Studi Litelatur: Peningkatan Kinerja Digital Forensik Dan Pencegahan *Cyber Crime*

Risky Mezi Muria[1], Arif Muntasa[2], Muhammad Yusuf[3], Ardi Hamzah[4]
[1,2,3,4] Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Trunojoyo Madura
[1]ria.muria97@gmail.com, [2]arifmuntasa@trunojoyo.ac.id, [3]muhammadyusuf@trunojoyo.ac.id,
[4]ardihamzah@trunojoyo.ac.id

ABSTRAK

Semakin kompleknya suatu permasalahan yang timbul akibat adanya suatu kemudahan dalam teknologi informasi menjadikan kejahatan *cyber attacks* semakin meningkat dan berbahaya bagi sistem dalam suatu negara maupun entitas. Kejahatan yang timbul harus dapat dideteksi dan segera dilakukan suatu tindakan pencegahan agar tidak ada pihak yang dirugkan atas suatu tindakan kejahatan teknologi tersebut. Penelitian ini bertujuan untuk mencari berbagai macam metode untuk meninjau dan melakukan investigasi serangan *cyber* untuk keamanan dalam digital forensic serta dapat memberikan masukan dan tambahan wawasan kepada seluruh pihak termasuk para penyidik atau praktisi dan pengguna di bidang forensik digital tentang berbagai macam metode yang dapat digunakan untuk mendeteksi dan mencegah serangan *cyber*. Penelitian ini dilakukan dengan melakukan studi literatur dari berbagai penelitian tentang serangan *cyber*. Metode penelitian yang digunakan adalah metode deskriptif kualitatif dengan mengambil data dari studi literasi atas penelitian tentang serangan *cyber*. Hasil dari penelitian studi literatur menunjukkan bahwa faktor yang dapat meningkatkan kinerja digial forensik adalah *Digital Forensics Framework For eviewing And Investigating Cyber Attacks* (D4I), digital organisasi dengan holistic, otentikasi biometrik dengan skema forensik gambar, sistem interkoneksi skala besar, arsitektur control LSS, sistem kontrol jaringan (AE-Safe), *Digital Forensic Readiness Index* (DiFRI), LEChain, *Verification Of Digital Evidence (VODE) Framework*, *Capsule of Digital Evidence* (CODE), *The Phase-oriented Advice and Review Structure* (PARS), sistem IEEE-14 dan IEEE-39 kontrol stabilitas, Sistem *Cyber-Fisik* (CPS), STPA-SafeSec, *Digital Evidence Reporting and Decision Support* (DERDS), ExperDF-CM model dan *Argumentation-Based Reasoner* (ABR).

Kata kunci: ***Cyber Crime, Cyber Attacks, Digital Forensik***

ABSTRACT

The more complex a problem that arises due to an ease in information technology makes cyber attacks increasingly dangerous and dangerous for systems within a country or entity. Crimes that arise must be detected and a preventive action taken immediately so that no party is harmed for a technological crime. This study aims to find various methods to review and investigate cyber attacks for security in digital forensics and can provide input and additional insight to all parties including investigators or practitioners and users in the field of digital forensics about various methods that can be used to detect and prevent cyber attacks. This research was conducted by conducting a literature study of various studies on cyber attacks. The research method used is descriptive qualitative method by taking data from literacy studies on research on cyber attacks. The results of the literature study show that the factors that can improve the performance of digital forensics are the Digital Forensics Framework For Reviewing And Investigating Cyber Attacks (D4I), holistic digital organization, biometric authentication with image forensics schemes, large-scale interconnection systems, LSS control architecture, system network control (AE-Safe), Digital Forensic Readiness Index (DiFRI), LEChain, Verification Of Digital Evidence (VODE) Framework, Capsule of Digital Evidence (CODE), The Phase-oriented Advice and Review Structure (PARS), IEEE-system 14 and IEEE-39 stability control, Cyber-Physical System (CPS), STPA-SafeSec, Digital Evidence Reporting and Decision Support (DERDS), ExperDF-CM model and Argumentation-Based Reasoner (ABR)

Keyword : Cyber Crime, Cyber Attacks, Digital Forensik

1. PENDAHULUAN

Dengan semakin berkembangnya teknologi pada saat ini terutama dalam hal penggunaan akses internet menjadikan segala sesuatu dapat diperoleh atau dilakukan dengan sangat mudah hanya dengan menggunakan jaringan internet. Disisi lain dengan adanya kemudahan tersebut telah menimbulkan berbagai masalah yang timbul pada berbagai aspek kehidupan masyarakat dengan suatu perubahan yang bertolak belakang yaitu terjadinya tindak kejahatan yang dilakukan oleh para pengguna teknologi (*cyber attacks*). Teknologi informasi sangat mempengaruhi komunikasi dan interaksi antar masyarakat di seluruh dunia, pelaku kejahatan dapat melakukan kejahatannya di belahan dunia manapun, tanpa terbatas jarak dan waktu.

Meningkatnya ketergantungan pengguna pada perangkat yang terhubung ini meningkatkan paparan pengguna terhadap serangan *cyber*. Tindakan perlindungan dan mitigasi yang ada tidak cukup untuk mengatasi penipuan serangan saat ini. Hal ini diperlukan untuk menegakkan tindakan pencegahan dan mitigasi yang efisien yang berorientasi pada penyerang, yaitu tindakan pencegahan yang khusus untuk penyerang atau kelompok penyerang yang melakukan serangan (Karafili et al., 2020).

Berdasaran data Badan Siber dan Sandi Negara (BSSN) terdapat kenaikan serangan *cyber* saat pandemik Covid-19 di Indonesia dengan jumlah serangan *cyber* sebesar 39,330,231 di tahun 2019 dan mengalami peningkatan 4 kali lipat dengan jumlah serangan *cyber* sebesar 189,937,542 di tahun 2020. Berikut merupakan data statistik serangan *cyber* di Indonesia (Pusat Operasi Keamanan Siber Nasional, 2020):

Sumber : Pusat Operasi Keamanan Siber Nasional, 2020

Kejahatan dunia maya (*cybercrime*) mulai berkembang dengan pesat seiring dengan perkembangan teknologi internet. Kejahatan dunia maya (*cybercrime*) sudah mulai berkembang dan bertransformasi dalam berbagai macam bentuk. Jenis *cybercrime* yang dilakukan pun bermacam-macam, dari penyebaran virus, pembobolan sistem (*cracking*), pemakaian kartu kredit secara ilegal (*carding*), sabotase terhadap perangkat digital, pencurian informasi suatu organisasi hingga *cyberterrorism*. Kejahatan digtal pada umumnya meningkalkan jejak digital atau barang bukti digital yang disebut sebagai *e-evidence*. *E-evidence* dapat berupa komputer, ponsel, kamera digital, hard disk, USB flash disk, memory card, dan lain sebagainya. Bukti digital ini adalah tentang kaslian dan integritas bukti digital itu sehingga bukti digital tersebut dapat dipercaya. Untuk dapat mewujudkan hal tersebut muncul sebuah proses investigasi bukti digital yang dikenal dengan forensik digital. Digital forensik adalah sebuah cabang dalam ilmu komputer yang mempelajari mengenai investigasi, analisa, *recovery*, dan managemen data dari media digital setelah terjadi aksi *cybercrime*.

Dalam suatu negara komponen yang terkomputerisasi adalah bagian dari infrastruktur penting pemerintah dan rentan terhadap peretas dan menjadi target serangan siber. Gangguan minor terhadap kinerja sistem bisa menyebabkan kerugian ekonomi yang cukup signifikan (Tabansky, 2011). Begitu pula dengan perusahaan, pencurian kekayaan intelektual serta pelanggaran keamanan dan data menjadi ancaman umum yang perlu diatasi. Sementara itu, dalam individu, perlu disadari adanya risiko terkait pencurian data dan penyebaran perangkat lunak dan virus yang berbahaya (Bendovschi, 2015).

Banyak penelitian yang ditujukan pada beberapa jenis serangan tunggal, seperti serangan tipuan tersembunyi (Kwon et al., 2013), serangan rahasia (Smith, 2015) dan (De Sá et al., 2017), serangan ulang (Mo & Sinopoli, 2009), serangan penolakan layanan (DoS) di (De Persis & Tesi, 2015) (Zhang et al., 2016) dan (Lu & Yang, 2020), serangan intrusi (Fu et al., 2018) dan kerentanan jaringan listrik (Huang et al., 2018). Selain itu, pekerjaan investigasi yang bertujuan untuk mempertimbangkan berbagai jenis serangan dalam model terpadu jarang terjadi, meskipun beberapa hasil penelitian tentatif (Fu et al., 2018) (Ge et al., 2021), misalnya, dalam (Teixeira et al., 2015), beberapa serangan yang mengandung DoS, replay attack, dynamic-zero attack dan serangan injeksi data, telah dimodelkan dalam kerangka terbatas sumber daya (Zhao et al., 2021). Secara umum, masalah keamanan dalam CPPS melibatkan dua aspek yaitu keamanan teori informasi dan keamanan teori kontrol. Shannon mengusulkan keamanan informasi-teori untuk pertama kalinya pada tahun 1949 (Shannon, C.E., 1949), membuka era penelitian keamanan informasi. Keamanan informasi terutama mengadopsi transmisi enkripsi data dan dekripsi menggunakan cara. Dari perspektif keamanan teori kontrol, perhatian utamanya adalah pengaruh serangan *cyber* pada indeks kinerja dinamis sistem (Kwon et al., 2013), seperti ketahanan, stabilitas, konvergensi cepat, dan sebagainya. Seperti disebutkan dalam (Koppu et al., 2020), untuk mendeteksi ancaman keamanan yang disebabkan oleh serangan cyber sedini mungkin. Menurut setiap serangan *cyber* jenis khusus, model sistem dirumuskan sesuai dengan jenis permasalahannya. Dengan analisis mekanisme dan deformasi rumus matematika, kerangka pemodelan generik diusulkan di bawah jenis serangan siber yang berbeda (Zhao et al., 2021).

Keamanan sistem digital dapat dipengaruhi oleh aspek keamanan siber karena sistem digital terdiri dari perangkat lunak dan saling terhubung oleh suatu jaringan. Keamanan sistem dapat berdampak besar pada keseluruhan sistem (Tolo & Andrews, 2020) (Peterson et al., 2019). Untuk menetapkan strategi yang dapat digunakan untuk menghilangkan atau memitigasi risiko, penting untuk mengidentifikasi bagian mana dari sistem yang rentan dalam hal keamanan dan bagian mana dari sistem yang rentan dalam hal keamanan siber (Shin et al., 2021). Yang et al., (2019) mempelajari serangan injeksi data palsu dalam jaringan sensor nirkabel dengan filter terdistribusi, dan (Smith, 2015) menganalisis serangan cyber rahasia dalam sistem kontrol jaringan, di mana perintah kontrol dari pengontrol dan sinyal pengukuran pabrik secara bersamaan dimanipulasi ke *o-set* efek terkait dan membuat serangan tidak terdeteksi (Al-Dabbagh et al., 2020).

Berbagai permasalahan serangan dunia maya yang terdapat pada zaman industri 4.0 saat ini telah memberikan bukti bahwa permasalahan tersebut merupakan suatu ancaman bagi sistem yang perlu untuk selalu diwaspadai oleh setiap organisasi ataupun perusahaan agar melindungi data-data yang bersifat rahasia dan sensitif serta kekayaan intelektual, informasi keuangan yang dapat dimanfaatkan secara pribadi dengan tujuan jahat. Dengan adanya deteksi dan pencegahan tersebut dapat meminimalisir dan menghindari suatu potensi terkait ancaman siber sehingga membutuhkan lebih banyak perhatian untuk mengembangkan keamanan siber yang lebih kuat.

2. METODOLOGI PENELITIAN

Jenis data yang akan digunakan dalam penelitian ini adalah data-data sekunder. Data sekunder diperoleh dengan melakukan studi literatur dari berbagai penelitian tentang serangan cyber dari jurnal baik itu jurnal nasional ataupun internasional. Model penelitian ini adalah dengan menggunakan model penelitian review literature dengan menggunakan metode meta analisis.

3. HASIL DAN PEMBAHASAN

Penelitian ini dilakukan untuk menjawab beberapa pertanyaan penelitian yang diantaranya adalah metode deteksi dan pencegahan yang dapat dilakukan untuk mengatasi suatu serangan pada dunia maya (*Cyber Attacks*) yang akan timbul pada suatu sistem entitas yang akan berguna bagi keamanan enitas tersebut maupun membantu para praktisi serta pengguna di bidang forensik digital.

Berbagai sistem alat canggih atas fungsi keamanan proteksi, deteksi, repon dan investigasi seperti YARA dan *Indicators Compromise* (IoCs) telah di kembangkan untuk berkontribusi dalam mengidenifikasi jejak atau bukti serangan dengan memberikan saran dimana langkah awal untuk memulai melakukan penyelidikan saat serangan terdeteksi. Namun sistem ini hanya memberikan hasil investigasi yang sedikit terhadap serangan *cyber* baru. Untuk meninjau dan menyelidiki serangan dunia maya (*cyber attacks*) dapat menggunakan *Digital Forensics Framework For eviewing And Investigating Cyber Attacks* (D4I) untuk meningkatkan tahap pemeriksaan dan analisis dari proses forensik digital (Dimitriadis et al., 2020).

Sejumlah peneliti akademis telah memberikan kontribusi suatu sistem untuk melindungi dari pelaku serangan tindakan kejahatan seperti serangan program otomatis yaitu *Bot Crime* (Kejahatan Bot) yang menjadi ancaman besar bagi keamanan aplikasi web misalnya seperti *web server forensics, database forensics, browser web Forensics.* Namun tidak cukup mampu untuk investigasi kejahatan bot dengan menggunakan forensik web. Salah satu tantangan forensik adalah mengimbangi kemajuan perangkat dan jaringan *Internet-of-Things* (IoT). Pentingnya mengintegrasikan prinsip forensik ketika membangun suatu sistem desain forensik juga dapat memperkuat kemampuan kesiapan forensik digital organisasi dengan holistic (Kebande et al., 2020) keadaan IoT saat ini dapat bermanfaat lebih banyak pada proses forensik dapat diintegrasikan. Rahman & Tomar, (2020) dalam penelitiannya telah memberikan suatu kerangka analisis baru untuk meningkatkan perlindungan atas serangan bot. Untuk mendeteksi serangan secara akurat (Ross et al., 2020) pada teknologi yang semakin canggih atau perangkat pintar *Internet-of-Things* (IoT) telah mengusulkan melalui otentikasi biometrik dengan skema forensik gambar yang kuat dan efektif untuk memvalidasi integritas data biometrik agar terhindar dari *cyber crime*. Al-Dabbagh et al., (2020) mampu mendeteksi dan mengisolasi serangan cyber rahasia yang memperhitungkan diagnosis serangan dunia maya dalam konteks sistem interkoneksi skala besar. Sasaran serangan cyber rahasia untuk menunjukkan efektivitas pendekatan deteksi pemodelan pendula. Mendeteksi serangan dunia maya dalam konteks sistem skala besar yang rentan terhadap serangan dengan mengeksploitasi struktur interkoneksi antar subsistem (Gallo et al., 2020) telah mampu mendeteksi dengan membuat arsitektur kontrol terdistribusi yang mengatur LSS kuat terhadap serangan *cyber*. Pendeteksian dan pencegahan serangan cyber dalam sistem kejadian diskrit dalam (Y. Li et al., 2020) telah menyelidiki masalah deteksi dan pencegahan serangan di NCSs dengan sistem kontrol jaringan kemampuan pengendalian AE-Safe. *Digital Forensic Readiness* sebagai sebuah komponen dalam keamanan sistem informasi pada suatu organisasi sebagai bentuk keamanan sistem informasi. Model *Digital Forensic Readiness Index*

(DiFRI) untuk mengukur tingkat kesiapan Institusi dalam menanggulangi aktivitas *Cyber Crime* (Widodo, 2016) dan (Pratama, 2020).

Bukti digital merupakan informasi yang sangat penting untuk menghindari dari gangguan atau serangan *cyber* agar tetap terjamin kerahasiaan dan keamaanannya yang lebih kuat dalam forensik digital maka perlukan keamanan yang kuat. Li et al., (2021) telah mengusulkan model perlindungan keamanan bukti digial untuk mencegah adanya suatu serangan cyber ataupun kecurangan dari pihak luar dimana model yang diusulkan yaitu LEChain terbukti dapat digunakan sebagai keamanan dan privasi unuk forensik digital yang meliputi seluruh aliran bukti mulai dari pengumpulan, pemeriksaan, analisis, dan pelaporan yang juga menyertakan data pengadilan. Dalam Horsman, (2020) Peran bukti digital juga di perhatikan keamanannya dengan penggunaan *Verification Of Digital Evidence (VODE) Framework* untuk mendukung interpretasi terhadap artefak dan data digital agar suatu bentuk data digital tidak disalah tafsirkan. Selain itu berbagai pengetahuan forensik digital yang andal untuk mendukung berbagi pengetahuan luas di bidang forensik digital *Capsule of Digital Evidence* (CODE) merupakan elemen yang diperlukan. CODE dan struktur memberikan persyaratan yang diperlukan agar pengetahuan dapat digunakan secara andal oleh pihak lain di dalam digital forensik. Hal ini menjadi mekanisme jaminan kualitas yang kuat untuk investigasi forensik digital, mendukung dengan menyediakan akses ke informasi yang andal (Horsman, 2020b). Memudahkan interpretasi investigasi digital forensik dalam (Sunde & Horsman, 2021) memperkenalkan metodologi *peer review* pertama yang terdokumentasi untuk bidang forensik digital yaitu *The Phase-oriented Advice and Review Structure* (PARS) yang efektif untuk pekerjaan digital forensik, dari tugas investigasi hingga kegiatan forensik dan proses analisis forensik.

Keamanan dan tindakan penanggulangan *cyber attacks* pada jaringan listrik integrasi informasi dan internet, menghadapi risiko serangan berbahaya, untuk menyimpulkan kondisi dan menjamin keamanan sistem (Zhao et al., 2021) mengatasi masalah serangan *cyber* tersebut dengan sistem IEEE-14 dan IEEE-39 kontrol stabilitas dan (Arnaboldi et al., 2020) meningkatkan permodelan Sistem *Cyber-Fisik* (CPS) untuk mengatasi serangan *cyber*. Analisis risiko keamanan dan keselamatan dari serangan cyber dalam (Shin et al., 2021) untuk mengatasi masalah keamanan dari serangan dunia maya dengan menggunakan STPA-SafeSec juga dapat memeriksa kesalingtergantungan antara faktor keselamatan dan keamanan dengan menyediakan pendekatan tunggal untuk mengidentifikasi batasan keamanan dan keamanan sistem dan menganalisis dampak terhadap keamanan oleh serangan *cyber*. Melindungi keamanan dari serangan *cyber* juga menghindari terhadap kerentanan keamanan yang tinggi dikarenakan media terbuka (Almutairi & Thomas, 2020).

Horsman, (2019) menilai keandalan kesimpulan forensik digital dengan temuan bukti potensial dengan membuat keputusan investigasi yang andal yang menghasilkan pelaporan bukti yang kredibel. Peningkatan pengawasan akan kualitas dan validitas bukti yang dihasilkan oleh praktisi dengan menggunaan kerangka *Digital Evidence Reporting and Decision Support* (DERDS) dengan penilaian investigasi yang menunjukkan bahwa validitas ilmiah dan keandalan forensik. Meningkatkan eksperimen Forensik Digital (OliveiraJr et al., 2020) telah menyajikan ExperDF-CM model konseptual untuk membantu peneliti Digital Forensik dalam merencanakan, melaksanakan, menganalisis, dan menyebarkan eksperimen. Penelitian (Karafili et al., 2020) membantu analis forensik selama analisis bukti dan proses atribusi serangan *cyber* pada dunia maya dengan *Argumentation-Based Reasoner* (ABR) yang dapat menjawab pertanyaan seperti, siapa yang mungkin menjadi pelaku serangan, siapa yang memiliki motif untuk melakukannya,

kemampuan apa yang dibutuhkan untuk melakukan serangan atau apa persamaannya dengan serangan sebelumnya.

4. KESIMPULAN

Organisasi harus siap secara Forensik Digital untuk memaksimalkan potensi mereka dalam merespon peristiwa *Cyber Crime* dan dapat dengan tepat menunjukkan identifikasi faktor-faktor yang berkontribusi terhadap kesiapan Forensik Digital serta bagaimana faktor-faktor ini bekerja bersama untuk mencapai kesiapan Forensik Digital dalam suatu organisasi. Faktor yang dapat meningkatkan kinerja digial forensik adalah *Digital Forensics Framework For eviewing And Investigating Cyber Attacks* (D4I), digital organisasi dengan holistic, otentikasi biometrik dengan skema forensik gambar, sistem interkoneksi skala besar, arsitektur control LSS, sistem kontrol jaringan (AE-Safe) *serta Digital Forensic Readiness* sebagai sebuah komponen dalam keamanan sistem informasi pada suatu organisasi sebagai bentuk keamanan sistem informasi. Model *Digital Forensic Readiness Index* (DiFRI) untuk mengukur tingkat kesiapan Institusi dalam menanggulangi aktivitas *Cyber Crime,* LEChain, penggunaan *Verification Of Digital Evidence (VODE) Framework*, *Capsule of Digital Evidence* (CODE), *The Phase-oriented Advice and Review Structure* (PARS), sistem IEEE-14 dan IEEE-39 kontrol stabilitas, Sistem *Cyber-Fisik* (CPS), STPA-SafeSec, *Digital Evidence Reporting and Decision Support* (DERDS), ExperDF-CM model dan *Argumentation-Based Reasoner* (ABR). Metode deteksi dan pencegahan untuk peningkatan kinerja digital forensic yang diawarkan dalam kerangka kerja sangat berguna dan memudahkan para forensik digital untuk terus memaksimalkan performanya untuk melindungi dari serangan *Cyber* di dunia maya.

DAFTAR PUSTAKA

[1] Al-Dabbagh, A. W., Barboni, A., & Parisini, T. (2020). Distributed Detection and Isolation of Covert Cyber Attacks for a Class of Interconnected Systems. *IFAC-PapersOnLine*, *53*(2), 772–777. https://doi.org/10.1016/j.ifacol.2020.12.829

[2] Almutairi, O., & Thomas, N. (2020). Performance Modelling of the Impact of Cyber Attacks on a Web-based Sales System. *Electronic Notes in Theoretical Computer Science*, *353*, 5–20. https://doi.org/10.1016/j.entcs.2020.09.016

[3] Arnaboldi, L., Czekster, R. M., Morisset, C., & Metere, R. (2020). Modelling Load-Changing Attacks in Cyber-Physical Systems. *Electronic Notes in Theoretical Computer Science*, *353*, 39–60. https://doi.org/10.1016/j.entcs.2020.09.018

[4] Bendovschi, A. (2015). Cyber-Attacks – Trends , Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*(April), 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

[5] De Persis, C., & Tesi, P. (2015). Input-to-state stabilizing control under denial-of-service. *IEEE Transactions on Automatic Control*, *60*(11), 2930–2944. https://doi.org/10.1109/TAC.2015.2416924

[6] De Sá, A. O., Carmo, L. F. R. D. C., & Machado, R. C. S. (2017). Covert Attacks in Cyber-Physical Control Systems. *IEEE Transactions on Industrial Informatics*, *13*(4), 1641–1651. https://doi.org/10.1109/TII.2017.2676005

[7] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*(December 2019), 100015. https://doi.org/10.1016/j.array.2019.100015

[8] Fu, R., Huang, X., Xue, Y., Wu, Y., Tang, Y., & Yue, D. (2018). Security Assessment for Cyber Physical Distribution Power System under Intrusion Attacks. *IEEE Access*, *7*, 75615–75628. https://doi.org/10.1109/ACCESS.2018.2855752

[9] Gallo, A. J., Barboni, A., & Parisini, T. (2020). On detectability of cyber-attacks for large-scale interconnected systems. *IFAC-PapersOnLine*, *53*(2), 3521–3526. https://doi.org/10.1016/j.ifacol.2020.12.1714

[10] Ge, H., Yue, D., Xie, X., Deng, S., & Dou, C. (2021). A unified modeling of muti-sources cyber-attacks with uncertainties for CPS security control. *Journal of the Franklin Institute*, *358*(1), 89–113. https://doi.org/10.1016/j.jfranklin.2019.01.006

[11] Horsman, G. (2019). Formalising investigative decision making in digital forensics: Proposing the Digital Evidence Reporting and Decision Support (DERDS) framework. *Digital Investigation*, *28*, 146–151. https://doi.org/10.1016/j.diin.2019.01.007

[12] Horsman, G. (2020a). Part 1:- quality assurance mechanisms for digital forensic investigations: Introducing the Verification of Digital Evidence (VODE) framework. *Forensic Science International: Reports*, *2*(August 2019), 100038. https://doi.org/10.1016/j.fsir.2019.100038

[13] Horsman, G. (2020b). Part 2:- quality assurance mechanisms for digital forensic investigations: Knowledge sharing and the Capsule of Digital Evidence (CODE). *Forensic Science International: Reports*, *2*(August 2019), 100035. https://doi.org/10.1016/j.fsir.2019.100035

[14] Huang, X., Qin, Z., & Liu, H. (2018). A Survey on Power Grid Cyber Security: From Component-Wise Vulnerability Assessment to System-Wide Impact Analysis. *IEEE Access*, *6*(November), 69023–69035. https://doi.org/10.1109/ACCESS.2018.2879996

[15] Karafili, E., Wang, L., & Lupu, E. C. (2020). An Argumentation-Based Reasoner to Assist Digital Investigation and Attribution of Cyber-Attacks. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/j.fsidi.2020.300925

[16] Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K.-K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. *Forensic Science International: Reports*, *2*(April), 100117. https://doi.org/10.1016/j.fsir.2020.100117

[17] Koppu, S., Kumar, P., Maddikunta, R., & Srivastava, G. (2020). *Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID- 19 . The COVID-19 resource centre is hosted on Elsevier Connect , the company ' s public news and information . January*.

[18] Kwon, C., Liu, W., & Hwang, I. (2013). Security analysis for Cyber-Physical Systems against stealthy deception attacks. *Proceedings of the American Control Conference*, 3344–3349. https://doi.org/10.1109/acc.2013.6580348

[19] Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Generation Computer Systems*, *115*, 406–

420. https://doi.org/10.1016/j.future.2020.09.038

[20] Li, Y., Tong, Y., & Giua, A. (2020). Detection and Prevention of Cyber-Attacks in Networked Control Systems. *IFAC-PapersOnLine*, *53*(4), 7–13. https://doi.org/10.1016/j.ifacol.2021.04.001

[21] Lu, A. Y., & Yang, G. H. (2020). Observer-Based Control for Cyber-Physical Systems under Denial-of-Service with a Decentralized Event-Triggered Scheme. *IEEE Transactions on Cybernetics*, *50*(12), 4886–4895. https://doi.org/10.1109/TCYB.2019.2944956

[22] Mo, Y., & Sinopoli, B. (2009). Secure control against replay attacks. *2009 47th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2009*, 911–918. https://doi.org/10.1109/ALLERTON.2009.5394956

[23] OliveiraJr, E., Zorzo, A. F., & Neu, C. V. (2020). Towards a conceptual model for promoting digital forensics experiments. *Forensic Science International: Digital Investigation*, *35*, 301014. https://doi.org/10.1016/j.fsidi.2020.301014

[24] Peterson, J., Haney, M., & Borrelli, R. A. (2019). An overview of methodologies for cybersecurity vulnerability assessments conducted in nuclear power plants. *Nuclear Engineering and Design*, *346*(February), 75–84. https://doi.org/10.1016/j.nucengdes.2019.02.025

[25] Pratama, Y. (2020). Making Of Digital Forensic Readiness Index (DiFRI) Models To Malware Attacks. *Cyber Security Dan Forensik Digital*, *3*(2), 1–5.

[25] Pusat Operasi Keamanan Siber Nasional. (2020). Laporan Tahunan Hasil Monitoring Keamanan Siber 2020. *Buletin Jendela Data Dan Informasi Kesehatan*, 29–33.

[26] Rahman, R. U., & Tomar, D. S. (2020). A new web forensic framework for bot crime investigation. *Forensic Science International: Digital Investigation*, *33*, 300943. https://doi.org/10.1016/j.fsidi.2020.300943

[27] Ross, A., Banerjee, S., & Chowdhury, A. (2020). Security in smart cities: A brief review of digital forensic schemes for biometric data. *Pattern Recognition Letters*, *138*, 346–354. https://doi.org/10.1016/j.patrec.2020.07.009

[28] Shannon, C.E. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, *28*(1), 656–715.

[29] Shin, J., Choi, J.-G., Lee, J.-W., Lee, C.-K., Song, J.-G., & Son, J.-Y. (2021). Application of STPA-SafeSec for a cyber-attack impact analysis of NPPs with a condensate water system test-bed. *Nuclear Engineering and Technology*. https://doi.org/10.1016/j.net.2021.04.031

[30] Smith, R. S. (2015). Covert Misappropriation Control Systems. *Control Systems, 2015 Issue 1*, *35*(January 2015), 82–92.

[31] Sunde, N., & Horsman, G. (2021). Part 2: The Phase-oriented Advice and Review Structure (PARS) for digital forensic investigations. *Forensic Science International: Digital Investigation*, *36*, 301074. https://doi.org/10.1016/j.fsidi.2020.301074

[32] Tabansky, L. (2011). Critical Infrastructure Protection against Cyber Threats. *Military and*

Strategic Affairs, *3*(2), 61–78.

[33] Teixeira, A., Shames, I., Sandberg, H., & Johansson, K. H. (2015). A secure control framework for resource-limited adversaries. *Automatica*, *51*, 135–148. https://doi.org/10.1016/j.automatica.2014.10.067

[34] Tolo, S., & Andrews, J. (2020). Nuclear facilities and cyber threats. *Proceedings of the 29th European Safety and Reliability Conference, ESREL 2019*, 4004–4013. https://doi.org/10.3850/978-981-11-2724-30966-cd

[35] Widodo, T. (2016). Pengembangan Model Digital Forensic Readiness Index (DiFRI) Untuk Mencegah Kejahatan Dunia Maya. *Jurnal Informatika Sunan Kalijaga*, *1*(1), 41–46.

[36] Yang, W., Zhang, Y., Chen, G., Yang, C., & Shi, L. (2019). Distributed filtering under false data injection attacks. *Automatica*, *102*, 34–44. https://doi.org/10.1016/j.automatica.2018.12.027

[37] Zhang, H., Cheng, P., Shi, L., & Chen, J. (2016). Optimal DoS Attack Scheduling in Wireless Networked Control System. *IEEE Transactions on Control Systems Technology*, *24*(3), 843–852. https://doi.org/10.1109/TCST.2015.2462741

[38] Zhao, Z., Ye, R., Zhou, C., Wang, D., & Shi, T. (2021). Control-Theory based Security Control of Cyber-Physical Power System under Multiple Cyber-attacks within Unified Model Framework. *Cognitive Robotics*. https://doi.org/10.1016/j.cogr.2021.05.001