CfDS
CENTER FOR DIGITAL SOCIETY

WSIS PRIZES 2018 CHAMPION

CASE STUDY SERIES #41

DECEMBER 2018

Merefleksi Strategi Keamanan Siber Nasional Inggris 2016-2021

Penulis
Anindita Lintang Pakuningjati

Editor
Lia Wulandari

Designer and Layouter
Naufal Alatas Radityasakti

Rangkuman NCSS UK 2016-2021 dan UK NCSC

Tuntutan membangun sebuah ekosistem digital yang aman di era modern mendorong pemerintah Inggris menaruh komitmen pada isu keamanan siber nasional. Komitmen ini diimplementasikan dalam strategi keamanan siber lima tahunan atau *National Cyber Security Strategy* dan pendirian lembaga pusat keamanan siber nasional atau *National Cyber Security Centre*. Tulisan ini memberikan gambaran mengenai lembaga keamanan siber Inggris dan strategi keamanan Inggris tahun 2016-2021 serta refleksi yang dapat dipetik pemerintah Indonesia dalam membuat strategi keamanan siber. Secara garis besar, strategi yang memiliki empat elemen utama yaitu *defend, deter, develop* dan aksi internasional ini merefleksikan tiga hal penting. Pertama ialah pentingnya cakupan sektor pada strategi. Kedua, adanya urgensi untuk menyiapkan infrastruktur keamanan siber. Terakhir, pentingnya pendekatan edukasi sebagai strategi berkelanjutan di ranah keamanan siber.

Pendahuluan

Data agen rahasia pemerintah Inggris bocor ke publik, jaringan transportasi publik diretas, kota-kota besar di Inggris kehilangan kendali akibat kekacauan lalu lintas. Kondisi diperparah dengan diretasnya jaringan kereta api nasional yang menyebabkan seluruh kereta berhenti bekerja. Puncak kekacauan terjadi ketika kontrol terhadap energi diambil alih melalui jarak jauh, dunia gelap seketika.

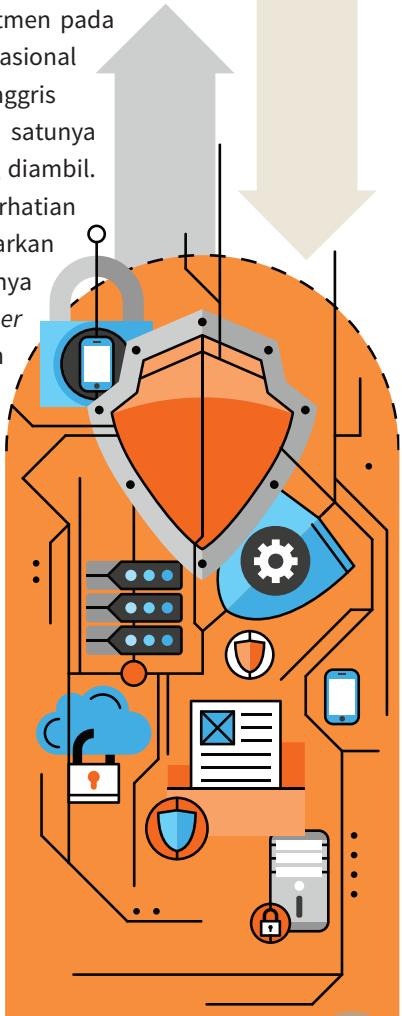
Cuplikasi situasi tersebut bukanlah adegan nyata, melainkan beberapa situasi adegan dalam sebuah film teranyar, *Johnny English Strikes Again* (2018), yang mengangkat skenario kekacauan saat Inggris mengalami serangan siber nasional. Meskipun terdengar dan terlihat hiperbola, ancaman-ancaman siber seperti yang diimajinasikan film *Jhonny English Strikes Again* ini sesungguhnya bukanlah ancaman semu sebab perkembangan teknologi digital dengan dampak signifikan pada praktik kehidupan bermasyarakat kini dibayangi oleh adanya peningkatan ancaman siber yang kini menjadi perhatian dunia.[1]

Ancaman siber tentu tidak dapat dianggap remeh sebab dunia digital sudah menjadi sebuah ekosistem yang melekat hampir di seluruh aspek kehidupan masyarakat seperti sektor pelayanan publik, infrastruktur hingga bisnis kecil dan raksasa.[2] Lonjakan ancaman siber selama satu dekade terakhir di dunia pun membuat serangan siber (*cyberattack*)

masuk dalam lima besar ancaman terbesar bagi dunia dalam World Economic Forum's Global Risk Report 2018.[3] Kondisi ini berdampak pada tuntutan atas ekosistem digital yang aman dan perhatian yang serius pada isu keamanan siber (*cybersecurity*) sebagai sebuah isu strategis yang membutuhkan aksi-aksi nyata.

Berkaitan dengan pengamanan siber, meskipun bukan menjadi aktor tunggal, pemerintah memegang peranan yang penting di dalam menjaga ekosistem digital yang stabil dan aman. Peranan pemerintah dalam upaya keamanan siber sangat mendasar untuk membangun sebuah pondasi sistem yang komprehensif.[4] Selain itu, pemerintah juga berperan sebagai pemain utama yang mengatur arus "permainan" keamanan siber.[5]

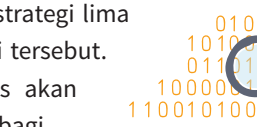
Salah satu pemerintah yang memiliki komitmen pada isu keamanan siber sebagai salah satu fokus agenda nasional ialah pemerintah Inggris. Keseriusan pemerintah Inggris dalam menangani isu keamanan siber ini salah satunya ditunjukkan di dalam langkah-langkah strategis yang diambil. Pertama dan utama, Pemerintah Inggris menaruh perhatian spesifik pada keamanan siber dengan mengeluarkan langkah-langkah strategis lima tahun dalam kaitannya dengan keamanan siber nasional dalam *National Cyber Security Strategy* 2016-2021. Kedua, pemerintah Inggris menginvestasikan £1.9 miliar dana ke dalam strategi 5 tahun tersebut. Ketiga, pemerintah Inggris membentuk lembaga khusus yang berfokus pada isu keamanan siber nasional bernama *National Cyber Security Centre* secara resmi bersamaan dengan peluncuran strategi nasional tersebut.[6]

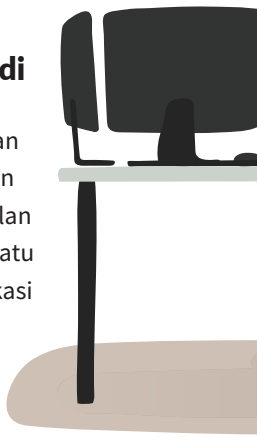


Langkah pemerintah Inggris untuk menaruh perhatian khusus pada isu keamanan siber didorong dengan kondisi peningkatan serangan siber setiap tahunnya. Pertumbuhan kasus *cyber-crime* meningkat tajam, hingga di tahun 2015 kasus criminal dan ancaman siber diperkirakan dapat melebihi kasus perdangan narkoba di Inggris.[7] Beberapa kasus nasional menjadi sorotan, misalnya, kasus kebocoran data pengguna TalkTalk pada tahun 2015[8] dan serangan siber pada sistem layanan

kesehatan nasional Inggris, NHS (*National Health Service*) pada tahun 2017[9] semakin mendesak pemerintah untuk berfokus pada isu keamanan siber. Selain itu, sebagai negara dengan pertumbuhan ekonomi nomor enam di dunia, keamanan siber Inggris, secara sadar maupun tidak, memberikan pengaruh yang signifikan pada perkembangan keamanan siber global.[10]

Studi kasus ini akan secara ringkas memberikan gambaran besar mengenai Strategi Nasional Keamanan Siber Inggris tahun 2016-2021. Pembahasan akan dimulai dengan ulasan mengenai perkembangan isu keamanan siber di Inggris akan ditampilkan untuk memberikan gambaran kondisi dan situasi yang mendasari pengambilan keputusan. Studi kasus ini kemudian akan mengupas strategi lima tahunan pemerintah Inggris yang diikuti dengan refleksi dari strategi tersebut. Kritik dan poin-poin penting dalam strategi pemerintahan Inggris akan menjadi *highlight* dari refleksi sebagai pembelajaran dan masukan bagi perkembangan keamanan siber di Indonesia kedepan.





Perkembangan Langkah Strategis Keamanan Siber di Inggris

Jauh sebelum agenda keamanan siber digaungkan, perubahan dunia teknologi komunikasi menjadi pendorong utama perhatian pemerintah Inggris pada bidang keamanan informasi.[11] Kemunculan teknologi telegram pada masa akhir abad ke-19 menjadi salah satu pemantik kesadaran pemerintah akan kerapuhan sistem komunikasi yang dapat berujung pada kebocoran informasi keamanan negara. Perkembangan komunikasi *wireless* dan *code making* pun menjadi pendorong lain bagi kebutuhan keamanan sistem informasi. Salah satu momentum penting di dalam perjalanan langkah-langkah strategis keamanan siber di Inggris adalah lahirnya *Government Communications Heaquarters* (GCHQ) di tahun 1919. Lembaga ini kemudian menjadi cikal bakal langkah strategis keamanan yang kemudian berfokus pada keamanan siber.[12]

Perubahan signifikan terjadi saat internet berkembang dalam sistem komunikasi dunia. *Cyberspace* menjadi ekosistem yang rentan terhadap ancaman keamanan. Pemerintah Inggris baik di level regional dan nasional menghadapi adanya peningkatan ancaman siber yang pesat.[13] Pertumbuhan ancaman siber ini tidak hanya datang pada level ancaman domestik namun juga mancanegara mengingat leburnya batas-batas geografis sebagai dampak dari internet dan fenomena "*Internet of Things*."[14]

Pada tahun 2009, pemerintah Inggris meluncurkan *Cyber Security Strategy* 2009 yang berujung pada pembentukkan multi agen *Cyber Security Operations Centre* (CSOC) yang digawangi oleh GCHQ dan dioperasikan bersama dengan *Communications Electronics Security Group* (CESG).[15] Pada tahun 2011, Pemerintah Inggris memperbaharui strategi keamanan siber dengan meluncurkan UK 2011 *National Cyber Security Strategy* (NCSS) yang kali ini dibangun oleh *Office of Cyber Security and Information Assurance* (OCSIA) dengan alokasi dana hingga tahun 2016 yang diperkirakan lebih dari £860 juta.[16]

Meskipun telah mengambil beberapa langkah strategis dan membentuk lembaga-lembaga koordinasi dalam isu keamanan siber, ancaman dan serangan siber terus meningkat secara signifikan. Paling tidak sebanyak 81% perusahaan besar dan 60% bisnis kecil tercatat mengalami kebocoran data siber[17] dan paling tidak sebanyak 2/3 bisnis-bisnis besar di UK menjadi target serangan siber selama tahun 2015 hingga 2016.[18] Strategi lima tahun ini masih dinilai gagal menjawab tantangan perubahan ancaman siber.[19] [20]

Akhirnya di tahun 2016, untuk menjawab tantangan keamanan siber yang kian kompleks, pemerintah Inggris meluncurkan strategi 5 tahunan teranyar untuk tahun 2016-2021. Nilai investasi dana untuk strategi ini pun meningkat cukup signifikan mencapai £1.9 miliar. Selain itu, peluncuran strategi itu juga diikuti dengan pendirian badan khusus yang berfokus pada penanganan isu keamanan siber yaitu *National Cyber Security Centre* (NCSC) di bawah naungan GCHQ. NCSC bekerja dalam ranah isu keamanan siber mulai dari pemahaman keamanan siber, merespon dan menangani insiden keamanan siber serta memelihara kapabilitas keamanan siber di UK baik di bidang industry maupun akademik. Selain itu, NCSC juga bertugas menjaga jaringan di sektor publik hingga swasta di Inggris.[21]

National Cyber Security Centre

a part of GCHQ

Strategi Keamanan Siber Nasional Inggris 2016-2021: Gambaran Umum dan Cakupan Strategi

Strategi keamanan siber nasional tahun 2016-2021 di Inggris memiliki satu visi untuk menjadikan Inggris aman dan kuat terhadap ancaman siber, makmur dan percaya diri di dunia digital. Melalui strategi terbaru ini pemerintah ingin memastikan setiap individu dapat menjalankan bisnis di lingkungan digital Inggris yang aman. Cakupan strategi dan juga ambisi yang ingin dicapai strategi ini cukup luas. Namun, keseluruhan strategi dapat dilihat dari empat (4) elemen utama pengejawantahan visi yaitu membela diri (*defend*), menghalangi (*deter*), mengembangkan (*develop*) dan aksi internasional (*international action*).[22] Masing-masing elemen terbagi menjadi beberapa langkah strategis, yang di dalamnya terdapat ambisi-ambisi yang ingin dicapai, pendekatan yang akan digunakan dan indikator keberhasilan.

Strategi nasional ini digunakan sebagai acuan untuk membuat kebijakan pemerintah, namun di sisi lain juga berupaya menyediakan visi yang koheren bagi sektor publik, swasta, masyarakat umum, akademisi maupun khalayak yang lebih luas. Cakupan strategi ini bersifat menyeluruh untuk seluruh kawasan United Kingdom. Selain itu, berkaitan dengan sektor yang menjadi cakupan strategi, pemerintah berupaya mencakup seluruh sektor ekonomi dan sosial mulai dari organisasi pemerintah hingga individu sipil.

1. *Defend*

Elemen ini bertujuan untuk mempertahankan dan membentengi diri sendiri dari perkembangan ancaman siber. Salah satu dimensi utama dari pertahanan adalah melindungi infrastruktur kritis nasional dari ancaman siber. Selain itu, pemerintah juga berupaya merespon insiden secara efektif dan memastikan jaringan, data dan sistem yang aman dan tangguh pada ancaman dan serangan siber. Salah satu poin penting yang perlu dicatat di dalam elemen pertahanan ialah adalah adanya ekspektasi terhadap masyarakat, bisnis atau industri dan sektor publik untuk memiliki pengetahuan dan kemampuan pertahanan diri sendiri.

Meskipun pemerintah memiliki ekspektasi terhadap 'kemandirian' masyarakat dan industri, Tech UK mencatat setidaknya terdapat 3 peranan pemerintah di ranah strategi pertahanan ini. Pertama, pemerintah bekerja bersama provider layanan komunikasi (CSPs) untuk memblokir serangan *malware* dengan cara membatasi akses terhadap domain dan website tertentu yang dikenal sebagai sumber *malware*. Kedua, pemerintah melakukan pencegahan aktivitas *pishing* dengan menerapkan standar sistem verifikasi email pada jaringan pemerintah. Ketiga, pemerintah

bekerja sama dengan penegak hukum dalam langkah perlindungan warga dari target serangan siber sebagai akibat kerapuhan insfrastruktur jaringan lintas negara.

2. *Deter*

Strategi ini dilakukan guna menghalangi serangan siber masuk ke dalam lingkungan digital Inggris, salah satunya dengan menjadikan Inggris sebagai target yang sulit bagi serangan dan ancaman siber dunia. Langkah-langkah yang dilakukan cukup komprehensif, meliputi deteksi, pemahaman, investigasi dan tindakan terhadap gangguan, termasuk dengan pengejaran dan penuntutan bagi pelaku kejahatan siber.[23]

Pendekatan kerja kolaboratif menjadi kunci di dalam implementasi strategi ini. Pemerintah Inggris menekankan pentingnya kolaborasi antara agensi intelijen, Kementerian Pertahanan, lembaga penegak hukum, *National Crime Agency* hingga agen internasional guna mengurangi kejahatan siber dan menghalangi serangan siber dunia. Kolaborasi memang dibutuhkan mengingat kompleksitas dan luasnya ruang digital yang memungkinkan celah-celah serangan terjadi. Selain itu, salah satu poin menonjol dalam langkah strategis pemerintah di dalam elemen strategi *deter* ialah kesadaran pemerintah akan pentingnya enkripsi guna melindungi informasi-informasi sensitif.

3. *Develop*

Strategi membangun (*develop*) dibutuhkan guna memperoleh dan menguatkan infrastuktur dan kapabilitas yang dibutuhkan untuk melindungi Inggris dari serangan dan ancaman siber.[24] Strategi ini memiliki peran yang krusial sebagai sebuah strategi jangka panjang untuk keberhasilan program-program pemerintah yang berkelanjutan. Strategi ini terimplementasikan salah satunya dalam langkah penguatan keterampilan berkaitan dengan keamanan siber yang berfokus pada pengembangan sumber daya manusia. Sebagai contoh, Pemerintah Inggris memiliki ambisi untuk menyediakan profesional yang kompeten, terlatih dan siap untuk menjaga stabilitas keamanan siber nasional, tidak hanya dalam jangka waktu 5 tahun tetapi untuk 20 tahun kedepan.

Di samping fokus pada pengembangan SDM, strategi *develop* juga menitikberatkan langkah pengembangan industri pada sektor keamanan siber dengan langkah-langkah investasi dan kerjasama dengan perusahaan untuk pengembangan produk yang berkaitan dengan keamanan siber. Salah satu langkah menonjol berkaitan dengan strategi pengembangan ini ialah alokasi proprosi dana Pertahanan dan Inovasi Siber sebesar £165 juta untuk mendukung

pengadaan inovasi di bidang pertahanan dan keamanan. Selain itu, pemerintah Inggris juga tidak melupakan investasi pada penelitian ilmiah dan teknologi dan integrasi program antara bidang keamanan nasional dengan area kebijakan lain.

4. Aksi Internasional

Selain berfokus pada ketiga strategi dalam negeri, pemerintah Inggris menyadari perlunya kerja sama internasional untuk keberhasilan jangka panjang. Oleh karena itu, pemerintah Inggris melebarkan kerja sama dengan beragam *stakeholders* internasional mulai dari pemerintah, organisasi multilateral internasional, komunitas internasional hingga penyedia layanan swasta. Selain itu, upaya promosi lingkungan siber yang kuat juga diambil guna meyakinkan satu kesepakatan tentang pentingnya keamanan siber mulai dari desain.

Refleksi Strategi: Infrastruktur dan Edukasi sebagai Kunci Strategi

Sebagai sebuah strategi nasional, UK NCSS 2016-2021 dapat menjadi salah satu referensi strategi yang fundamental untuk kebijakan keamanan siber nasional sebuah negara. Meski bukan contoh yang sempurna untuk sebuah strategi nasional, beberapa fokus strategi Inggris dapat dijadikan rujukan yang patut dipertimbangkan untuk dicontoh.

Secara general, strategi ini dapat dikatakan sebagai sebuah strategi yang komprehensif dalam menanggapi pertumbuhan ancaman siber global dan nasional.[25] Visi pemerintah Inggris pada strategi lima tahunan kali ini jelas dan juga percaya diri. Visi tersebut pun dijabarkan dalam empat pilar strategi utama yang jelas dengan tujuan-tujuan yang lebih mendetil lengkap dengan penjelasan langkah implementasi dan indikator keberhasilan.

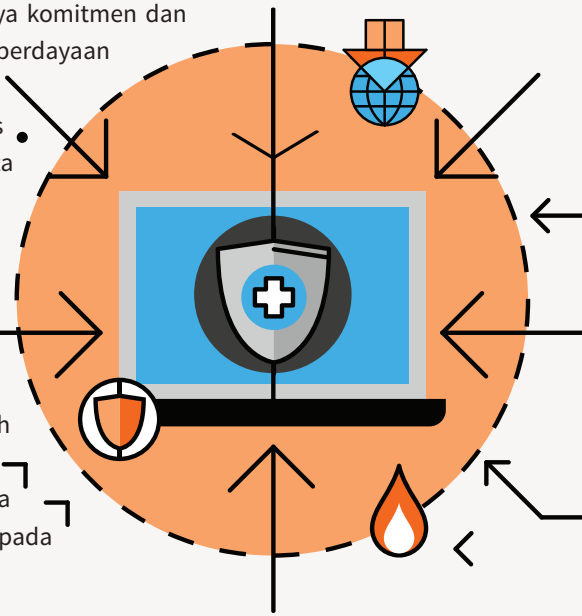
Meskipun demikian, strategi yang komprehensif juga dapat berdampak pada cakupan strategi yang terlalu luas. Strategi ini menuai kritik pada beberapa area yang dianggap terlalu luas dan belum mencakup beberapa area strategis yang krusial,[26] seperti minimnya fokus pada sektor privat yang dinilai sebagai salah satu kunci penting kekuatan keamanan siber sebuah negara,[27] Namun demikian, terlepas dari kurangnya perhatian pemerintah pada sejumlah sektor, tidak dapat dipungkiri bahwa jangka waktu lima tahun tidaklah cukup panjang untuk mengerjakan seluruh aspek keamanan siber pada sebuah negara.[28]

Terlepas dari cakupan atau jangkauan sektor pada strategi yang menuai beragam perspektif, setidaknya ada dua poin penting yang dapat dijadikan catatan untuk sebuah strategi nasional negara. Pertama ialah pentingnya dimensi infrastruktur di dalam strategi keamanan siber. NCSS 2016-2021 Inggris menerima kritik atas kurangnya startegi yang berkaitan dengan dimensi perlindungan dan infrastruktur keamanan siber.[29]

Sean Martin, general manajer Covata, sebuah perusahaan spesialis keamanan data di Inggris, mengatakan bahwa badan-badan di pemerintahan Inggris sendiri masih kesulitan untuk melakukan pertukaran informasi dan data secara aman, bahkan pada level yang paling mendasar sekalipun.[30] Persoalan pertukaran informasi dan data ini pun sesungguhnya telah menjadi catatan strategi lima tahun sebelumnya (2011-2016) berkaitan dengan perlunya sistem komputasi awan dalam perencanaan pemerintah.[31]

Pemerintah Inggris sendiri sebenarnya telah menyinggung permasalahan infrastruktur, utamanya di persoalan pertukaran data dan informasi, melalui strategi data enkripsi.[32] Hanya saja mengingat tingginya kerentanan akses pertukaran informasi dan data, nampaknya pendekatan baru yang berkaitan dengan teknologi komunikasi lain masih perlu menjadi perhatian khusus pada strategi keamanan siber nasional negara ini ke depannya.

Salah satu hal yang juga sangat penting, yang di satu sisi menjadi dimensi positif dari NCSS 2016-2021 adalah adanya komitmen dan pendekatan edukasi untuk pemberdayaan talenta-talenta profesional di bidang keamanan siber. Pemerintah Inggris menyadari realitas bahwa talenta-talenta profesional di bidang keamanan siber menjadi salah satu faktor inti dari sebuah sistem keamanan siber yang kuat.[33] Tanpa adanya sumber daya manusia yang mampu mengoperasikan dan menguasai teknologi serta melakukan inovasi, perencanaan sistem secanggih apapun akan menjadi sia-sia. Oleh karena itu pelatihan dan pendidikan sumber daya manusia memiliki peran yang signifikan pada sebuah strategi keamanan siber.



Pendekatan edukasi ini dapat menjadi salah satu refleksi penting bagi negara-negara lain. Selain memperikan sumber daya profesional, pendekatan edukasi juga dapat bermanfaat untuk menguatkan individu-individu agar lebih waspada dan dapat melakukan mitigasi keamanan siber secara mandiri.[34]

Kesimpulan

Keamanan siber telah menjadi sorotan dunia sebagai dampak tingginya pertumbuhan ancaman dan serangan siber dunia beberapa tahun belakangan. Sebuah ekosistem digital yang aman menjadi tuntutan di era yang modern. Dalam rangka menciptakan sebuah ekosistem digital yang aman, pemerintah perlu mengambil sebuah peran yang signifikan. Meskipun bukan satu-satunya aktor utama, pemerintah memegang peranan krusial dalam menyusun fondasi ekosistem melalui kebijakan-kebijakan yang diambil.

Pemerintah Inggris menjadi salah satu pemerintah yang sudah berkomitmen untuk menaruh fokus pada isu keamanan siber. Komitmen itu diimplementasikan melalui strategi nasional lima tahunan berkaitan dengan keamanan siber dan pendirian lembaga yang berfokus pada isu keamanan siber nasional atau *National Cyber Security Centre*. Perhatian pemerintah Inggris pada isu keamanan siber semakin menguat setelah investasi sebesar £1.9 miliar diberikan khusus untuk mengawal strategi nasional keamanan siber 2016-2021 negara ini.

Strategi lima tahunan teranyar milik Inggris ini memiliki empat elemen utama yaitu *defend, deter, develop* dan aksi internasional. Keempat elemen tersebut masing-masing memiliki langkah strategis, ambisi-ambisi yang ingin dicapai, pendekatan yang akan digunakan dan indikator keberhasilan.

Strategi lima tahunan teranyar milik Inggris ini memberikan sebuah refleksi mengenai pentingnya cakupan sektor pada strategi nasional. Mengingat luasnya sektor yang dipengaruhi oleh dunia siber, pemerintah tidak hanya perlu memperhatikan sektor-sektor publik, namun juga sektor privat yang turut andil dalam kesatuan ekosistem digital nasional. Selain itu, pemerintah juga perlu menyiapkan dan berfokus pada insfrastruktur keamanan siber pada setiap strateginya guna menghadapi pertumbuhan ancaman dan serangan siber yang kian besar. Terakhir, penting bagi pemerintah untuk melakukan pendekatan edukasi dan melakukan investasi sumber daya manusia. Investasi sumber daya manusia ini akan bermanfaat untuk memaksimalkan infrastruktur dan juga untuk kesuksesan keamanan siber yang berkelanjutan di masa yang akan datang.

Referensi

[1]Wayne Harrop and Ashle Matteson, 'Cyber Resilience: A Review of Critical National Infrastructure and Cyber-Security Protection Measures Applied in the UK and USA', in Frederic Lemieux (ed), *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice* (New York: Palgrave Macmillan), hlm.149-166.

[2]TechUK, 'techUK Analysis of National Cyber Security Strategy', n.d, TechUK . (Online). Diperoleh dari:http://www.techuk.org/component/techuksecurity/security/download/9627?file=techUK_Analysis_of_National_Cyber_Security_Strategy.pdf&Itemid=177&return=aHR0cDovL3d3dy50ZWNodWsub3JnL2luc2lnaHRzL25ld3MvaXRlbS85NjI3LWdvdmVybm1lbnQtcmVsZWFzZXMtbmF0aW9uYWwtY3liZXItc2VjdXJpdHktc3RyYXRlZ3k= > [diakses pada 9 oktober 2018].

[3]World Economic Forum, 'The Global Risks Report 2018 13th Edition', 2018. (Online). Insight Report World Economic Forum. Diperoleh dari: <http://www3.weforum.org/docs/WEF_GRR18_Report.pdf> [diakses 10 oktober 2018].

[4]TechUK, 'techUK Analysis of National Cyber Security Strategy'

[5]*Ibid*.

[6]Joe Kim, (2017) 'Cyber-security in goverment: reducing the risk', (Online). *Computer fraud & security*, 7, Diperoleh dari: <https://ac.els-cdn.com/S1361372317300593/1-s2.0-S1361372317300593-main.pdf?_tid=19411a4a-c718-4b88-9ed3-8a4564c1f9d8&acdnat=1539348393_6d0ee8277f48eaffffab9dc5544c650a> [diakses 11 oktober 2018]. pp.8-11

[7]Adeptis, (2015), London police chief Leppard admits cyber-crime failings, (Online). Diperoleh dari: https://adeptisgroup.com/london-police-chief-admits-cyber-crime-failings/ [diakses 12 oktober 2018].

[8]BBC, (2015), TalkTalk cyber attack: Website hit by 'significant' breach, (Online). Diperoleh dari: https://www.bbc.co.uk/news/uk-34611857 [diakses 12 oktober 2018].

[9]Lizzie Dearden, (2017), NHS trust hit by cyber attack cancels operations and asks patients not to come to hospital 'unless it is essential', (Online). Diperoleh dari: https://www.independent.co.uk/news/uk/home-news/cyber-attacks-uk-nhs-lanarkshire-scotland-hospitals-affected-patients-operations-ransomware-wannacry-a7913896.html [diakses 12 oktober 2018].

[10]Danielle Kriz, (2017), A Global Model: UK's National Cyber Security Strategy, (Online). Diperoleh dari: https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/ [diakses pada 10 oktober 2018].

[11]National Cyber Security Centre, (2017), Our History, (Online). Diperoleh dari: https://www.ncsc.gov.uk/information/our-history [diakses 9 oktober 2018].

[12]National Cyber Security, *The launch of the National Cyber Security Centre: A Snapshot of the Past, Present and Future of Cyber Security* (n.p, n.d) (Online). Diperoleh dari: https://www.ncsc.gov.uk/content/files/protected_files/news_files/The%20launch%20of%20the%20National%20Cyber%20Security%20Centre.pdf [diakses 8 oktober 2018].

[13]Kristan Stoddart. (2016) 'UK Cyber Security and Critical National Infrastructure Protection', *International Affairs*, 92(5),pp.1079-1105.

[14] Kristan Stoddart. 'UK Cyber Security and Critical National Infrastructure Protection', pp.1080-1081

[15] *Ibid*,. p.1085

[16] *Ibid*,. p.1087.

[17] Gov UK, *2010 to 2015 government policy: cyber security* (n.p, 2015) (Online) diperoleh dari: https://www.gov.uk/government/publications/2010-to-2015-government-policy-cyber-security/2010-to-2015-government-policy-cyber-security [diakses 8 oktober 2018].

[18] BBC, (2016), Cyber attacks: two-thirds of big UK businesses targeted. (Online) Diperoleh dari: https://www.bbc.co.uk/news/uk-36239805 [diakses 9 oktober 2018].

[19] TechUK, 'techUK Analysis of National Cyber Security Strategy.'

[20] National Cyber Security Centre, *National Cyber Security Strategy 2016*, (n.p, 2016).

[21] National Cyber Security Centre, (2017), About the NCSS. (Online). Diperoleh dari: https://www.ncsc.gov.uk/information/about-ncsc [diakses 7 oktober 2018].

[22] TechUK, 'techUK Analysis of National Cyber Security Strategy'.

[23] TechUK, 'techUK Analysis of National Cyber Security Strategy'.

[24] National Cyber Security Strategy, p.53.

[25] TechUK, 'techUK Analysis of National Cyber Security Strategy'.

[26] *Ibid*.

[27] Tracy Caldwell. (2017) 'The UK's 1.9bn cyber-security spend- getting the priorities right' *Computer fraud & security*, 3, (Online). Diperoleh dari: https://www.sciencedirect.com/science/article/pii/S1361372317300246 [diakses 10 oktober 2018]. pp.12-20

[28] TechUK, 'techUK Analysis of National Cyber Security Strategy'.

[29] *Ibid*,. p.18.

[30] *Ibid*,. p.16.

[31] Neville-Jones, P. and Phillips, M. (2012) 'Where next for UK cyber-security?', *The RUSI Journal*, 157(6), pp.32-40.

[32] Lihat NCSS 2016-2021 Inggri, implementasi strategi '*deter*'.

[33] Tracy Caldwell, 'The UK's 1.9bn cyber-security spend- getting the priorities right', p.14.

[34] Tracy Caldwell, 'The UK's 1.9bn cyber-security spend- getting the priorities right', p.15.

Center for Digital Society

Faculty of Social and Political Sciences
Universitas Gadjah Mada
Room BC 201-202, BC Building 2nd Floor,
Jalan Socio Yustisia 1
Bulaksumur, Yogyakarta, 55281, Indonesia

Phone : (0274) 563362, Ext. 116
Email : cfds.fisipol@ugm.ac.id
Website : cfds.fisipol.ugm.ac.id

facebook.com/cfdsugm
cfds.fisipol.ugm.ac.id
cfds_ugm
@cfds_ugm
@cfds_ugm
CfDS UGM