
Pembelajaran dari Pemecahan Enigma dalam Pengembangan Kerja Sama Sipil-Militer untuk Menghadapi Ancaman Siber di Indonesia

Yanto Manurung^{1*}, Prabaswari¹

¹Program Studi Ilmu Pertahanan, Universitas Pertahanan, Indonesia

*yasman35@outlook.com**

Article History:

Received : 28-09-2026

Accepted : 04-10-2026

Keywords: *Enigma; Hubungan Sipil-Militer; Pertahanan Siber; Kerja Sama Lintas Institusi; National Cyber Force*

Abstract: *Perkembangan teknologi informasi telah mengubah karakter ancaman terhadap keamanan nasional dari konflik konvensional menuju ancaman yang semakin kompleks di ruang siber. Pengalaman Perang Dunia II, khususnya keberhasilan Sekutu dalam memperoleh dan memanfaatkan informasi dari komunikasi terenkripsi Jerman melalui pemecahan Enigma, menunjukkan pentingnya kolaborasi antara berbagai keahlian dan institusi dalam mendukung keunggulan informasi. Penelitian ini bertujuan menganalisis pembelajaran dari pengalaman Inggris pada masa Perang Dunia II dan perkembangan kelembagaan keamanan sibernya untuk merumuskan konsep kerja sama sipil-militer yang relevan bagi Indonesia. Penelitian menggunakan pendekatan kualitatif dengan metode historis dan studi kepustakaan terhadap sumber yang berkaitan dengan Perang Dunia II, hubungan sipil-militer, serta perkembangan pertahanan siber. Analisis difokuskan pada perkembangan Government Code and Cypher School (GC&CS), transformasinya menjadi Government Communications Headquarters (GCHQ), pembentukan National Cyber Force (NCF), serta relevansinya bagi pengembangan kapabilitas siber Indonesia. Hasil kajian menunjukkan bahwa keberhasilan dalam menghadapi ancaman siber membutuhkan integrasi kemampuan sipil, militer, intelijen, penelitian, akademisi, dan industri melalui pembagian kewenangan serta mekanisme koordinasi yang jelas. Berdasarkan pembelajaran tersebut, penguatan kapabilitas pertahanan siber Indonesia perlu diarahkan pada model kolaboratif yang mengintegrasikan fungsi keamanan siber, pertahanan, intelijen, dan riset di bawah mekanisme pengawasan dan koordinasi yang jelas. Model tersebut dapat diwujudkan melalui penguatan*

kelembagaan yang telah ada atau pembentukan organisasi/satuan tugas lintas institusi dengan mempertimbangkan aspek hukum, kewenangan, sumber daya, dan akuntabilitas.

PENDAHULUAN

Penelitian dilatarbelakangi oleh peristiwa kekalahan Jerman pada Perang Dunia II. Pada masa Perang Dunia II, Jerman merupakan salah satu kekuatan militer utama di Eropa dan berhasil memperoleh sejumlah kemenangan pada tahap awal perang. Jerman kemudian menghadapi koalisi Sekutu yang melibatkan sejumlah negara, termasuk Inggris, Amerika Serikat, Uni Soviet, dan negara-negara lainnya. Salah satu faktor yang mendukung keberhasilan militer Jerman pada tahap awal perang adalah pengembangan dan penggunaan teknologi serta strategi militer yang relatif maju pada masanya (Putra, 2014). Selain itu salah satu teknologi kriptografi yang digunakan secara luas oleh Jerman berjasa dalam mengirimkan instruksi perang adalah Mesin sandi Enigma (Gambar 1). Penggunaan Enigma meningkatkan tingkat kerahasiaan komunikasi militer Jerman karena pesan yang dikirimkan dalam bentuk terenkripsi tidak dapat langsung dibaca oleh pihak yang tidak memiliki konfigurasi dan metode deskripsi yang sesuai. Enigma digunakan secara luas oleh berbagai unsur militer dan pemerintahan Jerman selama Perang Dunia II.



Gambar 1. Mesin Sandi Enigma

Sumber : Museum of Polish History (tvpworld.com,2018)

Selain penguasaan teknologi, tentunya juga terdapat faktor lain yang mempengaruhi Jerman sebagai bangsa yang kuat dan sulit untuk ditaklukkan diantaranya pengaturan administrasi dan logistik yang terorganisir, selain itu kondisi musuh-musuh Jerman pada tahun 1930-1940an juga sedang dalam posisi ekonomi yang krisis dan lemah, sehingga berhasil dimanfaatkan Jerman untuk memenangkan banyak pertempuran. Namun demikian, pada akhirnya Jerman mengalami kekalahan pada Perang Dunia II, hal ini juga disebabkan karena faktor-faktor internal dan eksternal yang mendasar diantaranya pengaruh gaya kepemimpinan Hitler, kesalahan strategi, obsesi pada rasisme dan keberhasilan pengungkapan mesin sandi Enigma oleh pihak Inggris (Ramadhan, 2019).

Keberhasilan Sekutu dalam memperoleh dan memanfaatkan informasi dari komunikasi terenkripsi Jerman melalui pemecahan Enigma merupakan salah satu faktor yang memberikan keunggulan intelijen selama Perang Dunia II. Pengalaman tersebut menunjukkan bahwa keunggulan informasi dapat diperoleh melalui kolaborasi antara berbagai keahlian, teknologi, dan institusi.

Pengembangan metode dan perangkat kriptanalisis di Bletchley Park melibatkan berbagai ilmuwan, matematikawan, insinyur, dan personel militer. Alan Turing merupakan salah satu tokoh penting dalam pengembangan metode dan perangkat yang mendukung pemecahan komunikasi terenkripsi Jerman. Pengalaman tersebut menunjukkan bahwa keunggulan informasi dalam peperangan dapat dibangun melalui kombinasi keahlian manusia, teknologi, dan koordinasi kelembagaan.

Ryamizard Ryacudu menjelaskan bahwa perang masa kini atau perang modern dapat berlangsung secara nonmiliter dan diarahkan untuk melemahkan sistem suatu negara secara menyeluruh (Ryacudu, 2015). Dengan kata lain, perang modern adalah suatu bentuk perang yang dilakukan secara non-militer dari negara maju atau luar negeri untuk menghancurkan suatu negara tertentu melalui bidang ideologi, politik, ekonomi, budaya, budaya – masyarakat, pertahanan dan keamanan nasional. Terjadi peralihan dari perang konvensional ke perang siber, mengingat saat ini seluruh infrastruktur vital negara hampir pasti melakukan digitalisasi sebagai inti pengelola sistem.

Dalam melakukan perang modern, aktor tidak lagi bergantung sepenuhnya pada komando militer, tetapi juga memberdayakan seluruh sumber daya potensial yang dapat membantu proses infiltrasi dalam perang siber termasuk masyarakat sipil. Sebagaimana terlihat dalam sejarah Perang Dunia II, pemerintah Inggris melibatkan ilmuwan, matematikawan, insinyur, ahli bahasa, dan personel militer dalam upaya menganalisis komunikasi terenkripsi Jerman di Bletchley Park. Alan Turing merupakan salah satu tokoh penting dalam proses tersebut. Penelitian ini akan mencoba menjawab pertanyaan utama yaitu bagaimana pembelajaran dari pengalaman pemecahan Enigma dan perkembangan kelembagaan keamanan siber Inggris dapat digunakan untuk merumuskan model kerja sama sipil-militer dalam memperkuat pertahanan siber Indonesia?

Untuk menjawab pertanyaan tersebut, tulisan ini akan menggunakan teori Hubungan Sipil Militer dari Huntington, sebagai dasar pembentukan konsep organisasi sipil-militer untuk pencegahan ancaman perang siber yang bersifat semesta. Dimana Sistem Pertahanan Negara yang bersifat semesta harus diselenggarakan secara dini, total, terarah dan berkelanjutan dengan melibatkan segenap komponen bangsa dan negara. Menggunakan metode kualitatif dengan data yang dikumpulkan melalui kajian literatur. Hasil akhir rekomendasi berupa kerangka kolaborasi sipil militer yang bisa digunakan dalam menghadapi perang siber modern.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan metode historis dan studi kepustakaan. Pendekatan kualitatif digunakan untuk memahami secara

mendalam perkembangan kerja sama sipil-militer dalam menghadapi ancaman berbasis informasi serta relevansinya terhadap pengembangan kapabilitas pertahanan siber di Indonesia. Metode historis digunakan untuk mengkaji pengalaman Inggris dalam menghadapi komunikasi terenkripsi Jerman pada Perang Dunia II, khususnya perkembangan *Government Code and Cypher School* (GC&CS), keterlibatan berbagai unsur keahlian dalam kegiatan kriptanalisis, perkembangan kelembagaan menuju *Government Communications Headquarters* (GCHQ), serta pembentukan *National Cyber Force* (NCF).

Data penelitian diperoleh melalui studi kepustakaan dengan memanfaatkan berbagai sumber yang relevan, meliputi buku, artikel jurnal ilmiah, dokumen kelembagaan, publikasi pemerintah, serta sumber sejarah dan keamanan siber yang dapat dipertanggungjawabkan. Sumber tersebut dipilih berdasarkan relevansi dengan tiga fokus utama penelitian, yaitu: (1) sejarah pemecahan komunikasi terenkripsi Jerman pada Perang Dunia II; (2) perkembangan hubungan dan kelembagaan sipil-militer dalam bidang intelijen dan keamanan siber Inggris; dan (3) konsep pengembangan kerja sama sipil-militer dalam menghadapi ancaman siber di Indonesia.

Analisis data dilakukan melalui beberapa tahapan. Tahap pertama adalah heuristik, yaitu mengidentifikasi dan mengumpulkan sumber-sumber yang relevan dengan topik penelitian. Tahap kedua adalah verifikasi sumber, yaitu menilai relevansi, kredibilitas, dan kesesuaian informasi yang diperoleh dari berbagai sumber. Tahap ketiga adalah interpretasi, yaitu menghubungkan fakta-fakta historis mengenai pengalaman Inggris dengan konsep hubungan sipil-militer dan perkembangan pertahanan siber. Tahap keempat adalah historiografi, yaitu menyusun hasil kajian historis secara sistematis untuk menjelaskan perkembangan kerja sama lintas keahlian dan kelembagaan dalam menghadapi ancaman berbasis informasi. Tahapan penelitian historis tersebut digunakan dengan mengacu pada prinsip penelitian sejarah yang mencakup heuristik, verifikasi, interpretasi, dan historiografi.

Selanjutnya, hasil kajian historis dianalisis secara konseptual dan komparatif dengan menggunakan perspektif hubungan sipil-militer Samuel P. Huntington. Analisis ini digunakan untuk mengidentifikasi bentuk hubungan, pembagian peran, mekanisme koordinasi, dan pengawasan antara unsur sipil dan militer dalam pengelolaan kapabilitas siber. Pengalaman kelembagaan Inggris kemudian dibandingkan secara konseptual dengan kondisi kelembagaan Indonesia untuk mengidentifikasi kemungkinan model kerja sama yang dapat dikembangkan sesuai dengan kebutuhan dan karakteristik sistem pertahanan Indonesia.

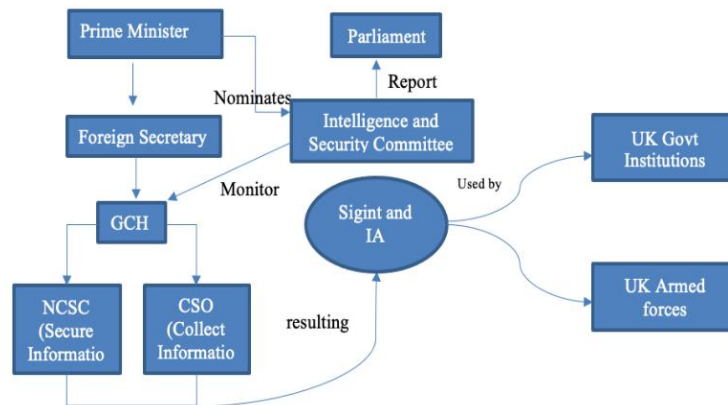
Tahap akhir penelitian adalah perumusan model konseptual kerja sama sipil-militer dalam menghadapi ancaman siber di Indonesia. Perumusan model mempertimbangkan beberapa aspek, yaitu pembagian kewenangan antara unsur sipil dan militer, keterlibatan institusi intelijen dan keamanan siber, dukungan akademisi dan industri, mekanisme koordinasi, dasar hukum, sumber daya manusia, serta pengawasan dan akuntabilitas. Model yang dihasilkan merupakan rekomendasi konseptual, bukan struktur kelembagaan resmi, sehingga penerapannya masih memerlukan kajian lebih lanjut dari aspek hukum, kelembagaan, anggaran, dan tata

kelola pertahanan. Hal ini sejalan dengan posisi naskah yang menempatkan model kekuatan siber Indonesia sebagai konsep awal yang masih memerlukan pengembangan lebih lanjut.

HASIL DAN PEMBAHASAN

Model Interaksi Kelembagaan Komponen Sipil dan Militer Inggris pada Era Perang Dunia II dan Perkembangannya

Saat perang dunia I, Angkatan Darat Inggris dan Angkatan Laut Inggris memiliki agen intelijen yang terpisah yaitu MI1b dan NID25 (National Cyber Force, 2020). Selanjutnya pada 1919, *Cabinet's Secret Service Committee* merekomendasikan pembentukan agen pemecah kode, kemudian dilakukan penggabungan MI1b dan NID25 dengan nama samaran "*Government Code and Cypher School*" (GC&CS), fungsi mereka yang diketahui adalah untuk memberi pertimbangan terkait keamanan penggunaan kode dan sandi yang digunakan oleh seluruh departemen pemerintah agar sesuai dengan ketentuan juga memiliki fungsi rahasia yaitu untuk mempelajari metode komunikasi sandi oleh pihak asing. Pada tahun 1920, GC&CS sukses membaca berita sandi kawat diplomatik Uni Soviet. Kemudian di tahun 1922, GC and CS pindah di bawah yuridiksi Kantor Luar Negeri Inggris, dan fokusnya bergeser dari militer luar negeri menjadi komunikasi radio diplomatik. Menjelang dan selama Perang Dunia II, khususnya sejak 1939, GC&CS meningkatkan kegiatan pemecahan kode dan analisis komunikasi militer negara-negara yang menjadi lawan Inggris, termasuk komunikasi yang menggunakan mesin sandi Enigma milik Jerman. Pada masa ini, GC&CS beranggotakan tidak hanya personel militer, tetapi juga matematikawan, insinyur, ahli bahasa, dan staf pendukung. Keterlibatan berbagai keahlian tersebut mendukung kegiatan analisis komunikasi dan pemecahan kode militer serta diplomatik Jerman selama Perang Dunia II (Sterling, 2008). Selanjutnya pada tahun 1946, GC&CS berganti nama menjadi *Government Communications Headquarters* (GCHQ). GCHQ bertugas sebagai organisasi keamanan dan intelijen yang menyediakan *signal intelligence* (*sigint*) dan jaminan informasi kepada pemerintah dan angkatan bersenjata Inggris. Misi utama GCHQ saat ini adalah untuk melindungi komunikasi pemerintah Inggris, melakukan *counter terrorism*, Keamanan Cyber, Penanganan kejahatan serius dan terorganisir, keuntungan strategis serta dukungan pertahanan. GCHQ dipimpin oleh seorang direktur yang didukung oleh 4 direktur jenderal. GCHQ berada di bawah tanggung jawab *Secretary of State for Foreign, Commonwealth and Development Affairs* dan menjadi bagian dari struktur pemerintahan sipil Inggris. Perdana Menteri juga menunjuk beberapa anggota parlemen dari berbagai partai sebagai anggota *Intelligence and Security Committee* yang bertugas mengawasi aktivitas intelijen dan keamanan, mereka melaporkan langsung kepada parlemen. GCHQ merupakan bagian dari layanan sipil. GCHQ sendiri memiliki sub organisasi yaitu *National Cyber Security Centre* (NCSC) yang bertugas mengamankan komunikasi dan informasi pemerintah Inggris dan *Composite Signals Organisation* (CSO) yang bertugas untuk mengumpulkan informasi (Smith, 1998). Kaitan hubungan sipil militer dalam peran GCHQ bisa kita lihat pada Gambar 2 berikut.



Gambar 2. Hubungan Sipil Militer dalam Keamanan Siber Inggris

Sumber : Smith (1998), Diolah oleh Penulis

Gambar 2 menunjukkan bahwa hubungan antara fungsi intelijen, pemerintahan sipil, dan unsur militer dalam sistem keamanan siber Inggris tidak berdiri secara terpisah. GCHQ berada dalam struktur pemerintahan sipil, sementara hasil dan kapabilitas intelijen serta keamanan siber mendukung kebutuhan pemerintah dan angkatan bersenjata. Pada saat yang sama, mekanisme pengawasan oleh lembaga legislatif menjadi bagian penting dalam menjaga akuntabilitas aktivitas intelijen.

Siber sebagai Domain Operasi dalam Pertahanan Inggris

Menghadapi era digitalisasi saat ini, Inggris terus meningkatkan kapabilitas dan keterampilan siber bagi personel serta pemimpin militernya (Pritchard, 2021). Ruang siber berkembang menjadi salah satu domain operasi yang memiliki keterkaitan erat dengan domain darat, laut, udara, dan ruang angkasa. Perkembangan tersebut mendorong perubahan dalam konsep dan operasi militer, terutama dalam aspek perlindungan komunikasi dan informasi digital serta penguatan kemampuan pertahanan dan operasi di ruang siber.

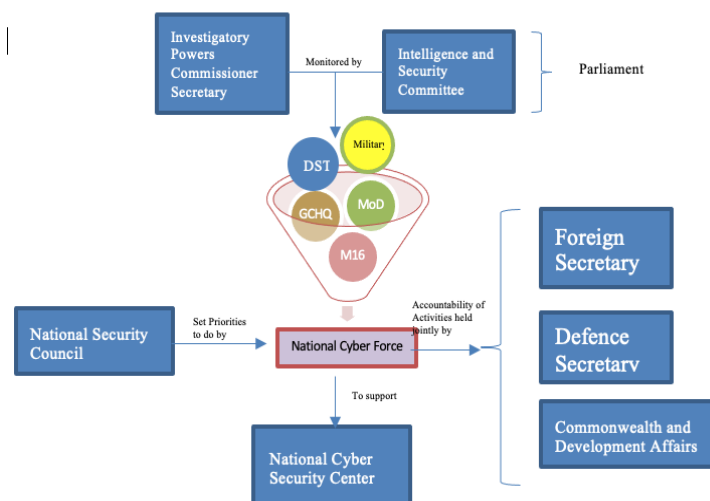
Militer Inggris, bersama dengan negara-negara NATO lainnya, terus berinvestasi dalam pengembangan sistem robotik dan otonom, *artificial intelligence*, pelatihan berbasis komputer atau sintetik, serta *Military Internet of Things* (Military IoT). Perkembangan teknologi tersebut perlu diimbangi dengan peningkatan kompetensi personel. Oleh karena itu, kebutuhan terhadap sumber daya manusia dengan keterampilan teknologi siber, seperti pemrograman, ilmu komputer, rekayasa data, dan operasi siber, menjadi semakin penting dalam mendukung kemampuan pertahanan pada berbagai domain operasi.

Untuk membangun strategi yang efektif maka perubahan ini akan mencakup kemampuan *defensive*, *offensive* serta kemampuan cyber juga hubungan yang lebih erat antara angkatan bersenjata, instansi pemerintah dan industri. Sektor pertahanan saat ini juga berjuang untuk pasokan dan permintaan keterampilan siber sama seperti industri lainnya.

Sebelumnya pada tahun 2020 Pasukan Cyber Nasional Inggris (NCF) yang merupakan kerja sama antara pertahanan dan intelijen telah dibentuk, badan ini beranggotakan anggota dari kementerian pertahanan (MoD), angkatan bersenjata, GCHQ, MI6 (*Secret Intelligence Service*) serta Laboratorium Ilmu dan Teknologi

Pertahanan (DSTL) (Corera, 2020) dengan tugas utama *National Offensive Cyber Program* yaitu perlawanan terhadap ancaman teroris, kriminal dan musuh negara. Personel MI6 bekerja bersama GCHQ dan unsur militer dalam kerangka *National Cyber Force*. Dengan dibentuknya pasukan ini, di masa depan saat angkatan bersenjata Inggris berperang, operasi cyber akan terintegrasi dengan militer tradisional. Pembentukan NCF awalnya tidak berjalan mulus karena perebutan otoritas antara departemen pertahanan dengan GCHQ, pada akhirnya disepakati bahwa *foreign secretary* dan *defence secretary* akan berperan pada tipe operasi yang berbeda.

Untuk menjaga akuntabilitas NCF, kegiatannya dilakukan secara bersama-sama dengan *Secretary of State of Foreign affairs, Commonwealth and Development Affairs* dan *Secretary of State for Defence*. NCF bertanggungjawab atas prioritas yang ditentukan oleh *National Security Council*, dan bekerja erat dengan petugas dari beberapa departemen pemerintahan untuk mencapai strategi dan rencana mereka. Selain itu mereka juga bertugas untuk mendukung keamanan siber dan *National Cyber Security Centre* dengan menangkal ancaman yang bisa mengganggu *confidentiality, integrity* dan *availability* dari data dan layanan di ruang siber. Agar operasi siber yang dilakukan NCF sesuai dalam koridor hukum maka diawasi oleh *Investigatory Powers Commissioner* dan *Intelligence and Security Committee of Parliament*. Secara singkat dapat dilihat pada gambar 3 berikut.



Gambar 3. HSM pada Pembentukan National Cyber Force UK 2020

Sumber : Diolah oleh Penulis

Gambar 3 menunjukkan bahwa NCF dibangun melalui integrasi unsur pertahanan dan intelijen dengan mekanisme pengarah dan pengawasan yang melibatkan pemerintah serta lembaga pengawasan. Struktur tersebut memperlihatkan bahwa kapabilitas operasi siber tidak berdiri sendiri, tetapi berada dalam kerangka kewenangan, prioritas keamanan nasional, dan mekanisme akuntabilitas.

Sinergitas Menghadapi Cyber Warfare

Melihat langkah strategis yang diambil Inggris melalui pembentukan *National Cyber Force* (NCF), penguatan kemampuan pertahanan dan operasi siber menjadi bagian penting dalam menghadapi perkembangan ancaman keamanan di ruang siber. Pengalaman Inggris tersebut dapat menjadi pembelajaran bagi Indonesia dalam

membangun kapasitas pertahanan siber yang melibatkan unsur sipil dan militer secara terkoordinasi. Indonesia saat ini telah memiliki beberapa institusi dan fungsi pada instansi pemerintah, baik sipil maupun militer, yang berkaitan dengan tata kelola dan keamanan ruang siber, di antaranya sebagai berikut:

Tabel 1. Instansi Pengelola Ruang Siber Indonesia

Nama Lembaga/Unit Institusi	Fungsi dan Ruang lingkup Siber
Badan Siber dan Sandi Negara	Cyber security and cryptography
Kementerian Komunikasi dan Informatika	Cyber Hygiene (penapisan konten negatif)
POLRI	Cyber crime
Kementerian Pertahanan	Cyber Defence and Cyber War
Kementerian Luar Negeri	Cyber Diplomacy
Kementerian Perdagangan	Cyber Commerce Fraud
BNPT	Cyber Terrorism
BIN	Cyber Espionage
PPATK dan KPK	Fraud Transaction Monitoring
Kemendikbud dikti	Cyber security education and culture

Sumber : www.kominfo.go.id

Dari ruang lingkup tata kelola di atas, yang akan disoroti lebih lanjut adalah bagaimana membangun sinergitas dalam menghadapi *cyber warfare*. Dalam konteks pertahanan siber, khususnya dalam menghadapi ancaman terhadap kepentingan pertahanan dan keamanan nasional, diperlukan keterlibatan institusi yang memiliki kewenangan dan kapasitas di bidang pertahanan, keamanan, intelijen, serta keamanan siber. Aktivitas tersebut mencakup upaya perlindungan, deteksi, pencegahan, dan respons terhadap berbagai ancaman di ruang siber. Dengan demikian, pembangunan kemampuan siber nasional tidak hanya berkaitan dengan aspek teknologi, tetapi juga mencakup koordinasi kelembagaan, sumber daya manusia, intelijen, dan kebijakan pertahanan.

Jika melihat model dari Inggris, mereka membentuk NCF melalui penggabungan beberapa personel institusi terkait dengan domain *cyber security and cryptography* (GCHQ), *Cyber Espionage* (MI6), *cyber defence* (MoD dan Military), *Cyber defence technology and Research* (DSTL). Dengan pengawasan langsung oleh parlemen. Hal ini dapat dianalisis melalui teori hubungan sipil-militer Huntington, khususnya mengenai kontrol sipil terhadap militer. Huntington membedakan kontrol sipil menjadi *subjective civilian control* dan *objective civilian control*. *Subjective civilian control* pada dasarnya dilakukan dengan memaksimalkan kekuasaan kelompok atau institusi sipil tertentu, sedangkan *objective civilian control* menekankan profesionalisme militer dan pembagian yang jelas antara ranah politik sipil dan profesionalisme militer (Huntington, 1981). Dalam konteks pembentukan kekuatan siber yang melibatkan unsur sipil dan militer, kedua konsep tersebut perlu dianalisis lebih lanjut untuk menentukan bentuk hubungan kelembagaan yang paling sesuai dengan sistem pertahanan dan ketatanegaraan Indonesia.

Maka jika diterapkan di Indonesia terdapat dua pilihan, apakah membentuk badan baru atau pembentukan satuan tugas permanen yang personilnya berasal dari

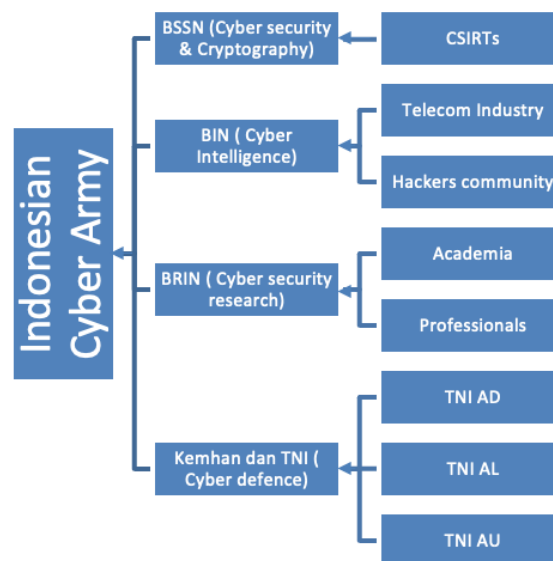
beberapa instansi terkait baik sipil dan militer dengan pelibatan empat fungsi yaitu pemerintahan sipil, militer, intelijen dan riset. Namun tentunya pelibatan pihak lain seperti industri, komunitas dan akademisi juga akan berkontribusi besar terhadap kemampuan dan daya tangkal siber Indonesia. Pada prinsipnya pembentukan “pasukan” siber ini harus bisa menjawab berbagai bentuk ancaman siber, termasuk ancaman terhadap pertahanan negara, *cyber espionage*, *cyber terrorism*, dan *cyber crime*, sesuai dengan karakter aktor, tujuan, dan kewenangan penanganannya.

Selaku penanggung jawab terkait *cyber defence* maka Kementerian Pertahanan dan TNI sebelum membentuk suatu “pasukan” siber perlu melakukan berbagai langkah dan tindakan sinergis agar kapabilitas pertahanan siber yang dibentuk mampu menghadapi berbagai ancaman siber. Untuk menciptakan sinergi dalam menghadapi perang siber, Kementerian Pertahanan perlu melakukan langkah-langkah awal sebagai berikut:

1. Kementerian Pertahanan harus mampu berkoordinasi dan memperkuat kerja sama dengan Badan Siber dan Sandi Negara (BSSN) dan Kementerian Informasi dan Komunikasi (Kemenkominfo) untuk menangkal dan mencegah potensi serangan siber menyerang *website*, informasi elektronik, jejaring sosial dan komunikasi di seluruh perbankan, organisasi, perusahaan dan pemerintah. Untuk dapat melindungi kedaulatan siber Indonesia.
2. Kementerian Pertahanan perlu membangun komunikasi dan koordinasi dengan penyelenggara telekomunikasi dan penyedia infrastruktur digital strategis untuk memperkuat pertukaran informasi mengenai potensi ancaman, kerentanan, dan gangguan terhadap infrastruktur komunikasi nasional.
3. Kementerian Pertahanan harus bekerja sama dengan organisasi keamanan, seperti Polri, BIN, BSSN, dan organisasi keamanan lainnya untuk menyatukan pandangan tentang berbagai ancaman dunia maya, seperti pemisahan tugas dan langkah penanganan terpadu sehingga dapat mencegah berbagai serangan siber di berbagai wilayah dunia siber Indonesia, termasuk manajemen kejahatan siber yang terukur hingga perang siber.
4. Kementerian Pertahanan perlu membangun mekanisme komunikasi dan kolaborasi dengan komunitas keamanan siber, praktisi keamanan informasi, peneliti keamanan, organisasi profesi, serta komunitas teknologi yang relevan untuk memperoleh masukan mengenai potensi dan perkembangan ancaman siber.
5. Kementerian Pertahanan harus menjalin kerja sama dengan berbagai perguruan tinggi yang memiliki pakar, ahli dan konsultan di bidang teknologi informasi, komunikasi dan dunia maya, untuk saling berdiskusi, berkoordinasi, tukar pengalaman dan tukar pendapat tentang berbagai ilmu, pengetahuan, inovasi, dan penemuan baru dalam teknologi dunia maya sehingga akan dapat meningkatkan keterpaduan dalam menghadapi ancaman *Cyber Warfare*.
6. Kementerian Pertahanan perlu menjalin hubungan kerja sama internasional melalui mekanisme kerja sama bilateral, tripartit, dan multilateral dengan negara-negara di dunia, mengembangkan norma dan mekanisme kerja sama internasional di ruang siber serta mendorong pencegahan konflik dan serangan siber yang dapat mengganggu hubungan antarnegara.

Dengan mempertimbangkan perspektif hubungan sipil-militer Samuel P. Huntington, pembentukan kekuatan siber di Indonesia perlu ditempatkan dalam kerangka kontrol sipil yang menjamin kejelasan kewenangan, profesionalisme, pembagian tugas, koordinasi, serta akuntabilitas antara unsur sipil dan militer. Dalam konteks pertahanan siber, keterlibatan unsur sipil dan militer tidak harus diwujudkan melalui pembentukan matra atau organisasi baru, tetapi dapat dikembangkan melalui mekanisme koordinasi dan integrasi kemampuan antar instansi sesuai dengan kewenangan masing-masing. Oleh karena itu, bentuk kelembagaan yang paling sesuai bagi Indonesia belum dapat ditentukan hanya berdasarkan konsep *subjective civilian control* atau *objective civilian control*, tetapi memerlukan kajian lebih lanjut dengan mempertimbangkan sistem ketatanegaraan, dasar hukum, struktur kelembagaan pertahanan dan keamanan, karakter ancaman siber, serta mekanisme pengawasan dan akuntabilitas.

Berdasarkan pertimbangan tersebut, model kekuatan siber Indonesia yang diusulkan dalam penelitian ini lebih tepat dipahami sebagai model konseptual kerja sama lintas institusi, bukan sebagai pembentukan matra atau organisasi militer baru. Model tersebut menempatkan unsur pemerintah sipil, militer, intelijen, keamanan siber, akademisi, dan industri dalam suatu mekanisme koordinasi yang memungkinkan pertukaran informasi, pengembangan sumber daya manusia, penelitian dan pengembangan teknologi, serta respons terhadap ancaman siber. Secara umum dapat digambarkan sebagai berikut :



Gambar 4. Model Konseptual Kerja Sama Sipil-Militer dalam Penguatan Pertahanan Siber Indonesia

Sumber : Diolah oleh Penulis

Gambar 4 menggambarkan model konseptual kerja sama lintas institusi yang melibatkan unsur sipil dan militer dalam penguatan pertahanan siber Indonesia. Model tersebut tidak dimaksudkan sebagai struktur organisasi baru, tetapi sebagai kerangka koordinasi yang dapat mengintegrasikan kemampuan pertahanan, keamanan siber, intelijen, riset, akademisi, industri, dan komunitas profesional sesuai dengan kewenangan masing-masing. Bentuk kelembagaan dan mekanisme

koordinasinya masih memerlukan kajian lebih lanjut, khususnya dari aspek hukum, pembagian kewenangan, sumber daya, dan akuntabilitas.

KESIMPULAN

Berdasarkan kajian historis dan konseptual yang dilakukan, pengalaman pemecahan komunikasi terenkripsi Jerman pada Perang Dunia II menunjukkan bahwa keunggulan informasi tidak hanya ditentukan oleh kemampuan militer, tetapi juga oleh keterlibatan berbagai keahlian dan institusi. Keterlibatan ilmuwan, ahli matematika, insinyur, analis intelijen, dan unsur militer dalam pengembangan kemampuan kriptanalisis di Inggris memperlihatkan pentingnya kolaborasi lintas bidang dalam menghadapi ancaman yang berbasis informasi. Oleh karena itu, keberhasilan pemanfaatan informasi dari Enigma lebih tepat dipahami sebagai salah satu pembelajaran mengenai pentingnya sinergi dan keunggulan intelijen dalam peperangan, bukan sebagai satu-satunya penyebab kekalahan Jerman.

Pengalaman Inggris juga menunjukkan adanya perkembangan kelembagaan dari *Government Code and Cypher School* (GC&CS) menuju *Government Communications Headquarters* (GCHQ) dan selanjutnya penguatan kemampuan melalui *National Cyber Force* (NCF). Perkembangan tersebut memperlihatkan bahwa menghadapi ancaman di ruang siber membutuhkan koordinasi antara unsur pertahanan, intelijen, keamanan siber, pemerintahan sipil, serta kemampuan penelitian dan teknologi. Dengan demikian, pembangunan kapabilitas siber tidak dapat hanya bertumpu pada satu institusi.

Dalam konteks Indonesia, model kerja sama sipil-militer dalam menghadapi ancaman siber perlu dibangun melalui integrasi fungsi pemerintahan sipil, militer, intelijen, keamanan siber, dan riset, dengan dukungan akademisi, industri, serta komunitas teknologi. Model tersebut dapat dilakukan melalui penguatan koordinasi antar instansi atau melalui pembentukan organisasi/satuan tugas lintas institusi. Namun, pilihan kelembagaan tersebut harus terlebih dahulu mempertimbangkan dasar hukum, pembagian kewenangan, mekanisme komando dan koordinasi, sumber daya manusia, pembiayaan, serta mekanisme pengawasan dan akuntabilitas.

Dengan demikian, temuan utama penelitian ini adalah bahwa penguatan pertahanan siber Indonesia lebih membutuhkan model kolaborasi lintas institusi yang terintegrasi daripada sekadar pembentukan organisasi baru. Penelitian selanjutnya perlu menguji model tersebut secara lebih mendalam, khususnya mengenai desain kelembagaan, pembagian kewenangan antara unsur sipil dan militer, mekanisme pengawasan, serta indikator efektivitas dalam menghadapi ancaman siber.

DAFTAR PUSTAKA

- Arquilla, J., & Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. RAND Corporation.
- Corera, G. (2020, November 19). *UK's National Cyber Force comes out of the shadows*. BBC News.
- Gaj, K., & Orłowski, A. (2003). *Facts and myths of Enigma: Breaking stereotypes*. Lecture Notes in Computer Science (Including Subseries Lecture Notes in

- Artificial Intelligence and Lecture Notes in Bioinformatics), 2656, 106–122.
https://doi.org/10.1007/3-540-39200-9_7
- Huntington, S. P. (1981). *The soldier and the state: The theory and politics of civil-military relations*. Belknap Press of Harvard University Press.
- Kardi, K. (2015). Demokratisasi Relasi Sipil-Militer pada Era Reformasi di Indonesia. *MASYARAKAT: Jurnal Sosiologi*, 19(2), 231–256.
<https://doi.org/10.7454/mjs.v19i2.4703>
- National Cyber Force. (2020). National Cyber Force Explainer.
- Pritchard, S. (2021, September 16). *UK armed forces confirms cyber as fifth dimension of warfare*. The Daily Swig.
- Putra, A. R. (2014). *Ideologi fasisme: Pemikiran Adolf Hitler atas konsep fasisme di Jerman* [Skripsi, Universitas Islam Negeri Syarif Hidayatullah Jakarta]. Institutional Repository UIN Syarif Hidayatullah Jakarta.
- Ramadhan, P. (2019). *Kill Hitler: Menelusuri jejak kekalahan dan kematian Hitler*. Araska.
- Robinson, P. (2008). *Dictionary of International Security*. Polity press.
- Rusfiana, Y. (2021). Aktualisasi sistem pertahanan rakyat semesta. *Jurnal Moderat*, 7(3), 483–492.
- Ryacudu, R. (2015). *Perang masa kini: Ancaman, tantangan bagi NKRI dan tuntutan menyikapinya*. The Global Review. https://www.theglobal-review.com/content_detail.php?lang=id&id=18022&type=2
- Smith, M. (1998). *Station X: The codebreakers of Bletchley Park*. Channel 4 Books.
- Sterling, C. H. (Ed.). (2008). *Military communications: From ancient times to the 21st century*. ABC-CLIO.
- Tippe, S. (2015). Relasi Sipil-Militer dalam Pemberdayaan Masyarakat Papua. *MASYARAKAT: Jurnal Sosiologi*, 19(2), 287–303.
<https://doi.org/10.7454/mjs.v19i2.4705>
- Turing, A. M. (2004). *The essential Turing*. Oxford University Press.