INTERDEPENDENCE JOURNAL OF INTERNATIONAL STUDIES
Volume 6 Nomor 1 Tahun 2025

Menjaga Keamanan Digital: Strategi serta Kebijakan Swiss dalam Mengatasi Ancaman *Ransomware*

Mokhamad Saiful Farisin[1]
[1]Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Brawijaya, Indonesia (saifulfariss@gmail.com)

ABSTRACT
The global rise in cybersecurity threats has also impacted Europe, with Switzerland experiencing ransomware attacks across diverse sectors, including private companies and banking institutions. This study aims to examine Switzerland's strategies and policies in response to these challenges. Using a descriptive methodology, data was gathered through a literature review. The findings reveal that Switzerland has implemented two primary strategies to address ransomware issues: the National Cybersecurity Strategy (NCS) and the National Cyber Security Centre (NCSC). In conclusion, the author proposes policy recommendations, such as enacting more comprehensive regulations and enhancing employee awareness within companies, to bolster Switzerland's defense against ransomware and improve preparedness and risk mitigation in the face of evolving cyber threats.
Keywords: cybercrime, ransomware, strategy, policy, Switzerland

ABSTRAK
Ancaman terhadap keamanan siber telah meningkat secara signifikan di seluruh dunia, termasuk di Eropa. Salah satu negara yang terkena dampaknya adalah Swiss, di mana serangan ransomware telah menyasar berbagai sektor, mulai dari perusahaan swasta hingga lembaga perbankan secara luas. Penelitian ini bertujuan untuk menganalisis strategi dan kebijakan yang diterapkan oleh Swiss untuk menghadapi tantangan tersebut. Metode penelitian yang digunakan adalah deskriptif, dengan pengumpulan data melalui studi pustaka. Hasil penelitian menunjukkan bahwa Swiss telah mengadopsi dua strategi utama dalam kebijakannya untuk menangani masalah ransomware, yaitu pembentukan National Cybersecurity Strategy (NCS) dan pendirian National Cyber Security Centre (NCSC). Di bagian akhir, penulis mengajukan beberapa rekomendasi kebijakan untuk memperkuat pertahanan Swiss terhadap ransomware, termasuk pengesahan regulasi yang lebih menyeluruh dan peningkatan kesadaran di kalangan karyawan perusahaan. Langkah-langkah ini diharapkan dapat meningkatkan kesiapsiagaan dan mitigasi risiko dalam menghadapi ancaman siber yang terus berkembang.
Kata Kunci: kejahatan siber, *ransomware*, strategi, kebijakan, Swiss.

PENDAHULUAN

Keberadaan internet menjadi sebuah penemuan yang sangat besar pada abad 21 yang memberikan dampak besar bagi kehidupan serta keseharian kita, dimana dengan adanya hal tersebut telah mengubah cara kita dalam berbagai macam hal, mulai dari berkomunikasi, bermain, berbelanja,

hingga bekerja, dalam hal hiburan internet ini mampu memberikan kemudahan bagi kita dalam melakukan akses saat kita ingin mendengarkan musik maupun menonton film (Pande, 2017). Dengan adanya internet ini mampu menjadikan kehidupan kita lebih nyaman, dimana banyak kemudahan dapat kita rasakan dengan adanya hal tersebut, sebagai contoh dahulu saat kita ingin melakukan pembayaran atas tagihan listrik kita harus mengantri dengan cukup panjang dan membutuhkan waktu yang juga tidak sebentar, dengan adanya internet ini kita mampu melakukan pembayaran atas tagihan tersebut dimanapun kita berada dengan hanya menekan melalui perangkat yang dimiliki. Selain itu dengan pesatnya teknologi, yang dahulunya berbagai macam kegiatan dilakukan melalui komputer, kini semakin berkembang dimana perangkat lain yang lebih fleksibel, seperti contohnya laptop dan smartphone. Teknologi telah berkembang pesat sehingga kita tidak lagi memerlukan komputer untuk menggunakan internet. Dengan keberadaan perangkat tersebut yang terhubung dengan internet, kita dapat melakukan segala hal dengan lebih mudah, sehingga sebagaimana telah dikatakan sebelumnya keberadaan internet mampu mempermudah kehidupan kita.

Dengan adanya kemudahan tersebut, dampak negatif dari adanya internet ini juga tidak dapat dihindarkan. Dewasa ini kita mengenal adanya istilah *cyber crime* atau kejahatan siber. Istilah kejahatan siber merupakan sebuah istilah yang digunakan untuk menggambarkan adanya aktivitas kriminal dimana komputer atau jaringan-jaringan yang ada dalam komputer dijadikan sebagai alat, target, atau tempat dari adanya aktivitas criminal (Das & Nayak, 2013). Dimana hal ini mencakup adanya peretasan alat elektronik, selain itu istilah ini ini juga digunakan untuk mencakup pengertian dari suatu kejahatan dimana komputer atau jaringan tadi digunakan untuk memungkinkan aktivitas ilegal, dengan dampaknya seperti menghentikan kereta api, memberikan sinyal yang salah pada pesawat sehingga target akan tersesat, menyebarkan data-data penting suatu negara terlebih lagi dalam hal militer yang penting jatuh ke tangan negara lain, menghentikan operasi media elektronik secara besar-besaran serta setiap sistem yang ada secara cepat.

Semakin berkembangnya teknologi juga diiringi semakin berkembangnya para pelaku kejahatan siber atau *cyber crime* ini. Para *cyber attackers* ini mengembangkan serangannya dengan cara-cara yang sangat canggih dan lebih siap, melakukan serangan kepada wilayah-wilayah yang mereka anggap cukup rentan dalam hal keamanan bidang sibernya, para pelaku ini biasanya melakukan serangan siber berupa pencurian data, perampokan, pencurian data pribadi, hingga membocorkan data-data penting lainya bersifat pribadi (Bernabe & Skarmeta, 2019). Salah satu wilayah yang juga tidak lepas dari keberadaan serangan siber ini adalah wilayah Eropa. Dengan semakin berkembangnya kejahatan siber di kawasan eropa ini, dapat dikatakan cukup memberikan dampak yang buruk baik secara fisik maupun virtual bagi warga negara benua ini, dimana hal ini sangat mengancam bagi seluruh warga yang ada, terutama dalam masalah keamanan atas data pribadi.

Dengan ancaman yang cukup nyata di kawasan ini, pada tahun 2013 dibentuklah CSSEU atau Cyber Security Strategy of the European Union dengan tujuan prioritasnya untuk melakukan pengurangan secara drastis atas aksi kejahatan siber. Dimana prioritas ini sejalan dengan upaya mereka untuk mencapai ketahanan siber, mengembangkan pertahanan siber, mengembangkan sumber daya dan

teknis demi tercapainya keamanan siber, serta menetapkan kebijakan ruang siber internasional dalam ruang lingkup Uni Eropa. Selain itu keberadaan kejahatan siber yang keberadaanya tidak dibatasi oleh batas negara karena internet yang bersifat global (Christou, 2018). Oleh karena itu, strategi yang dirasa efektif dalam mengurangi kejahatan siber harus mencakup beberapa hal seperti kolaborasi, koordinasi, dan kerjasama yang efektif, tidak hanya di dalam Eropa, tetapi juga dengan lembaga terkait, organisasi internasional, jaringan, dan aktor di negara dan wilayah lain. Inisiatif untuk mengatasi kejahatan siber tidak dimulai dengan CSSEU saja. Masalah kejahatan siber sudah diakui oleh European Community sejak tahun 1970-an dengan istilah *internet security* dimana hal ini berdampak pada serangkaian keputusan kerangka kerja, arahan, komunikasi, dan strategi yang bertujuan untuk menciptakan hukum yang jelas dan meningkatkan ketahanan siber dan keamanan informasi.

Dalam mengatasi ancaman siber ini, Eropa memiliki tata kelola regional bernama ENISA atau European Network and Information Security Agency. ENISA merupakan salah satu inisiatif keamanan siber yang ada paling awal di Uni Eropa yakni tepatnya pada tahun 2001. Dimana ENISA ini memiliki dua tugas utama yakni, pertama melakukan analisis resiko, memberikan saran, memfasilitasi kerjasama, dan meningkatkan kesadaran pada bidang keamanan siber. Kedua, membentuk standar dan berkontribusi pada upaya Uni Eropa untuk bekerja sama secara internasional demi mempromosikan isu keamanan siber dan informasi (Cavalry & Smeets, 2023). Meskipun terdapat mekanisme tata kelola regional, seluruh negara di kawasan ini juga tetap berupaya untuk meningkatkan pertahanan di negaranya masing-masing, salah satu negara yang tidak lepas dalam upaya melakukan peningkatan pertahanan ini adalah Swiss.

Pada sebuah survei yang dilaksanakan pada tahun 2011 oleh PwC Global, dapat dikatakan bahwa terjadi sebuah peningkatan atas kasus kejahatan siber di hingga mencapai 20% dimana pada tahun-tahun sebelumnya lebih tepatnya pada 2009 hanya 0%. Selain itu kasus kejahatan siber di Swiss pada tahun yang sama sendiri terjadi kepada kurang lebih di tahun 140 perusahaan yang berada di negara tersebut dimana mayoritas perusahaan tersebut adalah perusahaan perbankan (Paresti, 2016). Angka kenaikan kasus yang sangat tinggi ini menjadikan upaya Swiss dalam mengatasi ancaman kejahatan siber serta strategi yang berusaha mereka laksanakan menarik untuk dikaji lebih dalam.

METODE PENELITIAN

Penelitian ini bersifat deskriptif, sebagaimana dijelaskan oleh Sugiyono (2020), yang mengartikan penelitian deskriptif sebagai pendekatan untuk mengidentifikasi suatu variabel secara independen, baik itu satu variabel atau lebih, tanpa melakukan perbandingan antara variabel-variabel tersebut. Tujuan dari penelitian deskriptif adalah untuk mengkaji hubungan antar variabel. Data yang dianalisis bersifat kualitatif, yaitu data yang menyediakan informasi non-numerik mengenai proses, kondisi, dan peristiwa dalam bentuk narasi (Haryono dan Ilkodar 2005). Teknik pengumpulan data yang diterapkan adalah studi pustaka, yakni metode pengumpulan informasi dari berbagai literatur seperti buku, jurnal, artikel ilmiah, koran, dan sumber tertulis lainnya yang kredibel.

HASIL PEMBAHASAN

KASUS RANSOMWARE DI SWISS

Salah satu masalah ancaman keamanan siber di wilayah Swiss adalah ransomware, sebuah kasus ransomware yang cukup besar pernah terjadi di negara ini pada tahun 2015, dimana pada tahun tersebut terjadi sebuah

penyerangan yang dilakukan kelompok pembajak bernama Rex Mundi kepada salah satu bank yang berada di Swiss yakni bank Banque Cantonale de Genève atau BCGE. Dimana dalam serangan ini pelaku meminta tebusan pertamanya sebesar 25.000 euro atau sekitar 30.000 dollar dengan jaminan mereka tidak akan membocorkan data-data dari perusahaan perbankan tersebut, namun perusahaan tersebut menolak memberikan uang tebusan tersebut sehingga pelaku menurunkan nominal tebusan dan meminta tebusan keduanya yang hanya sebesar 10.000 euro atau sekitar 12.000 dollar, dengan tenggat waktu pada tanggal 9 Januari 2015 pukul 6 waktu setempat (Bank Info Security, 2015).

"The alleged hack and its seemingly small-scale demand -- $12,000 at current exchange rates -- speak to the prevalence and ease of a rapidly growing extortion industry that deals in stolen or hijacked data"

Hal diatas disampaikan oleh Bloomberg, dimana setelah diturunkannya nominal tebusan yang ada, bank BCGE tetap teguh pada pendirian mereka untuk tidak membayarkan uang tebusan sama sekali. Beberapa jam setelah melewati tenggat waktu yang diberikan oleh pelaku, mereka merilis seluruh data melalui sebuah laman berbagi dengan domain Uploadbaz.com, dimana data yang mereka bocorkan ini mencakup email, nomor telepon, hingga alamat email dari seluruh pengguna bank BCGE tersebut (NextGov FCW, 2015).

Dilansir dari sumber yang sama seperti diatas, kelompok The Rex Mundi ini merupakan kelompok pembajak yang dalam operasinya melakukan pembajakan dengan berupa ransomware yang virus ini nantinya akan mengunci perangkat sehingga korban perlu untuk membayar uang tebusan agar bisa mengakses kembali perangkat serta data-data yang ada didalamnya. Kelompok ini diidentifikasi telah ada dan melancarkan aksinya selama kurang lebih dua tahun sebelumnya atau sekitar tahun 2013 hingga tahun 2015, dimana dalam kelompok ini juga mencakup para peretas yang berasal dari Jerman, Austria, Perancis, hingga Amerika Serikat.

Ransomware sendiri merupakan salah satu ancaman terbesar dalam dunia keamanan siber, serangan dengan metode ini terjadi melalui lampiran email yang tidak dikenal dan berbahaya, situs web yang berbahaya, perangkat penyimpanan eksternal yang mudah terinfeksi, serta melalui aplikasi perangkat lunak, dimana nantinya ransomware ini akan menyebabkan kerugian yang cukup besar akibat waktu berhentinya sistem, biaya pemulihan, dan pembayaran tebusan. Dimana korban harus membayarkan tebusan yang diminta agar perangkat yang mereka miliki atau sistem yang mereka operasikan mampu berjalan dengan normal kembali, namun dibayarkannya tebusan ini juga tidak menjadi jaminan bahwa para pelaku ransomware ini akan mengembalikan perangkat atau sistem seperti semula (Teichmann dkk., 2023). Aksi kejahatan ransomware ini memiliki pola penyerangan dimana terdapat beberapa korban yang paling sering mereka incar, yang pertama adalah universitas dimana hal ini dikarenakan sistem keamanan siber pada tingkat universitas hanya memiliki sedikit tim dalam bidang keamanan datanya serta data di dalamnya yang cukup beraneka ragam. Selanjutnya yakni fasilitas kesehatan serta organisasi-organisasi pemerintahan, dimana menurut para pelaku ini mereka seringkali sangat membutuhkan data-data yang ada dalam perangkat atau sistem mereka sehingga mereka akan segera melakukan tebusan karena kebutuhan atas akses data tersebut. Yang terakhir yakni perusahaan atau organisasi dengan data yang cukup sensitif seperti perusahaan perbankan serta firma hukum, hal ini dikarenakan mereka akan bersedia membayar tebusan karena menghindari bocornya data-data yang mereka miliki serta yang utama yakni untuk menyelamatkan reputasi mereka.

Di Swiss sendiri, setidaknya sekitar 600 kasus kejahatan ransomware terjadi setiap minggunya sejak awal tahun 2016, dimana hal ini didasarkan hanya pada kasus yang dilaporkan oleh perusahaan maupun individu, dan dapat disimpulkan masih terdapat kasus-

kasus lain yang tidak terlapor. Laporan tersebut didapat dari The Swiss Federal Reporting and Analysis Centre for Information Assurance atau biasa dikenal dengan MELANI, namun organisasi tersebut tidak pernah mengeluarkan statistik secara resmi dikarenakan kasus-kasus yang tidak terlaporkan masih banyak sebagaimana disebutkan sebelumnya. Aksi-aksi sepanjang tahun 2016 tersebut, meminta uang tebusan mulai 400 hingga 2.000 franc, namun untuk beberapa kasus perusahaan besar para pelaku meminta uang tebusan hingga puluhan ribu franc (Penta, nd).

Dilansir dari portal berita Reuters, serangan siber yang terjadi di Swiss menjadi suatu ancaman yang besar bagi keberlangsungan perusahaan-perusahaan perbankan di negara tersebut. Hal ini sebagaimana disampaikan Mark Branson selaku Chief Executive dari Swiss Financial Market Supervisory Authority atau biasa dikenal FINMA.

"The risks connected with these attacks are growing in sync with the pace of global digitalisation. Cyber-attacks are now the most serious operational hazard facing the financial system, and both the private sector and public authorities should take them extremely seriously,"

Dalam konferensi tahunan FINMA tersebut, Mark Branson juga menyampaikan bahwa secara keseluruhan, bahwasanya bank-bank Swiss tampaknya menyadari risiko dan cukup siap untuk menghadapi serangan siber yang ada, dimana kemampuan bank untuk menangkal sekitar 100 serangan setiap harinya dari serangan malware pada sistem e-banking mereka. Namun, sebagai sebuah negara, Swiss tertinggal di belakang negara lain dengan pusat keuangan utama yang telah mendirikan pusat kompetensi keamanan siber atau menerapkan tes sistem secara menyeluruh untuk menguji kemampuan peretas dalam menembus sistem perbankan (Shields, 2018). Berdasarkan konferensi tersebut dapat dikatakan upaya-upaya yang dilakukan cenderung bersifat individu, masih belum terdapat sebuah badan khusus untuk menangani masalah-masalah keamanan siber di Swiss itu sendiri.

STRATEGI DAN KEBIJAKAN SWISS

Berdasarkan masalah terkait ancaman siber *ransomware* yang telah dijelaskan sebelumnya yakni semakin meningkatkan serangan siber terkhususnya serangan dengan menggunakan malware atau yang biasa juga disebut dengan aksi ransomware ini semakin meningkat di Swiss, sehingga berikut merupakan beberapa kebijakan yang sedang dijalankan oleh pemerintah Swiss dalam mengatasi masalah ini.

Strategi pertama yang dilakukan oleh Swiss adalah pembentukan National Strategy for The Protection of Switzerland Against Cyber Risks. Dalam mengatasi kasus *ransomware* ini, pemerintah Swiss mengeluarkan sebuah strategi dimana strategi ini dikeluarkan oleh Federal Department of Defence, Civil Protection and Sport atau DDPS.

Gambar 1. Strategi Keamanan Siber NCS.

Sphere of action 1	Measures	
Research and development	1	New risks in connection with cyber crime are to be researched
Sphere of action 2	**Measures**	
Risk and vulnerability analysis	2	Independent evaluation of systems Risk analyses to minimise risks in collaboration with authorities, ICT service providers and system suppliers
	3	Testing of ICT infrastructure for systemic, organisational and technical vulnerabilities
Sphere of action 3	**Measures**	
Analysis of the threat landscape	4	Establishment of a picture of the situation and its development
	5	Review of incidents for the further development of measures
	6	Case overview and coordination of inter-cantonal clusters of cases
Sphere of action 4	**Measures**	
Competence building	7	Establishment of an overview of the competence building offering and identification of gaps
	8	Filling of gaps in competence building and increased use of high-quality offerings
Sphere of action 5	**Measures**	
International relations and initiatives	9	Active participation of Switzerland in the area of Internet governance
	10	Cooperation at the international security policy level
	11	Coordination of those involved in initiatives and best practices relating to security and assurance processes
Sphere of action 6	**Measures**	
Continuity and crisis management	12	Strengthening and improving resilience to disturbances and incidents
	13	Coordination of activities, primarily with those directly involved, and support of decision-making processes with the relevant expertise
	14	Active measures to identify the perpetrator and possible impairment of its infrastructure in the event of a specific threat
	15	Establishment of a plan for management procedures and processes to ensure timely problem-solving
Sphere of action 7	**Measures**	
Legal foundations	16	Evaluation of existing legislation on the basis of measures and implementation concepts and prioritisation of immediate adjustment needs

Sumber: Federal Department of Defence, Civil Protection and Sport.

Dimana perlindungan infrastruktur informasi serta komunikasi dari ancaman siber merupakan salah satu kepentingan nasional Swiss, Dewan Federal membentuk strategi nasional untuk melindungi Swiss ancaman kejahatan siber, dengan beberapa tujuan utamanya yakni; Melakukan identifikasi dini ancaman dan bahaya di bidang siber, Peningkatan atas ketahanan infrastruktur

kritis, serta Upaya pengurangan efektif risiko siber, terutama kejahatan siber dan sabotase siber. Dimana strategi ini dibentuk pada tahun 2012 dan akan dilaksanakan hingga tahun 2017 (Federal Department of Defence Civil Protection and Sport DDPS, 2012). Berdasarkan strategi tersebut, dapat disimpulkan bahwasannya DDPS ini berusaha untuk menanggulangi ancaman-ancaman siber melalui 7 bidang. Pertama yakni dilakukan riset serta pengembangan, dimana risiko yang berkaitan dengan kejahatan siber perlu diteliti agar keputusan yang tepat dapat diambil sejak awal, proses penelitian dan pengembangan ini dilakukan secara mandiri oleh para aktor yang ada di bidang ilmu pengetahuan, sektor swasta, masyarakat, dan otoritas yang berwenang. Lalu kedua analisis resiko serta kerentanan, dimana semua unit otoritas publik yang kompeten dalam bidang teknologi dan keamanan siber harus mengidentifikasi risiko serta mengevaluasi dan menganalisis kemungkinan terjadinya dampak potensial kedepannya. Ketiga analisis lanskap ancaman, dimana kejadian-kejadian yang penting terkait ancaman keamanan siber dalam tingkat nasional harus diidentifikasi, dievaluasi, dan dianalisis. Secara singkat proses ini mengacu pada upaya untuk mengelola kejadian-kejadian nasional supaya informasi yang ada di dalamnya dapat digunakan oleh pihak yang bertanggung jawab untuk mengambil suatu tindakan yang sesuai.

Keempat pembangunan kompetensi, dimana seluruh aktor dari sektor swasta, masyarakat, dan otoritas harus diberitahu tentang risiko-risiko keamanan siber dan menerima pelatihan agar mereka dapat mengenali risiko-risiko tersebut dan mengambil langkah-langkah untuk meminimalkan dampak yang akan mereka rasakan. Tujuannya adalah untuk meningkatkan kesadaran dan keterampilan dalam menghadapi ancaman keamanan siber sehingga semua aktor dapat berkontribusi dalam melindungi diri mereka sendiri dan lingkungan mereka dari serangan siber. Kelima inisiatif serta hubungan antar aktor internasional, dimana pendekatan multi stakeholder diambil, dengan melibatkan berbagai kelompok kepentingan dan unit otoritas publik yang bertindak sesuai dengan peran mereka masing-masing, karena sifat global dari internet itu sendiri. Keenam keberlanjutan dan manajemen atas krisis, dimana berbagai macam aktor yang terlibat harus dikoordinasikan dalam seluruh tingkatan dalam upaya penanganan ancaman siber ini.

Dan terakhir adalah pembentukan hukum, dimana banyak undang-undang dan peraturan yang saat ini membentuk dasar hukum dalam ranah siber, dengan kata lain, ada kebutuhan untuk menjelaskan bagaimana administrasi dapat mengeluarkan ketentuan yang mengikat untuk mengurangi risiko siber. Ketika melaksanakan langkah-langkah diatas tersebut demi meningkatkan perlindungan Swiss terhadap risiko siber, kegunaan politik, ekonomi, serta struktur negara di Swiss harus diperhitungkan. Yang pada artinya bahwa seluruh pihak yang terlibat harus memahami sejauh mana aspek siber dari tugas dan tanggung jawab mereka masing-masing dan dengan mitra sosio-ekonomi dan politik mana langkah-langkah untuk meminimalkan risiko ancaman siber. Unit-unit yang bertanggung jawab dalam setiap langkah diharapkan untuk melakukan persiapan dan pelaksanaan langkah-langkah yang sesuai dengan posisi masing-masing, dimana hal ini dilakukan melalui berbagai macam kerjasama dengan mitra lain seperti otoritas publik baik itu dalam tingkat federal atau tidak, sektor swasta, bahkan hingga sektor masyarakat. Selain itu strategi ini juga dikenal dengan nama NCS atau National Cybersecurity Strategy.

Selain pembentukan NCS sebagai sebuah strategi utama negara dalam mengatasi permasalahan ancaman siber, Swiss pada akhirnya juga membentuk sebuah badan khusus demi menangani permasalahan siber nasionalnya, yakni NCSC atau biasa juga disebut dengan National Cyber Security Center. NCSC ini merupakan tulang punggung dari upaya keamanan siber di Swiss, sebagai pusat keamanan siber utama pemerintah federal, NCSC berfungsi sebagai garis pertahanan pertama bagi keberadaan layanan bisnis, layanan publik, lembaga

pendidikan, serta masyarakat umum terhadap ancaman keamanan siber. Peran pentingnya lembaga ini adalah mengkoordinasikan implementasi strategi keamanan siber nasional (NCS) dan memastikan ketangguhan digital negara, serta menjadi suatu aktor kunci dalam lanskap keamanan siber di Swiss (HSLU Hochshule Luzern, 2024).

Pentingnya keamanan siber telah semakin disadari oleh seluruh lapisan masyarakat. Dimana hal ini tidak hanya tentang melindungi bisnis dan individu di ranah siber tetapi juga sebagai salah satu tujuan utama dalam kebijakan luar negeri dan keamanan nasional dan internasional. Akibatnya, menjaga keamanan siber ini telah menjadi tanggung jawab federal yang utama yang juga menegaskan betapa seriusnya masalah ini. NCSC bertujuan untuk memperkuat keamanan siber dalam infrastruktur, ekonomi, sistem pendidikan, pemerintah, serta masyarakat umum. Misi ini dicapai dengan mengkoordinasikan implementasi Strategi Keamanan Siber Nasional (NCS). Untuk mencapai tujuan ini, NCSC ini dibangun di atas empat pilar strategis utama, yakni; 1) Membuat ancaman keamanan siber dapat dimengerti, 2) Menyediakan cara untuk mencegah serangan keamanan siber, 3) Membatasi kerusakan dari insiden keamanan siber, 4) Meningkatkan keamanan produk dan layanan digital.

NCSC ini pertama kali dibentuk pada tahun 2019 tepatnya pada 14 Juni, di bawah masa Presiden Ueli Maurer, badan ini pada awal pembentukannya dibawah FDF atau federal Department of Finance. Dengan pemimpin yang didelegasikan sejak awal 2019 atau tepatnya pada bulan Februari yakni Florian Schütz, yang nantinya akan memulai jabatannya sebagai pemimpin dari badan ini pada awal bulan Agustus. Florian yang berusia 37 pada saat itu akan memimpin sebuah tim dengan 30 anggota dibawahnya, dimana ia nantinya akan mengambil alih manajemen dari badan ini dan melaporkan secara langsung kepada FDF sebagai lembaga yang ada diatasnya (NCSC, 2019). Lalu pada 2 Desember 2022, Dewan Federal memutuskan untuk memindahkan NCSC ini dibawah the Federal Department of Defence, Civil Protection and Sport (DDPS) yang sebelumnya dibawah FDF, dengan pemimpin badan tetap sama yakni Florian Schütz. Hingga pada akhirnya per 1 Januari 2024 lalu, dibentuknya sebuah kantor khusus untuk badan ini (NCSC, 2023). NCSC ini nantinya juga akan bertanggung jawab penuh atas pembuatan NCS yang telah dijelaskan sebelumnya.

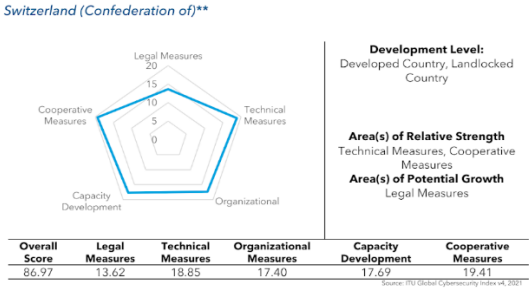
REKOMENDASI KEBIJAKAN

Dalam menentukan rekomendasi kebijakan dalam permasalahan keamanan siber di Swiss penulis menggunakan Global Security Index tahun 2020 yang diterbitkan oleh ITU Global Cyber Security Index v4, pada tahun 2021 (International Telecommunication Union, 2021). Dalam laporan tersebut, terdapat 5 pilar yang dijadikan acuan dalam menganalisis kemampuan serta kekuatan atas ancaman siber yang dimiliki oleh suatu negara, kelima pilar tersebut yakni *legal measure* dimana didalamnya terkait dengan memastikan adanya mekanisme hukum serta regulasi dalam mengatasi permasalahan ancaman siber, dengan tiga indikator yang ada yakni *countries with some form of cybersecurity legislation, data protection regulations,* dan *critical infrastructure regulations*. Lalu pada pilar yang kedua terdapat *technical measure* dimana didalamnya terkait dengan memastikan adanya implementasi secara teknis serta memastikan kapabilitas dari aktor nasional maupun badan-badan tertentu dalam upaya tercapainya keamanan siber, dengan tiga indikator yang ada yakni *active CIRTs, engaged in a regional CIRT,* dan *child online protection reporting mechanisms.*

Pilar ketiga yakni *organizational* dimana didalamnya terkait dengan memastikan strategi dari organisasi nasional dalam mengimplementasikan keamanan siber, dengan tiga indikator yang ada yakni *national cybersecurity strategies, cybersecurity agencies child online protection strategies,* dan *initiatives reported.* Pilar keempat yakni *capacity development* dimana didalamnya terkait dengan memastikan adanya edukasi,

pelatihan, serta pendanaan dari perkembangan upaya keamanan siber nasional, dengan tiga indikator yang ada yakni, *countries conduct cyber-awareness initiatives, countries with cybersecurity r&d programs,* dan *countries reported having national cybersecurity industries.* Pilar yang terakhir yakni *cooperation* dimana didalamnya terkait dengan memastikan adanya kerjasama diantara lembaga, perusahaan, serta negara dalam menangani permasalahan keamanan siber, dengan tiga indikator yang ada yakni, *countries engaged in cybersecurity public - private partnerships, countries with cybersecurity bilateral agreements,* dan *countries with cybersecurity multilateral agreements.* Dalam laporan tersebut yang disampaikan oleh International Telecommunication Unions tersebut Swiss atau Switzerland ini menempati urutan ke 42 dengan skor sebesar 86.97 dari sekitar 182 negara yang termasuk dalam laporan tahunan tersebut

Gambar 2. Global Cybersecurity Index 2020 Switzerland.



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
86.97	13.62	18.85	17.40	17.69	19.41

Source: ITU Global Cybersecurity Index v4, 2021

Sumber: Global Cybersecurity Index 2020.

Berdasarkan hasil index terkait dengan keamanan siber tersebut, jika didasarkan pada kelima pilar yang dijadikan indikator dalam laporan ini, Swiss mendapatkan poin paling tinggi dalam *cooperative measure*, dengan poin terendah yakni pada *legal measure* yang disusul dengan *organizational measure*. Berdasarkan data ini berikut merupakan beberapa rekomendasi kebijakan yang bisa penulis berikan bagi pertahanan siber dari negara Swiss.

Rekomendasi kebijakan pertama yang dapat penulis berikan adalah penetapan kebijakan hukum serta regulasi yang lebih komprehensif. Keberadaan hukum dan regulasi terkait keamanan siber menjadi salah satu hal yang memegang peranan penting dalam kehidupan sehari-hari kita. Keberadaan hal tersebut menjadi penting demi memastikan bahwa informasi yang kita miliki dilindungi dari ancaman siber. Hampir setiap aspek kehidupan keseharian kita telah terdigitalisasi, termasuk penyimpanan informasi-informasi penting, seperti riwayat kesehatan, data pribadi, dan hingga alamat email (Harris, 2024). Sehingga upaya pengamanan data ini sangat penting untuk dilakukan, demi keamanan pribadi maupun bersama. Keberadaan hukum terkait keamanan siber secara efektif berfungsi untuk melindungi pengguna dari serangan siber. Dengan skema serangan seperti *phishing*, *ransomware*, pencurian identitas, pelanggaran data, dan kerugian finansial. Keberadaan hukum penting untuk memperkuat pelacakan, pencegahan, dan mitigasi ancaman siber.

Swiss sendiri telah memiliki hukum yang mengatur terkait dengan keamanan data dalam dunia siber, yang diberi nama Swiss Federal Data Protection Act atau biasa juga disebut dengan FADP, yang diadopsi pada 25 September 2020, dimana FADP pada tahun 2020 tersebut menjadi pengganti dari bentuk sebelumnya yang disahkan pada tahun 1992 (Cookiebot, 2023). Dalam hal persyaratan keamanan data, Swiss sendiri tidak memberlakukan suatu standar yang khusus. Sebaliknya, negara mempertahankan sikap netral terhadap teknologi, dengan artian siapapun yang menggunakan jaringan internet harus menerapkan langkah-langkah teknis sendiri yang memadai dalam menghindari ancaman, jika didasarkan pada Pasal 8 Ayat 1 DPA (Reeves & Schneider, 2023). Dalam regulasi tersebut, secara spesifik pasal 24 DPA, disampaikan juga bahwasannya seluruh pihak yang menggunakan akses ini akan diberikan suatu kewajiban umum dalam hal adanya perilaku kejahatan dan segera untuk melaporkan jika terjadi suatu serangan siber ataupun menjadi korban dari suatu aksi kejahatan siber kepada pusat keamanan siber negara yakni NCSC. Selain apa yang disampaikan sebelumnya, para pengelola data

juga memiliki kewajiban untuk memberikan informasi kepada subjek yang bersangkutan– para pengguna layanan yang mereka miliki, dengan tujuan untuk melindungi subjek yang dimaksudkan. Sehingga dapat ditarik kesimpulan bahwa dengan adanya seperangkat regulasi ini setiap individu yang menggunakan internet memiliki tanggung jawab atas keamanan data pribadinya, dan setiap pemilik layanan daring juga memiliki tanggung jawab dalam upaya menjaga keamanan dari seluruh pengguna layanan mereka, dengan catatan mereka harus memberikan informasi terlebih dahulu terkait dengan apakah pengguna layanan mereka setuju atas apa yang dilakukan oleh pemilik layanan,

FADP terbaru ini secara garis besar dibentuk untuk meningkatkan perlindungan data nasional serta menyelaraskannya dengan GDPR demi berlangsungnya aliran data dari zona ekonomi Eropa ke Swiss. GDPR atau EU's General Data Protection Regulation merupakan seperangkat regulasi yang dimiliki oleh kawasan Uni Eropa dalam hal legal atas keamanan data kawasan.

Gambar 3. Perbedaan GDPR dan FADP

GDPR vs. new FADP

Requirement	Penalties
GDPR	For first or less serious violations: 2% of global annual turnover or €10 million For repeat or more serious violations: 4% of global annual turnover or €20 million.
FADP	Up to CHF 250,000 against a responsible individual, or if it would be too difficult to identify the individual, up to CHF 50,000 against the company.

Requirement	Information requirements
GDPR	Art. 13 GDPR specifies the minimum information that a privacy policy must include.
FADP	A privacy policy has less required information than under the GDPR. Must list all countries to which personal data is transferred.

Requirement	Records of processing activities
GDPR	Art. 30 GDPR specifies all information that must be included in the records.
FADP	Must include a list of countries to which data is exported.

Requirement	Data Protection Impact Assessments
GDPR	In cases of high risk, the supervisory authority must be consulted.
FADP	In cases of high risk, Data Protection Officer (DPO) can be consulted instead of the FDPIC.

Requirement	Data export
GDPR	Adequacy of export partners determined by the European Commission. Standard contractual clauses or other binding corporate rules.
FADP	Adequacy of export partners is determined by the Swiss Federal Council. EU standard contractual clauses or other binding corporate rules.

Requirement	Data breach notification
GDPR	Mandatory within 72 hours.
FADP	Mandatory "as soon as possible".

Requirement	Data Protection Officer
GDPR	Mandatory.
FADP	Recommended.

Sumber: https://www.cookiebot.com/en/swiss-fadp/.

Berdasarkan data yang dilampirkan di atas dapat dilihat bahwa FADP terbaru yang dikeluarkan oleh Swiss ini berusaha untuk sejalan dengan regulasi yang dimiliki oleh Uni Eropa. Meskipun Swiss termasuk dalam wilayah negara kawasan Eropa, namun tidak ada kewajiban bagi negara tersebut untuk memberlakukan regulasi yang ada di kawasan. Tapi jika berkaca pada upaya Swiss untuk meningkatkan keamanan siber nasional yang didasarkan pada GDPR, masih sangat jauh kedua regulasi tersebut jika dibandingkan. Selain itu dalam sumber lain dikatakan juga masih belum terdapatnya hukum atau regulasi yang secara khusus mengatur dan dapat diaplikasikan kepada perusahaan pribadi atau *private company* di Swiss (Global Data Privacy and Cybersecurity Handbook, 2023). Sehingga Swiss harus lebih sering melakukan evaluasi dan revisi pada hukum serta regulasi yang mereka miliki sehingga dasar hukum dalam mengatasi ancaman siber di negara ini dapat semakin kuat, selain itu dirasa sangat penting untuk segera membentuk regulasi yang dapat diaplikasikan kepada perusahaan-perusahaan yang berada di kawasan negara tersebut, sehingga upaya-upaya dalam menjaga keamanan siber nasional dapat mereka capai.

Rekomendasi kedua adalah upaya *raising awareness* bagi karyawan perusahaan. Kesadaran seluruh lapisan masyarakat atas keamanan siber ini menjadi suatu langkah penting mencapai keamanan siber nasional. Upaya peningkatan pemahaman ini dapat berhasil jika seluruh pihak menyadari bahaya saat menjelajahi web, rajin dalam memeriksa email, dan berhati-hati dalam berinteraksi secara online, dimana ketiga hal tersebut adalah komponen dari kesadaran atas bahaya ancaman keamanan siber. Memberikan edukasi serta pemahaman yang sesuai kepada setiap setiap masyarakat sangat penting untuk membangun kesadaran keamanan siber yang memotivasi perubahan perilaku dalam jangka waktu yang lama, dan berkelanjutan (Forbes, 2022).

Dalam konteks suatu perusahaan, upaya edukasi terkait keamanan siber ini menjadi hal yang penting saat dilihat dari

perspektif *risk management* atau manajemen risiko. Dengan semakin meningkatnya jumlah serangan siber yang terjadi setiap tahun, risiko jika tidak melakukan edukasi kepada karyawan atas kesadaran keamanan siber hanya akan terus menambah resiko ancaman bagi perusahaan. Pada sebuah data pada tahun 2021 saja, 85% pelanggaran data yang terjadi melibatkan unsur manusia didalamnya, dengan 94% malware dikirim melalui email. Selain itu Menurut IBM atau International Business Machines, rata-rata pelanggaran data pada tahun tersebut membuat kerugian sebesar 4,24 juta dollar, dengan 38% perusahaan terdampak kehilangan bisnis sebagai akibat dari adanya pelanggaran data yang dilakukan oleh para pelaku kejahatan siber.

Dalam konteks Swiss sendiri, pada tahun 2022 meluncurkan sebuah program *raising awareness* atas *cybersecurity* dalam sebuah kampanye kesadaran atas keamanan siber nasional bernama S-U-P-E-R.ch tepatnya pada 5 September 2022 (The Federal Council, 2022). Namun kampanye ini hanya berfokus pada upaya preventif untuk mendeteksi serta mencegah adanya penipuan melalui internet. Kampanye ini dibentuk NCSC, bersama dengan Swiss Crime Prevention serta pihak kepolisian, dimana informasi atas kampanye tersebut disediakan di situs kampanye S-U-P-E-R.ch. Dengan berupa contoh dari pesan-pesan penipuan dan masyarakat dapat menguji keterampilan baru mereka dengan kuis yang telah disediakan dalam website tersebut. Selain itu, kampanye ini juga dilaksanakan dalam bentuk disebarkannya informasi melalui poster dan media sosial.

Jika didasarkan pada kampanye tersebut saja, dapat dikatakan masih belum cukup meningkatkan kesadaran masyarakat atas keamanan siber, karena kampanye yang hanya berfokus pada isu penipuan online, padahal terdapat isu-isu keamanan siber yang juga menjadi masalah utama bagi Swiss, yakni ransomware itu sendiri. Sebanyak 60% dari seluruh perusahaan di Swiss terindikasi terkena malware, dengan 35% dari mereka harus membayar tebusan kepada pelaku (Organisator, 2022). Sehingga menurut penulis salah satu target yang sangat penting dalam upaya edukasi dan *raising awareness* adalah pihak perusahaan dan seluruh karyawan yang di dalamnya. Sehingga penulis merekomendasikan untuk pemerintah membuat suatu program khusus bagi perusahaan-perusahaan yang berada di negaranya untuk mengenalkan dan memberikan pelatihan dan pemahaman atas ancaman siber terkhususnya malware, karena dengan hal ini nantinya akan memberikan pemahaman lebih bagi karyawan sehingga akan menghindarkan perusahaan mereka menjadi korban dari kejahatan siber ransomware ini. Selain suatu program, kebijakan penting dibuat bagi perusahaan untuk terus melakukan program edukasi atas ancaman siber bagi karyawan yang mereka miliki secara berkala dan berkelanjutan, sehingga hal ini tidak hanya menjadi tanggung jawab pemerintah saja tetapi juga menjadi tanggung jawab dari masing-masing perusahaan.

Terdapat beberapa langkah yang dapat dilakukan oleh perusahaan dalam menjaga keamanan data yang mereka miliki, pertama melakukan penginstalan atas sistem keamanan ganda dan selalu melakukan pemeliharaan atas hal tersebut, kedua secara aktif melakukan identifikasi atas potensi serangan sehingga serangan dapat dihindari, ketiga memperkuat kondisi IT di perusahaan dan segera memberhentikan operasi atas perangkat yang dideteksi berbahaya, keempat dibuatnya strategi atas situasi terburuk dengan membuat rencana darurat atas serangan siber, dan kelima melakukan pencadangan data secara berkala. Beberapa langkah tersebut dapat menjadi acuan bagi pemerintah serta perusahaan dalam melakukan edukasi atas ancaman keamanan siber nasional.

KESIMPULAN

Berdasarkan analisi yang telah dilakukan sebelumnya dapat disimpulkan bahwa kebijakan keamanan siber yang diterapkan di Swiss saat ini masih berada pada tahap pengembangan dan belum menunjukkan hasil yang maksimal dalam menghadapi ancaman siber secara menyeluruh. Meskipun negara ini

telah meluncurkan kebijakan yang cukup penting seperti National Cybersecurity Strategy (NCS) dan mendirikan National Cyber Security Centre (NCSC), dampak dari kebijakan ini terhadap peningkatan keamanan siber secara keseluruhan masih belum terlihat secara signifikan.

Kebijakan yang ada saat ini cenderung tidak terfokus secara khusus pada ancaman *ransomware*, yang merupakan salah satu tantangan utama dalam lanskap keamanan siber. Untuk meningkatkan efektivitas strategi nasional ini, disarankan agar Swiss mengadopsi pendekatan yang lebih holistik dan komprehensif dalam menangani ancaman siber.

Rekomendasi utama meliputi penetapan regulasi yang lebih menyeluruh, yang tidak hanya mencakup tanggapan terhadap serangan *ransomware* tetapi juga mencakup berbagai jenis ancaman siber lainnya. Penting untuk adanya hukum atau regulasi yang secara khusus mengatur dan dapat diterapkan kepada perusahaan swasta di Swiss. Selain itu, penting untuk mengembangkan program peningkatan kesadaran yang lebih efektif untuk karyawan di berbagai sektor. Program ini harus fokus pada pelatihan dan pendidikan mengenai praktik keamanan siber yang baik, serta strategi mitigasi untuk mengurangi risiko serangan ransomware.

Dengan mengimplementasikan regulasi yang komprehensif dan meningkatkan kesadaran di kalangan karyawan, Swiss dapat memperkuat ketahanan sibernya secara keseluruhan dan mengurangi potensi dampak dari serangan ransomware, sambil memastikan bahwa semua aspek keamanan siber dipertimbangkan dalam strategi nasional.

DAFTAR PUSTAKA

Bank Info Security. (2015, January 12). Hackers Release Info from Swiss Bank. Retrieved from https://www.bankinfosecurity.com/hackers-release-info-from-swiss-bank-a-7781.

Bernabe, J. & Skarmeta, A. (2019). Challenges in Cybersecurity and Privacy - the European Research Landscape. River Publishers Series in Digital Security and Forensics: Denmark.

Cavalry, M. & Smeets, M. (2023). Regulatory cybersecurity governance in the making:the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy, 30*(7), 1330–1352.

Christou, J. (2018). The challenges of cybercrime governance in the European Union. *European Politics And Society, 19*(3), 355–375.

Cookiebot. (2023, July 20). FADP – Switzerland's Federal Act on Data Protection. Retrieved from https://www.cookiebot.com/en/swiss-fadp/.

Federal Department of Defence, Civil Protection and Sport DDPS. (2012). *National strategy for the protection of Switzerland against cyber risks*. Author.

Forbes. (2022, March 16). Cybersecurity Awareness: What It Is And How To Start. Retrieved from https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/.

Global Data Privacy and Cybersecurity Handbook. (2023, December 27). Key Data Privacy and Cybersecurity Laws. Retrieved from https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook.

Harris, E. (2024, April 19). Cybersecurity Laws and Policy: A Comprehensive Overview. Retrieved from https://pluralpolicy.com/blog/cybersecurity-laws-and-policy/#:~:text=Effective%20cybersecurity%20laws%20protect%20users,and%20mitigation%20of%20cyber%20threats.

HSLU Hochshule Luzern. (2024, May 16). The Essentials of Switzerland's Digital Law Part 7: Switzerland's Cybersecurity Strategy and Initiatives. Retrieved from https://blog.hslu.ch/majorobm/2024/05/

16/the-essential-of-switzerlands-digital-law-part-7-switzerlands-cybersecurity-strategy-and-initiatives-t-d1418/.

International Telecommunication Union. (2021). *Global Cybersecurity Index 2020.* ITU Publications. Authors.

Teichmann, F., Boticiu, S., & Sergi, B. (2023). The Evolution of Ransomware Attacks in Light of Recent Cyber Threats. How Can Geopolitical Conflicts Influence the Cyber Climate?. *International Cybersecurity Law Review, 4*(1), 259–280.

NCSC. (2019, June 14). Florian Schütz to become federal Cyber Security Delegate. Retrieved from https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/medienmitteilungen/newslist.msg-id-75421.html.

NCSC. (2023, May 24). Florian Schütz appointed director of the new Federal Office for Cyber Security. Retrieved from https://www.ncsc.admin.ch/ncsc/en/home/dokumentation/medienmitteilungen/newslist.msg-id-95371.html.

NextGov FCW. (2015, January 9). Hackers Leak Data from Swiss Bank that Rebuffed $12K Ransom Demand. Retrieved from https://www.nextgov.com/cybersecurity/2015/01/breach/143575/.

Organisator. (2022, April 28). 60 percent of Swiss companies affected by extortion malware. Retrieved from https://www.organisator.ch/en/management/it/2022-04-28/60-percent-of-swiss-companies-affected-by-erpress-malware/.

Paresti, A. (2016). Negara Liliput dalam Persoalan Digital: Upaya Upaya Swiss Menghadapi Ancaman Keamanan Siber. *Jurnal Analisis Hubungan Internasional, 5*(2), 495-506.

Penta. (nd). Ransomware growing in Switzerland. Retrieved from https://penta.ch/insights/ransomware-growing-in-switzerland.

Reeves, H. & Schneider, J. (2023). In a nutshell: data protection, privacy and cybersecurity in Switzerland. Walder Wyss Ltd.

Shields, M. (2018, March 27). Cyber-attacks biggest risk for Swiss banks - watchdog. Retrieved from https://www.reuters.com/article/idUSKBN1H3164/.