e-Jurnal Apresiasi Ekonomi Volume 10, Nomor 3, September 2022 : 321-331 ISSN Cetak : 2337-3997
ISSN Online : 2613-9774

EVALUASI KEBIJAKAN CYBER SECURITY SEKTOR PERBANKAN BANK BTN CABANG SURABAYA

EVALUATION OF CYBER SECURITY POLICY IN THE BANKING SECTOR OF BANK BTN SURABAYA BRANCH

Rudiatno[1], Aldea Mita Cheryta[2]

[1,2]Fakultas Ekonomi dan Bisnis, Universitas Wijaya Putra
email: rudiatno@uwp.ac.id[1], aldeamitacheryta@uwp.ac.id[2]

ABSTRAK

Penelitian ini membahas tentang evaluasi kebijakan *cyber security* pada sektor perbankan di Bank BTN Surabaya dengan menggunakan metode kualitatif dan teknik pengumpulan data *indepth interview* dan *focus group discussion*. Focus penelitian ini yaitu evaluasi kebijakan dan pencegahan kejahatan *cyber* pada perbankan. Lokasi penelitian ini dilakukan di Bank BTN Prioritas Cabang Surabaya, pemilihan lokasi penelitian ini disebabkan karena Bank BTN merupakan salah satu bank yang menerapkan langkah preventif dalam pencegahan *cybercrime*. Permalasahan yang akan dijabarkan dalam artikel ini adalah *Pertama,* Bagaimana dampak *cyber security* pada Bank BTN Cabang Surabaya? *Kedua,* Bagaimana strategi kebijakan pemerintah tentang *cyber security*? *Ketiga,* Bagaimana pencegahan kejahatan *cyber-crime* pada Bank BTN Cabang Surabaya? Kesimpulan penelitian ini adalah pada Bank BTN Surabaya menunjukkan langkah preventif yang baik dengan membentuk struktur organisasi khusus untuk menangani permasalahan legalitas dan penerapan aplikasi pencegahan kejahatan *cyber*. Bank BTN melakukan evaluasi kebijakan setiap dua minggu sekali sebagai bentuk evaluasi pencapaian target dan evaluasi bulanan yang dilakukan oleh atasan secara langsung. Lebih lanjut setiap enam bulan sekali Bank BTN Surabaya mendatangkan audit eksternal untuk dapat mengawasi dan memonitoring.

Keywords: Bank, Cyber Security, Evaluation

ABSTRACT

This study discusses the evaluation of cyber security policies in the banking sector at Bank BTN Surabaya using qualitative methods and data collection techniques indepth interviews and focus group discussions. The focus of this study is policy evaluation and prevention of cybercrime in banking. The location of this study was conducted at Bank BTN Prioritas Surabaya Branch, the selection of the location of this study was due to bank BTN being one of the banks that implemented preventive measures in preventing cybercrime. The problem that will be described in this article is First, How is the impact of cyber security on Bank BTN Surabaya Branch? Second, What is the government's policy strategy on cyber security? Third, How to prevent cyber-crime at Bank BTN Surabaya Branch? The conclusion of this study is that Bank BTN Surabaya shows good preventive steps by forming a special organizational structure to deal with legality issues and the implementation of cybercrime prevention applications. Bank BTN conducts policy evaluations every two weeks as a form of evaluation of target achievement and monthly evaluations carried out by their superiors directly. Furthermore, every six months Bank BTN Surabaya brings in an external audit to be able to supervise and monitor.

Keywords: Bank, Cyber Security, Evaluation

PENDAHULUAN

Evaluasi kebijakan merupakan salah satu upaya terpenting dalam pengambilan kebijakan publik. Terapan dari evaluasi mengasilkan suatu perbaikan yang nyata dan dapat menjadi acuan utama dalam perbaikan sebuah kebijakan, terlepas dari hal tersebut evaluasi juga menjadi standar utama dalam tahap akhir merumuskan kebijakan. Penelitian (Calderaro & Craig, 2020) menyimpulkan satu analisis bahwa pembuat kebijakan harus melanjutkan upaya mereka untuk meningkatkan pengetahuan di negara-negara yang belum menerapkan secara utuh tentang konektivitas.

Evaluasi selalu dihinggapi dengan adanya monitoring secara empiris, sehingga efektivitas

dari sebuah evaluasi dapat berfungsi lebih baik. Akan tetapi seringkali sebuah evaluasi dijadikan sebagai satu syarat normative untuk menerapkan sebuah kebijakan yang ada di masyarakat. Konsekuensi dari pembuat kebijakan yang demikian adalah mempertaruhkan kondisi keutuhan rakyat dalam mengembangkan kegiatan sosialnya. Terlebih jika arah suatu kebijakan tidak tepat sasaran, maka justru akan menjadi kontradiksi di dalam masyarakat, akhirnya adalah tingkat kepercayaan publik. Dewasa ini kepercayaan publik diukur berdasarkan survei-survei kuantitatif untuk menghitung apakah setiap individu merasa terbantu dengan adanya kebijakan tersebut.

Evaluasi kebijakan akan secara kontinu diterapkan pada kebijakan yang sifatnya masih baru sekaligus issue baru yang ada di masyarakat. Salah satu issue tersebut adalah *cyber security*, dimana hal tersebut merupakan tolak ukur utama dalam keberhasilan kebijakan transformasi. Tidak menutup kemungkinan sebuah kebijakan dapat berdampak buruk, dikarenakan arah dan tujuan sasaran kebijakan yang tidak dapat disesuaikan dengan kondisi empiris masyarakat. *Cyber security* menjadi hal yang sangat penting untuk dipertimbangkan kembali sehingga terdapat tingkat kepercayaan tinggi yang berimplikasi pada percepatan perputaran investasi.

Penelitian (Stevens et al., 2019) mengusulkan bahwa dalam suatu bidang krusial harus terdapat kerjasama intelijen dan keamanan sangat perlu ditingkatkan, tantangan *cyber security* tersebesar *cyber-crime* yang akan berimplikasi khusus pada kasus *Brexit* di Eropa. Kasus *Brexit* eropa menjadi pembelajaran dunia tentang pentingnya evaluasi *cyber security* untuk dapat secara eksis di tengah gempuran-gempuran para pelaku *cyber-crime.* Point utama dari Brexit eropa adalah lemahnya *cyber security* ketika itu untuk menghadapi serangan-serangan yang mungkin terjadi secara mendadak pada sektor perbankan.

Sektor perbankan merupakan sektor yang paling rentan untuk mendapatkan serangan cyber, mengingat begitu banyak transaksi yang terjadi pada sektor perbankan. Ekstrim dari sektor perbankan yang lemah misalnya dapat berimplikasi pada *parming, spoofing, keylogger, phising, sniffing* dan *carding*. Beberapa problem tersebut menjadi poin utama bagaiamana kebijakan pemerintah dalam menerapkan dan mengintinterpretasikan sehingga dapat menjaga stabilitas sektor perbankan. Auditor perbankan zaman digital membutuhkan kemampuan khusus untuk dapat menganalisis lebih baik dan tepat. Setidaknya (Rosati et al., 2020) mengingatkan bahwa insiden keamanan *cyber* megacu pada pemeriksaan proxy yang mapan untuk kualitas audit perbankan. Implikasinya adalah auditor dituntut untuk dapat memahami proxy-proxy tertentu sehingga dia dapat mengaudit perbankan modern dengan lebih baik.

Penelitian terbaru menginisiasi auditor yang menanggapi insiden *cyber security* dengan membebankan biaya tambahan lebih tinggi pada klien mereka (Lawrence et al., 2018; Li et al., 2020; Rosati et al., 2019). Bahkan pelanggaran *cyber security* dapat mengakibatkan kemungkinan audit ulang laporan keuangan pada saat terjadinya pelanggaran (Lawrence et al., 2018). Para auditor hendaknya memperbarui *skill* dan kemampuan mereka untuk mengaudit laporan keungan sehingga wawasan tambahan sehubungan dengan implikasi *cyber security* terhadap kualitas pelaporan keuangan (Rosati et al., 2020). Meskipun terdapat beberapa celah kelemahan pengendalian internal meningkatkan risiko audit, hal itu tidak menjadi penentu penurunan kualitas audit.

Fokus utama penelitian ini adalah sektor perbankan yang ada di Bank BTN Cabang Surabaya. Pengambilan fokus ini menjadi penting untuk memberikan literatur tentang evaluasi kebijakan *cyber security*. Harapan kedepan adalah bahwa penelitian ini berkontribusi secara nyata terhadap perkembangan ilmu pengetahuan sekaligus mengatasai problem empiris yang dihadapi masyarakat. Beberapa aksi serangan *cyber* terhadap perbankan di Indonesia akan disajikan melalui Tabel 1 sebagai berikut:

Tabel 1. Tren *Cyber Crime* Indonesia

No	Jumlah Penipuan Daring	Aksi Ilegal	Tahun
1	1.430	153	2017
2	1.781	263	2018
3	1.617	248	2019
4	1.319	303	2020
5	508	167	2021

Sumber: (Idntimes, 2021)

Berdasarkan Tabel 1 dapat dijelaskan bahwa *cyber-crime* di Indonesia massif terjadi dan tren cenderung meningkat kecuali pada tahun 2020 dan 2021 yang terindikasi adanya pandemi Covid-19. Sementara pada tahun 2017 dan 2018 mengalami peningkatan lebih dari 50% kasus *cyber-crime*. Hal ini mengindikasikan bahwa regulasi kebijakan *cyber-crime* dan peran serta *user* untuk mengurangi *cyber-crime* sangatlah dibutuhkan.

Cyber-crime yang terjadi di seluruh dunia berdampak eksplosif pada laporan keuangan tahunan setiap negara. Beberapa jenis lebih detail tentang *cyber-crime* akan dijelaskan pada Tabel 2 sebagai berikut:

Tabel 2. Jenis Kejahatan *Cyber Crime*

No	Jenis Kejahatan	Keterangan
1	Kejahatan *Phising*	*Cyber-crime* untuk melakukan penipuan dengan mengelabui korban
2	Kejahatan *Carding*	Kejahatan yang dilakukan dengan bertransaksi menggunakan kartu kredit milik orang lain
3	Serangan *Ransomware*	*Malware* atau *software* jahat yang bukan hanya bisa menginfeksi komputer, tapi juga menyandera data pengguna
4	Penipuan Online	Modus penipuan berkedok foto selfie KTP atau identitas diri lainnya
5	SIM *Swap*	Modus mengambil alih nomor ponsel seseorang untuk diretas
6	Peretasan Situs dan Email	Kejahatan dengan meretas situs atau email untuk mengubah tampilannya
7	Kejahatan *Skimming*	Kejahatan mencuri data kartu debit atau kredit untuk menarik dana di rekening
8	OTP *Fraud*	Kejahatan penyalahgunaan kode sekali pakai untuk mengakses atau menyelesaikan transaksi
9	Pemalsuan Data	Kejahatan dengan memalsulan data atau dokumen penting melalui internet
10	Konten Ilegal	Kejahatan memasukkan data atau informasi tidak benar, tidak etis, melanggar hukum atau mengganggu ketertiban umum
11	*Cyber Terorism*	Kejatahan yang mengganggu atau membuat kerusakan terhadap jaringan komputer
12	*Cyber Espionage*	Kejahatan memanfaatkan jaringan internet untuk memata-matai pihak lain
13	Menjiplak Situs Orang Lain	Kejahatan melanggar HKI atas orang lain di internet

Sumber: (Republika, 2021)

Tabel 2 menunjukkan berbagai macam *cyber-crime* yang terjadi di Indonesia, tidak menutup kemungkin pada tahun berikutnya akan muncul jenis kejahatan lain. Hal ini mengimpilkasikan bahwa potensi *cyber security* harus terus ditingkatkan, sehingga dapat mencegah *cyber-crime* yang berbeda. Penelitian ini secara aktif berupaya mengevaluasi kebijakan ebijakan *cyber-crime* pada sektor perbankan.

Berdasarkan UU Nomor 19 Tahun 2016 Pasal 31 ayat 2 menjelaskan bahwa "Setiap orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan". Legalitas perundangan ini berimplikasi bahwa *cyber security* telah diberikan landasan hukum, akan tetapi seringkali dalam penerapan kebijakan menjadi multitafsir sehingga arah dan tujuan dari kebjakan tersebut menjadi mengambang.

Tema besar dalam penelitian ini adalah evaluasi kebijakan, *cyber security*, dan perbankan. Dalam penelitian ini membahas debat paradigmatik untuk memberikan alternatif kebijakan yang tepat pada kebijakan *cyber security* sektor perbankan. Lokus penelitian ini adalah di Bank BTN Cabang Surabaya. Lebih

lanjut penelitian ini berupaya berkontribusi terhadap evaluasi kebijakan sehingga pembaruan kebijakan nantinya dapat lebih tepat dan terarah.

State of the art penelitian mengacu pada kebijakan mengacu pada kebijakan siber Amerika Serikat yang memiliki dua alasan penting yaitu: *Pertama,* Amerika Serikat menjadi *trendsetter* evolusi *cyber space*; *Kedua,* pelajaran dari kasus AS dapat diterapkan menginformasikan, dan keputusan kebijakan di negara lain (Lilli, 2020). Lebih lanjut penelitian ini akan berupaya menganalisis perspektif kebijakan di Amerika Serikat tentang perbankan untuk diterapkan di Bank BTN Cabang Surabaya. Rasionalisme dari kebijakan tersebut juga menjadi salah satu fokus penelitian yang dilakukan. Rasionalisme menjadi penting untuk mendapatkan kesesuaian dan implementasi yang maksimal ketika diterapkan di Bank BTN Cabang Surabaya. Lebih lanjut untuk menjelaskan letak *state of the art* penelitian ini akan dijelaskan pada bab selanjutnya menggunakan Vosviewer.

Urgensi penelitian ini adalah menganalisis kebijakan *cyber security* di Bank BTN Cabang Surabaya berdasarkan analisa awal peneliti bahwa seringkali kebijakan *cyber security* menjadi multitafsir. Selanjutnya penelitian ini berupaya untuk memberikan suatu strategi tentang upaya mempersempit ruang gerak *cyber-crime* yang merupakan implikasi dari *cyber security*. Problem awal tersebut akan dianalisis menggunakan perangkat kualitatif tentang evaluasi kebijakan.

Permalasahan yang akan dijabarkan dalam artikel ini adalah *Pertama,* Bagaimana dampak *cyber security* pada Bank BTN Cabang Surabaya? *Kedua,* Bagaimana strategi kebijakan pemerintah tentang *cyber security*? *Ketiga,* Bagaimana pencegahan kejahatan *cyber-crime* pada Bank BTN Cabang Surabaya?

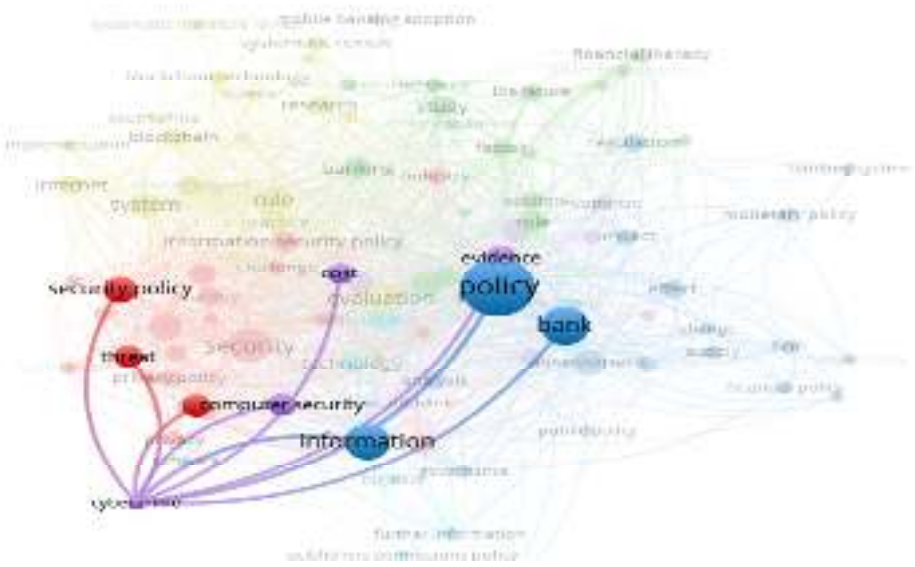
LANDASAN TEORI

Secara teoritis, peneliti akan menjelaskan beberapa penelitian terdahulu yang telah dilakukan dan dikumpulkan beberapa literatur artikel internasional yang relevan dengan penelitian yang akan dilakukan. Beberapa diantaranya yaitu penelitian (Rosati et al., 2020): Penelitian ini mendukung hipotesis awal yang dituliskan peneliti tersebut dan mendapati bahwa para auditor perbankan tidak menurunkan kualitas audit mereka meskipun terdapat issue *cyber security*. Penelitian ini menjadi landasan utama bahwa auditor di Amerika Serikat memiliki kompetensi yang baik, dan nantinya penelitian ini akan menganalisis lebih lanjut bagaimana femonena tersebut jika diterapkan di Indonesia. Perbedaan penelitian ini dengan penelitian yang akan dilakukan adalah secara metode penelitian ini menggunakan kualitatif untuk menjelaskan fenomena *cyber security* sedangkan penelitian yang dikutip menjelaskan melalui data empirik tentang audit di Amerika Serikat. Penelitian ini juga akan mengeksplorasi pada kebijakan pencegahan *cyber-crime* di Indonesia.

Penelitian (Elia, 2018)*:* Penelitian ini membahas problem Perancis dimana pemerintah mengambil alih kebijakan tentang *cyber-security* dan sedikit menentang pandangan bahwa letak intervensi pemerintah di bidang perekonomian. *Cyber security* dianggap sangat penting bagi pemerintah Perancis, sehingga negara mengambil alih peran tersebut menskipun terdapat stigma bahwa intervensi pemerintah terlalu jauh. Perbedaan penelitian ini dengan penelitian yang akan dilakukan adalah tentang evaluasi kebijakan di Indonesia akan memungkinkan jika pemerintah masuk lebih dalam hingga pada pembatasan legalitas sehingga *cyber security* dapat lebih terkontrol dan menimbulkan stabilitas yang kontinu. Selanjutnya penelitian ini akan berkontribusi terhadap literatur evaluasi kebijakan yang tepat pada bidang *cyber security* di Indonesia.

Penelitian (Huang & Li, 2018): Penelitian ini mengulas tentang lemahnya pengawasan dan juga fokus pendanaan pada *cyber security* di Taiwan. Penelitian ini menjadi dugaan awal untuk menganalisis sejauh mana intervensi pemerintah Indonesia di dalam pengawasan *cyber security* sektor perbankan di Indonesia, mengingat perbankan di Indonesia rawan untuk mendapatkan tindakaan *cyber-crime*. Persamaan penelitian ini adalah untuk mengamati bahwa apakah terdapat kesepakatan penelitian dengan kebijakan yang diterapkan oleh pemerintah. Setidaknya dugaan ini menjadi penting dan menarik untuk diamati sekaligus dianalisis sebagai salah satu referensi kebijakan *cyber security* pada sektor perbankan Indonesia.

Pemaparan berikutnya adalah hasil olah data Vosviewer yang akan menjelaskan letak *state of the art* penelitian ini berdasarkan *database Scopus* dan *google scholar* yang menjadi acuan banyak peneliti. Berdasarkan hasil analisis Vosviewer didapatkan hasil sebagai berikut:



Sumber: Vosviewer, data diolah oleh Penulis (2022)

Gambar 1. Hasil Olah Data Vosviewer

Berdasarkan hasil analisis *database google scholar* dan Scopus yang digunakan dalam aplikasi Harzing's Publish or Perish didapatkan data bahwa penelitian yang menggunakan tema *policy evaluation, cyber security,* dan banking yang terindeks Scopus belum ada. Ketiga tema tersebut secara kebaruan berdasarkan data Vosviewer menunjukkan kebaruan penelitian di literatur Scopus jika dipublikasikan di artikle internasional. Semakin kecil bulatan yang ditunjukkan pada Gambar 1 maka semakin sedikit penelitian tersebut terindeks *google scholar* dan Scopus. Berdasarkan gambar tersebut dapat kita lihat bahwa tema *cyber security* dan *banking* memiliki sembilan artikel pada Scopus. Letak kebarun dari penelitian ini adalah kontribusi pembahasan tentang evalausi kebijakan.

Teori Evaluasi Kebijakan

Menurut (Situmorang, 2016) evaluasi kebijakan diperlukan untuk mencegah kegagalan kebijakan sekaligus sesuai dengan arah dan tujuan yang telah ditentukan. Evaluasi kebijakan tidak hanya dilaksanakan di akhir, akan tetapi masuk pada proses tahapan sebuah kebijakan. Evaluasi setidaknya terdiri dari: *specification, measurement*, rekomendasi dan analisis. Beberapa tipe evaluasi kebijakan terdiri dari: 1) Evaluasi adalah kegiatan fungsional yang dipandang sebagai kegiatan yang sama dengan pembuatan kebijakan; 2) Evaluasi memiliki fokus pada kinerja sehingga memilih kejujuran dan efisiensi dalam implementasinya; 3) Evaluasi kebijakan berupaya memberikan jawaban terhadap pertanyaan kesesuaian kebijakan dengan tujual awal sekaligus memetakan keuntungan yang diraih maupun penerima keuntungan dari kebijakan tersebut.

Tujuan melaksanakan evaluasi adalah memberikan literatur dan pandangan tentang tujuan kebijakan, termasuk di dalamnya adalah eksternalitas kebijakan. Terdapat tiga unsur yang digunakan untuk pelaksanaan evaluasi, yaitu: 1) Mendiskripsikan luaran kebijakan yang merupakan hasil dari implementasi kebijakan; 2) Evaluasi berkaitan dengan perbaikan masalah sosial; 3) Evaluasi berkaitan dengan konsekuensi kebijakan yang berbentuk tindakan dan reaksi pemerintah.

Evaluasi kebijakan seringkali mengalami kendala pada proses tahapannya, beberapa kendala tersebut diantaranya adalah: 1) Ketidakpastian akan tujuan kebijakan; 2) Kasualitas; 3) Penyebaran dampak kebijakan, dimana dampak tersebut bagian dari kelompok di luar kelompok sasaran utama; 4) Tidak terbukanya akses data dan informasi yang relevan dalam pelaksanaan evaluas; 5) Resistensi pejabat, sehingga evaluator haru dapat mengemukakan objektifitas dalam mendapatkan pengetahuan; 6) evaluasi dapat mengurangi eksternalitas sehingga tidak mendapat banyak ekstensi atau mendapatkan pengabaian.

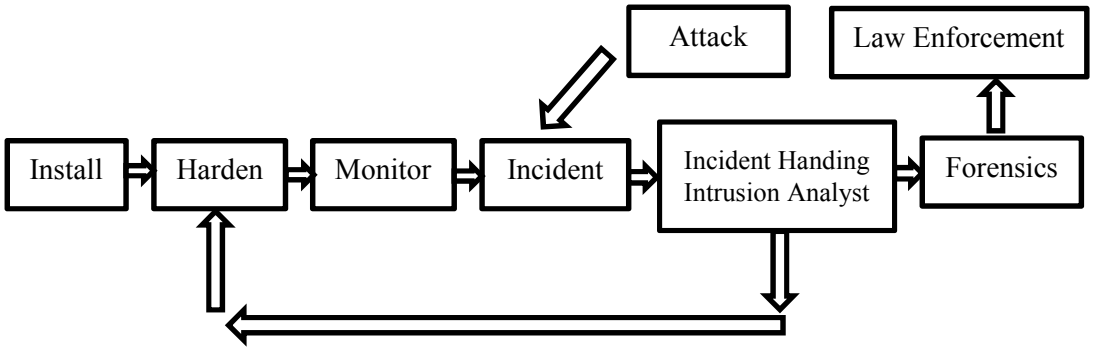
Lebih lanjut (Situmorang, 2016) menjelaskan bahwa terdapat beberapa penyebab kebijakan tidak memberikan dampak secara nyata sesuai dengan tujuan awal yaitu disebabkan oleh: 1) Sumber daya tidak mencukupi; 2) Metode evaluasi yang tidak tepat; 3) Kompleksitas

masalah publik sementara kebijakan fokus pada satu permasalahan; 4) Cara masyarakat merespon kebijakan juga sangat penting dalam proses evaluasi kebijakan; 5) Kontradiksi suatu kebijakan dengan kebijakan lainnya; 6) *Cost* yang tinggi; 7) Tidak memungkinkan menyelesaikan semua permasalahan publik; 8) Bersangkutan dengan sifat masalah yang akan diselesaikan berdasarkan tindakan dari pemegang kebijakan.

Teori Cyber Security

Cyber security adalah sekumpulan alat, kebijakan keamanan, perlindungan terhadap keamanan, tindakan, pelatihan, jaminan dan teknologi yang digunakan sebagai pelindung dalam lingkungan dalam lingkungan *cyber* dan organisasi asset pengguna. Organisasi ini yang terintehrasi dengan penghubung komputasi, infrastruktur, aplikasi, sistem komunikasi, dan totalitas informasi yang dikirimkan dalam lingkungan dunia maya (Ardiyanti, 2016).

Cyber-security merupakan salah satu upaya memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan asset pengguna terhadap risiko keamanan yang mungkin terjadi. Tujuan umum dari *cyber*-security adalah integritas didalamnya yang memungkinkan upaya mengutangi terjadinya ancaman serius *cyber*. Secara global *cyber-security* diterapkan berdasarkan lima bidang kerja yaitu: 1) Kepastian Hukum (legalitas *cyber-crime*); 2) Teknis dan tindakan procedural; 3) Struktur Organisasi; 4) *Capacity building* dan pendidikan pengguna; 5) Kerjasama internasional. Selanjutnya akan dijelaskan ruang lingkup *cyber-security* pada Gambar 2 sebagai berikut:



Sumber: (Ardiyanti, 2016)

Gambar 2. Ruang Lingkup Kebijakan Cyber Security

Data teoritis yang ada pada Gambar 2 menjelaskan bahwa ruang lingkup *cyber-security* dimulai dari install atau pengamanan yang dilakukan dalam perangkat keras yang digunakan dalam pengoperasian internet, monitor, yang memberikan peluang terjadinya *cyber-crime*. *Cyber-security* secara kompleks mekanisme melindungi dan meminimalkan gangguan kerahasiaan *(confidentiality)*, ketersediaan informasi *(availability)*, dan integritas *(integrity)*. *Cyber-security* merupakan upaya melindungi informasi dari adanya *cyber-attack*, beberapa pokok elemen kunci dalam *cyber-security* adalah: 1) Dokumen *security policy* adalah dokumen standar acuan menjalankan semua keamanan informasi; 2) *Information infrastructure* merupakan kelangsungan operasi menggunakan *hardware* dan *software*; 3) *Primere defense* yaitu komponen pertahanan infrastruktur informasi seperti *firewall*; 4) *Network monitoring system* yaitu memonitor kelayakan utilitas dan *performance* infrastruktur informasi; 5) *System information and evant management* berperan dalam memonitor kejadian jaringan terkai pada insiden keamanan; 6) *Network security assessment* berperan sebagai mekanisme *controlling* dan memberikan *measurement level* keamanan informasi; 7) *Human resource* dan *security awareness* terkait sumber daya. Variable lain yang perlu diperhitungkan adalah kelangsungan *physical security* yang berkaitan sistem elemen fisikal seperti bangunan *data center, disaster recovery system*, dan media transmisi.

METODE PENELITIAN

Penelitian ini adalah menggunakan metode kualitatif yang menggunakan wawancara, dokumentasi, dan observasi dalam menganalisis femomena permasalahan. Selanjutnya penelitian ini menganalisis data primer dan data sekunder untuk diterapkan menggunakan teori yang digunakan pada penelitian ini. Data tersebut akan dianalisis lebih mendalam sehingga membentuk suatu kesimpulan ilmiah-alamiah yang dapat diterima oleh berbagai kalangan, terutama dalam hal ini adalah sektor perbankan di Bank BTN Cabang Surabaya sebagai objek penelitian ini.

Penelitian deskriptif menganalisis wawancara, hasil survei, penelitian lapang, analisis isi *(content)*, media massa, dan penelitian komparatif sejarah. Penelitian ini menggunakan teknik penentuan informan *snowball sampling* yang memungkinkan peneliti mendapatkan informan tambahan ketika wawancara dilaksanakan. Lebih lanjut informan awal penelitian ini yaitu:

Tabel 3. Informan Penelitian

No	Nama Informan	Pekerjaan
1	Setia Budi	Teller Service Bank BTN Cabang Surabaya
2	Dedo Pratika	Customer Sevice Bank BTN Cabang Surabaya
3	Nanti Sulis	Teller Service Bank BTN Cabang Surabaya
4	Eric Saputra	Marketing Bank Sinarmas

Sumber: Data dioalah Penulis (2022)

Fokus penelitian ini adalah evaluasi kebijakan *cyber-security* sektor perbankan pada Bank BTN Cabang Surabaya. Issue ini menjadi sangat penting untuk diteliti berdasarkan *state of the art* yang telah dijelaskan dimuka. Hal ini sekaligus menjadi kebaruan penelitian yang dikombinasi teori yang digunakan dalam penelitian ini. Penelitian ini mengambil lokasi penelitian di Bank BTN Cabang Surabaya yang berlokasi di Jl. Pemuda No. 50 Embong Kaliasin, Kecamatan Genteng Kota Surabaya. Penelitian ini dilakukan pada salah satu perbankan di Kota Surabaya untuk lebih detail dan spesifik tentang pembahasan *cyber security*. Teknik analisa data menggunakan triangulasi data berdasarkan hasil wawancara *indepth interview*, dokumentasi, dan observasi.

HASIL DAN PEMBAHASAN

Interpretasi Teori Evaluasi Kebijakan

Berdasarkan perangkat teori evaluasi kebijakan seringkali sulit untuk tercipta kebijakan yang dapat diterima oleh semua pihak. Tentu saja hal ini tidak dapat melegakan semua pihak, karena sebuah kebijakan dibentuk berdasarkan permasalahan yang terjadi di masyarakat. Kebijakan *cyber security* mendapatkan porsi terbesar dalam terciptanya *economy digital*, disebabkan oleh system keamanan menjadi landasan utama dalam penciptaan sebuah aplikasi digital. Seringkali kebijakan *cyber security* di sektor perbankan memiliki celah-celah yang dapat dimanfaatkan oleh oknum tidak bertanggung jawab untuk melakukan kejahatan *cyber*. Artikel ini berupaya untuk menganalisis lebih lanjut berdasarkan perangkat teori evaluasi kebijakan.

Teori evaluasi kebijakan menginisiasi kendala yang terjadi pada tahapannya meliputi: 1) Ketidakpastian akan tujuan kebijakan, ketidakpastian tujuan kebijakan menjadi salah satu poin penting dalam keberlangsungan sebuah kebijakan. Terlepas dari dinamika permasalahan yang terjadi, bahwa tujuan dari kebijakan harus mengarah kepada salah satu pihak yang akan diterapkan kebijakan tersebut. Saling tumpah tindih kebijakan juga menjadi beberapa hal yang harus diperhitungkan oleh pengambil kebijakan publik; 2) Metode evaluasi yang tidak tepat, indikator keberhasilan yang kedua adalah metode evaluasi yang digunakan. Evaluasi secara kompleks seharusnya melibatkan audit internal dan audit eksternal, sehingga dapat tercipta suatu output yang dapat mengevaluasi secara detail kebijakan yang akan dihasilkan. Audit eksternal diperlukan sebagai salah satu bentuk evaluasi yang tidak terikat dengan kepentingan-kepentingan yang ada di internal, dan tentu saja hal ini akan menghasilkan suatu evaluasi yang lebih matang dan terarah; 3) Penyebaran dampak kebijakan, yaitu merupakan indikator yang berasumsi pada efek yang ditimbulkan akibat implementasi kebijakan tersebut. Dampak ini harus diperhitungkan secara matang dan saksama terhadap kondisi eksternal dari penerapan kebijakan. Seringkali penerapan kebijakan tidak mempertimbangkan dengan pasti tentang bagaimana *multiplier effect* yang ditimbulkan ketika implementasi kebijakan; 4) Tidak terbukanya akses data dan informasi yang relevan dalam pelaksanaan evaluasi, merupakan indikator berikutnya dalam ketidaktercapaian target kebijakan. Informasi data yang tidak utuh menyebabkan beberapa kebijakan publik menjadi sangat ambigu, dan tentu saja hal ini akan justru menimbulkan polemik di masyarakat; 5) Resistensi pejabat terkait, hal ini berimplikasi pada reformasi birokrasi. Suatu organisasi harus dapat menyesuaikan sistemnya dengan perkembangan masyarakat terkini sehingga tercipta suatu suasana organisasi yang ramah dan memiliki kesesuaian dengan kebutuhan publik. Beberapa pejabat berwenang yang enggan untuk bertransformasi akan menjadi beban tersendiri dalam penerapan evaluasi kebijakan; 6) Evaluasi

dapat mengurangi dampak eksternalitas, pada tahap evaluasi sangat membutuhkan evaluasi eksternal dan internal. Pada evaluasi internal akan menunjukkan beberapa dampak evaluasi terhadap internal organisasi, sementara itu evaluasi eksternal akan memperhitungkan dampak eksternalitas diluar organisasi.

Selanjutnya artikel ini akan membahas bagaimana kebijakan *cyber security* tidak memberikan dampak secara nyata menurut (Situmorang, 2016) sesuai dengan tujuan awal yang disebabkan oleh beberapa hal yaitu: 1) Sumber daya tidak mencukupi, sumber day aini mencakup kemampuan keamanan siber dalam menutup celah-celah yang memungkinkan terjadinya *cybercrime*. Tentu langkah preventif harus selalui diterapkan agar sebuah kebijakan dapat memiliki dampak secara kontinu; 2) Metode evaluasi yang tidak tepat, pihak perbankan haru secara cermat dalam menerapkan evaluasi sehingga tidak terjadi kekosongan evaluasi atau sebuah ketidaktahuan terhadap permasalahan yang terjadi di organisasinya. Selain itu dalam penerapan evaluasi harus mendapatkan momentum yang tepat agar dapat diterima oleh mayoritas anggota organisasi dan hal ini menjadi penting dalam sebuah evaluasi; 5) Kontradiksi kebijakan, perihal lain yang perlu diperhatikan oleh sektor perbankan adalah saling tumpang tindih kebijakan yang mengakibatkan multitafsir yang dipahami oleh anggota organisasi. Tumpang tindih kebijakan ini tidak hanya terjadi pada lingkungan organisasi terkadang juga terjadi diluar organisasi, sinkronisasi kebijakan legalitas eksternal dengan legalitas internal menjadi salah satu hal krusial berikutnya sehingga perlu dibentuk suatu divisi hukum yang khusus menangani sinkronisasi legalitas perundangan tersebut; 6) Cost yang tinggi, sebuah evaluasi yang matang tentu membutuhkan *cost* yang tidak sedikit. Anggaran ini harus selalui disisihkan dari hasil produksi yang dihasilkan, sehingga setiap saat dapat memungkinkan untuk melakukan evaluasi. Jumlah anggota organisasi menentukan besaran *cost* yang dibutuhkan, semakin tinggi *cost* yang dibutuhkan untuk setiap evaluasi yang dilakukan; 7) Tidak memungkinkan menyelesaikan semua permasalahan, persoalan teknis berikutnya dalam pengambilan kebijakan adalah keberpihakan kebijakan terhadap pihak tertentu. Tentu saja sebuah kebijakan publik tidak dapat secara adil menguntungkan semua pihak, karena memang dia harus memilih keberpihakan berdasarkan pandangan libertarianisme atau utilitarianisme. Keberpihakan ini saling bertentangan antara kebebasan tiap individu dengan kebebasan berdasarkan mayoritas masyarakat.; 8) Mekanisme penyelesaian konflik dari pemegang kebijakan, potensi kegagalan kebijakan berikutnya diakibatkan oleh mekanisme penyelesaian konflik yang kurang tepat. Hal ini disebabkan karena seorang pemimpin membutuhkan determinasi untuk dapat mengakomodir permasalahan yang terjadi pada organisasi mereka. Kemampuan mengakomodir ini menjadi landasan utama dalam mengatasi konflik internal yang terjadi.

Penelitian (Sari et al., 2019) menunjukkan hasil bahwa konsentrasi dalam pengembangan sebuah organisasi terletak pada Sumber Daya Manusia dan pelatihan khusus yang diberikan. Hal ini dilakukan untuk mempermudah pengembangan kebijakan dan menambah potensi produksi dari manajemen organisasi. Dukungan seruapa ditunjukkan oleh penelitian (Puspitasari & Kartika, 2019) bahwa sebuah evaluasi bidang organisasi memperhitungkan konsep Sumber Daya Manusia utamanya dalam pemberian kompensasi kinerja maupun penilai secara langsung oleh atasan. Penilaian ini menjadi penting sebagai langkah awal dalam mengevaluasi organisasi, hampir disetiap lini sektor organisasi memperhitungkan bagaimana evaluasi yang dilakukan oleh pemimpin langsung. Lebih lanjut penelitian (Syovina et al., 2020) kuantitas evaluasi yang mumpuni menimbulkan *trust* tinggi dalam masyarakat, hal ini terbukti dengan adanya *family business image promotion* yang secara stabil menjaga kualitas dan kuantitas barang sehingga dapat dipercaya meskipun tidak secara langsung dimiliki oleh *owner* pertama.

Hasil *indepth interview* yang dilakukan di Bank BTN menunjukkan bahwa evaluasi kebijakan dilakukan hampir di setiap bulan yang dilakukan oleh atasan langsung maupun evaluasi yang dilakukan oleh pihak eksternal. Hasil reduksi data yang dilakukan oleh Dedo selaku Teller prioritas Bank BTN Surabaya menunjukkan hasil sebagai berikut:

> "Di Bank BTN secara berkala dinilai oleh atasan secara langsung hampir di tiap bulan, bahkan kita ada evaluasi kebijakan setiap dua minggu sekali. Tujuan utamanya tentu untuk mencapai kriteria target yang ditentukan oleh perusahaan dan secara personal meningkatkan kualitas dan kapabilitas dari individu". (Wawancara dilakukan pada 4 Juni 2022 di Bank BTN Surabaya)

Berdasarkan wawancara yang telah dilakukan menunjukkan bahwa evaluasi

dilakukan hampir disetiap dua minggu sekali dan sebulan sekali untuk evaluasi yang dilakukan oleh atasan langsung. Sementara itu untuk evaluasi kebijakan *cyber security* pihak Bank BTN berkoordinasi dengan pihak IT selaku penyedia jasa keamanan *cyber* untuk mengambil langkah preventif sebagai antisipasi pencegahan maraknya kejahatan *cyber* yang terjadi. Hal ini didukung dengan wawancara yang dilakukan kepada Pak Budi selaku General Manager Bank BTN sebagai berikut:

> "Mengenai *cyber security* kita koordinasikan dengan ahli IT sekaligus dengan pihak kepolisian, sehingga kita bisa mengetahui modus-modus terbaru yang dilakukan oleh oknum tidak bertanggung jawab. Kita terus pelajari bagaimana modus tersebut dapat dicegah, karena tentu saja akan menimbulkan suatu kerugian secara massif jika pihak perbankan masih kecolongan dalam menerapkan keamana perbankan. Dan tentu ini mengurangi kepercayaan masyarakat untuk menabung di Bank BTN, maka dari itu saya sangat *concern* untuk pencegahan dan penanganan *cyber security* ini". (Wawancara dilakukan pada 4 Juni 2022 di Bank BTN Surabaya)

Koordinasi yang dilakukan oleh pihak Bank BTN dengan kepolisian dan pihak IT berfungsi sebagai pencegahan dan suatu langkah preventif dalam mengantisipasi kejahatan *cyber*. Faktor keamanan menjadi salah satu poin penting dalam keberlangsungan digital, terlepas dari hal tersebut tentu sebagai salah satu bentuk layanan pihak perbankan untuk dapat memberikan rasa nyaman dan aman ketika nasabah bertransaksi.

Interpretasi Teory Cyber Security

Penerapan kebijakan *cyber security* setidaknya berasumsi pada lima bidang kerja yaitu: 1) Kepastian Hukum, dalam hal ini pihak Bank BTN membentuk tim khusus untuk menangani legalitas hukum dan secara aktif berkoordinasi dengan pihak perbankan lain maupun dengan pihak kepolisian tentang bagaimana langkah preventif yang harus dilakukan sebagai bentuk pencegahan kejahatan *cyber*; 2) Teknis dan tindakan procedural, teknis pelaksanaan dilakukan oleh ahli dibidangnya yaitu bidang Teknologi Informasi yang dibentuk oleh pihak Bank BTN sebagai garda terdepan dalam menanggulangi kejahatan *cyber*. Umumnya koordinasikan dilakukan oleh pihak OJK selaku lembaga negara yang berwenang untuk mengecek ulang transaksi-transaksi yang mencurigakan; 3) Struktur organisasi, hal ini telah secara aktif dilakukan oleh pihak Bank BTN melalui pembentukan khusus Tim IT yang terstruktur dalam organisasi sehingga secara hierarki dapat mengusulkan secara langsung kepada pimpinan langkah apa yang harus dilakukan; 4) *Capacity building*, dalam hal ini Bank BTN kurang kompleks dalam memberikan literasi kepada nasabah tentang bagaimana peningkatan keamanan bertransaksi online termasuk cara pencegahan kejahatan *cyber* tidak dijelaskan secara detail oleh pihak Bank. Ini menjadi catatan khusus bagi pihak Bank BTN untuk meningkatkan kualitas layanana perbankan pada indikator *capacity building*; 5) Kerjasama internasional, perihal kerjasama internasional pihak Bank BTN tidak secara aktif langsung bekerjasama akan tetapi dalam implementasikan bahwa pihak kepolisian tentu telah berkoordinasi langsung dengan institusi internasional seperti FBI untuk mencegah kejahatan *cyber* meluas.

Berdasarkan penelitian (Putra, 2020) menunjukkan bahwa kepercayaan konsumen akan tinggi ketika review dari sebuah organisasi terwujud dengan baik. Hal ini berimplikasi pada Bank BTN bahwa citra dan layanan Bank BTN akan menjadi tolak ukur nasabah untuk dapat bertransaksi di Bank tersebut. Tentu menjaga marwah citra ini tidak mudah mengingat bentuk modus kejahatan *cyber* semakin bervariatif dan massif, akan tetapi ini bukan menjadi alasan utama untuk tidak memberikan pelayanan terbaik bagi nasabah. Penelitian (Yadewani et al., 2020) mengingatkan pentingnya platform digital sebagai *brand image* perusahaan. Dukungan promosi dan desain website yang baik tentu akan meningkatkan *trust* nasabah terlepas dari *issu*e kejahatna *cyber* yang tidak hanya dialami oleh Bank BTN akan tetapi oleh seluruh perbankan di Indonesia. Dengan adanya *brand image* yang baik, maka issue kejahatan *cyber* menjadi memudar sehingga dapat meningkatkan kepercayaan nasabah.

Strategi Kebijakan Pemerintah Terkait Cyber Security

Kita bisa memahami bahwa *cyber security* merupakan salah satu hal yang sanga krusial dalam perekonomian digital. Bahkan disemua sektor menjelaskan bahwa tingkat keamanan menjadi poin utama dalam keberlangsungannya. Pemerintah dalam hal ini tidak secara massif mengalokasikan dan beradaptasi dengan perkembangan zaman utamanya perkembangan *cyber security*. Penelitian ini menemukan bahwa muara dari strategi kebijakan *cyber security* yang kurang optimal adalah tentang alokasi anggaran

untuk pengembangan system keamanan. Berdasarkan perangkat teori yang telah diulas pada sub bab sebelumnya, didapati bahwa cara pemerintah dalam mengalokasi anggaran pengembangan *cyber security* masih kurang optimal. Ini berimplikasi pada kekuatan system *cyber security* yang dimiliki pemerintah.

Di sisi lain kita mendapati bahwa alokasi anggaran pemerintah akan sulit diimplementasikan karena system *cyber* sulit untuk diukur ketercapaiannya. Keamanan *cyber* diukur berdasarkan jumlah kasus *cyber* yang terjadi, dan itu hanyalah standar utama yang dapat diterapkan. Beda konteks dengan alokasi anggaran pendidikan misalnya, dia ada standarisasi ukuran ketercapaian pendidikan yaitu jumlah lulusan ataupun jumlah belajar siswa-siswi menjadi meningkat. Hal ini juga menjadi tantangan bagi pemerintah untuk dapat beradaptasi dengan alokasi anggaran *cyber security*.

Penelitian (Budhi, 2016) menganalisis bahwa kelemahan pemerintah terletak pada *innovation strategy,* keamanan data konsumen, Analisa (Karim, 2020) adalah bahwa pemrintah kurang memberikan ruang seluas-luasnya untuk keterbukan internet dan jaringan bagi masyrakatnya. Tentu hal ini menjadi krusial demi percepatan informasi yang ada di masyarakat, meskipun kita bisa pahami bahwa percepatan informasi juga dapat berujung pada hal negative. Poin utamanya adalah percepatan penyampaian informasi melalui koneksi internet belum dapat difasilitasi pemerintah dengan baik. Percepatan informasi ini dapat berujung positif mengingat berbagai informasi dapat diakses melalui internet dan media sosial.

Artikel ini menyarankan strategi kebijakan terkait *cyber security* sebagai berikut: 1) Membuka akses informasi dan ketersediaan jaringan yang baik; 2) Bekerjasama dengan kemanan *cyber* luar negeri; 3) Mengakomodasi programmer local; 4) Meningkatkan alokasi anggaran dan focus pada peningkatan *cyber security*; 5) Memperkuat seluruh institusi pemerintah dan menyiapkan ahli keamanan *cyber* di setiap posisi lembaga pemerintah. Beberapa strategi ini ditujukan untuk setidaknya mengurangi kejahatan *cyber* yang massif terjadi di Indonesia. Tentu besar harapan bahwa pemerintah dapat menangani dan mempersempit celah untuk *hacker* dapat melaksanakan aksinya.

KESIMPULAN

Cyber security pada sektor perbankan merupakan issue massif yang dialami oleh hampir seluruh perbankan di Indonesia. Tentu hal ini menjadi tantangan serius dan membutuhkan *effort* yang tinggi dalam upaya pencegahan maupun membatasi peluang terjadinya kejahatan *cyber*. Pada Bank BTN Surabaya menunjukkan langkah preventif yang baik dengan membentuk struktur organisasi khusus untuk menangani permasalahan legalitas dan penerapan aplikasi pencegahan kejahatan *cyber*. Secara aktif Bank BTN juga melakukan evaluasi kebijakan setiap dua minggu sekali sebagai bentuk evaluasi pencapaian target dan evaluasi bulanan yang dilakukan oleh atasan secara langsung. Lebih lanjut setiap enam bulan sekali Bank BTN Surabaya mendatangkan audit eksternal untuk dapat mengawasi dan memonitoring beberapa hal yang tidak sesuai dengan legalitas perundangan. Audit eksternal ini bisa berasal dari Bank Indonesia maupun Otoritas Jasa Keuangan yang berwenang dalam mendata dan memonitor transaksi keuangan perbankan.

Penelitian ini memiliki keterbatasan lokus penelitian pada satu tempat, sangat mungkin ditingkatkan dengan mengkomparasikan dengan perbankan lain untuk dapat membandingkan sekaligus menunjukkan keunggulan masing-masing perbankan. Diharapkan pada peneliti selanjutnya dalam menggunakan lokus penelitian lebih kompleks dan tidak terbatas pada tema *cyber security*. Lebih lanjut artikel ini dapat menjadi referensi logis tentang penerapan evaluasi kebijakan *cyber security* di sektor perbankan.

UCAPAN TERIMA KASIH

Kami selaku tim penulis mengucapkan terimakasih dan penghormatan yang tinggi kepada Universitas Wijaya Putra yang telah mendanai penelitian ini. Tidak lupa kami mengucapkan terimakasih kepada seluruh pihak yang terlibat secara langsung maupun tidak langsung dalam penelitian ini.

DAFTAR PUSTAKA

Ardiyanti, H. (2016). Cyber-security dan tantangan pengembangannya di indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *5*(1).

Budhi, G. S. (2016). Analisis Sistem E-Commerce Pada Perusahan Jual-Beli Online Lazada Indonesia. *Elinvo (Electronics, Informatics, and Vocational Education)*, *1*(2), 78–83. https://doi.org/10.21831/elinvo.v1i2.10880

Calderaro, A., & Craig, A. J. S. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third World*

Quarterly, *41*(6), 917–938. https://doi.org/10.1080/01436597.2020.1729729

Elia, D. D. (2018). *Industrial policy : the holy grail of French cybersecurity strategy ? Industrial policy : the holy grail of French cybersecurity strategy ?**. *8871*. https://doi.org/10.1080/23738871.2018.1553988

Huang, H., & Li, T. (2018). A centralised cybersecurity strategy for Taiwan A centralised cybersecurity strategy for Taiwan. *Journal of Cyber Policy*, *0*(0), 1–19. https://doi.org/10.1080/23738871.2018.1553987

Idntimes. (2021). *Serangan Siber Meningkat, Sektor Keuangan Paling Terancam*. https://www.idntimes.com/business/economy/helmi/hati-hati-sektor-keuangan-paling-terancam-nomor-2-kejahatan-siber/3

Karim, B. A. (2020). Pendidikan Perguruan Tinggi Era 4.0 Dalam Pandemi Covid-19 (Refleksi Sosiologis). *Education and Learning Journal*, *1*(2), 102. https://doi.org/10.33096/eljour.v1i2.54

Lawrence, A., Minutti-Meza, M., & Vyas, D. (2018). Is operational control risk informative of financial reporting deficiencies? *Auditing: A Journal of Practice & Theory*, *37*(1), 139–165.

Li, H., No, W. G., & Boritz, J. E. (2020). Are external auditors concerned about cyber incidents? Evidence from audit fees. *Auditing: A Journal of Practice & Theory*, *39*(1), 151–171.

Lilli, E. (2020). President Obama and US cyber security policy President Obama and US cyber security policy. *Journal of Cyber Policy*, *0*(0), 1–20. https://doi.org/10.1080/23738871.2020.1778759

Puspitasari, S., & Kartika, L. (2019). Evaluation of Job Analysys and Need for Trainingon Jakartapamong Praja Units. *Jurnal Apresiasi Ekonomi*, *7*(3), 219–231. https://doi.org/10.31846/jae.v7i3.237

Putra, E. (2020). Pengaruh Promosi Melalui Sosial Media Dan Review Produk Pada Marketplace Shopee Terhadap Keputusan Pembelian (Studi pada Mahasiswa STIE Pasaman). *Jurnal Apresiasi Ekonomi*, *8*(3), 467–474. https://doi.org/10.31846/jae.v8i3.298

Republika. (2021). *13 Jenis Kejahatan Siber | Republika Online*. https://www.republika.co.id/berita/r0sm8s6116000/13-jenis-kejahatan-siber

Rosati, P., Gogolin, F., & Lynn, T. (2019). Audit firm assessments of cyber-security risk: evidence from audit fees and SEC comment letters. *The International Journal of Accounting*, *54*(03), 1950013.

Rosati, P., Gogolin, F., Lynn, T., Gogolin, F., & Lynn, T. (2020). Cyber-Security Incidents and Audit Quality. *European Accounting Review*, *0*(0), 1–28. https://doi.org/10.1080/09638180.2020.1856162

Sari, V. N., Sari, M. W., Yulia, Y., & Wati, R. H. (2019). Marketing Strategy of Chicken Egg on Nrps Shop in Tanah Datar. *Jurnal Apresiasi Ekonomi*, *7*(1), 67–78. https://doi.org/10.31846/jae.v7i1.189

Situmorang, C. (2016). *Kebijakan Publik (Teori Analisis, Implementasi, dan Evaluasi Kerja)*. Social Security Development Institute (SSDI).

Stevens, T., Brien, K. O., Stevens, T., & Brien, K. O. (2019). *Brexit and Cyber Security*. *1847*. https://doi.org/10.1080/03071847.2019.1643256

Syovina, M., Sari, D. K., & Sari, D. K. (2020). Pengaruh Family Business Image Promotion Soraya Bedsheet Terhadap Social Media Engagement Dengan Brand Authenticity Dan Consumer-Company Identification Sebagai Variabel Mediasi (Survey on Facebook and Instagram Users). *Jurnal Apresiasi Ekonomi*, *8*(2), 221–234. https://doi.org/10.31846/jae.v8i2.285

Yadewani, D., Lukman Arief, M., & Indah Mursalini, W. (2020). Pengaruh Pemanfaatan Platform Sosial Media Pada Era Digital Terhadap Prestasi Mahasiswa Influence of Social Media Platform Utilization in Digital Disrupsy Era on Student Achievements. *Jurnal Apresiasi Ekonomi*, *8*(3), 521–527.