilitas operasi antara kekuatan darat, laut, udara, serta antariksa dan siber, diselenggarakan melalui:

Pembangunan Teknologi Pertahanan (hal. 26)

b) Mengembangkan teknologi sistem informasi pertahanan secara terintegrasi (*Network Centric Warfare*) guna pencapaian kesatuan komando (*Unity of Command*) dalam pencapaian keputusan.

c) Mengembangkan kapabilitas teknologi siber yang mampu melakukan perang siber melalui siber ofensif dan defensif, pemantuan, jaminan keamanan, penangkalan dan pembalasan, penyusupan, senjata maupun intelijen siber.

...namun seperti apa prakteknya?

Maturitas Siber TNI

Maturitas Siber Militer (disadur dari Blessing & Austin, 2020)

Dimensi Strategis: Siber dalam Doktrin TNI – TRIDEK (2018)...

Ancaman Nonmiliter (hal. 12, 15)

4) Sosial Budaya. Ancaman berdimensi sosial budaya dapat berupa konflik horisontal seperti pertikaian suku, agama, ras, dan antargolongan serta munculnya perilaku anarkis (*hooliganism*). Penggunaan teknologi informasi yang tidak terkontrol dapat memicu terjadinya benturan antar peradaban termasuk dampak peredaran dan penyalahgunaan narkoba yang dapat mengancam generasi muda. Demikian pula rendahnya kualitas SDM menyebabkan lemahnya daya saing yang berakibat meningkatnya korupsi dan pengangguran sehingga dapat memicu terjadinya kerawanan sosial.

6) Teknologi. Paradoks kemajuan teknologi di bidang informasi dan komunikasi yang saat ini masuk pada era Revolusi Industri 4.0, menimbulkan bentuk ancaman yang semakin kompleks, sehingga cara bertindak musuh akan semakin bervariasi dan akurat. Kejahatan memanfaatkan teknologi siber merupakan tindakan kriminal yang menggunakan kecanggihan teknologi. Demikian juga kejahatan terorisme melalui siber dan perang siber berupa serangan yang menggunakan teknologi elektronik dapat mengganggu aktivitas sosial dan ekonomi bangsa. Ancaman berdimensi teknologi dapat terjadi dalam bentuk penyalahgunaan penyebar biologi patogen untuk melancarkan bioterorisme dan perang biologi.

Daftar Pengertian (hal. 33)

8. **Ancaman Hibrida**. Ancaman Hibrida adalah ancaman yang bersifat campuran dan merupakan paduan antara ancaman militer dan nonmiliter. Ancaman hibrida antara lain mengombinasikan antara ancaman konvensional, asimetrik, teroris, dan perang siber serta kriminal yang beragam dan dinamis. Selain berbagai kombinasi ancaman tersebut, ancaman hibrida dapat juga berupa keterpaduan serangan antara penggunaan senjata kimia, biologi, radiologi, nuklir dan bahan peledak (*Chemical, Biological, Radiological, Nuclear and Explosive* /CBRNE) dan perang informasi.

...tidak dijelaskan secara khusus integrasinya dalam cara berperang TNI.

Doktrin TNI AD memasukkan ancaman siber sebagai ancaman militer bukan agresi...

Ancaman Militer (hal. 23-24)

2) Bukan agresi. Merupakan ancaman yang dapat menggunakan kekuatan senjata ataupun tidak bersenjata, baik berasal dari luar negeri maupun dalam negeri serta dilakukan oleh aktor negara maupun aktor bukan negara yang sangat mungkin membahayakan kedaulatan negara, keutuhan wilayah, dan keselamatan bangsa dengan berbagai aksinya antara lain gerakan separatis bersenjata, pemberontakan bersenjata, terorisme, pelanggaran wilayah perbatasan darat, spionase, sabotase, siber, dan *proxy war*.

Fungsi Teknis Militer Khusus (hal. 22)

b) Sandi dan Siber. Menyelenggarakan kemampuan intelijen, perlindungan, kodal dan informasi melalui kegiatan persandian (siber defensif pasif), siber penangkalan (defensif aktif), dan penindakan siber (siber ofensif) guna mendukung fungsi utama TNI AD.

Pertempuran Darat Masa Depan (hal. 38)

Berkembangnya pertempuran *multi-domain* menuntut TNI AD untuk mengembangkan jenis operasi serangan dan pertahanan yang akan berubah secara signifikan dengan mengutamakan kecepatan, akurasi, dan daya hancur yang besar. Strategi dan taktik pertempuran darat ke depan diyakini akan membentuk karakter pertempuran baru yang didominasi dengan peperangan teknologi informasi *(network centric warfare)* dan peperangan siber *(cyber warfare)* yang semakin kompleks dan membutuhkan sumber daya prajurit yang andal dan adaptif dalam pertempuran *multi-domain*.

...namun juga memberikan penjabaran cukup detail terkait integrasi peperangan siber dalam pertempuran.

Sementara untuk dua matra lain yang sangat bergantung pada teknologi mutakhir...

Doktrin TNI AU (2019) hal. 25

i. **Kemampuan Siber.** Kemampuan siber merupakan kemampuan TNI AU untuk melindungi dan menyerang balik serangan siber negara lain maupun pihak lain terhadap jaringan informasi, struktur dan sistem senjata yang dimiliki oleh TNI AU. Kemampuan siber juga digunakan untuk melindungi dan memberdayakan informasi serta mendapatkan dan menyerang informasi lawan/musuh serta jaringannya yang bertujuan untuk mendapatkan keunggulan informasi agar tercipta penguasaan udara.

Doktrin TNI AL (2018) hal. 80

34. **Perubahan Bentuk Ancaman.**

Kondisi dinamis lingkungan kehidupan manusia yang meliputi aspek ideologi, politik, sosial budaya, keamanan, teknologi, dan ruang hidup menjadi katalisator berkembangnya bentuk-bentuk ancaman baru. Kekuatan konvensional yang saling berhadapan di masa lalu saat ini telah mengalami perubahan dengan munculnya aktor-aktor non negara dalam berbagai wujud, melahirkan model-model serangan baru yang melandasi munculnya bentuk-bentuk ancaman baru seperti ancaman asimetris, *proxy war*, perang siber dan lain sebagainya. Perkembangan teknologi siber juga meningkatkan kemampuan untuk menyerang lawan langsung pada *center of gravity* atau pusat kekuatan lawan yang memengaruhi keseimbangan operasi dan strategi lawan selanjutnya berdampak pada kekalahan atau kehancuran lawan.

Doktrin TNI AU (2019) hal. 26-27

d. **Operasi Informasi.** Operasi informasi merupakan kegiatan/tindakan terencana dengan memanfaatkan kekuatan dan kemampuan terpadu untuk mempengaruhi, mengeksploitasi baik informasi, sistem informasi maupun proses pengambilan keputusan pihak lawan termasuk upaya pembentukan opini publik dengan tetap memelihara dan mempertahankan informasi serta sistem informasi milik sendiri. Bentuk operasi udara dalam operasi informasi yaitu operasi udara informasi yang memadukan berbagai kemampuan intelijen, teknologi informasi, komunikasi dan elektronika, psikologi, infolahta, dan penerangan. Tujuan dari operasi informasi adalah mencapai keunggulan informasi (*information superiority*). Keunggulan informasi adalah faktor yang sangat menentukan untuk memperoleh sasaran yang akurat sebelum dilaksanakan operasi udara, tanpa keunggulan informasi akan sulit dicapai keunggulan udara *(air superiority)*. Keunggulan informasi adalah suatu tingkatan dominasi informasi dimana pasukan kawan mempunyai kemampuan untuk mengumpulkan, mengendalikan, mengeksploitasi, dan melindungi informasi tanpa gangguan yang berarti dari pihak lawan atau musuh. Operasi Udara Informasi terdiri dari dua operasi yaitu Operasi Lawan Informasi Ofensif (OLIO), dan Operasi Lawan Informasi Defensif (OLID).

...TNI AU memiliki doktrin yang bisa dibilang lebih ofensif dalam penggunaan kemampuan siber.

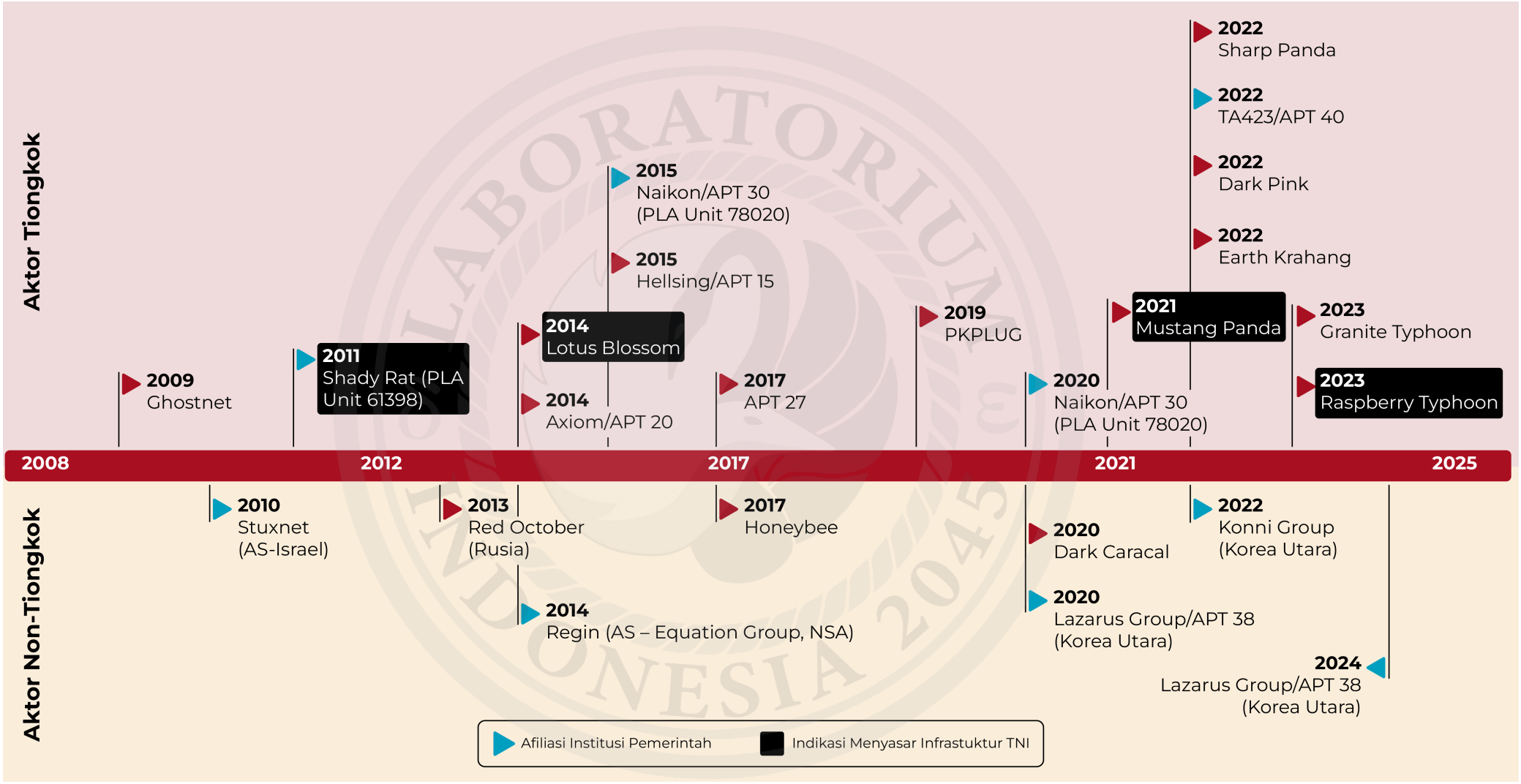
Dimensi Institusional: Struktur organisasi siber saat ini

Organisasi Inti	**Kemhan**	**Mabes TNI**	**Mabes TNI AD**	**Mabes TNI AL**	**Mabes TNI AU**
Organisasi Siber	**Pusat Pertahanan Siber**	**Satuan Siber TNI**	**Pusat Sandi dan Siber AD**	**Satuan Siber TNI AL**	**Satuan Siber TNI AU**
Pimpinan dan Kedudukan	**Bintang 1** Berada di Bawah Bainstrahan	**Bintang 1** Bertipe Balakpus, berada di bawah Panglima TNI	**Bintang 1** Bertipe Balakpus, berada di bawah KSAD	**Bintang 1** Bertipe Balakpus, berada di bawah KSAL	**Bintang 1** Bertipe Balakpus, berada di bawah KSAU

Dimensi Kapasitas: Latihan dengan negara lain

Nama Kegiatan	Tahun	Jenis	Mabes	Unit Peserta	Negara Lain
Gema Bhakti	2017-2022	Latihan Gabungan	TNI	Mabes TNI dan 3 matra	Amerika Serikat
Information System and Technology Exchange (ISTX)	2018-2019	Pelatihan Bilateral	TNI	Mabes TNI dan 3 matra	Amerika Serikat
BAE Systems Applied Intelligence (BAEs-AI)	2019	Pelatihan Bilateral	Kemhan	Pushansiber Bainstrahan	Inggris
Command, Control, Communications and Computer System (C4S) Subject Matter Expert Exchange (SMEE)	2021	Pertemuan Bilateral	AD	AD	Filipina
Cyber SMEE (Subject Matter Expert Exchange)	2022	Pertemuan Bilateral	AD	Mabes AD	Amerika Serikat
Army Cyber Commander Training Course	2023	Pelatihan Bilateral	AD	Pusat Sandi dan Siber TNI Angkatan Darat (Pussansiad)	Inggris
Super Garuda Shield	2024	Latihan Gabungan	TNI	Semua unit	Amerika Serikat
Cobra Gold	2025	Latihan Gabungan	AD	Staf Latihan TNI AD (Slatad)	Thailand, Amerika Serikat
Defense Cyber Marvel	2025	Pelatihan Bilateral	TNI	Pussansiad	Inggris

Ancaman siber terafiliasi negara terhadap Indonesia



Koridor Demokrasi

Norma internasional: UN 11 Responsible Cyber Norm

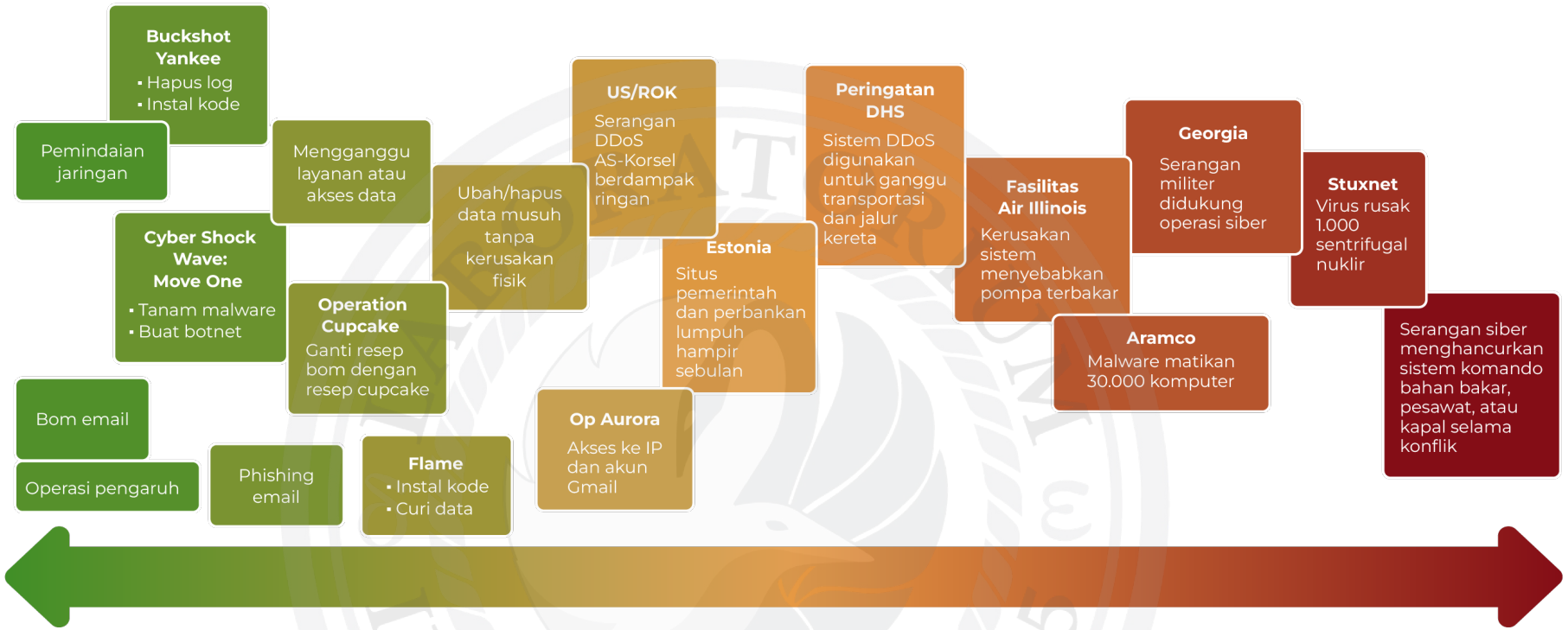
Operasi siber keluar koridor demokrasi: kasus *spyware*

Spyware	Periode Penggunaan	Perusahaan Perantara	Institusi Negara Pengguna	Target
FinFisher (Jerman)	2004, 2010, 2013, 2015, 2021	- Gamma TSE Group - Readarius M8 Sdn Bhd (Malaysia) - PT. Digital Solusi Prima	Lemsanneg/ BSSN, BNPT	- Aktivitas dan Masyarakat di Papua - Organisasi Non-Pemerintah aktivis/ oposisi politik secara global
Wintego Systems (Israel)	2019	- Ataka Enterprises PTE Ltd (Singapura - ESW Systems (Singapura)	POLRI	Target tidak jelas, jejak *spyware* ditemukan dalam situs yang meniru tribunnews.co
Intellexa Consortium (Berbasis di beberapa negara Eropa)	2021-2023	Tidak ditemukan	Tidak jelas penggunanya di Indonesia	Kemungkinan menyasar aktivis Papua karena jejak *spyware* ditemukan dalam situs seperti ewestpapua.org dan nindonesia.news
Candiru/ Saito Tech (Israel)	2020-2021	HeHa PT Ltd (Singapura)	POLRI	Target tidak jelas, jejak *spyware* ditemukan dalam situs menyerupai media daring seperti Tirto, Tribunnews, Media Indonesia dan ANTARA
NSO Group - Circles, Q Cyber (Israel)	2018-2022	Radika (PT. Radika Karya Utama)	BIN, POLRI	- Menteri Airlangga Hartarto - Penasihat Kemhan dan Kemlu - Dua pejabat senior TNI - Dua diplomat regional

Rekomendasi

Doktrin dan Strategi	Kelembagaan Organisasi Siber	Personil dan Talenta Siber	Hubungan Sipil Militer
1. Dokumen strategis baru mengenai gradasi ancaman siber dan batasan pelibatan TNI 2. Definisi ulang ancaman hibrida 3. Mendorong UU Keamanan Siber dan Keamanan Nasional	1. Meningkatkan Satsiber menjadi Kotama Ops, hingga nantinya Komando Gabungan 2. Mengkaji ulang fokus pengendalian konten dalam pengembangan Konten	1. Tangga karier yang jelas bagi perwira siber 2. Mendukung lahirnya perwira-perwira tinggi berlatar siber dengan pola mutasi dan promosi 3. Standarisasi kurikulum latihan terpadu 4. Rekrutmen talenta siber non teknis, seperti ahli hukum	1. Penguatan koordinasi operasi siber dengan institusi sipil 2. Mekanisme akuntabilitas dan pengawasan oleh DPR 3. Mempublikasikan dokumen strategi dan doktrin untuk diakses publik

Gradasi ancaman siber dan di mana operasi siber TNI bisa dilakukan?



Boleh merespons dengan tindakan balasan di bawah ambang kekuatan	Boleh menggunakan kekuatan dalam pembelaan diri

Operasi Pendukung

- Karakterisasi jaringan
- Operasi internet

Gangguan Siber

- Mengganggu aliran informasi atau fungsi sistem informasi tanpa kerusakan fisik atau cedera

Operasi Pendukung

- Kerusakan fisik terhadap properti atau menyebabkan cedera pada manusia

Lebih tersembunyi — **Kurang tersembunyi**

Sumber: Brown & Tullos, “On The Spectrum of Cyberspace Operations”, 2012.

TERIMA KASIH

@lab45.id | @lab45_ | LAB 45 | @lab45.id | lab45@lab45.id | www.lab45.id