Jurnal Kewarganegaraan
Vol. 6 No. 2 September 2022
P-ISSN: 1978-0184 E-ISSN: 2723-2328

Analisis Potensi Ancaman Asimetris Berdasarkan Kerentanan Keamanan Siber Sektor Industri Energi Baru Terbarukan (EBT)

Joko Yulianto[1] Suyono Thamrin[2] Yusuf Ali[3] Abdi Manab Idris[4]
Program Studi Ketahanan Energi, Fakultas Manajemen Pertahanan, Universitas Pertahanan Republik Indonesia, Indonesia[1,2,3,4]
Email: jokoyulianto429@gmail.com[1]

Abstrak

Awal Dekade ini merupakan tonggak awal transisi dari masa industri 4.0 menjadi Society 5.0. Perubahan era ini menyebabkan seluruh lapisan masyarakat harus dapat menyesuaikan diri dengan perkembangan teknologi. Dalam Society 5.0 dimana komponen utamanya adalah manusia yang mampu menciptakan nilai baru melalui perkembangan teknologi dapat meminimalisir adanya kesenjangan pada manusia dan masalah ekonomi dikemudian hari. akan tetapi dengan berkembangnya teknologi menyebabkan dampak pada Perkembangan konflik dan peperangan yang saat ini telah masuk ke babak baru. Ancaman yang dapat timbul beragam, tidak terlihat secara real dan tidak menentu. Ancaman tersebut adalah ancaman siber yang berpotensi menyebabkan kerugian besar bagi suatu negara. Salah satu dampak besar yang dapat terjadi di masa depan adalah serangan siber terhadap objek vital nasional atau infrastruktur kritis negara seperti pembangkit listrik. Pembangkit listrik energi terbarukan memanfaatkan teknologi tinggi yang terhubung ke jaringan distribusi besar yang menyebabkan jika tidak memperkuat pengamanan jaringan maka dapat menimbulkan black out listrik hingga pemadaman secara keseluruhan yang disebabkan oleh pihak yang tidak bertanggung jawab/non-state actors. Oleh sebab itu semua negara harus dapat mempersiapkan pembinaan, membentuk satuan baru dan memperkuat masing-masing pertahanan negara mereka.
Kata Kunci: Keamanan Siber, Ancaman Siber, Sektor Energi Terbarukan, Peperangan Asimetris

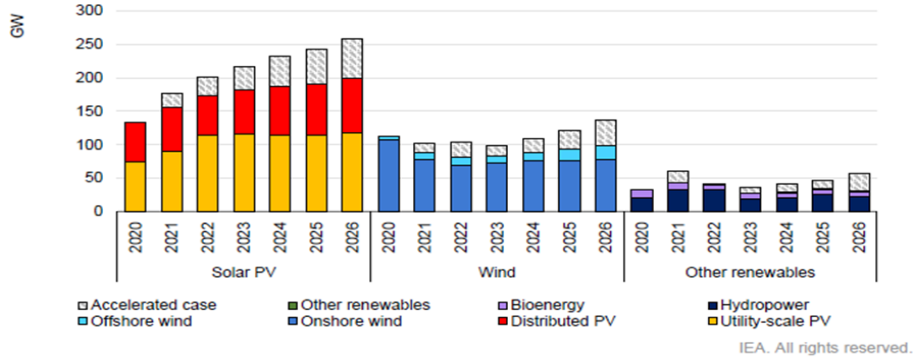
Abstract

The beginning of this decade was the initial milestone of the transition from the industrial period 4.0 to Society 5.0. The changes in this era have caused all walks of life to be able to adjust to technological developments. In Society 5.0 where the main component is humans who are able to create new value through technological developments, it can minimize gaps in humans and economic problems in the future. however, with the development of technology, it has an impact on the development of conflicts and wars that have now entered a new chapter. The threats that can arise are diverse, invisible in real terms and erratic. Such threats are cyber threats that have the potential to cause huge losses to a country. One of the major impacts that could occur in the future is cyberattacks against national vital objects or critical infrastructure of the country such as power plants. Renewable energy power plants utilize high technology connected to large distribution networks which causes if it does not strengthen network security, it can cause power blackouts to overall outages caused by irresponsible parties / non-state actors. Therefore, all countries must be able to prepare for development, form new units and strengthen each of their country's defenses.
Keywords: *Cybersecurity, Cyber Threats, Renewable Energy Sector, Asymmetric Warfare*

PENDAHULUAN

Perkembangan teknologi selama dekade terakhir memaksa dunia untuk mengembangkan energi terbarukan. Menurut *International Energy Association* (IEA) Energi terbarukan telah mengalami pertumbuhan yang belum pernah terjadi sebelumnya di Eropa [1]. Hal ini didukung oleh kondisi *net zero emission* setiap negara harus tercapai baik itu lambat maupun cepat [2]. Peningkatan pembangunan Energi Terbarukan harus terstandarisasi dan menerapkan semua

ISO, aturan SOP dan keamanan sesuai dari Industri yang memproduksi maupun kesepakatan dan kebijakan internasional terkait EBT [3]. Menurut IEA (2020) Perkembangan EBT di eropa ditunjukan pada gambar 1 [4]



Gambar 1. Perkembangan Energi Baru Terbarukan secara global [4]

Industri energi terbarukan menjadi penting karena negara-negara berusaha untuk menjauh dari bahan bakar fosil, tetapi pertumbuhan yang berkelanjutan dari sektor ini harus dikelola dengan mempertimbangkan keamanan siber karena telah diindikasi bahaya kerentanan dalam segala hal mulai dari pembangkit listrik hingga smart meter yang dapat hilang atau di manipulasi, hal ini akan menyebabkan gangguan pada grid/microgrid dari Energi Terbarukan [5-8]. Penyedia energi, pelanggan dan pengambil kebijakan serta pemerintah harus terbuka terhadap risiko ancaman siber [9]. Ancaman siber bersifat asimetris atau tidak langsung yang berpotensi mengancam keamanan data, informasi dan merugikan keuangan negara. Ancaman siber di tanggulangi di klasifikasikan menjadi operasi militer selain perang.

Operasi Militer Selain Perang bertujuan untuk membantu kementrian/lembaga dan polri dalam mengatasi ancaman yang dapat merugikan dan berdampak pada keamanan dan kedaulatan negara. Oleh sebab itu dibutuhkan postur pertahanan yang ideal agar dapat menangkal dan memitigasi ancaman siber terhadap infrastruktur negara khsusnya objek vital nasional seperti energi baru terbarukan dan sistem *smart grid* yang beroprasi.

Industri energi terbarukan sudah menjadi target utama para peretas, termasuk mereka yang ingin menyebarkan kampanye spionase, ransomware, dan bahkan serangan dengan tujuan menyabot sistem untuk memutus aliran listrik [10]. Usaha setiap negara yang melakukan transisi secara cepat dari energi konvensional menuju energi terbarukan mengarah ke babak baru di dunia siber dan *Internet of Things* (IoT) menghasilkan penjahat *non-state actor* yang siap mengeksploitasi sistem energi terbarukan [11].

Ancaman serangan siber pada objek vital energi terbarukan pertama kali dirasakan oleh proyek energi terbarukan di Amerika Serikat. Perusahaan tersebut bernama sPower, Instansi tersebut pemilik pembangkit listrik yang memanfaatkan tenaga surya dan angin mengalami serangkaian koneksi yang terputus antara pusat kendali utamanya dan lokasi pembangkit listrik jarak jauh [12]. Periode waktu henti yang singkat dan terputus-putus disinyalir disebabkan oleh serangan *Distributed Denial of Service* (DDoS) [13]. Hal serupa tersebut juga terjadi pada jaringan listrik di Ukraina tahun 2015/2016, peretas menggunakan kendali jarak jauh terhadap SCADA dan infrastruktur gardu induk. Meskipun kali ini serangannya bukan pada infrastruktur energi terbarukan melainkan energi konvensional namun serangan itu mengeksploitasi kerentanan dalam sistem yang serupa [14].

Keamanan siber menjadi penting berdasarkan Undang-undang privasi seperti GDPR (*General Data Protection Regulation*) dan DPA (*Data Protection Act*) 2018 dapat berarti denda

yang signifikan bagi instansi yang mengalami pelanggaran keamanan siber [15]. Selanjutnya Mempertimbangkan serangan dunia siber semakin canggih dengan *state non-actor* menggunakan berbagai taktik yang terus berkembang. Ini termasuk rekayasa sosial, malware dan ransomware. Keamanan siber yang baik akan menjamin data penting nasional tetap aman. Menurut *The Hidden Costs of Cybercrime*, sebuah studi yang dilakukan oleh McAfee dan CSIS (Pusat Studi Strategis dan Internasional), berdasarkan data yang dikumpulkan oleh Vanson Bourne, ekonomi dunia kehilangan lebih dari $1 triliun (sekitar £750 miliar) akibat dari ancaman siber [16].

Oleh karena itu perlu adanya solusi untuk mengamankan objek vital nasional Energi Baru Terbarukan (EBT) mulai dari identifikasi peningkatan ancaman serangan siber, penanganan dini, dan kebijakan yang mendukung pengamanan siber masa depan. Paper ini akan mengidentifikasi mengapa keamanan siber untuk aset energi terbarukan sangat rawan atas ancaman siber hingga baru-baru ini, potensi bahaya dan ancaman yang dapat menyebabkan ancaman objek vital nasional beserta solusi berupa postur pertahanan yang ideal untuk menangkal ancaman asimetris seperti serangan teknologi siber pada objek vital nasional bidang energi baru terbarukan.

METODE PENELITIAN

Metode Penelitian yang digunakan adalah Metode kualitatif dengan pendekatan studi literatur (kepustakaan) [32]. Studi kepustakaan berarti memanfaatkan bahan bacaan sebagai objek utama data [33], penelitian ini akan menghasilkan informasi berupa catatan dan data deskriptif yang terdapat di dalam teks yang diteliti secara eksploratif [34], Teknik Pengumpulan data dengan memanfaatkan berbagai sumber informasi yang dapat di validasi dan kepercayaan informasi tersebut dapat terukur (Studi Literatur). Pencarian terbatas dilakukan dengan menggunakan istilah "Peperangan Asimetris", "Keamanan Siber", "Industri Energi Baru Terbarukan", "Ancaman Siber", dan "Postur Sistem Pertahanan". Pencarian terbatas terkait tema dalam bahasa Inggris dan Indonesia dengan rentang tahun 2001 dan 2022, Hasil pencarian yang digunakan mulai dari artikel ilmiah, laporan hasil penelitian, ulasan, anekdot, prosiding, berita valid dan potongan opini oleh pihak berwenang dengan latar belakang keilmuan yang sangat baik [35-36].

HASIL PENELITIAN DAN PEMBAHASAN

Hasil Penelitian

Analisis Ancaman Siber

Keamanan siber adalah penerapan teknologi, proses, dan kontrol untuk melindungi sistem, jaringan, program, perangkat, dan data dari serangan siber. Keamanan siber bertujuan untuk mengurangi risiko serangan dunia maya dan melindungi objek vital dari eksploitasi sistem, jaringan, dan teknologi yang bersifat virus pada perangkat/aplikasi *hacker* yang tidak sah [17]. Adapun 5 jenis keamanan siber diuraikan sebagai berikut:

1. Keamanan Siber Infrastruktur Kritis. Infrastruktur kritis seringkali lebih rentan terhadap serangan daripada yang lain karena sistem SCADA (*Supervisory Control and Data Acquisition* atau kontrol pengawasan dan akuisisi data) sering mengandalkan perangkat lunak yang lebih lama. Operator layanan penting di sektor energi, transportasi, kesehatan, air dan infrastruktur digital Inggris, serta penyedia layanan digital terikat oleh Peraturan NIS (Peraturan Jaringan dan Sistem Informasi 2018). Di antara ketentuan lainnya, kebijakan nasional diharuskan untuk mengimplementasika langkah-langkah pengamanan secara teknis terhadap objek vital nasional, instansi, kementerian dan lembaga agar dapat mengelola keamanan data mereka. [18]

2. Keamanan Jaringan. Keamanan jaringan melibatkan pengalamatan kerentanan yang memengaruhi sistem operasi dan arsitektur jaringan Anda, termasuk server dan host, firewall dan titik akses nirkabel, serta protokol jaringan [19].
3. Keamanan *Cloud.* Keamanan cloud berkaitan dengan pengamanan data, aplikasi, dan infrastruktur di Cloud [20].
4. Keamanan IoT (*Internet of Things*). Keamanan IoT melibatkan pengamanan perangkat pintar dan jaringan yang terhubung ke IoT. Perangkat IoT mencakup hal-hal yang terhubung ke Internet tanpa campur tangan manusia, seperti alarm kebakaran pintar, lampu, termostat, dan peralatan lainnya [21].
5. Keamanan Aplikasi. Keamanan aplikasi melibatkan mengatasi kerentanan yang dihasilkan dari proses pengembangan yang tidak aman dalam desain, pengkodean, dan penerbitan perangkat lunak atau situs *website* [22].

Sebuah laporan baru oleh *think tank* pertahanan dan keamanan *Royal United Services Institute* (RUSI) telah menguraikan beberapa risiko ancaman dunia siber teratas selama transisi menuju energi terbarukan dari bahan bakar fosil. "Energi terbarukan menawarkan peluang besar bagi Inggris untuk menjadi lebih mandiri dalam produksi energi sambil mengurangi dampak perubahan iklim [23]. Transisi ini harus dilakukan dengan mempertimbangkan keamanan siber, menyadari ancaman siber di masa depan bagi masyarakat karena digitalisasi besar-besaran di sektor ini.," kata Sneha Dawda, peneliti keamanan siber di RUSI. Hal ini juga disebabkan karena teknologi energi terbarukan cenderung masih baru sehingga masih perlu adaptasi dan penyempurnaan industry energi terbarukan agar tidak rentan oleh serangan siber. Kerentanan teknologi energi terbarukan akibat dari ancaman serangan siber diuraikan sebagai berikut:

1. Keamanan siber tidak diprioritaskan untuk diperkuat selama fase desain untuk sebagian besar industri energi terbarukan yang beroperasi saat ini [24].
2. Kecenderungan industri energi terbarukan menggunakan Sistem SCADA dan sistem CCTV yang berkualitas rendah/murah yang siap pakai [25].
3. Komponen utama dipilih tanpa mempertimbangkan Keamanan siber [26].
4. Tidak ada kebijakan atau peraturan yang harus diikuti terkait keamanan siber pada sektor energi terbarukan [27].
5. Pembeli dan Penasihat Teknis untuk industri energi terbarukan cenderung tidak memeriksa Keamanan siber mulai dari transaksi, instalasi, penyelesaian hingga penerimaan.
6. Salah satu kekhawatiran utama yang dihadapi sektor energi terbarukan adalah risiko keamanan siber pada bagian rantai pasokan (*Supply Chain*) [28].

Penyedia energi terbarukan harus mengambil pendekatan yang lebih hati-hati dengan rantai pasokan, Pengoprasi energi terbarukan harus mengajukan banyak pertanyaan kepada pemasok/pihak industri EBT, Jika perlu dilakukan peningkatan maintain secara berkala. Sebagian besar perusahaan energi di belahan dunia semakin mendorong pelanggan untuk memasang *smart meter* (Pengukur Pintar) dan sensor lainnya. Namun, pengukur pintar dan perangkat IoT lainnya dapat rentan terhadap serangan siber. Hal ini disebabkan IoT berpotensi memberikan rute ke jaringan dan kemampuan untuk membangun botnet bagi penjahat siber.

Pelaksana/eksekutif perusahaan penyedia energi harus bisa melakukan Langkah taktis terkait IoT karena cukup sulit bagi pengguna untuk menambal kelemahan dan kekurangan perangkat IoT. Dibutuhkan regulasi dan kebijakan seperti undang-undang terkait keamanan desain untuk membantu meningkatkan keamanan siber dan dibutuhkan penelitian lebih lanjut tentang strategi mitigasi risiko dan rekomendasi yang berfokus pada kebijakan diperlukan.

Pembahasan

Postur Sistem Pertahanan dalam mengatasi Ancaman Siber

Sistem Pertahanan Negara memposisikan Tentara Nasional x sebagai komponen utama untuk menangkal ancaman militer (ancaman fisik) dibantu dengan komponen cadangan dan komponen pendukung, tetapi selain itu, Tentara Nasional x bertanggung jawab untuk melakukan Operasi Militer Perang dan Operasi Militer Lainnya Daripada Perang. Hal ini didasarkan pada Kebijakan Pertahanan Negara tahun 2018.

Pembangunan postur pertahanan negara dalam menghadapi ancaman siber harus mengikuti dan sejalan dengan Peraturan Menteri Pertahanan No. 82 Tahun 2014 [30] tentang pedoman pertahanan siber. lembaga yang menjadi leading sector terkait ancaman siber adalah Badan Siber Nasional. Badan Siber Nasional nantinya akan bekerja sama dengan Polri sebagai penegak hukum dalam mengambil tindakan hukum lebih lanjut setelah keamanan siber. Berdasarkan sifat ancamannya, Tentara Nasional x juga bertanggung jawab untuk mengantisipasi hal tersebut dengan membentuk unit-unit seperti Satuan Siber Tentara Nasional x yang dibentuk pada 13 Oktober 2017 [31].

Mengingat ancaman siber yang semakin maju dan mengancam objek vital nasional/infrastruktur informasi kritis, keamanan informasi dan digitalisasi di bidang pertahanan negara dan kementerian pertahanan. Pada awal tahun 2022, Satuan Siber Tentara Nasional x bekerjasama dengan Badan Siber Nasional memutuskan untuk membentuk satuan kecil. Unit ini mencegah dan merespon insiden keamanan informasi yang terkait langsung dengan bidang pertahanan negara di bawah Tentara Nasional x dan Kementerian Pertahanan.

Penggunaan Teknologi Siber harus dibarengi dengan pertahanan siber sebagai upaya mengantisipasi ancaman kejahatan digital, seperti upaya pembobolan kerahasiaan informasi, perusakan sistem elektronik, spionase, dan peretasan pada website Nasional telah terjadi penonaktifan. akun Instagram Kementerian Pariwisata serta berbagai tindakan melanggar hukum lainnya yang dilakukan oleh aktor non-negara atau orang yang tidak bertanggung jawab. Memperhatikan hal tersebut di atas, dunia maya perlu mendapatkan perlindungan yang tepat untuk menghindari potensi yang dapat merugikan individu, organisasi bahkan negara. Unit Siber Tentara Nasional x terdiri dari unit pelaksana meliputi unit pencegahan, unit pemulihan, unit bantuan dan unit penegakan. Kedepannya perlu ada pelatihan berkelanjutan terkait cyber security dan password.

KESIMPULAN

Energi baru terbarukan (EBT) telah mengalami pertumbuhan yang belum pernah terjadi sebelumnya di Eropa dan belahan dunia manapun namun dibalik perkembangannya terdapat Ancaman serius khususnya serangan siber. Ancaman serangan siber pada objek vital energi terbarukan pertama kali dirasakan oleh proyek energi terbarukan di Amerika Serikat. Perusahaan tersebut bernama sPower, Instansi tersebut pemilik pembangkit listrik yang memanfaatkan tenaga surya dan angin mengalami serangkaian koneksi yang terputus antara pusat kendali utamanya dan lokasi pembangkit listrik jarak jauh.

Periode waktu henti yang singkat dan terputus-putus disinyalir disebabkan oleh serangan *Distributed Denial of Service* (DDoS). Oleh karena Peranan pemerintah untuk membantu regulasi dan kebijakan taktis seperti undang-undang terkait keamanan desain untuk membantu meningkatkan keamanan siber dan dibutuhkan penelitian lebih lanjut tentang strategi mitigasi risiko dan rekomendasi yang berfokus pada kebijakan diperlukan. Postur pertahanan ideal dibutuhkan untuk menanggulangi ancaman asimetris seperti serangan siber yang berpotensi merugikan individu hingga negara.

DAFTAR PUSTAKA

Aghenta, L. O., & Iqbal, T. (2019). Design and implementation of a low-cost, open source IoT-based SCADA system using ESP32 with OLED, ThingsBoard and MQTT protocol. AIMS Electronics and Electrical Engineering, 4(1), 57-86.

Alabady, S. A., Al-Turjman, F., & Din, S. (2020). A novel security model for cooperative virtual networks in the IoT era. International Journal of Parallel Programming, 48(2), 280-295.

Alotaibi, I., Abido, M. A., Khalid, M., & Savkin, A. V. (2020). A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources. Energies, 13(23), 6269.

Anggito, A., & Setiawan, J. (2018). Metodologi penelitian kualitatif. CV Jejak (Jejak Publisher).

Bedi, G., Venayagamoorthy, G. K., Singh, R., Brooks, R. R., & Wang, K. C. (2018). Review of Internet of Things (IoT) in electric power and energy systems. IEEE Internet of Things Journal, 5(2), 847-870.

Buchanan, B. (2020). The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics. Harvard University Press.

Brangetto, P., & Aubyn, M. K. S. (2015). Economic aspects of national cyber security strategies. Brangetto P., Aubyn MK-S. Economic Aspects of National Cyber Security Strategies: project report. Annex, 1(9-16), 86.

Calamanti, G. (2021). Security and Climate Change linkage: Analyzing the European discourse until the Defence Roadmap.

Cole, E. (2011). Network security bible. John Wiley & Sons.

Darmalaksana, W. (2020). Metode Penelitian Kualitatif Studi Pustaka dan Studi Lapangan. Pre-Print Digital Library UIN Sunan Gunung Djati Bandung.

Dhar, S., & Bose, I. (2021). Securing IoT devices using zero trust and blockchain. Journal of Organizational Computing and Electronic Commerce, 31(1), 18-34.

Dutta, P., Choi, T. M., Somani, S., & Butala, R. (2020). Blockchain technology in supply chain operations: Applications, challenges and research opportunities. Transportation research part e: Logistics and transportation review, 142, 102067.

Fay, M., Hallegatte, S., Vogt-Schilb, A., Rozenberg, J., Narloch, U., & Kerr, T. (2015). Decarbonizing development: Three steps to a zero-carbon future. World Bank Publications.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. Computer networks, 169, 107094.

Hamzah, D. A. (2021). Metode Penelitian Kualitatif Rekontruksi Pemikiran Dasar serta Contoh Penerapan Pada Ilmu Pendidikan, Sosial & Humaniora. CV Literasi Nusantara Abadi.

Henrie, M. (2013). Cyber security risk management in the SCADA critical infrastructure environment. Engineering Management Journal, 25(2), 38-45

Idris, A. M., Sasongko, N. A., & Kuntjoro, Y. D. (2022). "AUKUS Cooperation in the Form of Australian Nuclear Submarine Technology for Stability in Indo-Pacific Region". International Journal of Research and Innovation in Social Science (IJRISS). 6(2), pp.745-750. DOI: https://dx.doi.org/10.47772/IJRISS.2022.6237

Idris, A. M., Sasongko, N. A., & Kuntjoro, Y. D. (2022). Energy Conversion and Conservation Technology in Facing Net Zero-Emission Conditions and Supporting National Defense. Trends in Renewable Energy, 8(1), 49-66.

IEA. 2021. Renewable 2021 Analysis and Forecast to 2026. International Energy Agency Report and Publication 2021.

Kammen, D. M., & Sunter, D. A. (2016). City-integrated renewable energy for urban sustainability. Science, 352(6288), 922-928.

Kementerian Pertahanan Republik Indonesia. 2017. Kebijakan Pertahanan Negara Tahun 2018. Kementerian Pertahanan Republik Indonesia

Khanna, M. (2021). COVID-19: A cloud with a silver lining for renewable energy?. Applied economic perspectives and policy, 43(1), 73-85.

Markopoulou, D., Papakonstantinou, V., & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. Computer Law & Security Review, 35(6), 105336.

Overland, I. (2019). The geopolitics of renewable energy: Debunking four emerging myths. Energy Research & Social Science, 49, 36-40.

Peraturan Menteri Pertahanan Republik Indonesia NOMOR 82 TAHUN 2014 tentang Pedoman Pertahanan Siber

Plėta, T., Tvaronavičienė, M., Casa, S. D., & Agafonov, K. (2020). Cyber-attacks to critical energy infrastructure and management issues: Overview of selected cases.

Pusat Penerangan Tentara Nasional Indonesia. 2022. Peresmian Military Computer Security Incident Response Team (Mil-CSIRT) TNI. https://tni.mil.id/video-607-peresmian-military-computer-security-incident-response-team-mil-csirt-tni.html

Samarati, P., di Vimercati, S. D. C., Murugesan, S., & Bojanova, I. (2016). Cloud security: Issues and concerns (pp. 1-14). Chichester: Wiley.

Tahaei, M., & Vaniea, K. (2019, June). A survey on developer-centred security. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 129-138). IEEE.

Vakulchuk, R., Overland, I., & Scholten, D. (2020). Renewable energy and geopolitics: A review. Renewable and Sustainable Energy Reviews, 122, 109547.

Walker, A., Desai, J., Saleem, D., & Gunda, T. (2021). Cybersecurity in Photovoltaic Plant Operations (No. NREL/TP-5D00-78755). National Renewable Energy Lab.(NREL), Golden, CO (United States).

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication infrastructures: Motivations, requirements and challenges. IEEE communications surveys & tutorials, 15(1), 5-20.

Yannakogeorgos, P. (2021). Cyber Competition and Global Stability. In The Future of Global Affairs (pp. 223-246). Palgrave Macmillan, Cham.

Yergin, D. (2006). Ensuring energy security. Foreign affairs, 69-82.

Zaheeruddin, & Manas, M. (2015). Analysis of design of technologies, tariff structures, and regulatory policies for sustainable growth of the smart grid. Energy Technology & Policy, 2(1), 28-38.

Zaman, G., & Cristea, A. (2011). EU structural funds absorption in Romania: obstacles and issues. Romanian Journal of Economics, 32(1), 41.