

## RESPON MASYARAKAT TERHADAP SISTEM *WHITELIST*: ALTERNATIF UNTUK AKSES INTERNET YANG LEBIH AMAN

### *PUBLIC RESPOND TO WHITELISTING: ALTERNATIVE FOR MORE SECURE INTERNET ACCESS*

Emyana Ruth Eritha Sirait

Puslitbang Aplikasi Informatika, dan Informasi dan Komunikasi Publik,

Badan Litbang SDM, Kementerian Komunikasi dan Informatika

JL. Medan Merdeka Barat No. 9, Jakarta Pusat 10110

emya001@kominfo.go.id

#### **ABSTRACT**

*Existing internet content filtering, known as blacklisting method such as Trust positive or Nawala, is still considered less effective to support safe and productive use of the Internet in the community. A more accurate system is needed, and whitelist system can be an alternative. This study has surveyed total 810 internet users in the schools (junior/senior high level) and the boarding schools, targeting students and principals/teachers, and also parents in the household with non-probability sampling techniques. The findings are then discussed in Focus Group Discussion with stakeholders and experts. The results show that the whitelist system receives good response from the respondents. However, whitelist is a complementary, not a substitute of the existing filtering; therefore the implementation should be based on demand and reserved to segmented users, and not to be applied nationally. Even it has good purposes, when it comes to the implementation stage, several challenges need to be deliberated in order to maximize its purpose. First is related to user information rights in order to remain protected, but not feel restricted. Second, whitelist is also expected to be the answer to overcome negative contents distribution accessed via mobile phone and through applications, social media, and instant messaging. Some other internet content managements can also be massively disseminated to complement content filtering system*

*Keywords: Whitelist, internet, access.*

#### **ABSTRAK**

Sistem penyaringan konten negatif di internet secara *blacklisting/blocking*, seperti Trust + atau Nawala, dinilai masih kurang efektif dalam mendukung penggunaan internet sehat dan produktif dalam masyarakat. Dibutuhkan sistem yang lebih akurat, dan sistem *whitelist* dapat menjadi alternatif pilihan. Dalam penelitian ini telah dilakukan survei dengan teknik sampling *non-probability*, kepada total 810 responden pengguna internet, yang terdiri dari murid dan kepala sekolah/guru di beberapa sekolah (SMP/SMA) dan pondok pesantren, serta orangtua di beberapa rumah tangga. Hasil survei kemudian dipertajam dalam FGD dengan pihak-pihak terkait dan pakar. Hasil penelitian menunjukkan bahwa sistem *whitelist* mendapat respon yang baik dari responden. Namun, *whitelist* merupakan komplementer, bukan substitusi dari sistem filter yang ada, sehingga implementasinya haruslah berdasarkan pilihan/permintaan dari pengguna (*demand driven*) dan ditujukan untuk kalangan tertentu, dan bukan menjadi kebijakan nasional. Walaupun bertujuan baik, beberapa tantangan penerapan sistem tersebut masih harus diperhatikan agar dapat bersifat jangka panjang dan mencapai manfaat yang diinginkan. Pertama, terkait kebutuhan informasi pengguna, diperlukan sistem yang dapat melindungi namun tidak membatasi informasi dan kreatifitas pengguna. Kedua, *whitelist* diharapkan dapat pula mengatasi penyebaran konten negatif dari akses yang dilakukan melalui *handphone*, dan yang diakses mayoritas aplikasi, media sosial, dan *instant messaging*. Selain itu, manajemen konten internet lainnya dapat disosialisasikan secara masif untuk mendukung sistem penyaringan konten.

Kata Kunci: *Whitelist*, internet, akses.

## PENDAHULUAN

Internet bagai pedang bermata dua, disatu sisi sangat dibutuhkan karena dapat memudahkan aliran informasi dan pengetahuan tanpa batas ruang dan waktu. Namun di sisi lain juga dapat merugikan jika internet digunakan secara tidak bertanggungjawab.

Faktanya, penyalahgunaan internet susah untuk dibendung, terbukti dengan banyaknya bermunculan situs-situs dengan konten negatif seperti pornografi, penipuan, perjudian, dan lain sebagainya. Pemerintah sebagai regulator, terus melakukan berbagai upaya untuk dapat meminimalkan penyalahgunaan internet di masyarakat. Salah satunya, manajemen regulasi melalui Peraturan Menteri Kominfo Nomor 19 Tahun 2014 yang mewajibkan para *Internet Service Providers* (ISP) untuk memasang filter situs negatif seperti Trust positif atau Nawala. Namun, *filtering* sebagai bentuk pengendalian konten seringkali bertentangan dengan kebebasan berekspresi dan efektivitas pengendalian konten di berbagai negara yang menerapkannya, selalu dapat dikelabui dengan keahlian teknis tertentu dari pengguna internet (Kurbalija, 2010). Demikian pula dengan metode *blocking* Trust positif yang dinilai masih kurang efektif, karena memiliki banyak celah untuk dapat 'dibobol' dan banyak situs negatif sejenis *malware* atau *spam* yang seringkali tidak tersaring. Oleh karena itu, upaya lain tengah dilakukan oleh Kementerian Kominfo untuk mencari instrumen internet aman yang efektif, yaitu dengan membangun sistem *Whitelist* Nusantara. *Whitelist* merupakan sistem untuk mengatur akses internet dengan cara mendaftar situs-situs dengan kriteria tertentu yang diperbolehkan untuk diakses. Dengan sistem ini masyarakat mempunyai pilihan untuk dapat mengakses

hanya situs-situs yang terjamin positif isinya. Masyarakat yang menjadi target pertama program tersebut yaitu institusi pendidikan di tingkat SD, SMP, SMA, dan pesantren dengan tujuan untuk melindungi para pelajar dari dampak buruk mengakses situs-situs negatif. Selain yang dikembangkan oleh pemerintah, sistem *whitelist* juga tengah dikembangkan oleh pihak penyelenggara jasa, seperti Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), bahkan ada beberapa ISP yang telah menawarkan paket-paket *whitelist* kepada masyarakat, namun memang masih kurang populer. Oleh karena itu, penelitian ini dimaksudkan untuk melihat permintaan dan kebutuhan masyarakat tertentu terhadap sistem *whitelist*.

Teknik *whitelisting* lebih dahulu dikenal sebagai alternatif dalam keamanan siber (*cyber security*), untuk mengatasi kelemahan dalam metode pengamanan konvensional seperti antivirus dan *firewalls* dalam menangkal *malware* (Beechey, 2010). Teknik ini pertama kali diperkenalkan oleh Fred Cohen di awal tahun 1990, dengan ide '*integrity shells*', yaitu program yang hanya mengizinkan eksekusi perangkat lunak yang sudah diketahui berintegritas (menggunakan *checklist database* untuk mengontrol integritas dan berdasar pada fakta bahwa virus harus memodifikasi program yang diinfeksi, sehingga menghancurkan integritas program tersebut) (Cohen, 1990).

Sebuah studi di Kanada tentang *whitelist* menemukan tiga jenis layanan yang berkembang berbasis *whitelist*. Pertama *whitelist* sebagai aplikasi (*application whitelisting/AWL*), seperti yang telah disebutkan sebelumnya, untuk mengatur aplikasi yang boleh di-*instal* pada sebuah komputer atau jaringan. *Application*

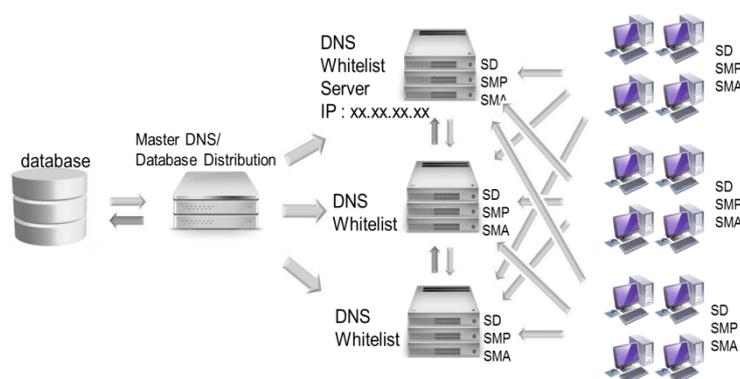
*whitelisting* dianggap sebagai salah satu teknik *IT security* yang handal dalam mengamankan *internet-connected networks and information* di beberapa negara (NCCIC/ICS-CERT United States, 2015, CSE Canada, 2015, ACSC Australia, 2016). Kedua, *email whitelisting* yang mendaftarkan nama pengirim dan penerima yang "aman" pada email untuk mengontrol *spam* dan dalam konteks ini dapat meningkatkan *deliverability* email tersebut. Ketiga, *whitelist* untuk mengelola *browsing* dan *traffic* internet. Hal ini dapat berguna bagi orang tua untuk mengontrol situs yang diakses oleh anak-anaknya, atau bagi penyedia layanan internet yang ingin memberikan layanan kepada konsumen terkait prioritas *traffic* tertentu pada internet, seperti *video streaming* atau aplikasi game (Lo, 2010).

Namun demikian, *whitelist* tidak dapat menggantikan sistem *scanning* konvensional. *Whitelist* berfungsi dengan baik dalam lingkungan yang kecil dan membutuhkan kontrol ketat, di mana keamanan lebih penting daripada kenyamanan, tetapi pengguna internet rata-rata tidak dapat mengandalkan sistem tersebut. Akan lebih baik jika *whitelist* dikombinasikan dengan *blacklist* (dan dengan teknik anti-virus lainnya) untuk membangun pertahanan berlapis (Bontchev, 2007).

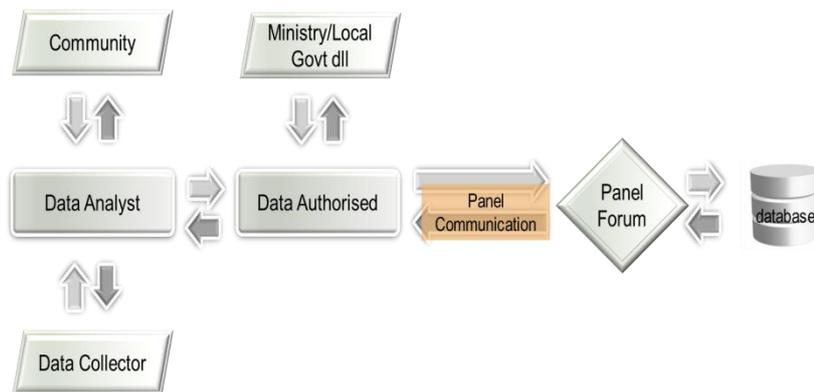
Sistem *whitelist* sebagai *web filtering* yang sedang dikembangkan oleh pemerintah

(Kementerian Kominfo) diberi nama Sistem *Whitelist* Nusantara, yang merupakan sistem berbasis *Domain Name System* (DNS) dengan menyimpan informasi tentang nama *host* ataupun nama domain dalam bentuk basis data di dalam jaringan Internet. Basis data yang disusun berisi situs *website* yang direkomendasikan memiliki konten positif untuk dapat diakses dan dipakai khususnya oleh pelajar tingkat SD, SMP dan SMA/ sederajat dan para santri di Pesantren. Hingga Juni 2016, terkumpul data kasar *positive list* dalam sistem *Whitelist* Nusantara yang berupa daftar domain .id (seperti .sch.id, .ac.id, .mil.id, .go.id) sejumlah 189.949 domain. Basis data ditentukan oleh Forum Panel *Whitelist* Nusantara yang terdiri dari perwakilan pihak-pihak terkait seperti Kementerian Pendidikan dan Kebudayaan, Kementerian PP&PA, Kementerian Agama, KPAI, PANDI, Nawala Nusantara, dan lain-lain (Direktorat Pemberdayaan Informatika, Direktorat Jenderal Aplikasi Informatika, 2016).

Sementara pihak swasta, melalui asosiasi APJII, juga mencoba untuk mengembangkan sistem *whitelist* lainnya. Beberapa ISP telah mencoba memasarkan produk *whitelist* kepada masyarakat, seperti Gmedia dan AmalaDNS.



Gambar 1. Sistem *Whitelist* Nusantara (Yamin, 2016)



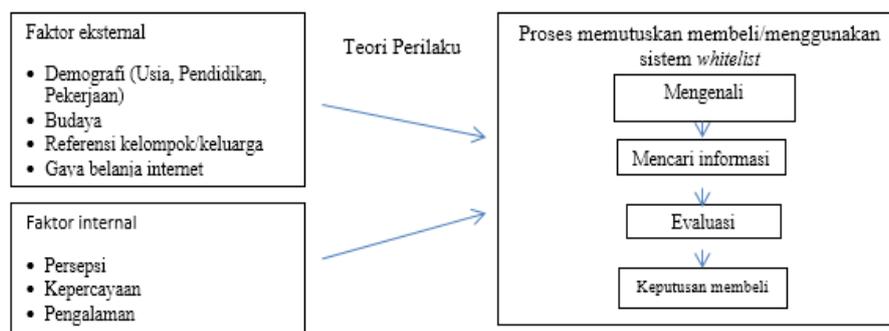
**Gambar 2.** Alur pengelolaan data pada *Whitelist* Nusantara (Yamin, 2016)

Perangkat lunak yang digunakan terdiri dari:

- Aplikasi *Whitelist* Nusantara
- Web Whitelist* Nusantara
- Database Whitelist* Nusantara
- Sistem DNS *Whitelist* Nusantara
- Sistem *BGP Router and Monitoring*

Sementara perangkat keras yang digunakan terdiri dari 2 Server untuk Aplikasi, *Web* dan *Database*, 3 Server untuk DNS, 2 Server untuk *BGP Router and Monitoring*, 2 *Firewall* dan 2 *Switch*. Untuk melihat sikap masyarakat terhadap penyaringan konten di internet dan mengetahui permintaan dan kebutuhan masyarakat terhadap penyaringan konten ecara *whitelist*, digunakan kerangka teori *consumer behavior*. Menurut Kotler dan Amstrong (1997), faktor utama yang mempengaruhi perilaku konsumen dalam melakukan

keputusan pembelian, yaitu faktor budaya, faktor sosial, faktor pribadi dan faktor psikologis. Menurut Hawkins et al (2001), keempat faktor pengaruh tersebut dapat disederhanakan menjadi dua faktor, yaitu pengaruh eksternal (budaya, sub budaya, demografi, status sosial, referensi kelompok dan keluarga, aktivitas pemasaran dan pengaruh internal (persepsi, pembelajaran, motivasi, kepribadian, sikap). Sementara proses keputusan pembelian seseorang konsumen terdiri dari tahapan-tahapan yang meliputi: pengenalan kebutuhan, pencarian informasi, evaluasi alternatif, keputusan membeli dan tingkah laku pasca pembelian (Kotler, 2007). Berdasarkan teori tersebut, kerangka konsep yang digunakan dalam penelitian ditunjukkan dalam Gambar 3.



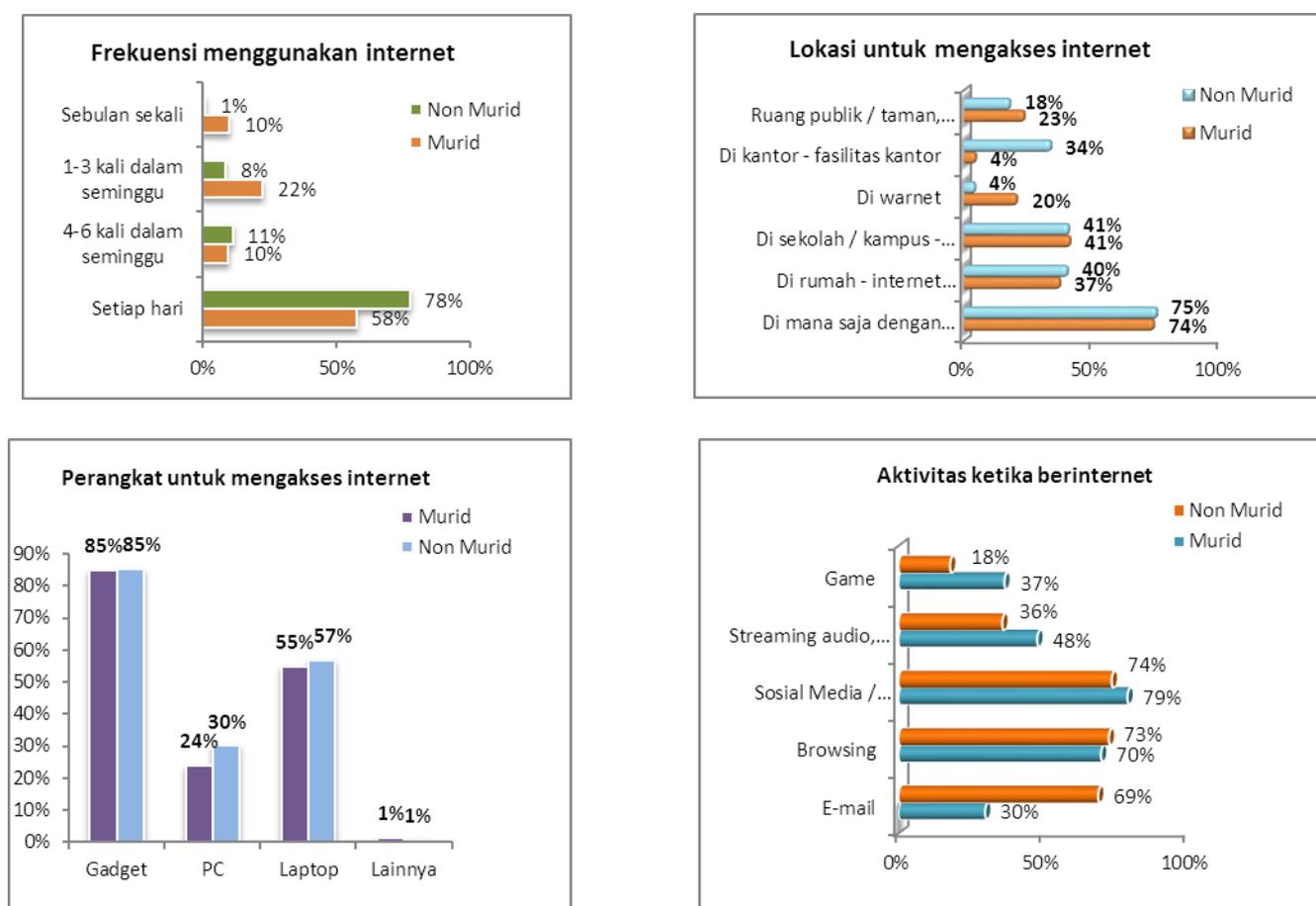
**Gambar 3.** Kerangka Konsep Peneliti

## METODOLOGI PENELITIAN

Pengumpulan data penelitian dilakukan melalui survei kepada pengguna internet yang menjadi target program *Whitelist* Nusantara, yaitu tenaga pendidik (Kepala Sekolah/guru) dan peserta didik di institusi pendidikan (SMP/SMA) dan Pondok Pesantren yang sudah terkoneksi internet, ditambah beberapa rumah tangga yang memiliki anak remaja. Teknik pengambilan sampel dilakukan secara non probabilistik dengan kuota 810 responden,

secara proporsional terdiri dari 405 orang murid dan 405 orang non murid (orangtua dan guru). Lokasi penelitian mencakup sembilan kota di Indonesia, yaitu Bandung, Surabaya, Semarang, Jakarta, Tangerang Selatan, Medan, Mataram, Banjarmasin, Makassar. Pemilihan lokasi didasari pada daerah dengan jumlah pengguna internet terbanyak di Indonesia, dilengkapi dengan keterwakilan dari daerah barat dan timur.

## HASIL DAN PEMBAHASAN



**Gambar 4.** Profil Responden Berdasarkan Pola Penggunaan Internet

Sumber : data diolah

Dari data-data pada Gambar 4 terlihat profil penggunaan internet oleh pelajar dan

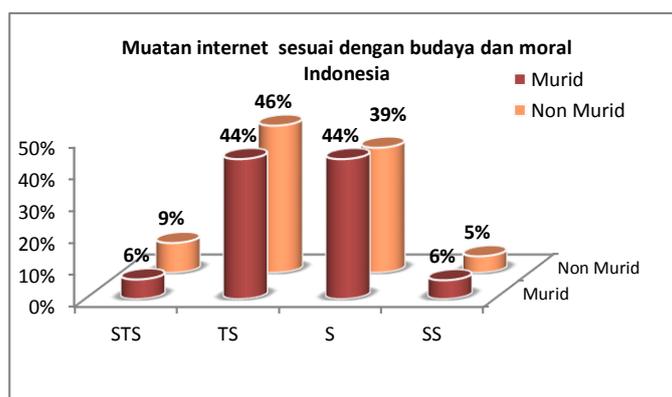
kalangan pendidik dewasa ini, yaitu dilihat dari frekuensi penggunaan internet, 58%-78%

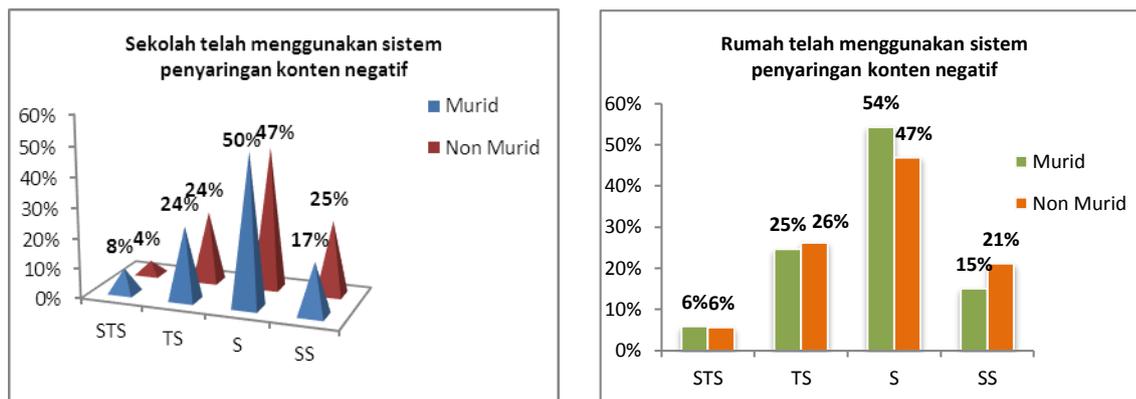
responden menggunakan internet setiap hari. Dilihat dari perangkat yang digunakan untuk mengakses internet, 85% responden menggunakan *gadget* (perangkat *mobile*) untuk mengakses internet. Berdasarkan lokasi untuk mengakses internet, 74%-75% responden mengakses internet di mana saja dengan menggunakan *smartphone*, sementara yang mengakses internet dengan fasilitas internet di sekolah atau berlangganan di rumah jumlahnya sekitar 37%-41%. Dilihat dari aktivitas yang kerap dilakukan di internet, 74%-79% responden mengakui aktivitas terkait penggunaan sosial media dan *instant messaging* menjadi aktivitas yang paling menonjol, diikuti 70%-73% responden yang menjawab *browsing*.

### Pengaruh Faktor Eksternal

Dari data-data pada Gambar 5 diketahui pengaruh faktor eksternal terhadap aktivitas responden berinternet. Dilihat dari

pendapatnya tentang muatan yang tersedia di internet, terdapat perbandingan yang hampir seimbang antara responden yang setuju dan tidak setuju bahwa muatan internet sesuai dengan moral dan budaya Indonesia. Selanjutnya, mayoritas 47%-50% responden setuju bahwa di lingkungan sekolah mereka telah menerapkan penyaringan konten penyaringan terhadap situs negatif. Sistem penyaringan situs negatif yang digunakan di sekolah umumnya yang disediakan oleh ISP yang dilanggan sekolah (mengacu pada *database Trust+*). Beberapa sekolah menambah sistem penyaringan tambahan seperti *proxy server* atau OpenDNS. Demikian pula pada pemakaian di rumah, mayoritas 47%-54% responden berpendapat bahwa akses internet di lingkungan rumah mereka sudah menerapkan penyaringan konten adapun sistem yang digunakan umumnya *Trust+* yang disediakan ISP.





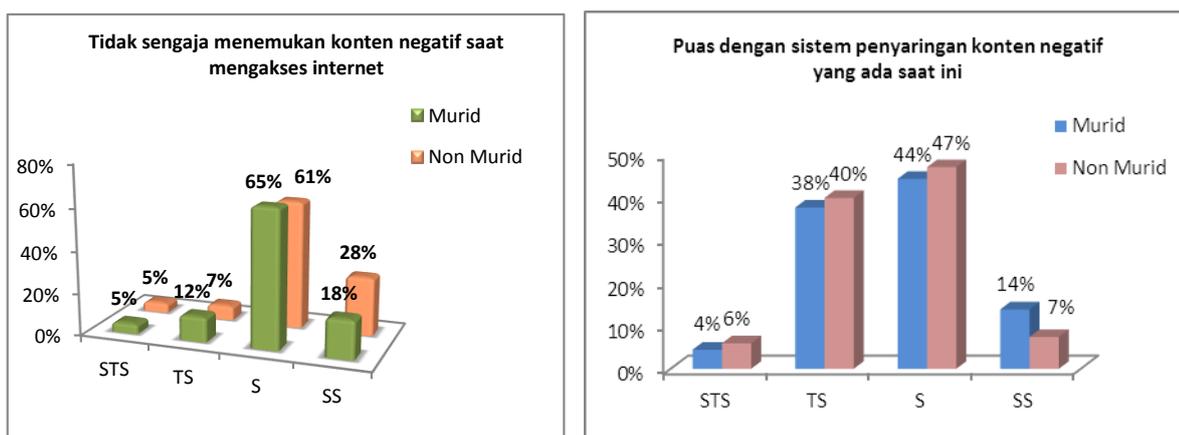
Note : STS = Sangat Tidak Setuju, TS = Tidak Setuju, S = Setuju, SS = Sangat Setuju

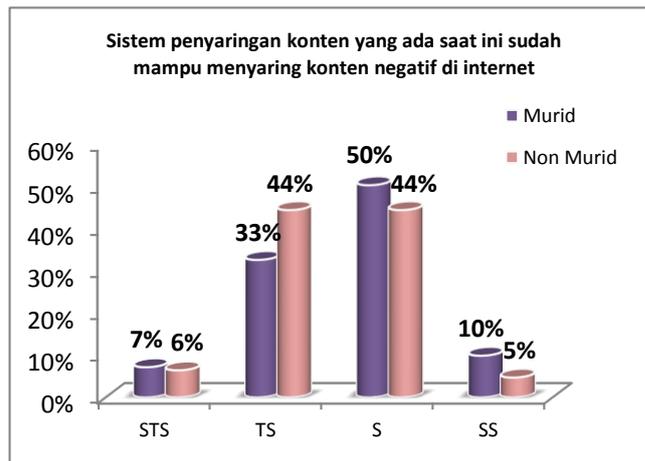
**Gambar 5.** Pengaruh Faktor Eksternal Terhadap Perilaku Responden Berinternet  
 Sumber : data diolah

### Pengaruh Faktor Internal

Dari data-data pada Gambar 6 diketahui pengaruh faktor internal terhadap aktivitas responden berinternet. Dilihat dari pengalamannya, 61%-65% responden merasa sering secara tidak sengaja menemukan konten negatif saat mengakses internet. Ketidaksengajaan mendapati konten negatif bisa disebabkan dari banyak hal seperti: pada iklan (ads) ketika mengakses suatu laman atau dari aplikasi yang berjenis *user generated content*. Dilihat dari sisi kepuasan responden terhadap sistem penyaringan situs negatif yang sudah diterapkan di Indonesia, ternyata lebih banyak 44%-47% responden yang sudah merasa puas, walaupun jumlahnya tidak dominan, sebab terdapat 38%-40% responden

yang masih tidak puas dengan sistem penyaringan yang ada. Hal ini menandakan beberapa kekurangan dirasakan oleh pengguna dari sistem penyaringan situs negatif yang ada sehingga perlu perbaikan. Dilihat dari pendapatnya apakah penyaringan konten yang ada saat ini sudah mampu menyaring konten negatif, lebih banyak murid (44%-50%) yang berpendapat setuju, walaupun tidak dominan, sementara pada kalangan pendidik komposisi yang setuju dan tidak setuju terhadap hal tersebut jumlahnya berimbang. Sistem *update database blacklist* bila dibandingkan dengan pertumbuhan konten negatif di internet sangat membutuhkan usaha yang lebih gencar untuk dapat terus membendung konten negatif yang sangat cepat bermunculan.



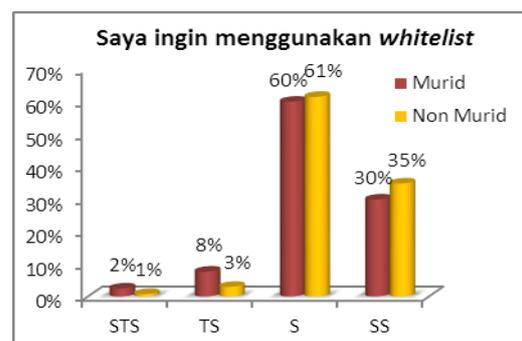
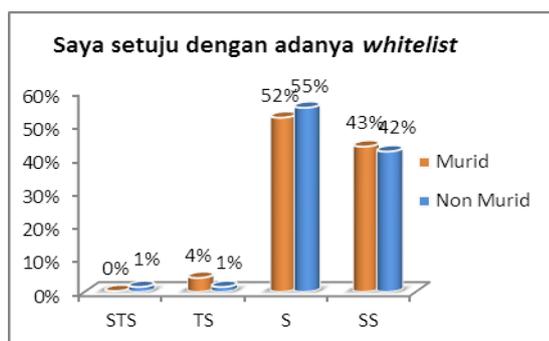


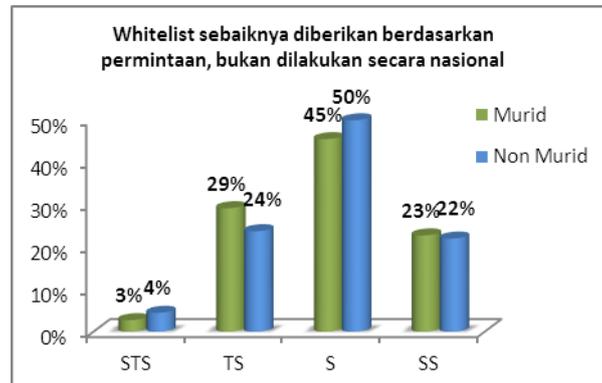
**Gambar 6.** Pengaruh faktor internal terhadap perilaku responden berinternet  
 Sumber : data diolah

### Respon Responden terhadap Sistem Whitelist

Dari data-data pada Gambar 7 terlihat bahwa sistem *whitelist* yang sedang dikembangkan oleh Kominfo mendapat respon yang baik dari sisi murid dan tenaga pendidik/orangtua. Mayoritas 95%-97% responden berpendapat setuju dan sangat setuju terhadap sistem ini, serta 90%-96% ingin dan sangat ingin menggunakan *whitelist*. Hal ini selaras dengan kebutuhan responden terhadap akses internet yang lebih ketat. Memang sistem *whitelist* pada akses internet pada dasarnya lebih ketat dibandingkan dengan sistem penyaringan *blacklist* yang ada sebelumnya. Namun demikian, sebagian besar (45%-50%) responden berpendapat bahwa

*whitelist* sebaiknya diberlakukan berdasarkan permintaan atau kebutuhan pengguna, bukan diberlakukan secara nasional. Pemberlakuan *whitelist* pada tahap awal memang ditujukan untuk beberapa segmen tertentu (sekolah, ponpes dan lingkungan rumah yang membutuhkan). Penerapan *whitelist* secara menyeluruh dapat menimbulkan dampak pro-kontra pada masyarakat karena akan membatasi akses masyarakat terhadap informasi melalui media internet. Jika ingin menyasar kalangan tertentu, maka perlu dilakukan segmentasi paket *whitelist* sesuai kebutuhan pengguna (misal: *whitelist* untuk lingkungan rumah, sekolah tingkat SD, SMP, SMA, dan lain-lain.)





**Gambar 7.** Perspektif responden terhadap sistem *whitelist*  
 Sumber : data diolah

### Analisis SWOT Sistem *Whitelist*

Temuan data-data kuantitatif tersebut selanjutnya dipertajam dan didiskusikan dengan pihak-pihak terkait (perwakilan sekolah dan pondok pesantren, perwakilan orangtua, Dinas Kominfo daerah, penyelenggara jasa internet/ISP, para operator telekomunikasi, dan asosiasi: APJII/PANDI/Nawala) serta para pakar dalam

*Focus Group Discussion* yang dilakukan beberapa kali untuk menggali tantangan dalam penerapan sistem *whitelist* dan harapan masyarakat terhadap sistem tersebut. Dari hasil pengumpulan data kualitatif dan kuantitatif dapat dilakukan analisis terhadap kekuatan (*strength*), kelemahan (*weakness*), peluang (*opportunity*) dan ancaman (*threat*) dari sistem *whitelist* seperti disajikan dalam Tabel 1.

**Tabel 1.** Analisis SWOT Sistem *Whitelist*

<b>Strength</b>	<b>Weakness</b>
<ul style="list-style-type: none"> <li>• Sistem <i>whitelist</i> lebih ketat, sehingga yang bisa diakses hanya situs yang diyakini positif isinya.</li> <li>• Sistem <i>whitelist</i> dapat menutup konten negatif yang menempel pada situs positif seperti: iklan atau <i>pop up</i>.</li> <li>• Terdapat Sistem <i>Whitelist</i> Nusantara yang sedang dikembangkan oleh Ditjen Aptika Kominfo sebagai peran pemerintah dalam memberi <i>supply</i> sistem secara gratis.</li> <li>• Sistem <i>whitelist</i> lainnya juga dikembangkan oleh pihak asosiasi (APJII) dan ISP, beberapa ISP bahkan telah mencoba memasarkan produk <i>whitelist</i></li> </ul>	<ul style="list-style-type: none"> <li>• Cara kerja tetap berbasis <i>domain</i>, sementara konten negatif dewasa ini lebih banyak disebarakan melalui aplikasi, media sosial dan iklan <i>online</i>.</li> <li>• Bagi ISP skala kecil, tidak dapat memproduksi sendiri sistem tersebut (<i>extra cost</i>).</li> <li>• Berdasarkan pengalaman beberapa ISP, produk <i>whitelist</i> masih kurang diminati, sehingga pada tahap awal implementasi, <i>whitelist</i> belum memiliki nilai jual, harus melalui ‘pemaksaan’.</li> </ul>

kepada masyarakat.

- Perawatan *database whitelist* dapat dilakukan secara terpusat, terdistribusi (pada masing-masing pengguna oleh administrator), atau kombinasi terpusat dan terdistribusi.

---

### **Opportunity**

- Ada kebutuhan yang besar dari masyarakat terhadap sistem penyaringan muatan/isi internet supaya layak konsumsi khususnya bagi anak/remaja.
- Mendorong penggunaan *domain .id* sebagai indikator *website* berkonten positif di Indonesia, dengan catatan registrasi ditertibkan.
- Didukung dengan sosialisasi manajemen konten internet lainnya seperti pengaturan menu *parental control* di aplikasi-aplikasi (misalnya di Youtube dan *play store* Android), semua aplikasi dapat diwajibkan memiliki menu tersebut; Penerapan sistem penyaringan yang sesuai dengan umur pengguna, ketika sudah tertib registrasi kartu prabayar; Pemingkatan konten dan segmentasinya sebagai referensi bagi masyarakat (seperti pada film).

---

### **Threat**

- Karena sifatnya pilihan, dikhawatirkan sistem tidak dipakai dalam jangka panjang oleh pihak sekolah/pesantren, jika dibandingkan dengan sistem kontrol dan pengamanan internet yang sudah dipasang di sekolah (seperti *proxy server*, Open DNS)
- Pengguna sistem merasa akses informasi, kreativitas, dan manfaat dari internet menjadi terbatas (di tahap awal hanya ditargetkan 250ribu situs). Banyak situs positif yang tidak menggunakan *domain .id*
- Perbedaan persepsi tentang definisi ‘positif’ pada daftar *whitelist* dan kategori/segmentasi kebutuhan pengguna (paket-paket informasi).
- Mekanisme *updating database whitelist* memakan waktu lama, sehingga menghambat pengguna dalam mencari informasi.
- Belum mengatasi dampak buruk/konten negatif internet dari akses yang dilakukan melalui *handphone*.

---

### **Tantangan Implementasi Sistem Whitelist**

Investasi biaya yang telah dikeluarkan untuk membangun sistem *whitelist* tentu dengan harapan bahwa sistem tersebut dapat bersifat jangka panjang dan digunakan secara efektif oleh pengguna yang disasar. Sementara berdasarkan hasil diskusi dengan beberapa pihak sekolah dan pondok pesantren, penggunaan internet di sekolah/pesantren sudah sedapat mungkin dikontrol oleh pihak sekolah/guru, seperti dituturkan oleh salah satu kepala sekolah sebagai berikut:

*“Fasilitas internet yang disediakan di sekolah telah diupayakan pemanfaatannya secara produktif untuk menunjang kegiatan belajar-mengajar. Internet digunakan untuk mencari sumber informasi atau mengerjakan tugas sekolah. Pihak sekolah telah melakukan pengawasan dan pendampingan terhadap penggunaan internet oleh siswa yang dilakukan melalui lab komputer dan WiFi sekolah, namun akses melalui handphone apalagi diluar sekolah*

*susah diawasi*” (Ahmad Nana, Kepala Sekolah SMAN 9 Tangerang Selatan dalam FGD tanggal 12 Mei 2016)

Namun demikian, peraturan yang diberlakukan oleh masing-masing sekolah terkait penggunaan internet di lingkungan sekolah berbeda-beda. Beberapa sekolah/pondok pesantren melakukan pembatasan yang ketat terhadap pemakaian *gadget/handphone/laptop* ketika berada di lingkungan sekolah, seperti di Ponpes Modern Selamat Semarang, Ponpes IMMIM Putera Makassar, dan SMAN 5 Makassar. Tetapi ada pula yang memberikan kelonggaran untuk mengakses internet termasuk Youtube dan media sosial dengan pertimbangan aplikasi tersebut dapat juga dipakai sebagai sarana belajar, seperti di SMKN 12 Bandung dan SMKN 2 Banjarmasin, namun dengan menambah proteksi terhadap akses internet yang tersedia pada fasilitas sekolah:

*“Fasilitas internet yang disediakan di SMKN 12 Bandung yaitu lab computer dan Wifi. Tidak ada pembatasan akses, dibuat terbuka termasuk untuk media sosial dan Youtube karena aplikasi tersebut juga dipakai untuk belajar. Untuk dapat mengontrol pemakaian internet oleh siswa di sekolah, telah diterapkan sistem filter internal dengan proxy server dan menggunakan aplikasi OpenDNS, selain menggunakan filter yang disediakan oleh provider.”* (Arfin Maulette, penanggungjawab bidang IT di SMKN 12 Bandung, dalam FGD tanggal 2 Mei 2016)

Di sisi lain, masih ada beberapa sekolah yang merasa belum menggunakan sistem penyaringan konten pada fasilitas internet di sekolah, seperti di SMK Tritech Medan. Dari

temuan ini tampaknya kebutuhan sekolah/pondok pesantren terhadap sistem *whitelist* berbeda-beda, dilihat dari ketersediaan sistem pengamanan akses internet. Ada sekolah yang urgen membutuhkan sistem *whitelist* karena belum menggunakan sistem penyaringan konten papun pada fasilitas internet di sekolah, namun ada pula yang berpendapat bahwa sistem *whitelist* belum menjadi kebutuhan penting di sekolahnya karena sudah menggunakan sistem penyaringan internal atau karena ketersediaan fasilitas komputer di sekolah yang masih terbatas sehingga masih mudah diawasi pemakaiannya oleh guru, seperti pada Ponpes Darunnajah Tangerang Selatan.

Kekuatan dari sistem *whitelist* terletak pada *database* yang dibangun, sehingga pengelolaan *database* menjadi penting untuk diperhatikan. Hal ini seperti yang diutarakan oleh M. Yamin, dari Nawala Nusantara, sebagai salah satu anggota tim *ad hoc* panel *database Whitelist* Nusantara.

*“Saat ini yang berjalan DNS blacklist, masih banyak kekurangannya. Selama 11 tahun terakhir selalu diperbaiki, namun tahun-tahun belakangan sudah mentok. Kunci dari penyaringan itu pada database-nya, yang paling penting pengelolaan database. Mau sistemnya apapun, database adalah yang paling penting.”* (M. Yamin, dari Nawala Nusantara, dalam FGD tanggal 16 Agustus 2016)

Perawatan *database whitelist* sebenarnya dapat dilakukan secara terpusat, terdistribusi (pada masing-masing pengguna oleh administrator), atau kombinasi terpusat dan terdistribusi. Sejauh ini, rancangan sistem *Whitelist* Nusantara menggunakan mekanisme pengelolaan *database* secara terpusat atau

*single database*, yaitu dilakukan oleh Forum Panel *Database Whitelist* Nusantara yang masih definitif. Namun, beberapa suara dari pihak sekolah sebagai calon pengguna sistem tersebut menghendaki mekanisme kombinasi terpusat dan terdistribusi, artinya ada administrator lokal di sekolah yang memungkinkan untuk menambah *database whitelist* sesuai kebutuhan sekolah. Hal ini seperti pada sistem *blacklist*, di mana pihak ISP dapat menambahkan daftar situs negatif sesuai aduan pelanggan, namun tetap mengacu pada *database Trust+*. Selain itu, terkait kecepatan dalam memperbaharui *database whitelist*, masih terdapat perbedaan pendapat antara perancang sistem dengan calon pengguna. Menurut M. Yamin, kehati-hatian dalam memasukkan suatu situs dalam daftar positif lebih penting sehingga tidak harus dilakukan dengan cepat, sementara beberapa suara dari calon pengguna menyatakan proses pembaharuan basis data *whitelist* perlu dibuat mudah dan cepat sehingga tidak akan membatasi akses informasi pengguna,

*“Ketika blacklist harus cepat responnya, karena impact-nya langsung dan harus segera di-block, sedangkan untuk whitelist tidak perlu cepat, yang pasti harus teliti. Kalau di blacklist jika salah memasukkan, masih bisa direvisi dan diperbaiki, sedangkan whitelist tidak bisa salah, harus teliti. Jadi respon time di whitelist bukan satu hal yang penting, yang penting itu ketelitian dalam menilai situs.”* (M. Yamin, Nawala Nusantara, dalam FGD tanggal 16 Agustus 2016)

*“Mekanisme dan proses updating basis data whitelist perlu dibuat mudah dan cepat sehingga tidak akan membatasi*

*akses informasi pengguna. Misalnya, sistem customizable artinya user dapat menambahkan langsung situs yang diperlukan sebagai whitelist atau ada fasilitas untuk merekomendasi situs whitelist”* (M. Yusran, Kepala Sekolah SMAN 5 Makassar, dalam FGD tanggal 2 Mei 2016)

Terkait hal-hal tersebut diatas, maka tantangan pertama bagi sistem *whitelist* yaitu memiliki nilai lebih dan mampu bersaing dengan sistem kontrol atau sistem penyaringan yang sudah dibangun oleh sekolah. Diharapkan sistem yang dibangun dapat melindungi tapi tidak membatasi informasi, kreativitas, kebutuhan pengguna internet. Sebab ada kekhawatiran dari pengguna terhadap terbatasnya *database*/daftar situs positif yang dapat diakses, khususnya pada tahap awal. Terlebih banyak situs positif di internet yang tidak/belum menggunakan domain .id. Ditjen Aptika Kemkominfo sendiri menargetkan hanya terkumpul 250ribu situs positif di tahap awal/di tahun 2016.

Untuk dapat menjawab tantangan ini, ada beberapa strategi yang dapat dilakukan pemerintah/Kemkominfo, di antaranya melakukan pengembangan sistem sehingga memiliki nilai lebih (*value added*) dari sistem pengamanan internet lainnya, seperti ada aplikasi *dashboard*; menyediakan portal *offline* untuk beberapa aplikasi yang direkomendasikan, namun sudah tersaring isinya; menyediakan aplikasi yang *user friendly* bagi publik untuk mengusulkan situs positif yang ingin ditambahkan/dikurangi dalam *database* selain itu juga dapat melakukan pengembangan *database* untuk mengakomodir kebutuhan informasi dan manfaat dari internet bagi pengguna sistem *whitelist*. Untuk itu perlu merangkul banyak

pihak terkait untuk bersama-sama membentuk forum panel *Whitelist* yang representatif dan memiliki wewenang untuk menyusun *database positive list* Indonesia.

Kemkominfo bekerjasama dengan Kementerian Pendidikan dan Kebudayaan dan Kementerian Agama, serta Pemerintah Daerah diharapkan dapat mendukung legalitas penerapan sistem *Whitelist* Nusantara di lingkungan sekolah/pesantren.

Pada tahap awal implementasi, melakukan pemilihan sekolah/pesantren yang *urgen* membutuhkan sistem *whitelist* untuk meningkatkan penggunaan internet secara positif di sekolah. Dalam alur pengelolaan *database whitelist*, memang dibutuhkan unsur kehati-hatian dalam menentukan kredibilitas usulan situs sebelum dimasukkan dalam *database*, namun response time tetap harus disepakati di awal sehingga tidak menghambat pengguna dalam mencari informasi. Ketika sistem sudah berjalan, Kominfo perlu menyusun mekanisme pengawasan terhadap penggunaan sistem oleh pengguna, sehingga dapat terus dilakukan perbaikan sistem jika ada kekurangan/belum sesuai dengan ekspektasi pengguna. Tantangan kedua bagi sistem *whitelist* yaitu terkait penyebaran konten negatif dewasa yang lebih banyak melalui aplikasi, media sosial dan iklan *online*. Hal ini seperti diutarakan oleh banyak penyelenggara jasa internet dalam forum FGD yang diadakan, salah satunya sebagai berikut:

*“Konten negatif itu tersebar tidak hanya dari domain, tapi juga di game online, aplikasi, slot iklan, posting di sosial media dan yang paling sulit adalah percakapan di chat. Domain atau situs sebenarnya trafiknya tidak begitu tinggi, perlahan website sudah mulai ditinggalkan.”* (Ariyanto Agus,

GM Network Security Management PT. Telkomsel, dalam FGD tanggal 22 Juni 2016)

Di samping itu, berdasarkan profil penggunaan internet dalam temuan penelitian, diketahui bahwa anak remaja lebih rentan terhadap dampak buruk/konten negatif internet dari akses yang dilakukan melalui *handphone*, dan yang diakses mayoritas media sosial/*instant messaging*, sehingga diharapkan sistem *whitelist* dapat menjadi solusi terhadap masalah tersebut. Terhadap tantangan ini, beberapa strategi yang dapat dilakukan pemerintah /Kemkominfo diantaranya Kemkominfo perlu menjalin kerjasama dengan pihak swasta, khususnya penyelenggara jasa internet dan operator telekomunikasi untuk menemukan konsep sistem *whitelist* yang dapat menjangkau akses internet melalui *handphone*, serta kuasa pada level aplikasi.

Sistem *whitelist* dapat didukung dengan sosialisasi manajemen konten internet lainnya, di antaranya pengaturan menu *parental control* di aplikasi-aplikasi tertentu, seperti Youtube dan *play store* Android. Atau dengan menyesuaikan atau mengaktifkan *save search* pada mesin pencari (*search engine*), sehingga *search engine* hanya menampilkan hasil pencarian yang pantas untuk ditampilkan. Fitur ini telah tersedia pada *search engine* besar di internet: Google, Yahoo, Bing, Youtube. Pemerintah dapat mensosialisasikan secara luas kepada pihak orangtua layanan manajemen konten internet yang sudah tersedia, untuk memperkuat fungsi pengawasan dari orangtua. Pemerintah dapat menjalin kerjasama dengan pihak penyedia aplikasi untuk menyediakan menu *parental control/parental lock* tersebut. Selain itu, pemerintah dapat pula melakukan pemeringkatan aplikasi/*website* baik di internet

dan segmentasinya sebagai referensi bagi masyarakat (seperti pada film dan *game online*). Ketika tertib registrasi kartu prabayar telah berlangsung di Indonesia, bisa didapatkan profil pengguna *gadget* dan internet yang lebih akurat, sehingga bisa dilakukan aplikasi *whitelist* yang dinamis, seperti pemberian layanan sesuai kriteria umur, bekerjasama dengan pihak operator. Tantangan ketiga terkait memasyarakatkan sistem *whitelist* agar dipahami dengan jelas dan menarik untuk digunakan. Untuk itu, strategi yang dapat dilakukan diantaranya Mendorong kampanye nasional tentang *whitelist* dengan kemasan yang menarik, mengarahkan anak untuk berpikir/berorientasi positif tentang internet, mengandung ekspektasi positif seperti menampilkan tokoh-tokoh yang sukses melalui internet atau bekerjasama dengan media, pendekatan inovasi melalui internet, sehingga dapat menarik pihak sekolah dan anak-anak untuk menggunakan sistem *whitelist*.

Menjalin kerjasama dan mengapresiasi pihak ISP yang telah memiliki/menawarkan paket *whitelist* kepada masyarakat. Selanjutnya, perlu diberikan insentif dan dukungan yang dibutuhkan sehingga makin banyak ISP yang mengembangkan/memasarkan paket serupa.

## KESIMPULAN DAN SARAN

Dari hasil penelitian diketahui bahwa karena sudah dilegalisasi melalui Peraturan Menteri Kominfo Nomor 19 Tahun 2014 tentang Penanganan Situs Internet Bermuatan Negatif, mayoritas responden sudah menggunakan sistem penyaringan situs negatif di internet (metode *blacklist*). Banyak pihak yang sudah merasakan manfaat sistem tersebut dalam menyaring situs-situs negatif. Namun, masih dijumpai pula kekurangan-kekurangan

sistem, seperti tetap ditemukan konten negatif yang tidak tersaring, utamanya pada iklan (ads) atau dari aplikasi yang berjenis *user generated content*. Dari hasil penelitian diketahui pula bahwa ada permintaan dan kebutuhan yang besar dari pengguna internet kalangan tertentu akan sistem penyaringan muatan internet yang lebih akurat. Keberadaan *whitelist* sebagai salah satu alternatif sistem yang akan ditawarkan pemerintah untuk menciptakan internet positif mendapatkan respon yang baik. Namun, penerapannya sebaiknya didasarkan atas permintaan dan diperuntukkan untuk pengguna kalangan terbatas, dan bukan untuk diberlakukan secara nasional karena akan menimbulkan banyak *noise* (pro-kontra).

Dalam implementasinya, beberapa tantangan penerapan sistem *whitelist* masih harus diperhatikan agar dapat bersifat jangka panjang dan dipakai secara efektif oleh pengguna. Sampai saat ini, dapat dikatakan bahwa sistem *whitelist* belum memiliki nilai jual, sehingga belum bisa diserahkan pada pasar (*market*). Untuk itu intervensi dari pemerintah diperlukan melalui penyediaan konten-konten positif serta ‘desain’ paket *whitelist* yang menarik. Untuk tahap awal implementasi di pihak sekolah dan pesantren yang menjadi target program, pemerintah bisa melakukan ‘pemaksaan’ melalui surat edaran, sampai pihak sekolah/pesantren merasakan manfaat dari sistem *whitelist* ini.

## UCAPAN TERIMA KASIH

Bersama ini kami ucapkan terima kasih kepada Tim Penelitian *Whitelist*, para peneliti, pimpinan dan pegawai Puslitbang Aptika dan IKP, serta semua pihak yang telah memperlancar dan membantu terselesainya penelitian ini.

## DAFTAR PUSTAKA

- Australian Cyber Security Centre (ACSC). (2016, April). *Implementing Application Whitelisting*. [http://www.asd.gov.au/publications/protect/application\\_whitelisting.htm](http://www.asd.gov.au/publications/protect/application_whitelisting.htm)
- Beechey, J. (2010). Application Whitelisting: Panacea or Propaganda?, SANS Institute.
- Bontchev, Vesselin. (2007). The dark side of whitelisting. Retrieved from <http://www.virusbtn.com/virusbulletin/archive/2007/08/vb200708-whitelisting>
- Cohen, Fred. (1990). Automated Integrity Maintenance for Viral Defense. *IFIP-TC11 Computers & Security*.
- Communications Security Establishment (CSE). (2015, March). Application Whitelisting Explained. IT Security Bulletin (ITSB-95) for the Government of Canada. <https://www.cse-cst.gc.ca/en/publication/itsb-95>
- Direktorat Pemberdayaan Informatika, Direktorat Jenderal Aplikasi Informatika. (2016). "Sistem *Whitelist* Nusantara untuk Menciptakan Internet Positif", slides presentasi dalam rapat 19 Juli 2016.
- Hawkins, D.I., R.J. Best, K.A. Coney. (2001). *Consumer Behaviour*, 8<sup>th</sup> edition, New York, USA: Mc.Graw-Hill, p.26.
- Kotler, P., & G. Armstrong. (2007). *Principles of Marketing*. Upper Saddle River, NJ: Prentice Hall.
- Kotler, Philip. (1997). *Marketing Management: Analysis, Planning, Implementation, and Control*, 9th Ed., Englewood Cliffs, NJ: Prentice Hall, Inc.
- Kurbalija, Jovan. (2010). *Sebuah Pengantar tentang Tata Kelola Internet*, ed. 1 Bahasa Indonesia, Penerbit: APJII dan DiploFoundation.
- Lo, Janet. (2010, November). Whitelisting for Cyber Security: What It Means for Consumers. Public Interest Advocacy Centre (PIAC), Canada. ISBN 1-895-060-94-X.
- National Cybersecurity and Communications Integration Center (NCCIC). (2015, Desember). Seven Steps to Effectively Defend Industrial Control Systems. <https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems>
- Yamin, M. (2016). "Sistem DNS *Whitelist* Nusantara", slides presentasi dalam Focus Group Discussion tanggal 16 Agustus 2016.

