Melihat Kembali Sejarah Kekalahan Jerman di Perang Dunia II: Konsep Kerjasama Sipil-Militer dalam Menghadapi Ancaman Perang Siber

Yanto Manurung[1*], Prabaswari[2]
[1,2]Universitas Pertahanan Republik Indonesia, Indonesia
yasman35@outlook.com*

SEIKAT
Jurnal Ilmu Sosial, Politik dan Hukum

e-ISSN: 2964-0962

SEIKAT: Jurnal Ilmu Sosial, Politik dan Hukum

https://ejournal.45mataram.or.id/index.php/seikat

Vol. 3 No. 6 Desember 2024

Page: 515-522

Available at:

https://ejournal.45mataram.or.id/index.php/seikat/article/view/1607

DOI:

https://doi.org/10.55681/seikat.v3i6.1607

Article History:

Received: 21-12-2024

Revised: 26-12-2024

Accepted: 27-12-2024

Abstract *: This study reviews the history of the causes of Germany's defeat in World War II, one of which was the successful hacking of their cipher machine called Enigma by Alan Turing from England. Alan Turing (1938) himself was a civilian scientist who worked at the Government Code and Cypher School (GC&CS), an agency formed by the British Government which was a combination of civilian scientists, intelligence agents of the British Army and Navy (A.M. Turing, 2004). The success of the Enigma hack illustrates that the synergy between civilians (scientists who hack algorithms) and the military operating in the field can bring victory in war. This paper will examine how the concept of civil-military relations can be adopted from the victory of Britain and its allies during World War II to the modern era today, where information warfare has transformed into cyberspace. This history is an important lesson for the world, especially Indonesia, in building a reliable concept of civil and military synergy to face the threat of today's cyber war contestation. This paper adapts Huntington's theory of Civil Military Relations. Using qualitative methods with data collected through literature reviews and interviews with representatives of military and civilian institutions. So the concept of the "cyber troops" model that is considered appropriate to be applied in Indonesia is in line with Huntington's Theory, namely subjective civil control with two alternative choices, namely the formation of a new institution or a permanent task force involving four functions, namely civil, military, intelligence and research.*

Keywords *: Enigma; Information War; Cyber; Synergy*

Abstrak : Penelitian ini mengulas sejarah penyebab kekalahan Jerman pada Perang Dunia II salah satunya dikarenakan berhasil diretasnya Mesin sandi mereka yang bernama Enigma oleh Alan Turing dari Inggris. Alan Turing (1938) sendiri merupakan seorang ilmuwan sipil yang bekerja di Government Code and Cypher School" (GC&CS), suatu badan yang dibentuk Pemerintah Inggris yang merupakan gabungan antara para ilmuwan sipil, agen intelijen Angkatan Darat dan Angkatan Laut Inggris (A.M. Turing, 2004). Keberhasilan peretasan Enigma menggambarkan bahwa sinergi antara sipil (ilmuwan yang meretas algoritma) dan militer yang beroperasi di Lapangan bisa membawa kemenangan dalam perang. Dalam tulisan ini akan ditelaah bagaimana konsepsi hubungan sipil-militer yang bisa diadopsi dari peristiwa kemenangan Inggris dan sekutu pada masa Perang Dunia II sampai dengan era modern saat ini, dimana perang informasi sudah bertransformasi dalam ruang siber. Sejarah ini menjadi pembelajaran penting bagi dunia khususnya Indonesia dalam membangun konsep sinergi sipil dan militer yang handal guna menghadapi ancaman kontestasi perang siber saat ini. Paper ini mengadaptasi teori Huntington tentang Hubungan Sipil Militer. Menggunakan metode kualitatif dengan data yang dikumpulkan melalui kajian literatur dan wawancara pada perwakilan dari institusi militer dan sipil. Sehingga konsep model "pasukan siber" yang dianggap sesuai untuk diterapkan di Indonesia adalah sejalan dengan Teori Huntington yaitu kontrol sipil subyektif dengan dua alternatif pilihan yaitu pembentukan lembaga baru atau satuan tugas permanen dengan pelibatan empat fungsi yaitu sipil, militer, intelijen dan riset.

Kata Kunci : Enigma; Perang Informasi; Siber; Sinergi

PENDAHULUAN

Penelitian dilatarbelakangi oleh peristiwa kekalahan Jerman pada Perang Dunia II. Pada Masa Perang Dunia II, Jerman merupakan salah satu kekuatan yang nyaris tidak dapat dikalahkan di bawah kekuasaan Adolf Hitler, meskipun pada saat itu Jerman "dikeroyok" oleh banyak negara besar seperti Rusia, Inggris, Perancis, Amerika, dan negara lainnya yang tergabung dalam sekutu. Faktor utama, yang paling mempengaruhi dalam setiap kemenangan Jerman adalah karena penguasaan teknologi militer yang mumpuni seperti senapan mesin, pesawat tempur bermesin jet (Me-163 dan Me-262), tank, mortar dan senjata modern lainnya(Putra, 2014). Selain itu salah satu teknologi penciptaan Jerman yang paling fenomenal dan berjasa dalam mengirimkan instruksi perang adalah Mesin sandi Enigma (Gambar 1). Dengan adanya mesin sandi Enigma secara otomatis pihak lawan Jerman, tidak dapat melakukan intelijen terhadap informasi terkait serangan Jerman dikarenakan informasi yang didapatkan tidak bisa dibaca karena tersandi oleh mesin sandi Enigma. Mesin ini menjadi mesin komunikasi utama yang digunakan sepanjang Perang Dunia II oleh Jerman(Schmidt & Code, 2001).

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 (Prasetya Ramadhan, 2019).

Pengungkapan mesin sandi Enigma oleh pihak Inggris yaitu Alan Turing, menjadi faktor kunci kekalahan Jerman, sebab dengan pecahnya sandi Enigma, maka pesan tersandi Jerman yang berisi strategi dan operasional taktis dapat dibuka hanya dalam waktu 20 menit (Gaj & Orlowski, 2003). Hal ini mengakibatkan Perang Dunia II ini bisa lebih cepat selesai, dengan kalahnya Jerman dari sekutu.

Kemampuan Alan Turing memecahkan sandi Enigma dengan menggunakan sistem komputasi menjadikan mesin ini sebagai cikal bakal komputer modern digital sehingga ia dijuluki sebagai Bapak Ilmu Komputer dan Artificial Intelligence(Gaj & Orlowski, 2003). Kejadian ini menjadi titik penting bahwa peretasan informasi menjadi ancaman yang serius dalam persaingan dua negara. Pihak yang mampu menguasai informasi tentunya akan lebih unggul dan akan dengan mudah memenangkan pertempuran. Pada masa abad 21 ini tentunya peperangan juga mengalami transformasi, begitu pula upaya peretasan informasi yang pada awalnya dilakukan dengan sistem komputasi sederhana bertransformasi menjadi perang siber.

Menteri Pertahanan Ryamizard mengatakan dalam forum diskusi terbatas yang diselenggarakan oleh Global Futures Institute (Pranoto, 2015), bahwa perang generasi keempat juga dikenal sebagai perang asimetris dengan menghancurkan sistem di negara target. 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 sejarah Perang Dunia II, militer Amerika merekrut Alan Turing seorang ilmuwan sipil untuk membantu memecahkan kode sandi Enigma. Sehingga diharapkan Indonesia juga dapat memaksimalkan Sinergi antara Sipil dan Militer dalam menghadapi ancaman perang siber. Penelitian ini akan mencoba menjawab pertanyaan utama yaitu bagaimana model kolaborasi sipil – militer yang sesuai dalam rangka menghadapi ancaman perang siber?

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 dan wawancara pada perwakilan dari institusi militer dan sipil. Hasil akhir rekomendasi berupa kerangka kolaborasi sipil militer yang bisa digunakan dalam menghadapi perang siber modern.

METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif untuk meneliti buku dan artikel-artikel yang telah dipublikasikan di jurnal nasional dan internasional yang berkaitan dengan sejarah Perang Dunia II dan konsep hubungan sipil-militer. Dalam meneliti sejarah Perang Dunia II, peneliti menggunakan metode sejarah yang terdiri dari empat tahapan yaitu heuristik (pengumpulan sumber) baik dari buku, jurnal, situs dan sebagainya. Kemudian dilakukan verifikasi dengan menyaring sumber sejarah hingga valid dan berkualitas. Kemudian interpretasi untuk menganalisis dan menafsirkan suatu peristiwa sejarah dengan jelas beserta dampaknya di masa depan. Dan yang terkahir adalah historiografi atau proses penulisan dari sumber yang ditemukan dan terverifikasi (Hidayat et al., 2020).

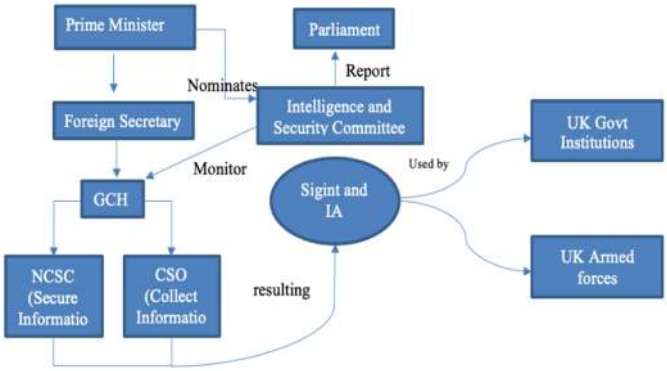
Penelitian ini juga bersifat deskriptif untuk menjelaskan pengertian dan hakikat perang siber serta solusi bagi masyarakat Indonesia dalam menyikapi perang siber. Kajian ini merupakan kajian orisinal yang berkaitan dengan isu perang siber, oleh karena itu kajian ini merupakan kajian konseptual. Metode pengumpulan data melalui studi literatur dari penelitian terdahulu, *focus group discussion* dan wawancara mendalam. Pembelajaran dari penelitian ini berkaitan dengan pengertian dan bentuk perang siber serta solusi yang dapat dilakukan negara Indonesia dalam menghadapi ancaman perang siber. Penelitian ini diharapkan dapat memecah kebingungan kita dalam menjelaskan perang siber, juga membantu semua pihak untuk lebih memahami bentuk-bentuk ancaman atau tantangan perang siber dan alternatif ide-ide yang dapat digunakan sebagai jawaban atas solusi melalui sinergitas sipil-militer.

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. Pada saat Perang Dunia II (1930) GC&CS bekerja untuk membuka kode militer musuh potensial mereka khususnya mesin sandi Enigma milik Jerman. Pada masa ini GC&CS beranggotakan tidak hanya militer tetapi juga matematikawan, insinyur, ahli bahasa dan staf pendukung sejumlah lebih dari 10.000 orang yang diisolasi di Bletchley Park. Mereka berhasil melakukan penetrasi terhadap komunikasi diplomatik dan sandi militer musuh serta membangun komputer digital pertama (Christopher H. 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. Direktur saat ini diampu oleh Sir Jeremy Fleeming, yang merupakan seorang sipil. GCHQ bertanggung jawab langsung Sekretaris Luar Negeri di bawah Perdana Menteri. 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, Michael (1998). *Station X*. Channel 4 books. p. 176. ISBN 0-330-41929-3). 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

Cyber Sebagai Dimensi Perang Kelima Inggris

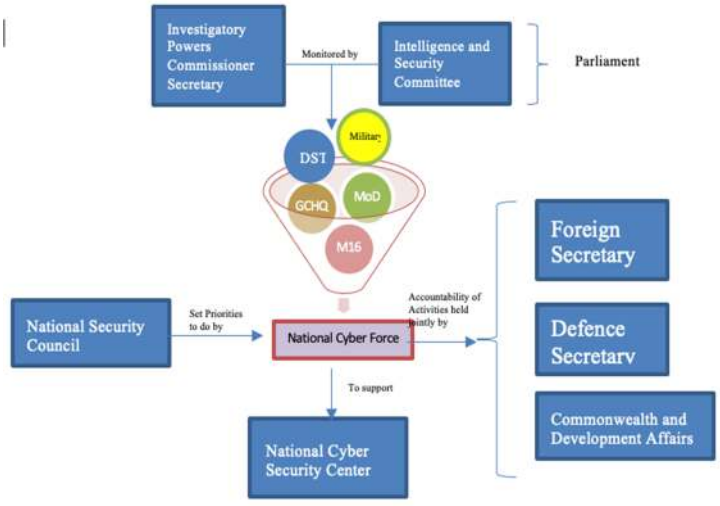
Menghadapi era digitalisasi saat ini, UK tengah bersiap melakukan investasi dalam peningkatan kapabilitas dan keterampilan siber bagi para pemimpin militernya (Swig, 2021). Status siber sebagai domain kelima selain laut, darat, udara dan ruang angkasa, memaksa pasukan militer mengubah operasional mereka. Perubahan ini meliputi perlindungan komunikasi digital, melalui penguatan kemampuan menyerang dan bertahan di ranah siber.

Militer Inggris, bersama dengan negara NATO lainnya, berinvestasi untuk sistem robotik dan autonomous, artificial intelligence, pelatihan berbasis komputer atau sintetik dan Military IoT. Perubahan ini tentunya harus diimbangi dengan kemampuan personel. Hal ini membuat proses rekrutmen generasi selanjutnya akan lebih dititikberatkan pada keterampilan teknologi siber jika dibanding sebelumnya. Sebab diharapkan militer dimasa depan akan memiliki kemampuan mengoperasikan seluruh lima domain perang. Salah satu keterampilan yang diharapkan adalah kemampuan programming, juga kemampuan lain yang setara dengan ilmuwan komputer, data engineer dan operator siber.

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 kerjasama antara pertahanan dan intelijen telah dibentuk, badan ini beranggotakan anggota dari kementerian pertahanan (MoD), angkatan bersenjata, GCHQ, M16 (Secret Intelligence Service) serta Laboratorium Ilmu dan Teknologi Pertahanan (DSTL) (corera, 2020 : https://www.bbc.com/news/technology-55007946) dengan tugas utama National Offensive Cyber Program yaitu perlawanan terhadap ancaman teroris, kriminal dan musuh negara. Pasukan M16 akan bekerja bersama GCHQ dan militer. 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 secretaray 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

Sinergitas Menghadapi *Cyber Warfare*

Melihat langkah strategis yang diambil oleh UK dalam membentuk National Cyber Force, dimana cyber sudah diresmikan sebagai matra kelima. Maka Indonesia tentunya juga perlu menyiapkan diri untuk mengantisipasi adanya ancaman Cyber Warfare. Sebenarnya, saat ini Indonesia sudah memiliki beberapa institusi maupun fungsi di instansi pemerintah baik sipil dan militer yang berkaitan dengan tata kelola ruang siber diantaranya 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)

Nama Lembaga/Unit Institusi	Fungsi dan Ruang lingkup Siber
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. Tentunya dalam konteks pertahanan siber yang bersifat offensive, maka institusi yang akan terlibat adalah institusi yang terkait dengan bidang pertahanan. Dimana dalam cyber defense dan cyber war yang menjadi fokus adalah kekuatan negara dalam menghadapi berbagai ancaman baik yang berasal dari dalam dan luar negeri di ruang siber. Sifat dari kegiatan ini akan mirip dengan aktivitas militer yang selalu siap sedia dan siaga baik dalam kondisi damai maupun perang. Kata kunci yang menjadi komponen dalam sub sistem ini adalah *cyber attack, cyber weapon, cyber espionage, cyber territory, cyber army*, dsb (Indrajit, 2021).

Jika melihat model dari Inggris, mereka membentuk NCF melalui penggabungan beberapa personel institusi terkait dengan domain cyber security and cryptography (GCHQ), Cyber Espionage (M16), cyber defence (MoD dan Military), Cyber defence technology and Research (DSTL). Dengan pengawasan langsung oleh parlemen. Hal ini sejalan dengan Teori Huntington bahwa kontrol sipil yang dianggap paling mungkin diterapkan adalah kontrol sipil subyektif, karena dilakukan dengan memperkuat kekuasaan kelompok sipil melalui penguatan institusi sipil tertentu misalnya parlemen atau presiden, konstitusi negara maupun penguatan kelompok sipil seperti pengusaha atau birokrat (Huntington, 2000).

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 tantangan ancaman Cyber war termasuk didalamnya cyber terrorism dan juga cyber crime yang mengganggu stabilitas dan keamanan nasional, sehingga diperlukan dukungan dari berbagai pihak yang bersifat semesta di ruang siber untuk menjaga kedaulatan NKRI di ruang siber.

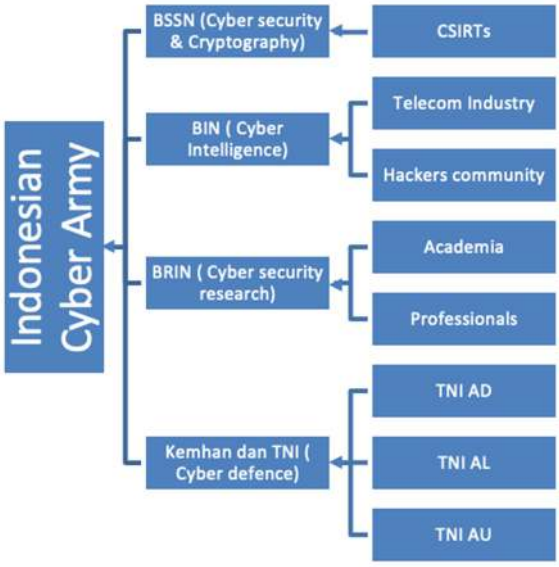
Selaku penanggung jawab terkait cyber defence maka Kementerian Pertahanan dan TNI sebelum membentuk suatu "pasukan" siber perlu melakukan berbagai langkah dan tindakan sinergis agar matra yang dibentuk mampu mengatasi segala ancaman cyberwar. Untuk menciptakan sinergi dalam menghadapi perang siber, Kementerian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

1. Kementerian Pertahanan harus harus mampu berkoordinasi dan memperkuat kerja sama dengan Badan Siber dan Sandi Negara (BSSN) dan Kementerian Informasi dan Komunikasi (Kemenkominfo) untuk menangkal, mencegah 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 harus menjalin komunikasi, koordinasi dan kerjasama dengan komunitas pelaku informasi dan komunikasi, seperti berbagai operator telepon, seperti Telkom, Indosat dan Excelcomindo, untuk memprediksi serangan siber berupa penyadapan yang biasa dilakukan oleh jaringan. penyerang agar keamanan telepon masyarakat Indonesia khususnya para pimpinan lembaga negara dapat terjamin dengan baik.
3. Kementeriaan 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 harus mampu memberdayakan komunitas hacker, komunitas jailbreak, komunitas blogging, komunitas media sosial, dan berbagai komunitas berita dan dunia maya lainnya untuk tetap terlibat dan memberikan informasi kepada Kementerian Pertahanan tentang berbagai potensi dunia maya. ancaman dan bertukar informasi tentang langkah-langkah yang akan diambil dalam menanggapi berbagai serangan siber yang membahayakan kedaulatan siber Indonesia.
5. Kementerian Pertahanan harus menjalin kerjasama 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 regulasi di dunia maya, menciptakan etika di antariksa, berjejaring dan mencegah saling menyerang antar negara di dunia maya, yang mau tidak mau akan merusak hubungan antarnegara.

Dari langkah-langkah di atas, diharapkan akan terbentuk suatu "pasukan" siber yang ideal dan mampu menjawab tantangan cyber warfare. Konsep Hubungan Sipil Milter sebagai jawaban kebutuhan matra siber, nampaknya menjadi kebutuhan mutlak dengan menimbang kemampuan TIK mumpuni yang kebanyakan dimiliki oleh organisasi sipil. Sehingga bentuk "pasukan" yang dianggap sesuai adalah yang sejalan dengan Teori Huntington yaitu kontrol sipil subyektif dengan bentuk konstitusional yang dibangun oleh sistem demokrasi melalui penguatan institusi sipil. Secara umum dapat digambarkan sebagai berikut :



Gambar 4. Konsep HSM Pada Pembentukan Indonesian Cyber Army

Sumber : Diolah oleh Penulis

Terlihat dari gambar 4, bahwa bentuk "pasukan" siber yang diusulkan terdiri dari beragam elemen baik dari sipil maupun militer. Selain itu pembentukan pasukan siber ini disesuaikan dengan kebutuhan negara apakah memerlukan bentuk pasukan siber yang permanen dalam bentuk badan struktural ataukah bersifat *ad hoc* dalam jangka waktu panjang yang ditentukan, sama awalnya dengan konsep pembentukan awal KPK. Tentunya hal ini memerlukan pertimbangan lebih lanjut baik dari segi yuridis maupun dari susut pandang kemampuan anggaran negara.

KESIMPULAN DAN SARAN

A. Kesimpulan

Saat ini dunia global sudah menyadari pentingnya peran "pasukan siber" untuk menghalau serangan siber yang mengancam infrastruktur vital negara dan juga melakukan perlawanan sebagai upaya pertahanan. Pembentukan pasukan siber Indonesia menggunakan teori Huntington akan melibatkan Hubungan sipil militer dari empat fungsi berbeda yaitu intelijen, keamanan siber, pertahanan siber dan riset sebagaimana yang dilakukan oleh Inggris. Inggris sendiri telah menyadari pentingnya peran pasukan peretas informasi sejak masa Perang Dunia II khususnya pada peristiwa pecahnya kode mesin sandi Enigma oleh Alan Turing. Sinergi sipil-militer yang sudah terbentuk sejak perang dunia II ini menunjukkan bahwa hal ini menjadi elemen kunci dalam pemenangan perang dan pertahanan suatu negara. Oleh karena itu, sinergi dalam menghadapi ancaman cyberwar sangat penting dan diperlukan bagi Indonesia. Kementerian Pertahanan harus mampu mendorong komunikasi, koordinasi, jaringan, dan jaringan kerja sama teknis untuk membentuk pasukan pertahanan siber yang mampu mempertahankan, mendeteksi, menangkis, dan mencegah serangan, potensi serangan ancaman perang siber secara dini.

B. Saran

Hasil penelitian ini berhasil memberikan konsep awal hubungan sipil-militer yang bisa digunakan dalam pembentukan pasukan siber Indonesia. Perlu dilakukan penelitian lanjutan untuk lebih mematangkan konsep pasukan siber yang telah disusun, pada penelitian ini opsi alternatif masih diberikan dalam dua pilihan yaitu pembentukan pasukan siber dalam bentuk kelembagaan/ organisasi baru dalam arti pemerintah membentuk struktur baru atau dalam bentuk *ad hoc* dalam jangka waktu panjang yang ditentukan. Sehingga masih perlu didalami bentuk mana yang lebih sesuai untuk diterapkan. Disamping itu rincian tugas dari masing-masing fungsi juga perlu dijelaskan antara kewenangan dari pihak sipil dan militer yang tergabung dalam pasukan siber, sehingga bisa menjadi rekomendasi yang lebih matang bagi para pengambil keputusan.

DAFTAR PUSTAKA

Gaj, K., & Orlowski, 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

Hidayat, A. A., Arifin, F., Dais, T. R., & Wahyuni, E. S. (2020). Dari Orang Belanda Sampai Elit Bumiputera: Kajian Sejarah Freemasonry di Kota Cirebon 1900-1942. *Agastya: Jurnal Sejarah Dan Pembelajarannya, 10*(2), 145. https://doi.org/10.25273/ajsp.v10i2.5402

Huntington, S. P. (1981). *The Soldier and The State*. Belknap Press.

John Arquilla, D. R. (2001). *Networks and Netwars : The Future of Terror, Crime, and Military*. Rand Corporation.

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.

Pranoto, A. (2015, March 30). No Title. The Global Review.

Prasetya Ramadhan. (2019). *Kill Hitler : Menelusuri Jejak Kekalahan dan Kematian Hitler*. Araska.

Putra, A. R. (2014). Ideologi fasisme (pemikiran adolf hitler atas konsep fasisme di jerman). 16–20.

Robinson, P. (2008). *Dictionary of International Security*. Polity press.

Rusfiana, Y. (2021). Aktualisasi sistem pertahanan rakyat semesta. *Jurnal Moderat, 7*(3), 483–492.

Schmidt, T., & Code, G. (2001). Breaking Germany ' s Enigma Code.

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.