JURNAL ABDI INSANI
Volume 11, Nomor 2, Juni 2024
http://abdiinsani.unram.ac.id. e-ISSN : 2828-3155. p-ISSN : 2828-4321

EDUKASI PENGGUNAAN INTERNET DALAM DIPLOMASI DAN UPAYA MENGATASI ANCAMAN KEAMANAN SIBER BAGI MAHASISWA HUBUNGAN INTERNASIONAL UNIVERSITAS TANJUNGPURA

Educating on Internet Use in Diplomacy and Efforts to Counter Cyber Security Threats For International Relations Students at Universitas Tanjungpura

Hardi Alunaza*

Prodi Hubungan Internasional Universitas Tanjungpura

Jalan Prof Dr Hadari Nawawi, Pontianak Kalimantan Barat

*Alamat Korespondensi: hardi.asd@fisip.untan.ac.id

(Tanggal Submission: 13 Maret 2024, Tanggal Accepted : 24 April 2024)

Kata Kunci :

Penggunaan Internet, Citra Positif, Keamanan Siber, Privasi Data

Abstrak :

Kegiatan pengabdian ini didasarkan pada semakin banyak masalah yang dihadapi mahasiswa Hubungan Internasional yang berhubungan dengan ancaman keamanan siber. Hal tersebut sebagai akibat dari penggunaan internet yang tidak dapat dihindari. Tetapi banyak mahasiswa yang tidak mengetahui batasan privasi yang harus dijaga agar terhindar dari dampak negatif penggunaan internet. Edukasi dalam kegiatan pengabdian ini menjadi penting agar mahasiswa memahami strategi yang dapat dilakukan untuk menghindari ancaman keamanan siber. Kegiatan ini dilaksanakan di bulan Mei tahun 2023 dengan memberikan sosialisasi menggunakan metode edukasi, tanya jawab dan diskusi. Metode tersebut digunakan dalam edukasi terkait penggunaan internet dengan bijak yang berdampak terhadap peningkatan pemahaman mahasiswa mengenai langkah yang harus dilakukan agar terhindar dari ancaman keamanan siber. Setelah mengikuti kegiatan, mahasiswa menjadi lebih paham mengenai pentingnya penggunaan media sosial secara bijak dalam meningkatkan citra positif pengguna dan juga negara dan menjaga privasi data. Mahasiswa mengetahui strategi menjaga privasi data. Serta, upaya yang dapat dilakukan untuk pemulihan data. Setelah mengikuti kegiatan pengabdian ini, mahasiswa menjadi lebih peduli dalam melindungi data pribadi dan privasi di dunia maya. Mahasiswa juga memahami perlunya kolaborasi untuk mewujudkan keamanan siber.

Key word :

Internet Use, Positive Image,

Abstract :

This community service activity is based on the increasing number of problems faced by International Relations students related to cyber security threats, a

Cyber Security, Data Privacy	consequence of the unavoidable use of the internet. However, many students are unaware of the privacy boundaries that must be maintained to avoid the negative impacts of internet usage. Education in this community service activity becomes important so that students understand the strategies that can be implemented to avoid cyber security threats. This activity was carried out in May 2023, providing socialization using educational methods, question and answer sessions, and discussions. The method is used in educating related to the wise use of the internet, which impacted the enhancement of students' understanding of the steps that must be taken to avoid cyber security threats. After participating in the activity, students become more aware of the importance of using social media wisely to enhance positive image of users and the country, and to maintain data privacy. Students are aware of strategies to maintain data privacy, as well as efforts that can be made for data recovery. Following this community service activity, students become more concerned about protecting personal data and privacy in social media. Students also understand the necessity of collaboration to achieve cybersecurity.

Panduan sitasi / citation guidance (APPA 7th edition) :

Alunaza, H. (2024). Edukasi Penggunaan Internet Dalam Diplomasi dan Upaya Mengatasi Ancaman Keamanan Siber Bagi Mahasiswa Hubungan Internasional Universitas Tanjungpura. *Jurnal Abdi Insani, 11(2), 1199-1206*. https://doi.org/10.29303/abdiinsani.v11i2.1505

PENDAHULUAN

Perkembangan dalam bidang teknologi telah menghasilkan berbagai dampak rumit pada kehidupan manusia serta hubungan internasional. Dengan adanya internet, batasan negara yang sebelumnya diterima dan diikuti oleh kesepakatan global mulai terasa tidak jelas (Luqman, 2021). Globalisasi memunculkan tantangan baru untuk manusia di bumi, termasuk perubahan cara berpikir tentang kebutuhan internet (Nurhaidah & Musa, 2015). Walaupun globalisasi membawa manfaat bagi kehidupan manusia, globalisasi juga menimbulkan efek negatif. Ancaman keamanan siber menjadi salah satu masalah serius yang muncul baru-baru ini (Rahmawati, 2019). Selain itu, penggunaan internet untuk membentuk opini publik dan internasional melalui kampanye, propaganda, dan agitasi menjadi lebih mudah dan murah dibandingkan masa sebelumnya, memungkinkan kelompok tertentu untuk mempromosikan kepentingan mereka dengan efisien.

Serangan dunia maya seperti cybercrime dan cyberwar berisiko tidak hanya merugikan keamanan pribadi dengan mengakses aset yang dimiliki manusia (Soewardi, 2013). Insiden-insiden mencolok meliputi pencurian identitas dan data, pembajakan akun, penyebaran virus melalui *file* dan situs *website* beserta kode-kode vital, sampai tindakan fitnah, penistaan, dan pencemaran nama baik. Saat ini, juga terjadi penyanderaan atas informasi kritis yang sering terjadi. Semua ini menyebabkan kekhawatiran dalam masyarakat akibat kehilangan privasi dan ancaman terhadap hilangnya aset dan harta (Situmeang, 2021). Dunia siber pun kerap dijadikan alat politik dengan menyebarkan informasi palsu untuk tujuan provokasi politik atau manipulasi ekonomi (Amilin, 2019).

Paradigma keamanan nasional kini telah berkembang menjadi lebih inklusif, mencakup perlindungan keamanan individu bagi warganya (Renaud & Coles-Kemp, 2022). Salah satu tanggung jawab utama negara adalah menyediakan perlindungan terhadap warganya dari ancaman kejahatan siber. Kejahatan siber ini memiliki potensi untuk merusak privasi dan informasi rahasia secara besar-besaran, yang jika terus meningkat dapat menimbulkan kekhawatiran luas di kalangan masyarakat. Keterbatasan dalam penguasaan teknologi oleh negara dan ketiadaan peraturan yang ketat tentang pertahanan siber dapat membahayakan keamanan negara secara signifikan (Sutra & Haryanto, 2023).

Negara atau kelompok yang memiliki kepentingan dapat dengan mudah mengakses infrastruktur kritis milik negara lain (Aji, 2023). Tingkat ketergantungan masyarakat terhadap teknologi informasi semakin meningkatkan risiko yang dihadapi (Arianto, 2021). Saat ini, hampir semua elemen ekonomi, sosial, dan pertahanan sangat bergantung pada internet. Dari kegiatan perbankan, transaksi ekonomi, pemeliharaan dan operasional transportasi, manajemen persenjataan, hingga komunikasi sosial, semuanya terikat pada konektivitas internet (Kristiyono, 2015). Dengan akses global ini, setiap orang di seluruh dunia memiliki potensi yang sama untuk mengakses dan potensial merusak sistem yang ada, termasuk kemampuan untuk meretas dan mengendalikan aset serta pertahanan, baik individu maupun negara, dengan cara yang sangat mudah (Weu, 2020).

Tidak terbatas pada skala negara saja, di lingkungan kampus pun mahasiswa sering menjadi target dari serangan keamanan siber. Meningkatnya penggunaan internet di antara mahasiswa berpotensi membahayakan keamanan nasional, terutama karena internet telah menjadi bagian esensial dari kehidupan mahasiswa, termasuk untuk keperluan belanja online, pembayaran tagihan, pencarian informasi, komunikasi, hingga mendukung kegiatan sehari-hari melalui media sosial (Kurniawan et al., 2021). Meskipun secara langsung memberikan keuntungan bagi penggunanya, situasi ini juga menciptakan potensi celah keamanan yang kerap tidak terdeteksi. Pihak-pihak yang tidak bertanggung jawab memanfaatkan celah tersebut untuk keuntungan pribadi (Wibowo et al., 2023). Penting untuk diingat bahwa semua pengguna teknologi siber adalah bagian dari sebuah negara yang konkret, dengan identitas dan keberadaan di dalam wilayah suatu negara. Dengan demikian, setiap ancaman keamanan siber yang ditujukan kepada mereka, baik secara individu maupun bersama-sama, berpotensi memiliki efek langsung atau tidak langsung terhadap keamanan negara tersebut (Pratama, 2013).

Dari permasalahan yang sudah disebutkan di atas, maka dianggap penting bagi pemerintah untuk berkolaborasi dengan berbagai pihak dalam mengatasi masalah ini. Akademisi termasuk salah satu kelompok yang dapat diajak berkolaborasi dalam pembangunan sistem keamanan global. Hal ini dikarenakan suatu negara tidak akan mampu memberikan perlindungan secara simultan kepada semua elemen. Oleh karena itu, kolaborasi dan kerjasama dianggap krusial dalam upaya menanggulangi ancaman keamanan siber. Tujuan kegiatan pengabdian ini adalah untuk memberikan edukasi perihal pemahaman penggunaan teknologi dan diplomasi sebagai upaya mengatasi ancaman keamanan siber bagi mahasiswa hubungan internasional Universitas Tanjungpura.

METODE KEGIATAN

Kegiatan pengabdian ini dilaksanakan dengan tiga metode yakni pemberian edukasi materi mengenai diplomasi publik yang digunakan sebagai alat untuk meningkatkan citra positif dan upaya menghindari ancaman keamanan siber, tanya jawab, dan dokumentasi dan pelaporan (Maryuni *et al*., 2023). Metode pelaksanaan kegiatan ditulis dalam bentuk analisis kualitatif seperti penjelasan berikut ini:

a. Edukasi materi, tahapan ini merupakan tahap inti dari pelaksanaan pengabdian ini. Pada tahapan ini tim pengabdian memberikan edukasi mengenai dua hal secara umum yakni bagaimana memahami aktivitas diplomasi publik dan penggunaan media secara bijak dalam meningkatkan citra positif pengguna dan juga negara, kedua strategi menghindari ancaman keamanan siber dalam aktivitas penggunaan media sosial sehari-hari.
b. Tanya jawab, tahapan ini tim pengabdian menganalisis hal-hal yang belum diketahui mahasiswa media dalam aktivitas diplomasi publik yang bisa dimanfaatkan oleh masyarakat sipil dan juga negara. Setelah melakukan tanya jawab, tim pengabdian memberikan saran dan solusi mengenai kendala yang selama ini sering ditemui mahasiswa ketika bersinggungan dengan media dan internet dalam kehidupan sehari-hari.

c. Dokumentasi dan pelaporan, tahapan ini adalah tahapan akhir dari proses pengabdian kepada masyarakat. Setelah proses tanya jawab selesai, tim pengabdian melakukan dokumentasi dengan para narasumber dan mahasiswa untuk keperluan pelaporan.

HASIL DAN PEMBAHASAN

Kegiatan pengabdian kepada masyarakat ini bertujuan untuk memberikan edukasi dan pemahaman yang baik kepada mahasiswa Hubungan Internasional Universitas Tanjungpura perihal penggunaan internet dan media dengan bijak dalam aktivitas diplomasi di ranah publik. Hal ini mendukung tujuan kegiatan pengabdian yang kedua yakni untuk mencegah dan mengantisipasi terjadinya ancaman keamanan siber di kalangan mahasiswa. Pelaksanaan kegiatan ini dilakukan di Bulan Mei tahun 2023 yang dibagi menjadi tiga bagian yakni edukasi mengenai internet dan diplomasi di ranah publik, pencegahan ancaman keamanan siber di kalangan mahasiswa, dan ditutup dengan diskusi dan tanya jawab.

Gambar 1. Pembukaan Kegiatan Pengabdian Kepada Masyarakat

Edukasi Penggunaan Internet dengan Bijak dalam Praktek Diplomasi Publik

Pemateri pertama menjelaskan mengenai perkembangan diplomasi publik. Perkembangan aktivitas diplomasi publik dipengaruhi oleh adanya globalisasi yang kian hari kian masif dan menjadikan batas negara menjadi semakin kabur. Perkembangan kemajuan teknologi juga mendorong manusia di bumi untuk menjadi aktif menggunakan internet dalam memenuhi kebutuhan sehari-hari (Harahap & Harahap, 2023). Internet menjadi alasan berubahnya sifat diplomasi yang dilakukan oleh negara, dari formal menjadi tidak formal. Aktivitas diplomasi publik dalam hal ini menjadi penting karena melibatkan semua stakeholder di suatu negara untuk mempromosikan kepentingan negara (Jayanti *et al*., 2019). Memberikan pemahaman sikap, budaya, dan kepentingan nasional dalam proses komunikasi ke publik mancanegara. Salah satu cara yang paling efektif digunakan adalah dengan memanfaatkan internet.

Perkembangan pemahaman mengenai diplomasi publik juga berubah karena adanya sasaran dalam aktivitas diplomasi (Pujayanti, 2017). Mulai dari sasaran negara dengan negara, negara dengan publik, publik dengan negara, publik dengan publik yang semuanya menggunakan internet dan media sosial dalam prosesnya. Perspektif diplomasi publik yang mendasar yang perlu untuk dipahami adalah adanya koordinasi kebijakan di tingkat nasional mengenai kepentingan nasional apa yang ingin dicapai (Ramadhan & Sari, 2022). Hal tersebut dijelaskan dalam bentuk rasionalitas kebijakan yang diambil. Dilakukan dengan menampilkan pesan secara konsisten dan menghindari kontradiksi. Serta dilakukan dengan memperluas kerja sama dan membangun komitmen dengan menggunakan semua saluran komunikasi. Aktivitas diplomasi publik ini dapat dikatakan berhasil karena dipengaruhi oleh dua hal penting yakni adanya pertukaran informasi dan interaksi.

Dalam era globalisasi modern, internet telah menjadi kekuatan yang mempengaruhi hampir setiap aspek kehidupan manusia, termasuk diplomasi publik (Malik, 2017). Diplomasi publik adalah

upaya negara untuk mempengaruhi opini, sikap, dan tindakan negara lain melalui berbagai saluran komunikasi. Penggunaan internet dalam diplomasi publik telah memungkinkan negara-negara untuk berkomunikasi secara langsung dengan khalayak global, mengubah lanskap diplomasi secara substansial. Internet memungkinkan negara-negara untuk menyebarkan pesan mereka secara lebih luas dan efisien. Platform media sosial seperti Twitter, Facebook, dan Instagram memberikan forum bagi diplomat untuk berinteraksi dengan publik secara langsung, mengumumkan kebijakan, dan menjawab pertanyaan dengan cepat. Misalnya, seorang duta besar dapat menggunakan akun Twitter resminya untuk memberikan informasi tentang kegiatan diplomatik negaranya atau memberikan penjelasan tentang peristiwa internasional terkini.

Gambar 2. Edukasi oleh Pemateri Kegiatan Pengabdian Kepada Masyarakat

Internet juga dapat memfasilitasi dialog antara negara dan masyarakat sipil. Organisasi non-pemerintah (NGO), aktivis, dan warga biasa dapat dengan mudah mengakses informasi dan berpartisipasi dalam diskusi global tentang isu-isu politik, ekonomi, dan sosial. Ini menciptakan kesempatan bagi negara-negara untuk mendengarkan kekhawatiran dan aspirasi masyarakat internasional, serta untuk mempromosikan nilai-nilai dan kebijakan mereka. Internet memungkinkan diplomasi publik menjadi lebih inklusif dan terbuka. Melalui situs web resmi, blog, atau platform berbagi video seperti YouTube, negara-negara dapat menyediakan akses kepada masyarakat global untuk memahami kebijakan luar negeri mereka dan proses pengambilan keputusan. Transparansi semacam itu dapat meningkatkan legitimasi dan kepercayaan terhadap pemerintah, serta mengurangi ketegangan antara negara dan masyarakat internasional.

Sementara internet menawarkan banyak keuntungan dalam diplomasi publik, juga ada tantangan yang harus diatasi. Salah satunya adalah masalah kontrol informasi dan propagasi berita palsu (hoax). Dalam lingkungan online yang tidak teratur, pesan diplomatik dapat terdistorsi atau disalahartikan dengan cepat. Oleh karena itu, penting bagi negara-negara untuk mengembangkan strategi yang cerdas dalam mengelola citra mereka secara online dan untuk secara aktif melawan informasi yang salah. Secara keseluruhan, penggunaan internet dalam diplomasi publik telah membuka pintu baru bagi komunikasi internasional dan memperluas cakrawala partisipasi publik dalam proses diplomatik. Namun, untuk memanfaatkan sepenuhnya potensi internet dalam diplomasi, negara-negara perlu terus mengembangkan strategi komunikasi yang efektif dan responsif terhadap dinamika dunia digital yang terus berubah. Dengan demikian, internet tidak hanya menjadi alat untuk menghubungkan dunia secara digital, tetapi juga sebagai kekuatan yang membentuk diplomasi global di abad ke-21.

Edukasi Upaya Mengatasi Ancaman Keamanan Siber

Di era digital saat ini, keamanan siber menjadi isu penting yang mempengaruhi individu, perusahaan, dan negara di seluruh dunia. Ancaman keamanan siber, seperti malware, ransomware, phishing, dan serangan DDoS, terus berkembang menjadi lebih canggih, menuntut respons yang sama canggihnya untuk melindungi infrastruktur kritis dan data sensitif. Upaya mengatasi ancaman ini

membutuhkan pendekatan multifaset yang melibatkan teknologi, kebijakan, dan kesadaran individu. Salah satu langkah pertama dalam mengatasi ancaman keamanan siber adalah pengembangan dan penerapan teknologi keamanan yang canggih. Ini mencakup firewall, antivirus, anti-malware, dan solusi deteksi intrusi yang dapat memantau dan melindungi jaringan serta sistem dari serangan. Enkripsi data juga vital, memastikan bahwa data tetap aman bahkan jika diakses oleh pihak yang tidak berwenang. Salah satu jalan yang dapat diambil oleh mahasiswa adalah dengan tidak memberikan data pribadi kepada siapa pun untuk keperluan apa pun. Selain itu, penggunaan teknologi otentikasi dua faktor (2FA) dapat secara signifikan mengurangi risiko akses tidak sah ke akun dan sistem.

Pemateri kegiatan juga mengingatkan mahasiswa bahwa menggunakan kemajuan teknologi saja tidak cukup untuk melawan ancaman keamanan siber. Hal terpenting yang perlu diperhatikan adalah dengan melakukan edukasi dan meningkatkan kesadaran pengguna merupakan komponen krusial lainnya. Individu dan organisasi harus dilengkapi dengan pengetahuan tentang praktik keamanan siber terbaik, termasuk penggunaan kata sandi yang kuat, kehati-hatian terhadap email phishing, dan pentingnya pembaruan perangkat lunak reguler. Program pelatihan keamanan siber harus menjadi bagian rutin dari pelatihan karyawan, dan kampanye kesadaran publik dapat membantu masyarakat luas memahami risiko dan bagaimana melindungi diri mereka sendiri online.

Jika menilik isu ancaman keamanan siber, pada tingkat nasional dan internasional, kebijakan dan regulasi yang efektif sangat diperlukan untuk mendukung upaya keamanan siber. Hal ini dapat mencakup undang-undang yang mewajibkan perusahaan untuk melindungi data pribadi pengguna, standar keamanan untuk infrastruktur kritis, dan kerjasama lintas batas dalam mengejar pelaku kejahatan siber. Kebijakan juga harus mendorong pembagian informasi tentang ancaman siber antara sektor publik dan swasta, memungkinkan semua pihak untuk merespons ancaman baru dengan lebih cepat dan efektif. Mengingat sifat lintas batas dari banyak ancaman siber, kolaborasi internasional penting dalam mengatasi masalah ini. Negara-negara harus bekerja sama melalui forum multilateral, seperti Perserikatan Bangsa-Bangsa atau Interpol, untuk menyelaraskan upaya penegakan hukum, berbagi intelijen tentang ancaman, dan mengembangkan standar keamanan siber global. Kerjasama semacam itu juga dapat membantu mengatasi tantangan yurisdiksi yang sering menghambat penyelidikan dan penuntutan kejahatan siber.

Pemateri juga menyinggung perihal pesiapan dan respons insiden yang efektif adalah kunci untuk meminimalkan dampak serangan siber ketika terjadi. Ini mencakup memiliki rencana respons insiden yang terperinci, tim respons insiden siber yang terlatih, dan prosedur untuk pemulihan data dan sistem. Latihan simulasi serangan juga dapat membantu organisasi dalam mempersiapkan skenario nyata dan memastikan bahwa mereka dapat merespons dengan cepat dan efektif untuk meminimalkan kerusakan. Dengan menggabungkan teknologi keamanan yang canggih, pendidikan pengguna seperti edukasi mengenai kesadaran pengguna di tingkat mahasiswa, adanya kebijakan dan regulasi yang mendukung, kolaborasi internasional, dan kesiapan respons insiden, dunia dapat membuat langkah signifikan dalam mengatasi ancaman keamanan siber. Meskipun tantangan akan terus berkembang, pendekatan komprehensif ini memberikan dasar yang kuat untuk melindungi infrastruktur kritis dan data sensitif dari risiko yang terus meningkat di ruang siber.

Pada sesi tanya jawab, banyak mahasiswa belum mengetahui mengapa data pribadi dapat dicuri oleh orang lain. Hal ini menjadi tidak asing karena mahasiswa sering kali mengunggah postingan yang berbau data pribadi seperti melakukan upload halaman biodata di paspor, atau klaim hadiah yang mengharuskan mereka memberikan data seperti NIK dan biodata pribadi lainnya. Selain itu, semakin hari semakin banyaknya informasi yang beredar, sehingga terkadang mahasiswa mengalami kendala dalam menentukan mana informasi yang valid dan mana informasi yang tidak benar.

Gambar 3. Sesi Tanya Jawab dengan Peserta Kegiatan

KESIMPULAN DAN SARAN

Berdasarkan pelaksanaan kegiatan pengabdian di kalangan mahasiswa Hubungan Internasional dapat disimpulkan bahwa penggunaan internet menjadi hal yang tidak dapat dihindari dalam menjalankan aktivitas kehidupan mahasiswa. Termasuk untuk mempromosikan kepentingan negara di mata publik mancanegara. Akan tetapi, dalam proses penggunaannya perlu dihindari hal yang berhubungan dengan ancaman keamanan siber seperti pencurian data pribadi, malware, dan lain-lain. Setelah mengikuti kegiatan pengabdian, mahasiswa Hubungan Internasional menjadi lebih paham mengenai pentingnya menjaga data pribadi dan menjadi perlu adanya privasi terkait postingan yang diunggah di dunia maya. Langkah yang dapat dilakukan yakni dengan membuat kata sandi yang kuat, periksa pengaturan privasi, dan menggunakan jaringan wifi yang aman. Mahasiswa juga mengerti terkait perlunya kolaborasi invividu pada tingkat nasional dan internasional yang menggabungkan teknologi keamanan yang canggih didukung dengan adanya edukasi bagi para pengguna internet untuk menghindari ancaman keamanan siber.

UCAPAN TERIMAKASIH

Kami selaku tim pelaksana kegiatan pengabdian kepada masyarakat menyampaikan ucapan terima kasih yang sebesar-besarnya kepada Komahi Universitas Tanjungpura yang sudah berkenan menjadi panitia untuk melaksanakan kegiatan pengabdian kami. Ucapan terima kasih juga kami sampaikan kepada LPPM Universitas Tanjungpura yang sudah memfasilitasi tim pengabdian dalam menjalankan kegiatan pengabdian dari Fakultas Ilmu Sosial dan Ilmu Politik dan dapat berbagi dengan mahasiswa Program Studi Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Tanjungpura Pontianak.

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi). *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Amilin. (2019). Pengaruh Hoaks Politik dalam Era Post-Truth terhadap Ketahanan Nasional dan Dampaknya pada Kelangsungan Pembangunan Nasional. *Jurnal Kajian LEMHANNAS RI*, *39*, 5–12.

Arianto, B. (2021). Pandemi Covid-19 dan Transformasi Budaya Digital di Indonesia. *Titian: Jurnal Ilmu Humaniora*, *5*(2), 233–250. https://doi.org/10.22437/titian.v5i2.15309

Harahap, A. F. R., & Harahap, A. M. (2023). Peran Digitalisasi Dalam Meningkatkan Partisipasi Publik Pada Pengambilan Keputusan Tata Negara. *Jurnal EDUCATIO: Jurnal Pendidikan Indonesia*, *9*(2), 769–776. https://doi.org/10.29210/1202323208

Jayanti, A. D., Suwartiningsih, S., & Ismoyo, P. J. (2019). Diplomasi Publik Korea Selatan di Indonesia Melalui Sektor Pendidikan Korea International Cooperation Agency (Koica). *Kritis*, *28*(1), 11–28.

https://doi.org/10.24246/kritis.v28i1p11-28
Kristiyono, J. (2015). Budaya Internet: Perkembangan Teknologi Informasi dan Komunikasi Dalam Mendukung Penggunaan Media di Masyarakat. *Scriptura*, *5*(1), 23–30. https://doi.org/10.9744/scriptura.5.1.23-30
Kurniawan, R., Alhakim, A., Safero, B., Valeria, J., Angelina, S., Internasional Batam, U., Gajah Mada, J., -Sei Ladi, B., & Riau, K. (2021). Penggunaan Internet yang Sehat dan Aman di Kalangan Masyarakat dan Pelajar. *Jurnal ABDIMASA Pengabdian Masyarakat*, *4*(2), 15–21.
Luqman, L. (2021). Implikasi Diplomasi Pertahanan terhadap Keamanan Siber dalam Konteks Politik Keamanan. *Jurnal Diplomasi Pertahanan*, *6*(2). https://doi.org/10.33172/jdp.v6i2.654
Malik, D. D. (2017). Pendekatan Komunikasi Internasional. *Jurnal Common*, *1*(2). https://doi.org/10.34010/common.v1i2.574
Maryuni, S., Alunaza, H., Anistya S, W., Rusdiono, Pardi, Umniyah, A., & Cantika, S. (2023). Edukasi Proses Reintegrasi Bagi Korban Perdagangan Manusia di Kecamatan Sajingan Besar Kabupaten Sambas. *I-Com: Indonesian Community Journal*, *3*(1), 41–51. https://doi.org/10.33379/ICOM.V3I1.2136
Nurhaidah, & Musa, I. (2015). Dampak Pengaruh Globalisasi Bagi Kehidupan Bangsa Indonesia. *Jurnal Pesona Dasar*, *3*(3), 1–14. https://doi.org/10.24815/pear.v7i2.14753
Pratama, E. A. (2013). Optimalisasi Cyberlaw Untuk Penanganan Cybercrime Pada E-Commerce. *Jurnal Bianglala Informatika*, *I*(1), 1–10.
Pujayanti, A. (2017). Gastrodiplomasi-Upaya Memperkuat Diplomasi Indonesia. *Jurnal Politica*, *8*(1), 38–56.
Rahmawati, C. (2019). Tantangan dan Ancaman Keamanan Siber Indonesia di Era Revolusi Industri 4.0. *Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO AAU)*, *1*(1), 299–306.
Ramadhan, A. R., & Sari, V. P. (2022). Diplomasi Digital Jepang Terhadap Indonesia Melalui Akun Instagram @Jpnambsindonesia Pada Periode Duta Besar Masafumi Ishii Dalam Upaya Mengelola Citra Jepang. *Padjadjaran Journal of International Relations*, *4*(1), 36. https://doi.org/10.24198/padjir.v4i1.34700
Renaud, K., & Coles-Kemp, L. (2022). Accessible and Inclusive Cyber Security: A Nuanced and Complex Challenge. *SN Computer Science*, *3*(5), 1–14. https://doi.org/10.1007/s42979-022-01239-1
Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi Sebagai Bentuk Kejahatan Sempurna Dalam Perspektif Hukum Siber. *Sasi*, *27*(1), 38. https://doi.org/10.47268/sasi.v27i1.394
Soewardi, B. A. (2013). Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) Yang Tangguh Bagi Indonesia. *Potensi Pertahanan*, 31–35.
Sutra, S. M., & Haryanto, A. (2023). Upaya Peningkatan Keamanan Siber Indonesia oleh Badan Siber dan Sandi Negara (BSSN) tahun 2017-2020. *Global Political Studies Journal*, *7*, 56–69. https://doi.org/10.34010/gpsjournal.v7i1
Weu, M. R. (2020). Kerjasama Pemerintah Indonesia dan Pemerintah Kerajaan Inggris Dalam Bidang Keamanan Siber. *Global Political Studies Journal*, *4*(2), 154–169. https://doi.org/10.34010/gpsjournal.v4i2.5879
Wibowo, K., Hidayat, U., & Yasin, V. (2023). Kajian Cyber Security Dalam Rangka Koperasi Menghadapi Revolusi Industri 4.0. *JISAMAR*, *7*(3), 634–645. https://doi.org/10.52362/jisamar.v7i3.1132

