e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 11 No 3 Tahun 2024 Hal. : 891-897

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

UPAYA MENINGKATKAN PERTAHANAN NEGARA DARI ANCAMAN SIBER MELALUI STRATEGI PENGEMBANGAN SENJATA SIBER DI INDONESIA

Yaser Muhammad Hatim, Priyanto, Ahmad G. Dohamid, Suhirwan

Prodi Peperangan Asimetris, Fakultas Strategi Pertahanan,

Universitas Pertahanan Republik Indonesia

Abstrak

Dalam era kehidupan modern yang dipenuhi teknologi komunikasi, akses dan pertukaran informasi di masyarakat semakin mudah. Namun, kemudahan tersebut juga membawa dampak negatif, seperti peluang untuk tindakan anti sosial dan kejahatan siber yang semakin kompleks seiring peningkatan intelektual masyarakat, keamanan internetpun menjadi sangat penting. Di Indonesia, kekhawatiran terhadap kejahatan siber meningkat. Meskipun telah berlakunya Undang-Undang ITE kasus kejahatan dunia maya masih terus meningkat setiap tahun, menunjukkan perlunya kewaspadaan masyarakat dalam menghadapi perkembangan teknologi. Studi ini menyoroti kasus pembobolan internet banking pada tahun 2001 dan mendiskusikan urgensi keamanan siber di tengah sisi gelap internet. Penelitian ini fokus pada upaya meningkatkan pertahanan negara dari ancaman siber melalui strategi pengembangan senjata siber di Indonesia. Dengan pendekatan deskriptif kualitatif, penelitian ini mengeksplorasi literatur dengan kata kunci Cybercrime, Pertahanan Negara, dan Senjata. Temuan penelitian menunjukkan bahwa penggunaan framework DFEL dapat meningkatkan akurasi dan mengurangi waktu deteksi serangan siber. Peran Satsiber TNI dan Cyber Police POLRI menjadi krusial dalam upaya pencegahan dan penanganan kejahatan siber, dengan pembentukan satuan khusus sebagai langkah proaktif. Kesimpulannya, keamanan dan ketahanan siber memerlukan kerjasama antara sipil dan militer, dengan pengembangan senjata siber sebagai langkah strategis untuk menghadapi ancaman siber di Indonesia.

Kata Kunci: Kejahatan Siber, Pertahanan Negara, Senjata.

*Correspondence Address : yaser.hatim@sp.idu.ac.id
DOI : 10.31604/jips.v11i3.2024. 891-897

PENDAHULUAN

Kehidupan modern yang didukung oleh teknologi komunikasi memberikan kemudahan bagi masyarakat untuk menyerap dan berbagi berbagai informasi kepada individu maupun masyarakat (Rosmaladewi & Abduh, 2019). Dalam perkembangannya, penggunaan internet membawa banyak sisi negatif (Arianto & Anggraini, 2019). Hal ini meningkatkan peluang terjadinya tindakan anti sosial dan perilaku kriminal yang selama ini dianggap tidak mungkin terjadi. Seperti yang dikatakan sebuah teori, kejahatan adalah produk masyarakat itu sendiri. Artinya masyarakat itu sendiri yang menciptakan kejahatan. Semakin tinggi tingkat intelektual masyarakat, maka kejahatan yang lebih canggih juga dapat terjadi di masyarakat (Alghamdi, I, 2020). Di Internet, masalah keamanan sangat diperlukan. Sebab tanpa pengamanan, data pada sistem yang ada di internet dapat dicuri oleh orang yang tidak bertanggung jawab. Seringkali suatu sistem jaringan berbasis internet memiliki kelemahan atau sering disebut lubang keamanan. Jika lubang tidak ditutup, pencuri bisa masuk dari lubang tersebut. Pencurian data dan sistem dari Internet, termasuk dalam kasus kejahatan komputer. Cybercrime merupakan kejahatan yang sering dilakukan di Internet (Sarre dkk., 2018).

Di Indonesia masalah *cybercrime* telah menjadi perhatian baik masyarakat maupun pemerintah, sebelumnya belum ada peraturan UU ITE yang secara khusus mengatur tentang cybercrime, sebelumnya masalah cybercrime ditindaklanjuti dengan undang-undang yang berkaitan dengan masalah tersebut. Namun saat ini kasus cybercrime diatur dalam UU ITE (Saleh, 2022). Kasus cybercrime diatur dalam Undang-Undang ITE Nomor 8 Tahun 2011 dan selanjutnya dihadapkan pada perubahan Undang-Undang Nomor 19 Tahun 2016, khususnya pada pasal 27-30 terkait dengan perilaku yang tidak dianjurkan untuk dilakukan di dunia maya (Arwana, 2022). Kejahatan di dunia maya tidak dapat dihindari meskipun telah dibuat undang-undang yang mengaturnya, namun setiap tahun kasus kejahatan dunia maya di Indonesia semakin meningkat. Masyarakat diharapkan lebih bijak dalam menyikapi perkembangan teknologi yang ada, masyarakat diharapkan lebih berhati-hati dalam memberikan informasi pribadi. Karena perkembangan teknologi informasi tidak hanya memberikan pengaruh positif tetapi juga negative (Rahmat dkk., 2022).

Salah satu kasus cybercrime yang pernah terjadi di Indonesia adalah kasus pembobolan internet banking milik Bank Central Asia ditahun 2001 yang dilakukan oleh Steven Haryanto. Menarik untuk disimak, ketika pelaku salah ketik clickbca.com Steven Haryanto berhasil melakukan aksinya dengan mencatat 130 user ID dan Personal Identification Number milik Nasabah Bank Central Asia, hanya meminta maaf kepada Bank BCA karena dianggap tidak melakukan tindakan kriminal dan hanya dibuat atas dasar menguji tingkat keamanan sistus tersebut (Mashdurohatun dkk, 2017). Urgensi keamanan siber semakin mendesak karena internet memiliki sisi gelap tertentu (Rizal & Yani, 2016). Sehingga diperlukan Kerjasama dari beberapa pihak terkait khususnya POLRI sebagai pihak yang memiliki tugas memberi keamanan dan ketentraman dalam menyelesaikan permasalahan ini. Berdasarkan permasalahan yang telah diuraikan, dalam menghadapi maraknya cybercrime, diperlukan profesionalisme yang tinggi dari aparat kepolisian. Hal ini dapat diwujudkan dengan terus meningkatkan kualitas sumber daya POLRI baik secara kuantitas maupun kualitas (Maltha dkk., 2019).

Cyberspace seperti yang dikenal di Indonesia, merupakan wilayah operasional yang menciptakan,

menyimpan, mengubah, dan bertukar informasi dengan menggunakan listrik atau elektromagnetisme (Achmadi dkk., 2020). Sebelumnya, kontrol regional menjadi fokus utama; Namun di era teknologi yang semakin maju ini, pengendaliannya lebih bersifat virtual, yaitu penguasaan dan pengelolaan dunia maya yang tersimpan dalam big data. Gudang senjata dunia maya dibangun dengan mengeksploitasi kelemahan pertahanan target. Indonesia saat ini masih dalam tahap pengembangan dan penguatan, belum mengarah pada pengembangan senjata siber yang mampu melakukan serangan balik saat perang siber (Anjani, 2021). Data penelitian yang menunjukkan bahwa tren serangan siber global semakin meningkat seiring dengan meningkatnya jumlah pengguna internet. Untuk memperkuat pertahanan siber, Indonesia perlu mempertimbangkan pengembangan senjata siber (Rizal & Yani, 2016). Sehingga dalam penelitian ini, penulis akan melakukan kajian terkait upaya meningkatkan pertahanan negara dari ancaman siber melalui strategi pengembangan senjata siber di Indonesia.

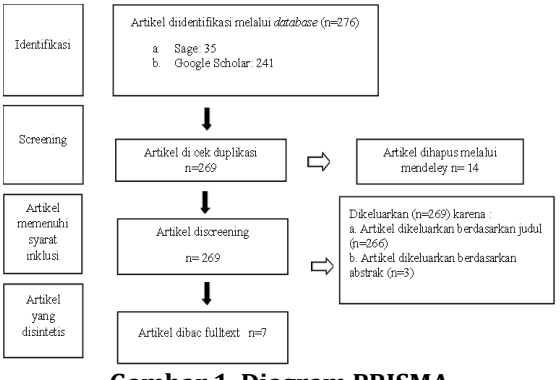
METODE PENELITIAN

Penelitian ini mengadopsi pendekatan deskriptif kualitatif. Pendekatan deskriptif kualitatif ini mengharuskan pengumpulan data yang bersifat deskriptif dan berasal dari konteks alami atau realitas dalam masyarakat. Tinjauan pustaka dalam penelitian ini dilalui dengan penyeleksian secara sistematis yang ditelusuri dari database internasional. Penulis melakukan pencarian sumber data dari berbagai database antara lain menggunakan Sage Journal (https://www. https://journals.sagepub.com//), dan Google Scholar. Metode pencarian literatur melibatkan penggunaan kata kunci yang relevan dengan pertanyaan penelitian. Daftar kata kunci yang menjadi dasar dalam pencarian literatur mencakup *Cybercrime*, Pertahanan Negara, dan Senjata. Artikel dicari dalam Bahasa Inggris, dengan rentang tahun publikasi terbatas pada 5 tahun terakhir (2018-2023). Penelitian ini akan mendeskripsikan serta menjelaskan mengenai bagaimana kajian literatur dari upaya meningkatkan pertahanan negara dari ancaman siber melalui strategi pengembangan senjata siber di Indonesia.

HASIL DAN PEMBAHASAN

Diagram (PRISMA)

Gambar 1. Menunjukkan langkah-langkah seleksi artikel dengan mengikuti petunjuk dari *Preferred Reporting Systematic Reviews and Meta-analysis* (PRISMA). Pada pencarian awal, ditemukan 276 artikel yang diterbitkan antara tahun 2018-2023. Selanjutnya, dilakukan proses penyaringan artikel, di mana hanya 7 artikel yang memenuhi kriteria yang dipilih untuk tahap berikutnya. Artikel tersebut kemudian dievaluasi kualitasnya, sehingga akhirnya terdapat 7 artikel yang disintesis dan disertakan dalam laporan penelitian dari tinjauan pustaka.



Gambar 1. Diagram PRISMA

Peneliti melakukan seleksi terhadap artikel yang didapatkan dan melakukan ekstraksi data pada masing-masing artikel yang didapatkan dari tiap

database. Hasil artikel di*review* terkait kajian dari pentingnya upaya meningkatkan pertahanan negara dari ancaman siber melalui strategi pengembangan senjata siber di Indonesia**.**

Strategi Pengembangan Senjata Siber di Indonesia guna Meningkatkan Pertahanan Negara dari Ancaman Siber

Keamanan siber dapat didefinisikan sebagai serangkaian kegiatan dan tindakan yang ditujukan untuk mencegah serangan, penyusupan, atau ancaman lain melalui elemen dunia maya. Banyak literatur terkait deteksi serangan siber dijelaskan bahwa dengan percepatan pertumbuhan aplikasi internet of things atau IoT dalam beberapa tahun terakhir (Wardana dkk., 2022). Terakhir, kota menjadi lebih pintar untuk mengoptimalkan sumber daya dan meningkatkan kualitas hidup masyarakat. Di sisi lain, IoT menghadapi masalah keamanan yang parah seperti kerahasiaan, integritas, privasi, dan ketersediaan (Dévai, 2016). Untuk mencegah kerusakan permanen dari serangan dunia maya, peneliti mengusulkan kerangka kerja, yang disebut DFEL, untuk mendeteksi intrusi internet di lingkungan IoT. Melalui hasil eksperimen, para peneliti menemukan bahwa DFEL tidak hanya meningkatkan akurasi pengklasifikasi untuk memprediksi serangan siber, tetapi juga secara signifikan mengurangi waktu deteksi (Wardana dkk., 2022).

Dalam beberapa dekade setelah terciptanya Internet, dunia maya telah menjadi area konflik karena negara-negara meningkatkan kemampuan dunia maya mereka dengan menciptakan gudang senjata dunia maya yang canggih; menambahkan personel khusus dan struktur kekuatan, dan terlibat dalam dan mencari penelitian mutakhir dan pengembangan sumber daya kemampuan ofensif dan defensive (Lewis & Timlin, 2008). Senjata yaitu suatu alat yang mengancam atau menyebabkan kerusakan fisik, fungsional, atau mental terhadap struktur, sistem, atau organisme Akibatnya, jaringan dapat didefinisikan sebagai senjata internet jika model komputer ditujukan untuk menghancurkan integritas atau aksesibilitas data di TI musuh (Setiawan, 2018). Sistem ini terutama digunakan untuk peralatan pertahanan. Dengan demikian, senjata dunia maya adalah kode komputer atau perusakan fisik, operasi atau kerusakan pada struktur atau sistem infrastruktur penting yang digunakan atau dirancang untuk tujuan yang mengancam (Alghamdi, I, 2020).

Dalam dunia militer, keberadaan tentara siber sudah menjadi hal yang tidak terelakkan, karena Amerika Serikat, Korea Utara, China, Singapura, Australia, dll sudah memiliki tentara siber. pada Oktober 2017, TNI membentuk satuan jaringan atau satsiber dengan tujuan melindungi sumber daya informasi di lingkungan TNI dari gangguan dan penyalahgunaan atau eksploitasi oleh pihak lain. Dalam beberapa kasus, investasi yang diperlukan untuk mengembangkan dan menerapkan kemampuan siber mungkin kurang dari kemampuan kinetik. Jika efek dari sistem senjata *cyber* menguntungkan militer dengan cara apa pun, pengembalian investasi bisa jauh lebih tinggi daripada opsi lainnya (Arianto & Anggraini, 2019). TNI di bawah Kementerian Pertahanan telah membentuk Satuan Siber (Satsiber) untuk melakukan kegiatan dan operasi pertahanan siber. Satsiber eksisting merupakan organisasi satgas yang bertugas melaksanakan kegiatan dan operasi siber di lingkungan TNI AD dalam rangka mendukung tugas pokok TNI AD. Satsiber yang ada telah menjadi satuan kerja yang memiliki fungsi sebagai pengawasan dan pertahanan

dalam menghadapi *Cyberattacks* dan kejahatan serta memberikan tanggapan cepat dan melaporkan kepada pimpinan TNI AD dengan tujuan melindungi institusi TNI AD dari potensi ancaman kejahatan dan *Cyberattacks*. Ada empat fungsi yang dimiliki oleh Satsiber TNI yaitu Deteksi, Proteksi, Recover dan Memastikan Existing (Wardana dkk., 2022).

Tidak hanya dalam lingkup TNI saja, dalam lingkup POLRI pengamanan siber juga dilakukan. Salah satu langkahnya adalah dengan membentuk *Cyber Police*, yang dimulai dengan mengeluarkan surat edaran dari Kepala Kepolisian Republik Indonesia (KaPOLRI), nomor SE/2/11/2021, yang membahas Kesadaran Budaya Etis untuk Mewujudkan Ruang Digital Indonesia yang Bersih, Sehat, dan Produktif. Surat edaran tersebut adalah keputusan untuk merespons permintaan Presiden agar Kepolisian Republik Indonesia lebih berhati-hati dalam menangani kasus-kasus yang diduga melanggar Undang-Undang Nomor 11 Tahun 2008 yang telah diubah oleh Undang-Undang Nomor 19 Tahun 2016. Cyber Police melakukan kegiatan Cyber Patrol dengan memantau setiap kegiatan di dunia maya terutama melalui media sosial dan berbagai platform lainnya (Rais & Songkarn, 2022).

Sebagai institusi yang bertugas sebagai penghubung dalam hal tersebut, polisi juga tidak kenal lelah dalam bekerja dan berinovasi menghadapi setiap peristiwa dan kejadian di tengah masyarakat. Keberadaan *Cyber Police* diharapkan dapat menciptakan suasana nyaman bagi pengguna media sosial dan berbagai platform lainnya. Sementara itu, POLRI secara berkesinambungan memantau dan melatih anggotanya agar dapat bersikap preventif dalam penanganan kasus-kasus yang terjadi di dunia maya (Pratama & Bamatraf, 2021).

Dengan ini, bisa diungkapkan bahwa tugas *Cyber Police* tidak hanya terbatas pada penanganan pengaduan atau laporan dari masyarakat, melainkan juga melibatkan upaya pencegahan melalui kegiatan sosialisasi dan hubungan publik cyber guna memastikan bahwa masyarakat mendapat informasi yang akurat dan untuk mencegah penyebaran hoaks. Semoga ini terus berkembang dan memberikan manfaat yang lebih besar bagi masyarakat secara umum (Maltha dkk., 2019).

Untuk memastikan bahwa manfaat potensial dari sistem senjata siber presisi terwujud dan masalah yang diangkat oleh pencela diminimalkan, beberapa langkah harus diambil untuk menciptakan kemampuan yang efektif. Pertama, militer profesional akan membentuk korps khusus operator siber. Operator ini tidak boleh "bertopi ganda" yaitu, mereka tidak boleh memiliki tanggung jawab terkait teknologi tetapi berpotensi bertentangan dalam intelijen atau komunikasi (Sarre dkk., 2018). Personil harus didedikasikan untuk misi operasi dunia maya dan menerima pelatihan yang sesuai dalam melakukan operasi tempur untuk memastikan integrasi yang efektif dengan sistem senjata militer konvensional. Operator dunia maya harus dilatih dalam Undang-Undang konflik bersenjata untuk mengurangi kemungkinan melakukan operasi yang melanggar undang-undang tersebut, karena operator akan dimintai pertanggungjawaban atas tindakan mereka dengan cara yang sama (Wardana dkk., 2022).

SIMPULAN

Keamanan dan ketahanan siber menjadi aspek pemerintahan yang penting untuk dipromosikan dan diperkuat guna mendukung pertumbuhan ekonomi nasional serta

mencapai ketahanan nasional. Pembangunan ketahanan dan keamanan siber yang handal tidak dapat terlepas dari partisipasi serta kolaborasi militer, dengan mengoptimalkan semua komponen masyarakat yang terlibat dalam kerjasama sipil-militer. Penguatan hukum siber di Indonesia sangat penting, untuk memperjuangkan pertahanan negara. Oleh karena itu, menjadi tanggung jawab bersama antara pemerintah, aparat penegak hukum, TNI, POLRI serta seluruh elemen masyarakat untuk memerangi gejolak *cybercrime*. Upaya yang bisa dilakukan adalah melalui pengembangan sistem senjata siber yang presisi dalam pertempuran untuk mengurangi risiko bahaya bagi operator siber yang menggunakan kemampuan, risiko terhadap kombatan musuh, dan risiko bagi warga sipil. Faktor penting yang perlu diperhatikan dalam pengembangan senjata siber adalah faktor Sumber Daya Manusia (SDM) Indonesia yang handal, khususnya di bidang IT. Oleh karena itu, diperlukan dukungan dan kerja sama dari organisasi pertahanan siber Indonesia yang memiliki keahlian di bidang peretasan.

DAFTAR PUSTAKA

Achmadi, B., Zauhar, S., & Bambang, S. H. (2020). The Implementation of the Defense Industrial Base (DIB) a Comparative Study of Indonesia and Brazil. Wacana, 22(2), 141–152.

Alghamdi, I, M. (2020). A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide. International Journal of Engineering Research Technology, 09(06), 1321–1330. https://www.ijert.org/research/a-descriptive-study-on-the-impact-of-cybercrime- and-possible-measures-to-curtail-its-spread-worldwide-IJERTV9IS060565.pdf

Anjani, N. H. (2021). Cybersecurity Protection in Indonesia. Center for Indonesian Policy Studies, 9, 1–12.

Arianto, A. R., & Anggraini, G. (2019). Building Indonesia'S National Cyber Defense and Security To Face the Global Cyber Threats Through Indonesia Security Incident Response Team on Internet Infrastructure (Id-Sirtii). Jurnal Pertahanan & Bela Negara, 9(1), 17. https://doi.org/10.33172/jpbh.v9i1.515

Arwana, Y. C. (2022). Victims of Cyber Crimes in Indonesia : A Criminology and Victimology Perspective. Semarang State University Undergraduate Law & Society Review, May, 181–200. https://doi.org/10.15294/lsr.v2i2.53754

Dévai, D. (2016). Proliferation of Offensive Cyber Weapons : Strategic Implications and Non-Proliferation Assumptions. Academic and Applied Research in Military and Public Management Science, 15(1), 61–73. https://doi.org/10.32565/aarms.2016.1.6

Lewis, J. A., & Timlin, K. (2008). Cybersecurity and Cyberwafare. Ideas for Peace and Security, 55, 1–36.

Maltha, H. S., Suradinata, E., Djaenuri, M. A., & Lukman, S. (2019). Mitigating Strategy of Cyber Crime for Indonesian National Police. International Journal of Recent Technology and Engineering, 8(3S2), 472–475. https://doi.org/10.35940/ijrte.c1105.1083s219

Manihuruk, H., & Tarina, D. D. Y. (2020). State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News. International Journal of Multicultural and Multireligious Understanding, 7(5), 27–36. http://ijmmu.com/index.php/ijmmu/article/view/1590

Mashdurohatun, A., Sidji, R., Gunarto, & Mahmutarom. (2017). Factors causing banking cyber crime in Indonesian. International Journal of Economic Research, 14(15), 293–311.

Pratama, B., & Bamatraf, M. (2021). Tallinn manual: Cyber warfare in Indonesian regulation. IOP Conference Series: Earth and Environmental Science, 729(1). https://doi.org/10.1088/1755-1315/729/1/012033

Putra, B. A. (2022). Cyber Cooperation between Indonesia and the United States in Addressing the Threat of Cyberterrorism in Indonesia. International Journal of Multicultural and Multireligious Understanding, 22–33. https://doi.org/dx.doi.org/10.18415/ijmmu.v9i10.4058

Rahmat, A. F., Mutiarin, D., Pribadi, U., & Rahmawati, E. (2022). Overseeing Cyber-Neighborhoods: How Far the Indonesian National Police Effort in Handling Cybercrime? International Conference on Public Organization, 209(Iconpo 2021), 549–555.

Rai, I. N. A. S., Heryadi, D., & Kamaluddin N., A. (2022). The Role of Indonesia to Create Security and Resilience in Cyber Spaces [Peran Indonesia dalam Membentuk Keamanan dan Ketahanan di Ruang Siber]. Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional, 13(1), 43–66. https://doi.org/10.22212/jp.v13i1.2641

Rais, M. A., & Songkarn, P. (2022). Hacker and the Treat for National Security: Challenges in Law Enforcement. Indonesian Journal of Counter Terrorism and National Security, 1(1), 45–66. https://doi.org/10.15294/ijctns.v1i1.56728

Rizal, M., & Yani, Y. (2016). Cybersecurity Policy and Its Implementation in Indonesia. JAS (Journal of ASEAN Studies), 4(1), 61. https://doi.org/10.21512/jas.v4i1.967

Rosmaladewi, R., & Abduh, A. (2019). the Impact of Information Technology on Efl Teaching in Indonesia. ELT Worldwide: Journal of English Language Teaching, 6(1), 21. https://doi.org/10.26858/eltww.v6i1.9802

Saleh, G. S. (2022). Juridical Analysis of the Crime of Online Store Fraud in Indonesia. Jurnal Hukum Dan Peradilan, 11(1), 151. https://doi.org/10.25216/jhp.11.1.2022.151-175

Sarre, R., Lau, L. Y. C., & Chang, L. Y. C. (2018). Responding to cybercrime: current trends. Police Practice and Research, 19(6), 515–518. https://doi.org/10.1080/15614263.2018.1507888

Setiawan, R. (2018). Indonesia Cyber Security : Urgency To Establish Cyber Army In The Middle Of Global Terrorist Threat. Journal of Islamic World and Politics, 2(1). https://doi.org/10.18196/jiwp.2109

Taufik, A. F. (2021). Indonesia's cyber diplomacy strategy as a deterrence means to face the threat in the indo-pacific region. Journal of Physics: Conference Series, 1721(1). https://doi.org/10.1088/1742-6596/1721/1/012048

Wardana, A., Gunaryo, G., & Yogaswara, Y. H. (2022). Development of Cyber Weapons to Improve Indonesia's Cyber Security. Journal of Sosial Science, 3(3), 453–459. https://doi.org/10.46799/jss.v3i3.334

Wiramanggala, R., Khaerudin, K., & Sudiarso, A. (2021). Indonesian Defense Industry Development Strategy as Responses of Cyber Threat to Support State Defense. International Journal of Social Science Research and Review, 4(5), 18–25. https://doi.org/10.47814/ijssrr.v4i5.140