HACKER SEBAGAI AKTOR NON-NEGARA : *CYBER WARFARE* SEBAGAI DAMPAK PENYADAPAN PEJABAT NEGARA INDONESIA OLEH INTELIJEN AUSTRALIA

Yusep Ginanjar

Abstract

In 2013 it was revealed that wiretapping had been done by Australian intelligence towards a number of high-ranking officials in Indonesia. This invited the reaction of Indonesian hackers to destroy thousands of important sites in Australia and it is getting a reply from Australian hackers. Of course this is a bad precedent for Indonesia's relationship with Australia. Since its presence in international politics, hackers have been considered non-state actors. This research uses a qualitative method with a phenomenological approach. The purpose of this study is to describe the phenomenon of cyber warfare carried out by both parties as an attempt to attack and maintain the country's sovereignty over their respective versions. The conclusion in this study is the mirror of this cyber war case that hackers are included as non-national actors for their contribution in international politics.

Keywords: *Hackers, Cyber, Indonesia, Australia, non-state actor.*

Pendahuluan

Adanya kemajuan teknologi merupakan bagian keinginan dari masyarakat secara luas mengenai kemudahan dan fleksibelitas dalam meunjang kehidupan sehari-hari. Namun ternyata disamping kemajuan tersebut ternyata juga memunculkan kerumitan dan berbagai persoalan yang belum bisa diselesaikan. Salah satu kerumitan yang muncul dari adanya kemajuan teknologi tersebut adalah *hacker*.

Kemunculan *hacker* jika dilihat dari kacamata budaya merupaka sub-kultur yang memerangi tatanan kehidupan masyarakat yang sudah ada. Mereka hadir dari berbagai dinamika eksperimental baik secara keilmuan maupun secara sosial

masyarakat khususnya kalangan anak muda. Ada kondisi hegemoni dalam kehidupan berbangsa dan bernegara. Dimana hegemoni yang diciptakan adalah oleh para penguasa negara yang dalam hal ini adalah pemerintah. Maka, meminjam hegemoni yang dimaksud oleh Antonio Gramsci yang menurutnya bahwa pemerintahan rezim fasis berhasil menyebarluaskan pengaruhnya karena sangat didukung oleh organisasi infrasturktur terkait, yang mana di dalamnya terdapat kepatuhan intelektual karena berbagai faktor kultural atau yang mendominasi lainnya (Patria & Arif, 2015).

Kaitannya dengan pernyataan Gramsci adalah bahwa kemapanan yang sudah tercipta oleh rezim yang sudah berkuasa dilawan oleh intelektualitas melalui dunia ilmu dan teknologi oleh para *hacker* untuk para penguasa baik pemerintah maupun para konglomerasi yang dianggap bisa saja kebijakannya merugikan rakyat banyak. Hal tersebut berkaitan dengan kebanyakan visi para *hacker* yaitu kebebasan. Para *hacker* menciptakan kebebasannya sendiri dalam mengekspresikan realitas sosial.

Jika dipandang dari kacamata hubungan internasional maka kemunculan *hacker* yang berinteraksi melintasi batas negara, meruntuhkan pandangan mengenai *statecentric*, karena kehadirannya merupakan manifestasi dari aktor non-negara yang cenderung awalnya absurd namun perlahan tapi pasti kehadiran para hacker menjadi sebuah entitas yang semakin diakui kehadirannya sebagai aktor non negara yang bisa mempengaruhi interaksi global dalam berbagai aspek.

Kohane dan Nye dalam teori interdependensi kompleks menekankan pada tiga hal, yaitu: 1) bahwa Negara bukanlah aktor satu-satunya, terdapat aktor transnasional sebagai pemain utama;

2) *Hard power* bukanlah satu-satunya instrumen yang bisa mendominasi, ekonomi dan penggunaan lembaga-lembaga internasional adalah instrumen utama; 3) keamanan digantikan oleh kesejahteraan sebagai isu utama (Fitri & Rani, 2013: 936). Merujuk pada pernyataan Keohane dan Nye, *hacker* bisa termasuk dalam aktor non-negara yang memainkan perannya.

Namun terlepas dengan keterkaitannya dengan sudut pandang gramsci mengenai hegemoni serta kohane dan Nye yang dikaitkan dengan hacker, ada berbagai tipe dari hacker itu sendiri, namun yang lebih mengemuka biasanya *white hacker* dan *black hat hacker*. Secara sepintas tentu terlihat simpel dalam pengkategorian tersebut dimana kita akan digiring pada pemikiran white hacker adalah hacker yang baik, dan *black hat hacker* adalah yang jahat.

Tentu ada perbedaan dan persamaan dalam mekanisme kerjanya. Akan tetapi ketika sudah menyangkut soal idealisme dan nasionalisme mereka bisa bersatu dalam satu isu. Hal tersebut bisa dilihat dari adanya beberapa peristiwa yang terjadi perang *hacker* antar negara yang berkaitan dengan isu sosial, ekonomi, dan politik diantaranya seperti penyerangan Sony Pictures Entertainment pada tahun 2014, pihak peretas atau kelompok hackernya bernama Guardians of Peace dan intelijen Amerika Serikat menuduh bahwa dalah dibalik penyerangan tersebut adalah Korea Utara, meskipun demikian Korea Utara membantah terlibat dalam kasus tersebut, (suara.com, 2015).

Dua peristiwa lainnya adalah penyerangan yang dilakukan oleh hacker rusia dan china. Pada tahun 2015 hacker rusia berhasil membobol gedung putih dengan cara masuk ke komputer yang terhubung dengan jaringan gedung putih dan selanjutnya

mereka juga melumpuhkan situs Departemen luar negeri Amerika Serikat (AS). Selain itu, pada tahun hacker asal China juga berhasil masuk dalam jaringan melalui *phising e-mail* yang pada akhirnya mereka berhasil mencuri informasi rahasia militer Amerika Serikat termasuk rencana proyek rudal dari para kontraktor yang bekerja untuk Angkatan Laut Amerika Serikat (merdeka.com, 2019).

Keterkaitan antara isu sosial politik dengan hacker ternyata juga berlaku pada Indonesia. Berbagai peristiwa sosial dan politik diwarnai dengan serangan-serangan *hacker* dengan berbagai isu dan kepentinganya, termasuk salah satunya peristiwa penyadapan pejabat Indonesia yang berujung pada perang *hacker* antara negara Indonesia dengan *hacker* negara australia. Hubungan antara Indonesia dengan Australia sebelum isu peyadapan pejabat negara Indonesia memang pasang surut. Pada era Soekarno hubugan indonesia dan Australia meregang hal tersebut berkaitan dengan perbedaan pandangan mengenai komuisme, lalu pada era Soeharto sempat membaik sampai disepakati *Agreement on Maintaining Security* (AMS). Namun peristiwa meninggalnya lima orang wartawan Asutralia di Indoesia yang diduga dibunuh dan persoalan papua barat kembali mejadikan hubungan indonesia dan Australia dalam ketegangan (Firth, 2011). Di era reformasi penyadapan pejabat negara Idonesia khususnya presiden Susilo Bambang Yudhoyono telah dilakukan pada tahun 2009 mejadi preseden buruk bagi hubungan kedua negara.

Terungkapnya hal tersebut setelah mantan intelejen Amerika Serikat, Edward Snowden membongkarnya dan merilis dalam situs wikileaks.org. Hal tersebut tentu mengundang reaksi berbagai pihak tertama pemerintah Indonesia. Salah satu pihak yang merasa paling bertanggung jawab adalah kementrian

komunikasi dan informasi (kemenkominfo) yang pada saat itu menterinya adalah Tifatul sembiring. Tifatul menjelaskan bahwa standar komunikasi para pejabat negara sangat baik, namun akan membuat standarisasi yang baru agar tidak mudah disadap, (kominfo.go.id,2013).

Selain dari komifo yang bereaksi, Badan Intelejen Negara (BIN) pun bereaksi dan langsung berkoordinasi dengan presiden, serta melakukan koordinasi juga dengan badan intelejen Australia. Badan intelejen indonesia dan australia bersepakat bahwa tidak akan ada lagi penyadapan yang dilakukan kedepannya. (BBC.com, 2013). Namun hal tersebut tentu belum bisa menjadi jaminan bahwa kesepakatan itu bisa dijalankan, karena jelas bahwa kepentingan adalah yang menjadi prioritas utama dengan melakukan hal apapun.

Langkah pertama yang dilakukan oleh negara Indonesia adalah menarik duta besar indonesia untuk Asutralia sebagai salah satu bentuk protes Idonesia terhadap Australia. Selain untuk protes, hal tersebut dilakukan untuk memintai keterangan secara langsung pada duta besar Indonesia untuk Australia, serta presiden Yudhoyono yang memerintahkan untuk menghentikan sementara kerjasama bilateral sampai adanya penjelasan dari pihak Australia. Pelanggaran tersebut juga mendapat reaksi dari kementrian pertahanan Indonesia yang menunda sementara kerjasama yang dilakukan oleh keduanegara tersebut.

Kejadian tersebut memicu bayak reaksi diluar pemerintahan, baik kalangan masyarakat umum maupun komunitas dunia maya yang lebih sering disebut dengan netizen atau warga dunia maya. Perbincangan mengenai penyadapan tersebut tentu mengalami peningkatan di bulan November 2013

tersebut. Apalagi ketika para hacker asal Indonesia meyerukan perang siber agar menghacurkan website-website milik pihak Australia baik pemeritahanya ataupun yang swastanya. Era 4.0 merupakan tren otomasi serta penyimpanan dan pertukaran data terkini pada masa ini. Hal tersebut tentu membuat pemerintah Indonesia berpikir untuk mengamankan rahasia negara.

Pada saat itu hasil pantauan PoliticaWave ada data yang menunjukkan bahwa *tren awareness* perbincangan mengenai berbagai isu seputar penyadapan oleh Australia ini melibatkan percakapan 27.146 para pengguna internet, yang terdiri dari 71.406 *buzz. "Potential reach netizen* yang terbawa arus perbincangan itu sebanyak 65.808.077 akun. begitu pernyataan PoliticaWave mengenai hasil pantauannya selama tiga hari sejak 18 November 2013 (tempo, 2013). Percakapan sekitar enam puluhlima juta akun tersebut tidak terlepas dari peran *hacker* yang semakin memberikan porsi pada kasus ini untuk semakin dibicarakan oleh banyak orang.

Semakin banyak reaksi baik dari pemerintah maupun dari non-pemerintah semakin menumbuhkan rasa nasionalisme satu sama lain antar kelompok *hacker* khususnya yang ada di Indonesia. Dewasa ini *hacker* dianggap sebagai aktor hubungan internasional sebagai aktor non-negara dengan segenap perannya baik yang positif maupun dalam hal yang negatif. Sehingga berkaca dari kasus perang *hacker* Indonesia dengan *hacker* Australia menjadi semakin penting untuk dapat memberikan porsi *hacker* sebagai aktor hubungan internasional non-negara.

Sejarah kemunculan *Hacker*

Sebutan *hacker* secara terminologi ketika ada sekelompok mahasiswa dari Tech Model Railroad Club di Laboratorium Kecerdasan Artifisial Massachusetts Institute of Technology (MIT) melakuka peretasan terhadap berbagai komputer pada tahun 1959 di Amerika Serikat (Suheimi,1991). Pada awalnya penggunaan kata *hacker* merupakan hal yang sangat positif, karena hal itu diartikan sebagai seseorang yang memiliki kemampuan untuk merombak segala sesuatu yang berkaitan dengan komputer serta didalamnya termasuk mengotak-atik sistem untuk menjadikan hasil yang lebih baik. Menjadi berbeda makna dan bahkan lebih cenderung pada hal negatif karena ada suatu peristiwa dimana pada tahun 1981, ada perkumpulan yang bernama *Chaos Computer Club* (CCC) mereka membobol jaringan komputer yang dimiliki oleh German Bildschirmtext serta hal tersebut menyebabkan kerugian bagi sebuah bank. Pada sepuluh tahun kemudian setelah kejadian itu, tahun 1991 tepatnya awal Januari menyerang sistem departemen pertahanan dengan alasan kecewa pada sistem jaminan sosial dan departemen Tenaga Kerja.

Pendefinisian dari kata *hacker* itu sendiri sebetulnya tidak ada kesepakatan. Malah sebaliknya Balock (2015), menyatakan bahwa untuk mendefinisikan *hacker* maka dari definisi itu akan memunculkan pertanyaan dan pernyataan yang baru. Ada hal menarik ketika mendefinisikan *hacker* dimana ternyata media-lah yang mengkonstruksikan definisi *hacker* bisa menjadi negatif atau mejadi positif. Dari pendefinisian tersebut paling tidak ada tiga tipe karakteristik dari *hacker*, yaitu :

1. *White hat Hacker (Peretas topi putih).*
   Peretas jenis ini sering disebut sebagai profesional keamanan atau peneliti keamanan. Peretas seperti itu dipekerjakan oleh suatu organisasi dan diizinkan untuk menyerang organisasi

untuk menemukan kerentanan yang mungkin dapat dieksploitasi oleh penyerang.

2. *Black hat hacker* (peretas Topi Hitam)

   Dikenal juga sebagai cracker, jenis hacker ini disebut sebagai orang jahat, yang menggunakan pengetahuannya untuk tujuan negatif. Mereka sering disebut oleh media sebagai para peretas.

3. *Gray Hat Hacker* (Peretas topi abu-abu)

   Peretas jenis ini adalah perantara antara topi putih dan peretas topi hitam. Misalnya, seorang hacker topi abu-abu akan bekerja sebagai profesional keamanan untuk suatu organisasi dan secara bertanggung jawab mengungkapkan semuanya kepada mereka; namun, ia mungkin meninggalkan pintu belakang untuk mengaksesnya nanti dan mungkin juga menjual informasi rahasia, yang diperoleh setelah kompromi dari server target perusahaan, kepada pesaing (Balock,2015).

Dilihat dari definisi diatas maka membutuhkan skill atau kemampuan yang mumpuni agar bisa menguasai perangkat lunak dan juga kemampuan untuk melindungi diri sendiri dalam arti pergerakannya tidak bisa terlacak. Selain itu, keterampilan penting untuk menjadi peretas elit adalah paling tidak harus memahami mengenai berbagai lapisan model dan memahaminya pada lapisan bawah, lapisan fisik (perangkat) (Kevin,2016).

Tidak terlepas dari definisi di atas serta tipe dari para hacker itu, maka segala kejadian yang berkaitan dengan kondisi era digital saat ini ternyata juga merambah ke Indonesia dan Australia. Tentu hal tersebut akan mempengaruhi kondisi sosial, politik, ekonomi, serta aspek kehidupan lainnya di Indonesia dan Australia.

Hacker di Indonesia dan Australia

Era 4.0 masuk di Indonesia seiring dengan mejamurnya para hacker di Indonesia. Secara kuantitas pada tahun 2015 indonesia menempati urutan pertama hacker dunia dengan prosentase presentase 38 % membawahi Cina 33 %, Amerika 6,9 %, Taiwan 2,5 %, Turki 2,4 %, India 2 %, dan Rusia 1 % (Farid, 2015).

Jika melihat secara sejarah, komunitas hacker di Indonesia mayoritas berdiri pada sekitar tahun 2000-an. Pada tahun 2000 pertama kali *hacker* Indonesia diperkarakan secara hukum, yaitu seorang anak bernama Wenas Agustiawan yang belum genap berusia 17 tahun yang juga sebagai pendiri komunitas *antihackerlink* melakukan kegiatan pembobolan puluhan situs baik dalam maupun luar negeri.

Selain itu, salah satu tokoh terkenal dalam dunia Informasi Teknologi (IT) adalah Onno W Purbo. Tidak bisa dipugkiri bahwa Onno W.Purbo merupaka salah satu tokoh TI Indonesia yang paling dikenal. Teryata bukan hanya di Indonesia, aka tetapi di kancah internasional Onno juga memiliki tempat sebagai ahli IT. Onno merupakan aktor utama di balik peristiwa terbukanya frekuensi 2,4 Gigahertz yang diperuntukan bagi masyarakat. *Hack* (peretasan) yang dilakukan Onno sederhana, ia mengajarkan manfaat teknologi internet nirkabel via 2,4 Ghz pada masyarakat luas. Padahal pada saat itu para pengambil kebijakan yang terkait dengan internet masih menetapkan aturan yang sangat ketat

mengenai frekuensi tersebut yang apabila ada pihak yang meggunakannya tanpa izin akan berujung pada kasus pidana.

Deretan *hacker* Indonesia diantaranya adalah mereka yang mempunya identitas samaran baik yang sudah diketahui atau pun yang sampai sekarag belum diketahui identitas aslinya diataranya adalah Hmei7, Xnuxer, E5a_Cyb3r, XsvsHacker, Mr Dick, Jim Geovedi, Bio666x. Kasus yang pernah dilakukan serta spesialisasi mereka cukup bervariasi. Mulai dari pembobolan sampai dengan percobaan keamanan situs website dan komputer mereka lakukan.

Peretas Australia telah mengakses uang, informasi pribadi, dan basis data pemerintah swasta melalui metode tidak jujur di internet selama beberapa dekade. Ada beberapa kelompok hacker Asutralia diantaranya adalah Sydney Python (SyPy), Sec Talks IoT Melbourne, Melbourn, Random Hacks of Kindness Sydney, SecTalks Melbourne, Random Hacks of Kindness berbasis di Melbourne, Hackerspace Brisbane.

Para *hacker* di Australia bisa merupakan perseorangan, grup, dan bahkan berkelompok. Aksi yang mereka lakukan biasanya berupa pencurian data, pencurian finansial, menutup rumah sakit, mengekspose data pribadi yang sensitif, penyerangan terhadap pemerintah, dan banyak hal lainnya. Terkini adalah hasil survey mengenai pencurian *enterprise resource planning (ERP)* yang dihadapi oleh 64% responden, melaporkan ada pelanggaran sistem ERP mereka dalam 2 tahun terakhir (Abbot & Walace, 2019). Peretasan tersebut mengarah pada persoalan bisnis yang dijalankan oleh banyak perusahaan baik yang kecil maupun yang besar khususnya yang menggunakan ERP software.

Hubungan Indonesia-Australia

Indonesia bukan hanya sekedar mitra dagang yang sangat penting Australia. Di bawah pemerintahan presiden Yudhoyono, Indonesia merupakan penyokong Australia dalam berbagai forum penting di kawasan untuk mencapai kerjasama dalam mengatasi berbagai masalah, seperti terorisme, penyelundupan manusia, pencucian uang, dan berbagai bentuk kejahatan antarnegara lainnya. Pada hakikatnya bahwa negara tidak jauh berbeda dengan yang namanya individu manusia. Negara juga tidak bisa hidup sendiri dan membutuhkan negara lain untuk mencapai keinginannya. Maka ada keinginan untuk melakukan hubungan antar negara yang lazimnya kita sebut dengan hubungan internasional (*international relations*) (Jackson & Sorensen, 2005). Begitu juga dengan Asutralia dan Indonesia sebagai negara tentu membutuhkan satu dengan yang lainnya, terlebih lagi Indonesia dan Asutralia saling berdekatan atau dengan kata lain bertetangga.

Hubungan kedua negara mengalami pasang surut dalam berbagai dinamika berbangsa dan bernegara. Adanya hubungan yang harmonis sudah terjalin semenjak Indonesia mendeklarasikan diri menjadi negara pada tahun 1945. Akan tetapi dalam perjalanannya kedua pihak sering terlibat selisih faham dalam berbagai kasus diantaranya adalah mengenai konfrontasi antara Indonesia dengan Malaysia, kasus Timor-Timur, persoalan separatis papua, dan permasalahan-permasalahan lainnya yang sangat sering bisa menciptakan konflik antar negara. Akan tetapi kedua belah pihak yang bertetangga ini masih bisa menyelesaikan dengan baik tanpa konflik.

Penyadapan pihak Australia

Penyadapan yang dilakukan lintas batas negara, sebetulnya telah lama terjadi. Peristiwa penyadapan dewasa ini tidak terlepas dari penyadapan di masa lalu, hal itu diawali pada saat ditemukannya alat untuk melakukan perekaman pada pesawat telepon di Amerika pada tahun 1890 dan hal tersebut pada tahun 1928 ketika John F. Kennedy dan Lyndon B. Johnson sedang memerintah diperbolehkan atau legal penggunaannya oleh FBI (*Federal Bureau Investigation*). Seiring dengan kemajuan teknologi selanjutnya, penyadapan juga berkembang dilakukan pada *mobile phone*, website, Internet, frequency utility, satellite, dan alat-alat tekhnologi lainnya, sampai pada akhirnya penyadapan ini tidak jarang dilakukan untuk tujuan negatif (Sujadmiko,2014).

Penyadapan yang dilakukan oleh pihak Australia jelas melanggar UU No. 36 tahun 1999 tentang Telekomunikasi dan UU No. 11 Tahun 2008[1] tentang Informasi dan Transaksi Elektronik. Perlakuan yang tidak terpuji tersebut dilakukan oleh Australia atas dasar kepentingan diplomatik (yang dianggap mempunyai kekebalan atau hak imunitas atas hukum yang ada). Akan tetapi dalam kenyataannya, hal tersebut bertentangan dengan undang-undang republik indonesia maupun hukum internasional.

Penyadapan yang dilakukan tentu sangat merugikan pihak Indonesia sebagai korban penyadapan. Kerugian yang paling mudah ditebak adalah, bocornya rahasia negara termasuk salah

[1] Pada saat terjadi penyadapan, yang berkaitan dengan komunikasi dan transaksi elektronik yang masih berlaku adalah UU no 11 tahun 2008. Sedangkan saat ini UU tersebut sudah diganti menjadi UU no 19 tahun 2016.

satu diantaranya adalah kebijakan luar negeri yang akan diambil oleh negara Indonesia. Sudah bisa diprediksikan bahwa, ketika Australia mendapatkan data dari Indonesia, maka Australia akan dengan sangat mudah untuk membaca serta mengantisipasi kebijakan yang diambil oleh Indonesia.

Selain dari hukum nasional Indonesia, dalam kacamata hubungan internasional, Australia juga melanggar aturan konvensi internasional (*Vienna Convention on Diplomatic Relation*) pada tahun1961 yang ditandatangani oleh para pihak, termasuk Indonesia dan Australia.

Perang Hacker (Aktor non-negara) sebagai dampak Penyadapan

Seperti yang sudah diungkapkan sebelumnya bahwa hacker merupakan sub-kultur perlawanan terhadap sistem yang sudah mapan dan bagi sebagian para hacker, nasionalisme serta keberpihakan pada rakyat adalah hal penting. Bukan hal yang berlebihan jika masyarakat indonesia termasuk hacker Indonesia sangat marah karena tidak tanggung-tanggung yang menjadi sasaran target penyadapan tersebut adalah orang-orang penting yang ada di negara Indonesia. Berikut adalah data pejabat negara yang disadap oleh pihak Australia :

Gambar 1.Daftar Pejabat Indonesia yang Disadap Australia

Sumber : abc.net.au

Terjadinya perang hacker Indonesia dan Australia, tidak terlepas dari rasa nasionalisme mereka pada negaranya masing-masing, dimana kedua belah pihak berada pada keyakinannya bahwa negara mereka benar dan harus mendapatkan pembelaan dari mereka. Mengenai benar dan salahnya negara mereka, yang paling utama adalah membela negaranya terlebih dahulu.

Sebelumnya sudah dijelaskan bahwa, hacker merupakan *non-state actor* yang mengambil peran dalam interaksi hubungan internasional. Saat ini pelaku penyerangan dalam dunia siber tidak hanya untuk melakukan kejahatan kriminal dalam konteks mendapatkan finansial saja, namun juga dilakukan oleh kelompok teroris dan *hacktivis* yang kental dengan muatan politis. Karakter serangan siber yang anonim, juga memberikan peluang pada aktor negara untuk melibatkan diri dalam serangan siber jika diperlukan (Chandra, 2018).

Kasus penyadapan yang dilakukan memunculkan reaksi dari para hacker Indonesia yang langsung melakukan penyerangan terhadap berbagai situs yang dimiliki Australia baik yang swasta maupun yang milik pemerintah, hal tersebut jelas merugikan pihak australia. Diantara puluhan situs yang diretas oleh hacker indonesia ada diantaranya milik pemerintah yang sangat strategis yaitu situs badan intelejen dan kepolisian.

Para *hacker* indonesia bergerak melintasi batas-batas negara dan mempunyai pola yang tidak sistemik menjadikan sulit untuk dideteksi. Hal tersebut terbukti ketika pemerintah Indonesia dan Australia mengakhiri konflik yang diakibatkan oleh penyadapan sejumlah pejabat tersebut, namun para *hacker* masih saja terus melangsungkan *cyber warfare* diantara mereka dan keduabelah pihak mengalami kesulitan dalam menghentikan dan mengidentifikasi sebanyak mungkin para hacker yang terkait.

Kelompok yang dari awal bahkan sebelum ada reaksi dari pemerintah pusat melakukan serangan yaitu Anonymous Indonesia (AnonIndo) tetap melakukan serangan meskipun antar pemerintah sudah berdialog. Meskipun pemerintah dan pihak swasta dari Australia menganggap bahwa penyerangan itu merupakan kejahatan.

Mengenai *hacker* sebagai kejahatan atau bukan, dalam kajian hubungan internasional masih perlu ditegaskan bahwa apakah hacker termasuk dalam aktor non-negara yang dimasukan dalam klasifikasi *trans crime organizations* (organisasi kriminal antar negara) atau bukan. Hal tersebut memang perlu diperjelas mengingat bisa saja aktor negara terlibat atau memfasilitasi *hacker* untuk *cyber warfare*.

Tidak ada data yang jelas bahwa apakah pemerintah indonesia juga menggunakan hacker dalam konfilk penyadapan ini atau tidak. Namun yang jelas, pemerintah Indonesia cenderung melakukan pembiaran dan seperti diuntungkan dengan hadirnya *hacker* dalam konflik penyadapan ini.

Penutup

Perang siber yang terjadi atara *hacker* indonesia dan Australia telah memberikan gambaran bahwa perang saat ini telah memasuki era siber dimana perangkat lunak komputer menjadi alat yang bisa mematikan suatu negara. Perang *hacker* sebagai dampak dari penyadapan pejabat negara indonesia oleh Australia merupakan suatu bukti bahwa peran siber dalam ranah politik telah mempunyai kontribusi yang cukup sgnifikan. Dari kondisi ini ternyata dalam kajian hubunga internasional memberikan ruang bahwa *hacker* merupakan aktor hubungan internasional non-negara.

Hadirnya *hacker* sebagai aktor non negara, masih memerlukan klasifikasi dan ruang pembuktian apakah termasuk dalam entitas kriminal trans nasional atau entitas positif yang memberikan manfaat yang baik pada dunia. Namun hal yang saat ini bisa dipastikan adalah bahwa, sebagai sebuah entitas atau aktor non-negara dalam hubungan internasional, maka pemerintah dapat memberdayakan untuk kepentingan nasionalnya.

Daftar Pustaka

David Yacobus, konflik *hacker* sebagai non-state actor dalam ketegangan hubungan indonesia – australia pada tahun 2013. Jurnal prodi peperangan asimetris | juni 2017 | volume 3 nomor 2.

Farid Aulia Tanjung. 2015. Mengintip Fenomena Dunia Hacker Di Indonesia. (Tersedia di https://www.maxmanroe.com/mengintip-fenomena-dunia-hacker-di-indonesia.html. D

Firth, S. (2011). Australia in International Politics : An Introduction to Australia's Foreign Policy.New South Wales: Allen & Unwin

Kevin, Cardwell (2016).Essential Skills for Hackers. Elsevier

Michelle Slatalla,Joshua Quittner. 1993. Masters of Deception: The Gang That Ruled Cyberspace.

Nezar Patria dan Andi Arief. 2015. Antonio Gramsci : Negara & Hegemoni.Yogyakarta, Pustaka Pelajar. Hlm 21

Pinto zakiri handoko. 2014. Politeness strategies in tony abbot's speech concerning australia-indonesia tapping issue. Brawijaya University.

Suheimi, 1991. Kejahatan Komputer. Yogyakarta : Andi Offset. Hlm 33

Sujadmiko, Bayu. (2014). PENYADAPAN LINTAS NEGARA/KEDAULATAN DITINJAU DARI HUKUM INTERNASIONAL.https://www.researchgate.net/publication/305462455_PENYADAPAN_LINTAS_NEGARAKEDAULATAN_DITINJAU_DARI_HUKUM_INTERNASIONAL/citation/download

Yudha, chandra. 2018. Penguatan kerjasama cybersecurity: keniscayaan untuk ASEAN. Majalah masyarakat ASEAN.kemenlu

Tempo. Penyadapan dan Perang Hacker jadi Sorotan Netizen. https://tekno.tempo.co/read/531360/penyadapan-dan-perang-hacker-jadi-sorotan-netizen.

https://www.abc.net.au/news/2013-11-18/custom-indonesia-spying-slide-3/5099216

Merdeka. com, Ulah-ulah Hacker China dan Rusia sampai Ganggu Indonesia. https://www.merdeka.com/dunia/ulah-ulah-hacker-china-dan-rusia-sampai-ganggu-indonesia.html

Suara.com. Inilah 7 Serangan Hacer Terbesar Sepanjang Sejarah. https://www.suara.com/tekno/2015/03/18/062600/inilah-7-serangan-hacker-terbesar-sepanjang-sejarah