ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

FAKTOR PENYEBAB PENGEMBANGAN SIBER DI INDONESIA PADA ERA PEMERINTAHAN JOKOWI TAHAP I

Muhammad Rangsang Agung
Program Studi Pasca Sarjana Ilmu Hubungan Internasional, Universitas Indonesia
Korespondensi* : muhammad.rangsang@ui.ac.id

ABSTRACT
Indonesia's commitment in carrying out Revolution Military Affairs (Revolusi Krida Yudha) *– which is mandated through the Defense Minister Regulation No. 19/2012 – slows down during President Joko Widodo's first term administration as the government tightens budget for cyber defense. From regional context, this issue is anomalous given Indonesian relative political and economic prowess. This paper aims at identifying those challenges that hinder the military revolution. This article uses qualitative analysis method and the sources of military change introduced by Theo Farrell & Terry Terriff, of which explains how cultural, political and technological aspects might become the cause of changes in military. Through such analyses, this paper finds how those aspects are behind the difficulties in transforming Indonesian military. As such, related stakeholders need to apply concrete actions to solve the obstacles that deter the development of cyber security in the context of Revolution Military Affairs in the future*

Keywords: *Revolution Military Affairs, Cyber Defense, Military Change, Cyber Security*

ABSTRAK
Komitmen di dalam melakukan *Revolution Military Affairs* (Revolusi Krida Yudha) yang dicanangkan pada Peraturan Menteri Pertahanan Nomor 19 Tahun 2012 terkendala dengan pengetatan anggaran pertahanan siber di era pemerintahan Joko Widodo tahap I. Dalam hal ini, terdapat paradoks ketika melihat bahwa hal ini berlangsung di Indonesia yang memiliki pengaruh politik dan kemampuan ekonomi yang signifikan dibanding negara-negara ASEAN lainnya. Tulisan ini bermaksud mengkaji faktor-faktor yang menjadi kendala upaya revolusi militer tersebut. Dalam menganalisis kendala tersebut, penulis menggunakan analisis kualitatif dan teori sumber perubahan militer dari *Theo Farrell & Terry Terriff* yang menjelaskan bahwa aspek kultural, politik dan teknologi menjadi penyebab munculnya perubahan militer. Hasil analisis menunjukkan bahwa permasalahan di bidang-bidang tersebut menjadi faktor-faktor di balik kendala di dalam proses perubahan militer di Indonesia. Dengan demikian, dibutuhkan langkah-langkah kongkrit dari setiap pemangku kepentingan terkait untuk mengatasi permasalahan pengembangan *cyber security* dalam konteks *Revolution Military Affairs* kedepannya.

Kata Kunci: Revolusi Krida Yudha, Pertahanan Siber, Perubahan Militer, Keamanan Siber

PENDAHULUAN

Di dalam studi Hubungan Internasional pasca-Perang Dingin,

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

terdapat perubahan pola pergeseran ancaman dari ancaman tradisional ke ancaman non-tradisional. Ancaman *state centric* dari konsep negara-bangsa yang dipetakan dalam perjanjian Westphalia tidak lagi menjadi satu-satunya permasalahan bagi negara-negara di dunia. Ancaman tradisional yang masih terkait dengan sekat batas negara kini berdampingan dengan permasalahan modern yang menjadi ancaman lintas batas negara. Isu seperti terorisme, kesehatan, lingkungan, perdagangan orang, hingga terorisme siber mencuat pasca-Perang Dingin.

Ancaman terorisme siber, sebagai salah satu ancaman non-tradisional, merupakan permasalahan serius yang harus dihadapi negara-negara dunia. Pada tahun 2014, *World Economic Forum* (WEF) mengeluarkan laporan yang mengatakan bahwa ancaman siber adalah tantangan global nomor empat terbesar di dunia, setelah perubahan iklim, pengangguran, ketidakadilan dan kemiskinan (Forum, 2014). Hal ini merupakan akibat dari begitu banyaknya serangan siber yang sudah terjadi dalam lingkup global. Serangan kelompok teroris etnik Tamill – yang mengirim 800 email setiap hari selama dua minggu ke kedutaan Sri Lanka – menjadi salah satu contoh nyata bentuk terorisme siber (Denning, 2000). Sementara itu, pada tahun 2013, *The New York Times* melaporkan mengenai serangkaian serangan siber terhadap institusi keuangan AS (Perlroth & Sanger, 2013). Tidak hanya itu, Kane Gamble, seorang *hacker* dari Inggris, dihukum 2 tahun penjara pada tahun 2018 setelah berhasil membobol informasi rahasia CIA (Dixon, 2018).

Ancaman siber tidak hanya terjadi di luar negeri, tetapi juga di Indonesia. Salah satunya adalah peristiwa penyadapan Indonesia oleh pemerintah Australia yang dibongkar oleh mantan staf *National Security Agency*, Edward Snowden. Selain itu, pimpinan tertinggi kepolisian Indonesia, Jendral Tito Karnavian, mengatakan bahwa ancaman terorisme sudah banyak beralih menjadi *cyber terrorism* dan *cyber jihad* (Kominfo, 2016a). Rekrutmen, pelatihan, hingga tutorial pembuatan bom kini banya dilakukan secara virtual. Lebih jauh lagi, kondisi mengancam tersebut membuat *Akamai Technologies*, sebuah perusahaan survey Amerika Serikat, menempatkan Indonesia sebagai negara terentan nomor 3 dunia untuk serangan siber (Parameswaran, 2015). BSSN, dikutip oleh media internasional, secara tidak langsung mengamini hal ini dengan

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

menyatakan bahwa terdapat peningkatan serangan siber sejumlah 98 juta pada tahun 2019, dibanding "hanya" sejumlah 12 juta pada tahun 2018 (Hutton, 2020).

Pada tahun 2012, pemerintah Indonesia sebenarnya sudah berupaya untuk mengantisipasi hal ini melalui program Kekuatan Minimum Esensial *(Minimum Essential Force/MEF)*. Sesuai yang digariskan Peraturan Menteri Pertahanan Nomor 19 Tahun 2012, penyelarasan MEF diharapkan dapat memberi perhatian untuk ancaman siber di Indonesia (Kementerian Pertahanan RI, 2012). Hal ini menjadi salah satu bagian di dalam perubahan Revolusi Krida Yudha, atau *Revolution in Military Affairs* (RMA), di dalam tubuh kemiliteran Indonesia (Miles & Huberman, 1992). Revolusi ini ditargetkan akan selesai pada tahun 2024 nanti (Kementerian Pertahanan RI, 2012).

Namun demikian, keseriusan pemerintah Indonesia di dalam melakukan pengembangan RMA dan pertahanan siber dipertanyakan dengan adanya pengetatan anggaran. Sebuah laporan dari AT Kierney menyebutkan bahwa Singapura adalah negara dengan persentase anggaran pertahanan siber terbesar di ASEAN dengan jumlah 0.22 persen dari GDP nya di tahun 2017 (Brandon, 2018). Malaysia adalah negara kedua dengan jumlah 0.08 persen dari GDP. Sementara itu, pada tahun tersebut Indonesia dan negara-negara lainnya hanya menginvestasikan kurang dari 0.04 persen dari GDP masing-masing negara tersebut (Brandon, 2018). Hal ini menjadi ironis karena, menurut lembaga riset pasar e-Marketer, populasi pengguna internet di Indonesia mencapai 83,7 juta orang pada 2014 (Kominfo, 2014). Angka ini menempatkan Indonesia di peringkat ke-6 terbesar di dunia dalam hal jumlah pengguna internet.

Berdasarkan paradoks tersebut, tulisan ini melihat adanya kemunduran dalam pengembangan keamanan siber pada Rezim Presiden Joko Widodo, terutama ketika dikaitkan dengan pengaruh politik dan kemampuan ekonomi Indonesia yang signifikan dibanding negara-negara ASEAN lainnya. Indonesia adalah negara besar yang memiliki sumber daya alam dan manusia yang besar, akan tetapi terlihat tertinggal dibanding negara-negara ASEAN lain untuk urusan inisiatif perkembangan pertahanan terorisme siber.

Adapun, penulis telah mengelompokkan penelitian-penelitian sebelumnya terkait dengan pengembangan keamanan siber menjadi dua kategori, yaitu kategorisasi pengembangan

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

keamanan siber di negara asing dan di negara Indonesia. Semua penelitian tersebut berbentuk kajian kualitatif. Penelitian-penelitian dengan kategorisasi pengembangan siber di negara asing (Baumard, 2017; Cheng et al., 2014; Schallbruch & Skierka, 2018; Tabansky & Israel, 2015) memiliki dua sintesis argumen diantaranya adalah : (1) pengaturan keamanan siber sangat fundamental di dalam pengelolaan suatu negara dikarenakan hal tersebut terkait infrastruktur yang penting, serta (2) lahirnya teknologi baru berbentuk *advanced persistent threats (APTs)* yang mengancam suatu negara membutuhkan *grand strategy* untuk menjamin keamanan siber dan perlindungan privasi masyarakat.

Lebih lanjut lagi, penelitian dengan kategorisasi pengembangan keamanan siber di negara Indonesia (Chotimah et al., 2019; Islami, 2017; Primawanti & Pangestu, 2020; Rizal & Yani, 2016) memiliki dua argumen sintesis, yaitu : (1) keadaan *Cybersecurity* indonesia masih memiliki banyak celah, sehingga membutuhkan formulasi dan implementasi strategi yang mapan untuk keamanan siber, serta (2) Kebutuhan untuk menerapkan *military confidence building* demi penegakkan ketahanan nasional di ruang siber. Berdasarkan tinjauan pustaka yang penulis lakukan, dapat dilihat bahwa tidak terdapat penelitian yang membahas mengenai pengaturan keamanan siber di era pemerintahan Joko Widodo tahap I dengan menggunakan perspektif perubahan *Revolution Military Affairs* (RMA). Dengan demikian, hal tersebut menjadi celah penelitian yang menjadi dasar di balik penulisan artikel ini,

Dalam hal ini, tulisan ini terbagi menjadi empat bagian, yaitu bagian pendahuluan, metode, hasil dan pembahasan, serta bagian simpulan. Kerangka analisa penulis tulis di bagian hasil dan pembahasan.

METODE

Penelitian ini bertujuan untuk mengkaji faktor-faktor yang menjadi penyebab dari pengembangan siber di era pemerintahan Joko Widodo Tahap I. Untuk mencapai tujuan tersebut, tulisan ini akan menggunakan teori sumber perubahan militer milik Theo Farrell & Terry Terriff sebagai pisau analisa yang akan ditelaah dengan menggunakan metode analisis kualitatif dengan pendekatan deskriptif.

Menurut Winartha, metode analisis kualitatif deskriptif bertujuan untuk membuat deskripsi, gambaran atau lukisan secara sistematis, faktual dan akurat

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

mengenai fakta-fakta, sifat-sifat serta hubungan antar fenomena yang diselidiki (Winartha, 2006). Sementara itu, menurut Nazir, pendekatan penelitian deskriptif adalah penelitian yang berusaha memberikan gambaran mengenai suatu keadaan tanpa adanya perlakuan langsung terhadap obyek penelitian (Nazir, 2005). Dalam hal ini, peneliti berusaha memberikan gambaran atas kondisi yang menjadi penyebab dari pengamanan siber di Indonesia dengan sejernih mungkin.

Data yang digunakan dalam tulisan ini merupakan data sekunder yang diperoleh dari buku, jurnal, media daring, serta laman resmi pemerintah, melalui laman Kementerian Pertahanan, KPU dan Kominfo, yang didapatkan secara daring. Dalam konteks ini, teknik pengumpulan data yang penulis gunakan diantaranya adalah melalui studi kepustakaan serta pengumpulan data dari media *online*. Setelah itu, data sekunder yang penulis dapatkan akan dianalisis melalui teknik triangulasi data. Data sekunder merupakan data yang didapatkan melalui sumber tidak langsung sehingga perlu dicocokkan dengan data primer. Teknik triangulasi memperbandingkan kedua data tersebut untuk membuat penelitian ini menjadi lebih ilmiah.

HASIL DAN PEMBAHASAN

Sumber Perubahan Militer

Menurut Hammes, di dalam konteks perubahan *Revolution Military Affairs* (RMA), persenjataan manusia sudah masuk ke dalam revolusi generasi keempat. Karakteristik dari revolusi persenjataan generasi keempat adalah penggunaan jaringan politik, ekonomi, sosial dan militer untuk meyakinkan para pembuat keputusan dari pihak musuh bahwa tujuan strategis mereka sulit untuk tercapai (Hammes, 2005). Perang dilakukan dengan melibatkan media global yang akan menimbulkan keunggulan strategis ataupun taktis terhadap lawan. Selain itu, perang sudah menggunakan segala jejaring yang tersedia, termasuk jejaring berbasis IT untuk mengalahkan lawan. Oleh karena itu, jejaring pertahanan siber berbasis IT menjadi penting di dalam RMA generasi keempat.

RMA, atau dalam konteks Indonesia dikenal dengan sebutan Revolusi Krida Yudha, adalah suatu topik yang telah banyak dibahas oleh para pemikir di dalam ilmu militer. Colin Gray di dalam buku "*Strategy for Chaos*" menyebutkan bahwa Revolusi Krida Yudha memiliki model sembilan langkah (Gray, 2002). Steven Metz dan James

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

Kievit di dalam buku "*Pattern of Military Revolutions"* juga menjelaskan mengenai lima langkah di dalam RMA (Metz & James, 1995). Adapun, Richard Hundley menjelaskan mengenai empat langkah di dalam fase pembentukan Revolusi Urusan Militer (Hundley, 1999). Tulisan-tulisan tersebut membahas secara cukup komprehensif proses perubahan RMA suatu negara dilihat dari perspektif yang berbeda-beda.

Berbeda dengan tulisan-tulisan para pemikir militer lainnya, Theo Farrell & Terry Terriff memiliki teori tersendiri terhadap sumber perubahan militer atau dalam RMA. Teori yang akan dipakai di tulisan ini tersebut menjadi unik dibandingkan teori-teori lainnya karena dikaitkan dengan aspek kultural. Salah satu aspek ini, menurut tulisan ini, menjadi cocok untuk dipakai dalam hal meneropong situasi di Indonesia, dikarenakan kekentalan budaya militer di Indonesia.

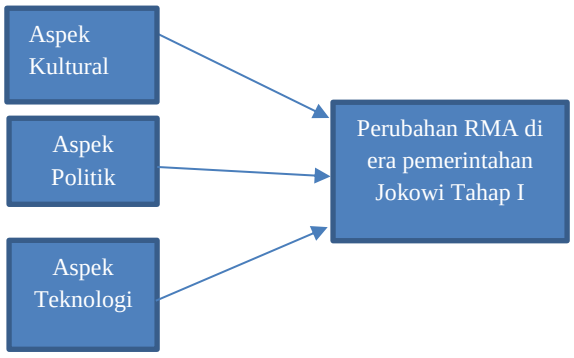
Indonesia menjalani pemerintahan yang bersifat otoriter dari militer selama selama tiga dekade pada saat rezim Orde Baru, ketika Indonesia dipimpin Soeharto selama 32 tahun. Walaupun periode tersebut sudah berakhir, hingga kini masih banyak jabatan strategis di kementerian-kementerian yang diampu oleh kalangan militer. Kondisi ini juga yang pada akhirnya membedakan Indonesia sebagai negara demokratis, dengan berbagai negara lainnya yang menganut sistem yang serupa.

Secara garis besar, Farrel dan Terriff beranggapan bahwa sumber perubahan militer didasari oleh tiga aspek, yaitu, **kultural, politik** dan **teknologi** (Farrell & Terriff, 2002). Dalam hal ini, **aspek kultural** terkait dengan kepercayaan intersubjektif yang berpengaruh terhadap aktor, situasi, dan tindakan mereka. Norma, serta kebudayaan tersebut bersifat intersubjektif karena berakar dan direproduksi melalui praktik sosial. Sementara itu, **aspek politik** dan **strategi** terkait dengan kepemimpinan politik di dalam menentukan strategi untuk menghadapi perubahan tantangan dan ancaman. Hal ini membutuhkan *political will* yang dibentuk oleh proses politik di dalam organisasi pemerintahan. Adapun, **aspek teknologi** terkait dengan pengembangan penelitian di dalam teknologi persenjataan militer suatu negara. Hal ini dipengaruhi oleh perkembangan yang dilakukan oleh para peneliti, yang diperkuat oleh jaringan sosial yang kuat. Model analisa teori

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

Sumber Perubahan Militer dapat dilihat pada Tabel I, sebagai berikut :

Tabel I Sumber Perubahan Militer



Aspek Kultural

Doktrin perang Indonesia adalah sistem pertahanan semesta yang mengandalkan pada pertahanan diri, mobilisasi nasional dan strategi militer *hybrid* dari persenjataan konvensional dan strategi gerilya. Doktrin ini adalah upaya pragmatik yang berdasarkan pada realita bahwa persenjataan Indonesia hanya cukup untuk model strategi gerilya dan konvensional (Indonesia, 2002). Taktik dan doktrin ini sudah mengakar dan menjadi budaya di TNI semenjak 1945 yang menjadi *mindset* TNI selama bertahun-tahun.

Budaya yang mengakar selama bertahun-tahun ini, menurut Dr. Hasyim Gaitama, berimplikasi kepada rendahnya *awareness*, atau kesadaran, terhadap adanya ancaman *cyber* attack internasional yang dapat melumpuhkan infrastrukur vital suatu negara (Ardiyanti, 2014). Walaupun begitu, TNI sudah mengupayakan berbagai kerja sama berbasis *capacity building* di bidanng Teknologi Informasi dengan Institut Teknologi Del (IT Del) selama tiga tahun, dari tahun 2014 sampai 2017. Ketiga program itu antara lain: penyiapan model perang *cyber*, seminar *military cyber intelligence* and *cyber operation*, serta *cyber camp* atau pekan *cyber* (Ardiyanti, 2014, p. 101).

Akan tetapi, upaya tersebut tentu saja tidak semerta-merta langsung dapat merubah secara langsung budaya TNI menjadi lebih professional. Munculnya wacana pelibatan perwira TNI untuk bertugas di institusi sipil dianggap sebagai langkah mundur upaya reformasi tubuh TNI (JPNN, 2019). Direktur organisasi hak asasi manusia Imparsial, Al Araf, menganggap bahwa TNI seharusnya lebih berkonsentrasi kepada reorganisasi tubuh TNI di dalam menghadapi ancaman terorisme siber. Hal ini, menurut dia, seharusnya dilakukan melihat kecenderungan restrukturisasi organisasi-organisasi militer dunia internasional.

Aspek Politik

Visi Presiden Indonesia terkait pertahanan Indonesia adalah Poros

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

Maritim dan Nawacita. Cita-cita Poros Maritim Dunia sejak tahun 2014 meliputi pembangunan proses maritim dari aspek infrastruktur, politik, sosial-budaya, hukum, keamanan,dan ekonomi. Penegakkan kedaulatan wilayah laut NKRI, revitalisasi sektor-sektor ekonomi kelautan, penguatan dan pengembangan konektivitas maritim, rehabilitasi kerusakan lingkungan dan konservasi *biodiversity*, serta peningkatan kualitas dan kuantitas SDM kelautan, merupakan program-program utama dalam upaya mewujudkan Indonesia sebagai poros maritim dunia (Kominfo, 2016b). Lima poros maritim tersebut dapat dilihat sebagai berikut; *Pilar pertama*, pembangunan kembali budaya maritim Indonesia; *Pilar kedua*, Berkomitmen dalam menjaga dan mengelola sumber daya laut dengan fokus membangun kedaulatan pangan laut melalui pengembangan industri perikanan dengan menempatkan nelayan sebagai pilar utama; *Pilar ketiga*, Komitmen mendorong pengembangan infrastruktur dan konektivitas maritim dengan membangun tol laut, pelabuhan laut, logistik, dan industri perkapalan, serta pariwisata maritime; *Pilar keempat*, Diplomasi maritim yang mengajak semua mitra Indonesia untuk bekerja sama pada bidang kelautan; *Pilar kelima*, Membangun kekuatan pertahanan maritim.

Selain itu, visi Nawacita, yang merupakan program prioritas Jokowi Tahap I, adalah sebagai berikut (KPU, 2014); 1) Menghadirkan kembali Negara untuk melindungi segenap bangsa dan memberikan rasa aman pada seluruh warga negara; 2) Kami akan membuat pemerintah selalu hadir dengan membangun tata kelola pemerintahan yang bersih, efektif, demokratis, dan terpercaya; 3) Membangun Indonesia dari pinggiran dengan memperkuat daerah daerah dan desa dalam kerangka negara kesatuan; 4) Memperkuat kehadiran negara dalam melakukan reformasi sistem dan penegakan hukum yang bebas korupsi, bermartabat dan terpercaya; 5) Meningkatkan kualitas hidup manusia Indonesia; 6) Meningkatkan produktivitas rakyat dan daya saing di pasar internasional sehingga bangsa Indonesia bisa maju dan bangkit bersama bangsa-bangsa Asia lainnya; 7) Mewujudkan kemandirian ekonomi dengan menggerakkan sektor-sektor strategis ekonomi domestik; 8) Melakukan revolusi karakter bangsa dan; 9) Memperteguh ke-bhinneka-an dan memperkuat restorasi sosial Indonesia

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

Dapat dilihat, visi presiden tidak menyebutkan mengenai pembangunan IT di Indonesia. Dalam hal ini, *political will* dari pemerintahan Jokowi Tahap I belum mengarah ke arah pembangunan IT di bidang *cyber defense* di Indonesia. Visi presiden lebih ke arah kemaritiman, bukan modernisasi pertahanan berbasis komputerisasi (IT). Hal ini bisa dipahami, mengingat ancaman besar China di laut China Selatan yang membutuhkan atensi lebih dari pemerintah Indonesia (Junef, 2018). Secara logika, Persenjataan yang dibutuhkan untuk mengatasi hal itu lebih ke kapal perang atau pesawat tempur yang bisa menjelajah laut dan udara.

Aspek Teknologi

Tulisan ini berargumen bahwa Pemerintah Indonesia kurang memerhatikan aspek penelitian dan pengembangan di bidang pertahanan siber. Hal ini bisa dilihat bahwa, pada tahun 2016, anggaran litbang Kementerian Pertahanan tercatat hanya Rp. 1,45 trilyun, atau hanya sejumlah 1,2% anggaran pertahanan Republik Indonesia (Chairil, 2019). Hal ini sangat disayangkan mengingat teknologi *cyber defense* membutuhkan kegiatan pengembangan dan penelitian yang lebih di bidang tersebut. Amanat Perpres Nomor 5 Tahun 2010 akan menjadi sia-sia dikarenakan keengganan untuk lebih serius di dalam pengembangan teknologi siber.

Selain permasalahan di bidang penganggaran, terdapat juga masalah di bidang sumber daya manusia. Dalam hal ini, pemenuhan personil untuk kegiatan penelitian dan pengembangan masih baru terpenuhi sekitar 70-80% dari kebutuhan (Dzikri, 2016). Padahal, kegiatan litbang membutuhkan personil-personil yang cakap dan matang di dalam bidang penelitian dan pengembangan. Hal ini tentu saja membutuhkan menajemen yang baik di dalam konteks tersebut, mengingat amanat dari Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 tentang pedoman pertahanan siber, sebagai berikut (Kementerian Pertahanan RI, 2014);

> Aset utama dalam cyber security adalah personel atau SDM yang memainkan peran sangat penting dalam pertahanan siber. Tantangan terbesar dalam implementasi pertahanan siber adalah menyediakan SDM yang kompeten dan senantiasa cepat dan sigap mengikuti dinamika lingkungan siber yang terus berkembang seiring berkembangnya teknologi dan kondisi sosial masyarakat. Untuk itu strategi pengembangan SDM harus didukung dengan program peningkatan kompetensi yang berkesinambungan.

Hal tersebut secara logika akan sulit terjadi mengingat banyaknya mutasi

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

personel dan pejabat di bidang penelitian dan pengembangan di Kementerian Pertahanan. Mutasi ini dapat terjadi dikarenakan proses politik dan sosial terkait birokrasi yang terjadi dalam institusi terkait. Mutasi dan pemindahan tentu saja akan mengganggu proses kerja dikarenakan personil dan pejabat baru harus melakukan adaptasi yang tentu saja akan memakan waktu lagi. Hal ini diharapkan akan menjadi catatan bagi pemerintahan Jokowi Tahap II untuk melakukan reformasi manajemen sumber daya manusia di lingkungan Kementerian Pertahanan.

Isu pengembangan persenjataan juga menjadi kendalan di Indonesia. Menurut Dr. Hasyim Gautama, industri Indonesia masih lemah di dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi *cyber* (Ardiyanti, 2014). Hal ini sebenarnya merupakan sektor vital di dalam usaha pengembangan pertahanan siber. Diharapkan, muncul kebijakan pemerintah yang dapat mengatasi isu ini agar industry pertahanan Indonesia menjadi lebih baik kedepannya.

SIMPULAN

Berdasarkan penelaahan di tulisan ini, penulis menyimpulkan bahwa kesulitan pengembangan *cyber security* dalam konteks *Revolution Military Affairs* di era pemerintahan Jokowi Tahap I dikarenakan permasalahan di dalam aspek kultural, politik dan teknologi. Permasalahan di dalam aspek kultural disebabkan oleh mengakarnya doktrin grilya dan strategi konvensional selama bertahun-tahun di tubuh TNI. Sedangkan permasalahan politik disebabkan oleh belum adanya *political will* yang kuat di dalam merubah RMA di tubuh TNI. Adapun permasalahan teknologi disebabkan oleh kurangnya anggaran dan manajemen Sumber Daya Manusia yang berhubungan penelitian dan pengembangan di tubuh Kementerian Pertahanan. Selain itu, sektor industri masih kesulitan di dalam memproduksi perangkat keras yang berhubungan dengan pertahanan siber.

DAFTAR PUSTAKA

Ardiyanti, H. (2014). Cyber-Security Dan Tantangan Pengembangannya Di Indonesia. *Politica*, *5*(1), 95–110.

Baumard, P. (2017). Cybersecurity in France. In *Springer* (1st ed.). Springer. http://link.springer.com/content/pdf/10.1007/978-3-319-54308-6.pdf

Brandon, J. (2018). *Why ASEAN Needs to Invest More in Cybersecurity*. 2018-05-09. https://asiafoundation.org/2018/05/09

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

/why-asean-needs-to-invest-more-in-cybersecurity/

Chairil, T. (2019). *Tiga hal yang harus dilakukan Prabowo , calon presiden yang kini jadi menteri pertahanan*. https://theconversation.com/tiga-hal-yang-harus-dilakukan-prabowo-calon-presiden-yang-kini-jadi-menteri-pertahanan-126455

Cheng, D., Chong, A., Ekman. Alice, de La Neuville, T. F., Longdi, X., Cherian, S., & Ventre, D. (2014). *Chinese Cybersecurity and Defense* (D. Ventre (ed.); 1st ed.). ISTE Ltd.

Chotimah, H. C., Iswardhana, M. R., & Pratiwi, T. S. (2019). Penerapan Military Confidence Building Measures dalam Menjaga Ketahanan Nasional Indonesia di Ruang Siber. *Jurnal Ketahanan Nasional*, *25*(3), 331–347. https://doi.org/10.22146/jkn.50344

Denning, D. (2000). Cyberterrorism : The Logic Bomb versus the Truck Bomb. *Global Dialogue*, *2*(4), 29–37.

Dixon, H. (2018). *British 15-year-old gained access to intelligence operations in Afghanistan and Iran by pretending to be head of CIA, court hears*. The Telegraph. https://www.telegraph.co.uk/news/2018/01/19/british-15-year-old-gained-access-intelligence-operations-afghanistan/

Dzikri, I. (2016). Negara dan Kapasitas Adopsi Inovasi: Studi Kasus Tranformasi Pertahanan Indonesia Periode 1998-2014. *Global: Jurnal Politik Internasional*, *18*(2), 131–151. https://doi.org/10.7454/global.v18i2.305

Farrell, T., & Terriff, T. (2002). The Sources of Military Change. In *Lynne Rienner Publishers* (1st ed.). Lynne Rienner Publishers. http://www.gbv.de/dms/sub-hamburg/346119464.pdf

Forum, W. E. (2014). *Risk and responsibility in a hyperconnected world* (Issue January). http://www3.weforum.org/docs/WEF_RiskResponsibility_HyperconnectedWorld_Report_2014.pdf

Gray, C. S. (2002). Strategy for Chaos: Revolutions in Military Affairs and the Evidence of History. In C. Gray & W. Murray (Eds.), *Frank Cass* (1st ed., Vol. 82, Issue 1). Frank Cass. https://doi.org/10.2307/20033454

Hammes, T. X. (2005). War evolves into the fourth generation. *Contemporary Security Policy*, *26*(2), 189–221. https://doi.org/10.1080/13523260500190500

Hundley, R. (1999). *Past Revolutions, Future Transformations: What Can the History of Revolutions in Military Affairs Tell Us about Transforming the U.S. military?* http://www.rand.org/pubs/monograph_reports/2007/MR1029.pdf [Accessed 10 September 2015]

Hutton, J. (2020). *Indonesia moves to beef up cyber security with data protection law*. The Straits Times. https://www.straitstimes.com/asia/se-asia/indonesia-moves-to-beef-up-cyber-security-with-data-protection-law

Indonesia, R. P. (2002). *UNDANG-UNDANG REPUBLIK INDONESIA NOMOR 3 TAHUN 2002 TENTANG PERTAHANAN NEGARA*. https://peraturan.bpk.go.id/Home/Details/44421/uu-no-3-tahun-2002

Islami, M. J. (2017). Tantangan Dalam

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau Dari Penilaian Global Cybersecurity Index. *Jurnal Masyarakat Telematika Dan Informasi*, *8*(2), 137–144. https://doi.org/10.17933/mti.v8i2.108

JPNN. (2019). *Pelibatan TNI ke Institusi Sipil Sebuah Kemunduran di Era Reformasi*. https://m.jpnn.com/news/pelibatan-tni-ke-institusi-sipil-sebuah-kemunduran-di-era-reformasi

Junef, M. (2018). Sengketa Wilayah Maritim di Laut Tiongkok Selatan. *Jurnal Penelitian Hukum De Jure*, *18*(2), 219–240. https://doi.org/10.30641/dejure.2018.v18.219-240

Kementerian Pertahanan RI. (2012). *LAMPIRAN PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA NOMOR 19 TAHUN 2012 TENTANG KEBIJAKAN PENYELARASAN MINIMUM ESSENTIAL FORCE KOMPONEN UTAMA*. https://www.kemhan.go.id/ppid/wp-content/uploads/sites/2/2016/10/Permenhan-Nomor-19-Tahun-2012-Lampiran-1.pdf

Kementerian Pertahanan RI. (2014). *PERATURAN MENTERI PERTAHANAN REPUBLIK INDONESIA NOMOR 82 TAHUN 2014 TENTANG PEDOMAN PERTAHANAN SIBER*. https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf

Kominfo. (2014). *Pengguna Internet Nomor Enam Dunia*. https://kominfo.go.id/content/detail/4286/pengguna-internet-indonesia-nomor-enam-dunia/0/sorotan_media

Kominfo. (2016a). *Kapolri: Ada terorisme siber, rekrutmen & pelatihan bom lewat online*. Kominfo. https://kominfo.go.id/content/detail/8523/kapolri-ada-terorisme-siber-rekrutmen-pelatihan-bom-lewat-online/0/sorotan_media

Kominfo. (2016b). *Menuju Poros Maritim Dunia*. https://www.kominfo.go.id/content/detail/8231/menuju-poros-maritim-dunia/0/kerja_nyata

KPU. (2014). *Visi-Misi Program Aksi Ir. H. Joko Widodo – Drs. H.M. Jusuf Kalla Pemilu Presiden dan Wakil Presiden Tahun 2014*. Kpu. https://www.kpu.go.id/koleksigambar/Visi_Misi_JOKOWI-JK.pdf

Metz, S., & James, K. (1995). STRATEGY AND THE REVOLUTION IN MILITARY AFFAIRS: FROM THEORY TO POLICY. In *U.S. Army Strategic Studies Institute*. https://www.jstor.org/stable/resrep11727?seq=1#metadata_info_tab_contents

Miles, B. M., & Huberman, M. (1992). Analisis Data Kualitatif Buku Sumber Tentang Metode-Metode Baru. In *UIP*. UIP.

Nazir, M. (2005). *Metode Penelitian*. Jakarta Ghalia Indonesia.

Parameswaran, P. (2015). *Indonesia' s Cyber Challenge Under Jokowi*. https://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/

Perlroth, N., & Sanger, D. (2013). *CyberAttacks Seem Meant to Destroy. Not Just Disrupt*. Nyt.

ISSN 2614-4336
VOL. 6 No.2 HAL. 91-103

https://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html

Primawanti, H., & Pangestu, S. (2020). DIPLOMASI SIBER INDONESIA DALAM MENINGKATKAN KEAMANAN SIBER MELALUI ASSOCIATION OF SOUTH EAST ASIAN NATION (ASEAN) REGIONAL FORUM. *Jurnal Ilmiah Hubungan Internasional*, *02*(01), 1–15. https://journal2.unfari.ac.id/index.php/globalmind/article/view/89

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61=78.

Schallbruch, M., & Skierka, I. (2018). Cybersecurity in Germany. In *Lexology* (1st ed.). Springer. https://www.lexology.com/library/detail.aspx?g=1b339fd8-d32b-4187-8c71-d459d794124e

Tabansky, L., & Israel, I. Ben. (2015). Cybersecurity in Israel. In *Cybersecurity in Israel* (1st ed.). Springer. https://doi.org/10.1007/978-3-319-18986-4

Winartha, I. M. (2006). *Metodologi Penelitian Sosial Ekonomi*. Andi Ofsset.

PROFIL SINGKAT

Muhammad Rangsang Agung, S.Sos, lahir di tanggal 27 April 1986. Setelah meraih gelar sarjana di Universitas Jember pada tahun 2010, saya bekerja di beberapa perusahaan sebelum akhirnya menjadi PNS di Kementerian Pendidikan dan Kebudayaan. Saya sekarang menjalani program pendidikan Paska Sarjana Ilmu Hubungan Internasional di Universitas Indonesia dengan menggunakan program Beasiswa Kemendikbud.