Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber Di Indonesia

Pratama Persadha

Chairman Lembaga Riset Keamanan Siber CISSReC
E-mail: -

Abstract— Hacktivism is becoming a trend that is being loved globally. The hacktivism trend was born at the same time as the information technology revolution, especially when people became increasingly dependent on smartphones and the internet. This has more or less affected aspects of cybersecurity in various countries. Because generally hacktivism appears with socio-political motives. Many countries have made cybersecurity one thing to study before deciding to cooperate with other countries. Also for Indonesia, cybersecurity has become an important factor in seeing national security. Several popular issues have shown that hacktivism has become a trend in Indonesia as well.

***Keywords*—: Hacktivism; Hacktivist; Cybersecurity; hackers; social politics.**

I. PENDAHULUAN

Beberapa tahun terakhir peristiwa terkait keamanan siber mendapatkan perhatian publik dunia dan tanah air lebih banyak. Berbeda dengan beberapa dekade yang lalu, dimana peretasan tidak selalu berhubungan dengan masyarakat, kini berbagai peristiwa dan serangan siber langsung dirasakan imbasnya ke masyarakat bahkan juga dilakukan oleh masyarakat karena semakin mudahnya belajar ilmu peretasan dari internet. Peretasan yang membuat kerugian materi kecil sampai besar mengintai masyarakat.

Pada kuartal pertama 2020, BSSN mengumumkan bahwa Indonesia mendapatkan serangan siber sebanyak 88 juta kali, naik 13 kali lipat dibanding tahun 2019. Tentunya jumlah serangan yang tercatat tersebut bisa berbeda dengan kondisi di lapangan, mengingat banyak serangan siber yang tidak terdeteksi dan juga tidak dilaporkan dengan berbagai alasan. Bahkan serangan salah satunya paling banyak lewat aplikasi zoom meeting, yang bahkan sering dipakai oleh negara.

Pada awal 2019 tepatnya bulan Maret, publik dikejutkan dengan kabar bocornya 13 juta data pengguna BukaLapak. Setahun kemudian pada kuartal pertama 2020 publik Kembali terkejut dengan bocornya 91 juta data pengguna Tokopedia, bahkan ada database anggota Kepolisian RI yang dicuri dari sistem kepolisian. Ini menjelaskan bahwa keamanan siber saat ini seharusnya harus menjadi prioritas.

Diantara berbagai serangan siber tersebut muncul satu tren serangan siber yang dinamakan *hacktivism*, sebuah serangan siber dengan motif politik. Di Indonesia peretasan model ini mulai muncul mengikuti beberapa isu politik hangat di masayrakat. Seperti saat isu RUU KPK pada 2019 lalu. Protes mahasiswa dan berbagai elemen diikuti oleh ebebrapa peretasan pada instansi pemerintah, salah satunya adalah situs remsi Kemendagri.

Tak selalu politik, beberapa tahun sebelumnya protes terkait mahalnya harga kuota internet juga muncul pada website milik Telkomsel. Dengan teknik deface peretas melakukan protes menulis di halaman depan website Telkomsel bahwa harga kuota internet perusahaan plat merah ini sangat mahal dan mencekik masyarakat bawah.

Hacktivism menjadi salah satu sarana yang mudah digunakan oleh peretas dalam menyuarakan aspirasi social politik atau bahkan menyampaikan pesan ideologisnya. Peristiwa-peristiwa *hacktivism* ini ternyata sudah menjadi bagian sejarah Indonesia.

II. METODE PENELITIAN

Dalam penelitian ini peneliti menggunakan pendekatan kualitatif deskriptif analitis.. Jenis data yang digunakan berasal media pemberitaan dan data sekunder berasal dari literatur-literatur yang mendukung data. Kemudian pada teknik pengumpulan data terdiri dari dokumentasi studi kepustakaan, kemudian teknik analisa datanya dianalisa dari setiap peristiwa dan juga teori yang ada.

III.HASIL DAN PEMBAHASAN

Hacktivism kegiatan meretas dan *hacktivist* sendiri dimaknai sebagai pelakunya, aktivis yang menyuarakan aspirasi lewat hacking atau kegiatan peretasan. Diawal perkembangannya setiap peretas memiliki kode etik (ethos). Etika hacker mengacu pada perasaan benar dan salah, pada ide-ide etis yang dimiliki komunitas ini bahwa pengetahuan harus dibagikan dengan orang lain yang dapat mengambil manfaat darinya, dan bahwa sumber daya penting harus digunakan daripada disia-siakan.

Doktrin yang umum digunakan oleh para peretas dewasa ini antara lain adalah berbagi, keterbukaan, desentralisasi, akses gratis ke komputer dan perbaikan dunia, terutama penegakan demokrasi serta hukum yang adil yang dijalani masyarakat dunia.

Ideologi seperti inilah yang dipegang oleh peretas, menjadi alas an kuat bagaimana anonymous bersikap pada setiap Tindakan otoriter dan pada puncaknya ada upaya membuka informasi lewat aksi wikileaks. Keduanya muncul dari semangat kode etik hacker yang menjadi idelogi bagi mereka.

Hacktivist-hacktivism mulai dikenal dan naik daun pada tahun-tahun 1990-an dengan motif politik ideologis dalam melakukan aksinya. *Hacktivist* sendiri berasal dari kata hack dan activism, artinya dapat dipahami bahwa *hacktivism* adalah sebuah aksi 'demonstrasi' di dunia maya menggunakan yang teknik hacking.

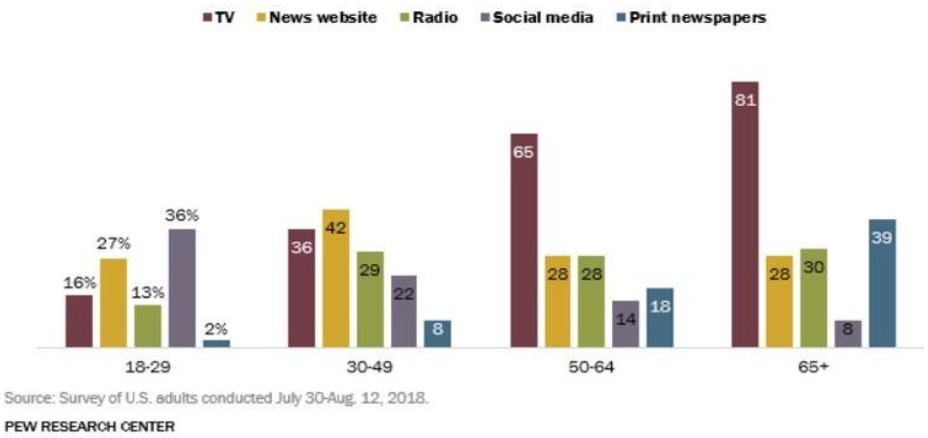
Hacktivist berbeda dengan tipe peretas lainnya. Karena motivasi mereka melakukan peretasan didasari oleh keinginan adanya perubahan social politik, bukan terkait finansial. Ada pesan yang dibawa oleh si peretas, baik politik, sosial maupun ideologi.

Target peretasan para *Hacktivist* ini bukanlah masyarakat umum, target mereka umumnya adalah pemerintah dan juga industry besar di sebuah negara maupun Lembaga serta korporasi multinasional. Dalam banyak peretasan oleh *hacktivist* terlihat jelas bagaimana Lembaga besar menjadi sasaran, bahkan kini juga bergeser ke individu-individu dengan pengaruh besar. Mengapa hal ini dilakukan? Utamanya jelas untuk mendapatkan perhatian dari masyarkat luas dan juga pihak penguasa.

Dengan fakta ini tidaklah mengejutkan bahwa *hacktivist* dianggap pemerintah dan media sebagai "penjahat" dan merupakan ancaman bagi masyarakat. Metode dari *hacktivism* sendiri dapat berupa website mirroring, wifi sniffing, phising, DDos, Website defacement maupun teknisi terbaru lainnya.

Mengapa *hacktivism* menjadi pilihan Sebagian orang? Secara umum ada ketidakpuasan pada saluran komunikasi publik seperti media massa. Tidak beragamnya pemilik media (*diversity of ownership*) akan menhasilkan berita yang tidak beragam dan sarat kepentingan dari para pemilik modal media tersebut (*diversity of content*). Kondisi yang demikian ini dikhawatirkan membuat publik seperti diarahkan dengan model berita agar sesuai dengan tujuan pemodal maupun pemilik media, dengan berbagai cara. Hal ini yang membuat Sebagian individu memilih menyuarakan pendapatnya lewat kegiatan peretasan.

Kondisi media massa yang tidak idel dengan kepemilikan yang tidak beragam atau oligarki membuat ruang untuk mengkritisi kebijakan pemerintah menjadi berkurang. Terutama di Indonesia kita melihat media menjadi alat tawar politik, sehingga akibatnya ruang kritis itu harus sesuai dengan motif politik maupun kondisi politik dari pemilik media. Akhirnya masyarakat memilih mengekspresikan politiknya lewat salah satunya media sosial. Sebatas bersuara atau bahkan menjadi influencer. Bahkan di AS, milenial lebih percaya terhadap berita yang ada di media sosial dibandingkan di media massa.



Gambar 1. Penelitian di AS terkait kepercayaan pada media dan media sosial

Motivasi *hacktivist* untuk melakukan aksinya bermacam-macam, mulai dari perasaan sepenanggungan, kesamaan agama, kesamaan suku warna kulit dan juga karena adanya rasa ketidakadilan yang perlu disuarakan. Beberapa contohnya adalah anarkisme, patriotisme, nasionalisme, maupun terorisme. Kemudian motif rasa keadilan akan persamaan hak sipil ini meluas dan mengglobal. Berbagai kegiatan hacktivism diketahui memperjuangkan hak asasi manusia di beberapa neagra yang masih dalam kancah perang. Bahkan kekuatan global ini juga mendorong hacktivism untuk membela hak-hak kaum marginal yang tidak memerlukan identitas negara, seperti hak LGBT dan juga pengungsi Rohingya.

Khusus untuk isu LGBT, Indonesia harus mewaspadai ini dari sekarang. Disaat ini Lembaga pemerintahan seperti TNI-Polri sedang membersihkan LGBT dari lingkungan masing-masing, bisa berimbas pada aksi hacktivist dengan motif membela LGBT. Ini karena di eropa dan AS, membela LGBT menjadi sebuah tren tersendiri. Karena itu kembali pada isu keamanan siber, negara harus sedini mungkin menyiapkan segala sarana prasarana pendukung.

Hacktivist setidaknya memiliki 3 hal yang mendukung dalam aksinya. Pertama, menjadi seorang partisipan dalam *hacktivism* tidak memerlukan dana yang besar. Yang diperlukan mutlak hanya dua, yaitu computer dan akses internet. Dengan itu aktivitas menyuarakan pendapat lewat jalan peretasan sudah bisa dimulai.

Kedua, *hacktivist* memiliki anonimitas di internet, namun hal ini dimiliki bila sang peretas sudah menguasai secara teknis dan juga memiliki perangkat pendukung yang layak. Anonimitas ini menjadi kunci agar hacktivist tidak dikenali dalam waktu yang lama. Bahkan karena sangat rahasia indentitasnya, para hacktivist ini sering kali tidak mengenal satu sama lain, karena proses interaksinya tergantung dari operasi yang sifatnya virtual dan tidak bertemu langsung.

Ketiga, *hacktivist* memiliki kerentanan diserang lebih rendah, dibandingkan aktor seperti negara maupun korporasi multinasional. Salah satunya disebabkan hacktivist cenderung membatasi akuisisi teknologi yang umum dipakai awam. Ini membuat hacktivist tidak mudah diprofiling lewat perangkat yang dijual bebas dan punya mengirimkan data secara illegal kepada servernya, sebagai updaya espionage. Selain itu karena longgarnya "organisasi" menjadikan hacktivist tidak mudah berpindah dan lebih fleksibel, sehingga sulit terdeteksi.

Hacktivism digunakan pertama kali oelh para peretas dan seniman *Cult of the Dead Cow.* Bagi mereka, *hacktivism* dimaksudkan sebagai upaya menegakkan hak asasi manusia dan keterbukaan pertukaran informasi. Jadi konsep hacktivist ini adalah benar-benar menjadi aktivis.

Pada perkembangannya *hacktivism* ini meluas untuk membantu perjuangan politik suatu negara terjajah. Aksi *hacktivism* yang paling besar di dunia salah satunya adalah aksi membela Palestina. Setiap terjadi agresi ke wilayah Palestina di Gaza maupun di Tepi Barat, maka akan diikuti oleh konsekuensi peretasan terhadap infrastruktur pemerintah Israel. *Hacktivism* Palestina ini tidak hanya dari dunia Arab, bahkan dari Pakistan, Sebagian Eropa Barat dan negara eks Sovyet berpenduduk muslim. Bahkan banyak peretas di AS yang notabene bukan muslim juga membangun kekuatan untuk membantu Palestina dengan menyerang sejumlah situs AS dan Israel.

Berikut beberapa kejadian *hacktivism* yang pernah terjadi di Indonesia

A. Situs web Telkomsel

Pada April 2017, situs web Telkomsel mengalami *deface*. Dalam protesnya, si peretas mengungkapkan keluhan atas mahalnya tarif kuota internet dari Telkomsel, padahal Telkomsel adalah provider telekomunikasi dengan jangkauna paling luas di tanah air. Si peretas memberikan pesan seolah meminta Telkomsle menghentikan praktek monopoli terselubungnya. Nama tampilan yang tadinya Telkomsel pun diubah menjadi "Telkomnyet".

Gambar 2. Website Telkomsel diretas

Ketika insiden siber itu terjadi, sebagian warganet ada yang mengucapkan terima kasih pada sang *hacker* anonim itu dan mendukung pesan protes yang disampaikan. Situs web baru bisa dipulihkan beberapa hari kemudian. Telkomsel meminta maaf kepada seluruh penggunanya terkait kejadian ini.

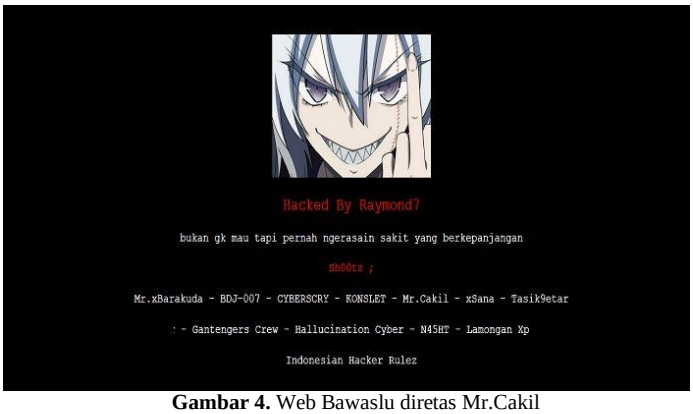
B. Situs web Indosat Ooredoo

Dua hari setelah situs web Telkomsel diretas, pada 29 April 2017, giliran situs web resmi Indosat jadi korban. Berbeda dengan Telkomsel yang menyerang situs utama, *hacker* kali ini menyerang situs web sub-domain saja. Hal ini terjadi karena sebelumnya Indosat Ooredoo menyindir Telkomsel lewat *Twitter* soal peretasan yang menimpa mereka. Hal tersebut tergambar dari pesan yang diberikan peretas saat melakukan *deface* subdomain: *arena.indosatooredoo.com*. Berkaitan dengan peretasan tersebut, Indosat mengungkapkan jika pihaknya akan terus meningkatkan keamanannya supaya hal serupa tidak terjadi kembali

Gambar 3. website Indosat diretas

C. Situs web Bawaslu

Pada 2018, remaja berusia 18 tahun bernama Dendy Syaiman atau yang lebih dikenal dengan nama Mr.Cakil melakukan *deface* pada *sub-domain* milik bawaslu *inforapat.bawaslu.go.id*. Seperti umumnya situs milik pemerintah, pengamanan pada situs Bawaslu memang sangat kurang. Pelaku sendiri akhirnua ditangkap setelah ditelusuri nama kode sang peretas.



Gambar 4. Web Bawaslu diretas Mr.Cakil

D. ***Peretasan Situs DPR***

Saat aksi Omnibus Law UU Cipta Kerja ramai ditolak melalui aksi demonstrasi, ternyata situs Dewan Perwakilan Rakyat (DPR), yakni dpr.go.id ikut diretas hacker. Peretasan terhadap DPR terjadi berulang kali sebelum aksi Omnibus Law. Yang cukup mengagetkan adalah meski sudah berulang kali diretas, namun pihak kesekretariatan DPR tetap tidak menambahkan fitur SSL pada website resmi DPR.

Padahal keberadaan SSL sebagai fitur keamanan dasar sangat dibutuhkan oleh sebuah website. Ini tentu sangat disayangkan. Karena kondisi seperti inilah situs-situs pemerintah digemari oleh para hacker pemula karena lrelatif mudah ditembus.

Gambar 5. Website DPR menjadi korban deface

E. Situs web Kemendagri

Pada 22 September 2019, *sub-domain* milik Kemendagri mengalami *deface* dan menampilkan pesan yang menunjukkan kesedihannya akan kondisi KPK. Empat hari setelah kejadian, pelaku ditangkap. Pemuda 21 tahun asal Pasuruan, Jawa Timur itu mengaku telah men-*deface* sekitar 600 web dari dalam maupun luar negeri. Saat ini pelaku berinisial ABS ditahan kepolisian. Dari hasil penyelidikan ia mengaku alasan meretas untuk menguji kemampuan TI-nya.

Gambar 6. Situs Kemendagri diretas

F. Situs web KPAI

Situs web Komisi Perlindungan Anak Indonesia (KPAI) diretas dengan menampilkan pesan politik terkait dengan RUU KUHP. Setelah pemulihan web, KPAI mengatakan, tidak akan memperpanjang kasus *deface* secara hukum.

Gambar 7. Situs KPAI diretas

G. Hacktivist Indonesia vs Timor Leste

Pada 30 Juni 1997, Departemen Luar Negeri (Deplu) Indonesia dikejutkan oleh sekelompok Urban Kaos yang mengganti tampilan situsweb Deplu. Mereka menampilkan tiga kata kunci yang menjadi alasan mereka meretas situsweb Deplu: "Free East Timor".

Pesan mereka jelas tidak hanya terkait lemahnya system milik Deplu. Lebih jauh mereka melakukanaksi hacktivism dan mendukung kemerdekaan Timor Leste. Sejak 1996 memang banyaks erangan yang ditujukan ke situs pemerintah Indonesia, pelakunya tidak hanya Urban Kaos. Tujuan mereka untuk mengalihkan perhatian masyarakat dunia dan Indonesia pada nasib Timor Timur (sebelum menjadi Timor Leste).

Total lebih dari 28 situs remsi pemerintah Indonesia diretas oleh urban kaos dan kelompok pro Timor Timur lainnya. Mereka mengubah wajah semua situsweb tersebut dengan menampilkan logo "*Portuguese Hacker Against Indonesian Tyranny*" dan bahkan ditambahkan kalimat solidaritas mendukung pengusutan kasus penembakan Santa Cruz yang menewaskan 250 warga Timor Timur pada 1991.

22 November 1997 kelompok yang menamakan diri Portuguese Hackers Against Indonesia (PHAI) meretas situs lembaga pemerintah Indonesia. Lalu pada 10 Februari 1997 kelompok Toxyn meretas situsweb Deplu. Mereka mengganti logo situsweb dengan tulisan "Welcome to the Department of Foreign Affairs Fascist Republic of Indonesia". Bahkan pada 24 April 1997 kelompok Toxyn meretas situs Angkatan Bersenjata Republik Indonesia (ABRI). Mereka melakukan deface dan menulis "Profesional Killers, Made in Indonesia" dengan latar belakang tentara memegang senjata di halaman situs ABRI. Aksi terus berlanjut dan kelompok Kaotik meretas 43 situs Indonesia sepanjang 1998. Majalah online *Phrack Magazine* sebuah media para pertas bahkan menyebut aksi retas simpatisan Timor Leste ke Indonesia ini sebagai bentuk *hacktivism* massif pertama di dunia. Selain dikampanyekan oleh para *hacktivist*, usaha membantu kemerdekaan Timor Leste juga dibantu penyedia layanan internet *Connect Ireland* membuat *country code top-level domain* (ccTLD) untuk Timor Timur dengan kode *.tp***.** Kode tersebut adalah singkatan dari Timor Portuguese. Dengan memiliki domain sendiri, seolah Timor Timur saat itu sudah setara dengan negara lain seperti Indonesia dengan domain .id-nya. Rentetan aksi itu tentu saja memantik reaksi. Pada 1999 domain .tp mulai diserang. Penyerangan ini sistematis dan berlangsung lama, dari 18 lokasi berbeda, dan menarget domain bernama .tp. Space Rogue, yang saat itu menjadi editor *Hackers News Network* bependapat bahwa penyerangan itu dilakukan sekelompok peretas yang bersimpati kepada pemerintah Indonesia.

Dari seluruh contoh diatas, kasus *hacktivism* Indonesia vs Timor Leste menarik untuk dilihat. Bila ditelisik lebih jauh apakah ada kemungkinan actor-aktor hactivism pro Timor Leste tersebut adalah proxy dari negara lain yang sedang menjalankan operasi distintegrasi pada Indonesia.

Tentu kita patut melihat siapa saja yang bisa menjadi actor *hacktivism*. Aktornya memang harus non-state, bukan negara dan motif gerakannya beda dengan negara. Operasi yang dilakukan negara semacam itu masuk dalam golongan cyber espionage dan information warfare, sebagai praktek intelijen maupun perang informasi.

Jadi kita bisa membedakan, bahwa Gerakan wikileaks adalah gerakan *hacktivism* massif karena dilakukan oleh actor non-state. Namun bila aksi semacam wikileaks dilakukan oleh negara maupun korporasi multinasional dengan alas an politik maupun finansial, itu masuk dalam *cyber espionage* dan *cyberwar*. Nmaun sekali lagi akan sangat sulit menganalisa setiap kejadian *hacktivism* di sebuah negara konflik apakah terbebas dari *proxy* negara lain atau tidak.

IV. KESIMPULAN

Hacktivism telah menjadi bagian sejarah di tanah air dan saat ini masih digunakan sebagai bagian dari menyampaikan pendapat secara illegal. "Peminatnya" masih banyak karena aksinya mudah mendapatkan perhatian dari siapapun terutama pemerintah dan juga dunia internasional.

Hacktivism lahir dan tumbuh bersaman dengan mulai pudarnya kepercayaan masyarakat pada media massa. Namun secara paradoks, *hacktivism* membutuhkan media sebagai corong keberhasilan aksinya, tanpa media jelas aksi para *hacktivist* ini tidak terpantau oleh masyarkat maupun stakeholders.

Pada akhirnya *hacktivism* tidak bisa dipisahkan dari dinamika ruang siber global dan tanah air, apalagi kemunculannya adalah dari niatan menjaga demokrasi dan keadilan hukum dimanampun berada. Ideologinya yang ideal membuat siapapun bisa ikut aktif menyuarakan dan berpartisipasi. Namun pada prakteknya *hacktivism* ini juga beririsan dengan *cyber espionage* dan juga *cyberwar*. Aktor utamanyalah yang akan menentukan aksi yang dilakukan ini tergolong hactivism, *cyber espionage* atau malah sudah masuk dalam *cyberwar.*

V. DAFTAR PUSTAKA

Mikhaylova, G. (2014). The" Anonymous" Movement: *Hacktivism* as an Emerging Form of Political Participation.

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: toward a *hacktivist* ethic. ACM SIGCAS Computers and Society.

Wall, D. (Ed.). (2003). Crime and the Interne

https://www.merdeka.com/peristiwa/pelaku-skimming-di-bali-kebanyakan-diotaki-warga-bulgaria-dan-rumania.html

https://www.liputan6.com/news/read/4234135/bssn-88-juta-serangan-siber-selama-pandemi-covid-19-salah-satunya-lewat-zoom

https://katadata.co.id/berita/2020/07/05/91-juta-data-pengguna-tokopedia-yang-bocor-masih-bisa-diunduh-gratis

https://republika.co.id/berita/q0i9rr9917000/dituntut-facebook-group-petinggi-teknologi-israel-mundur

https://keuangan.kontan.co.id/news/pakar-siber-angkat-bicara-soal-kasus-pembobolan-atm-bank-dki-oleh-satpol-pp

https://www.theregister.com/2017/06/01/china_cybersecurity_law/

https://tirto.id/membela-timor-timur-meretas-indonesia-cy6e