e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 12 No 4 Tahun 2025 Hal. : 1402-1408

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

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

PEMBELAJARAN DARI KONFLIK RUSIA-UKRAINA BAGI PENGEMBANGAN KEBIJAKAN PELINDUNGAN INFRASTRUKTUR INFORMASI VITAL TERHADAP ANCAMAN SIBER

Emanuel Ario Bimo, Amarulla Octavian, Suyono Thamrin, Rudy Laksmono

Program Studi Ilmu Pertahanan, Pascasarjana, Universitas Pertahanan, Indonesia

Abstrak

Infrastruktur informasi vital merupakan salah satu sasaran utama serangan siber pada situasi konflik, sebagaimana terlihat pada konflik Rusia-Ukraina yang telah memberi bukti empiris mengenai pentingnya pelindungan infrastruktur informasi vital dari berbagai jenis ancaman siber, baik saat perang konvensional maupun ketika masih pada tahap konflik yang berada di bawah ambang batas perang konvensional. Penelitian ini bertujuan untuk menganalisis pembelajaran penting yang diperoleh dari konflik tersebut bagi pengembangan kebijakan pelindungan infrastruktur informasi vital terhadap ancaman siber. Menggunakan metode kualitatif deskriptif terhadap beberapa literatur penelitian terdahulu yang relevan, hasil penelitian ini menemukan bahwa konflik tersebut memberi pelajaran penting bagi pengembangan kebijakan pelindungan infrastruktur informasi vital terhadap ancaman siber, yaitu keniscayaan penguatan redundansi dan ketahanan dalam desain infrastruktur informasi vital, peningkatan kesiapsiagaan dan kemampuan respons dalam menghadapi ancaman siber, pembangunan kemandirian kemampuan siber nasional, serta pengembangan kerja sama lintas pemangku kepentingan di bidang siber. Aspek-aspek pembelajaran tersebut merupakan keniscayaan bagi pengembangan kebijakan yang efektif dalam melindungi infrastruktur informasi vital terhadap ancaman siber, terutama pada situasi konflik.

Kata Kunci: Pelindungan Infrastruktur Informasi Vital, Ancaman Siber, Konflik Rusia-Ukraina, Situasi Konflik.

PENDAHULUAN

Konflik Rusia-Ukraina yang telah berlangsung sejak aneksasi semenanjung Krimea oleh Rusia pada tahun 2014 merupakan salah satu fenomena geopolitik yang penting di abad kedua

*Correspondence Address : emanuelariob@gmail.com
DOI : 10.31604/jips.v12i4.2025. 1402-1408
© 2025UM-Tapsel Press

puluh satu (Petraeus & Roberts, 2023). Jika dibandingkan dengan konflik lainnya, konflik ini telah menunjukkan bahwa perang modern tidak lagi terbatas pada domain perang konvensional, akan tetapi turut meluas ke domain siber (Albakjaji & Almarzoqi, 2023). Infrastruktur informasi vital (IIV) seperti pusat data, infrastruktur komunikasi, serta objek vital berbasis sistem siber, merupakan salah satu target utama dari serangan siber pada konflik ini (Aviv & Ferri, 2023; Anakhov et al., 2023).

Pagnacco (2021) mendefinisikan IIV sebagai segala sistem dan jaringan informasi yang saling terhubung, di mana gangguan atau kerusakan terhadap sistem dan jaringan tersebut dapat berdampak serius terhadap keamanan, keselamatan, dan/atau kemakmuran ekonomi masyarakat, maupun terhadap fungsi pemerintahan serta perekonomian suatu negara. IIV, yang setidaknya mencakup sistem komunikasi, jaringan energi, layanan keuangan, dan sistem kendali industri, merupakan tulang punggung fungsi sosial dan ekonomi modern. Kerentanan IIV terhadap serangan siber dapat mengakibatkan konsekuensi yang luas dan merusak, mulai dari gangguan layanan publik hingga ancaman terhadap keamanan nasional.

Serangan siber didefinisikan sebagai tindakan yang dilakukan dengan menggunakan jaringan komputer untuk mengganggu, menghancurkan, menurunkan kualitas, atau mencegah akses terhadap komputer dan jaringan, maupun informasi yang terkandung di dalamnya (Carlo & Obergfaell, 2024). Serangan siber yang terjadi selama konflik Rusia-Ukraina telah membuka mata berbagai pihak di seluruh dunia tentang pentingnya kebijakan pelindungan IIV dalam menghadapi ancaman siber yang semakin kompleks dan canggih. Konflik Rusia-Ukraina telah memberikan bukti empiris tentang penggunaan serangan siber dalam situasi konflik yang berada di bawah ambang batas perang maupun dalam perang konvensional, baik untuk tujuan taktis hingga strategis.

Insiden-insiden seperti serangan malware NotPetya pada tahun 2017, yang awalnya menargetkan Ukraina tetapi kemudian menyebar secara global, telah menunjukkan potensi kerusakan lintas batas dari serangan siber terhadap IIV. Pada awal invasi Rusia ke Ukraina tahun 2022, Rusia bahkan melancarkan *hacking* terhadap satelit komunikasi Viasat yang menjadi tulang punggung jaringan komunikasi Ukraina serta beberapa negara Eropa lainnya. Kompleksitas dan kecanggihan serangan-serangan ini menunjukkan perlunya pendekatan yang lebih holistik dan adaptif dalam kebijakan pelindungan IIV terhadap ancaman siber.

Di samping meningkatkan kesadaran dan urgensi mengenai pentingnya pelindungan IIV, fenomena empiris konflik Rusia-Ukraina juga memberi pembelajaran penting dalam pengembangan kebijakan pelindungan IIV terhadap ancaman siber. Bentuk-bentuk ancaman siber yang telah terjadi pada konflik Rusia-Ukraina berpotensi untuk terulang kembali di masa depan, bahkan dapat berkembang menjadi semakin kompleks dan berdaya rusak tinggi. Oleh karena itu, fenomena-fenomena yang telah terjadi pada konflik Rusia-Ukraina perlu menjadi unsur pertimbangan penting dalam pengembangan kebijakan pelindungan IIV. Berdasarkan latar belakang tersebut, penelitian ini bertujuan untuk menganalisis beberapa pembelajaran dari konflik Rusia-Ukraina yang berguna bagi pengembangan kebijakan pelindungan IIV terhadap ancaman siber.

METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan

analisis deskriptif. Penelitian deskriptif bertujuan untuk mendeskripsikan suatu fenomena beserta karakteristik dan ciri yang terkandung di dalamnya (Gall, Gall & Borg, 2007). Metode dan pendekatan tersebut dinilai sesuai untuk diterapkan dalam penelitian ini karena kegunaannya dalam menguraikan hal-hal terkait ancaman siber terhadap IIV pada konflik Rusia-Ukraina serta upaya-upaya pelindungan IIV yang dapat dijadikan pembelajaran dari fenomena empiris konflik Rusia-Ukraina secara menyeluruh.

Data penelitian ini diperoleh melalui studi kepustakaan terhadap dokumen resmi dan literatur penelitian terdahulu yang relevan dengan topik penelitian. Data yang telah terkumpul selanjutnya diolah dan dianalisis untuk menemukan tema-tema penting terkait fenomena empiris pada konflik Rusia-Ukraina yang relevan bagi pengembangan kebijakan pelindungan IIV terhadap ancaman siber.

HASIL DAN PEMBAHASAN

Ancaman Siber terhadap IIV pada Konflik Rusia-Ukraina

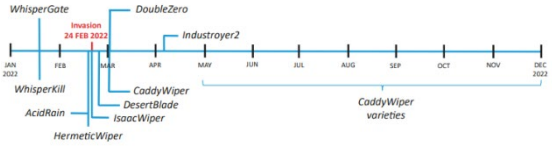
Konflik Rusia-Ukraina berawal sejak Rusia menganeksasi Semenanjung Krimea pada tahun 2014 (McCrory, 2020). Konflik tersebut berlanjut hingga bereskalasi menjadi perang terbuka sejak Rusia mulai menginvasi Ukraina pada bulan Februari 2022. Pola ancaman siber terhadap IIV pada konflik Rusia-Ukraina cenderung menyasar dimensi ketersediaan (*availability*) layanan dan data serta informasi yang disediakan oleh IIV. Pola tersebut dilakukan melalui bentuk-bentuk serangan *distributed denial of service* (DDoS), *hacking*, dan penyisipan *malware* ke sistem informasi dan komputasi IIV (Aviv & Ferri, 2023; Fedorchak, 2024; Lin, 2022; Brantly & Brantly, 2024; Song dkk., 2024; Arnold dkk., 2024; Harknett & Smeets, 2022). Beberapa bentuk ancaman ini tercermin dari ancaman seperti *malware Industroyer* dan *BlackEnergy3* yang menyerang sistem kendali industri sektor energi Ukraina sejak 2015, ancaman *malware Notpetya ransomware* sejak tahun 2017 yang mengenkripsi dan menyandera data, ancaman *malware Wiperware* pada tahun 2022 yang menghapus data, maupun *hacking* yang melumpuhkan satelit Viasat pada tahun 2022.

Serangan DDoS yang dilancarkan oleh Rusia berdampak pada gangguan hingga kelumpuhan berbagai situs dan sistem informasi yang bersifat sangat penting, terutama beberapa *website* pemerintah Ukraina (Lin, 2022). Brantly & Brantly (2024) mengemukakan bahwa aktor yang paling banyak melancarkan serangan DDoS Rusia terhadap Ukraina (sekitar 39,6% dari total serangan DDoS) adalah "*The People's CyberArmy*" (Народная Cуберармия), sebuah kelompok *hacktivist* asal Rusia. Ukraina juga turut membentuk tentara siber sukarela yang disebut "*Ukrainian IT Army*" dari sekumpulan penduduknya untuk mendukung upaya ofensif maupun defensif di domain siber dalam menghadapi Rusia (Aviv & Ferri, 2023; Done, 2023; Lin, 2022). Fenomena-fenomena empiris tersebut menunjukkan bahwa aktor ancaman siber tidak terbatas pada aktor negara saja, melainkan turut melibatkan aktor non-negara, baik yang bekerja secara terkoordinasi dengan aktor negara maupun yang bertindak sendiri karena faktor-faktor emosional, seperti sentimen nasionalisme.

Notpetya ransomware diduga dikembangkan oleh Rusia untuk menyasar data-data penting pada sektor-sektor IIV Ukraina. *NotPetya* menggabungkan fungsionalitas *ransomware* tradisional dengan kemampuan untuk menyebarluaskan dirinya dalam jaringan secara perlahan (Sai & Kumar, 2019). Hal ini turut mengakibatkan penyebarluasan

Notpetya ke berbagai negara selain Ukraina, mulai dari negara-negara Eropa, Asia, hingga Amerika (Sai & Kumar, 2019).

Selain *ransomware* yang mengenkripsi dan menyandera data, Rusia juga banyak melancarkan ancaman *malware* yang bertujuan untuk menghapus atau merusak data melalui penggunaan *Wiperware*. Pada tahun pertama invasi Rusia terhadap Ukraina, sembilan varian *Wiperware* telah digunakan untuk mengganggu berbagai sektor IIV Ukraina, terutama infrastruktur teknologi informasi, komunikasi, energi, transportasi, perawatan kesehatan, bisnis komersial, dan media (Arnold dkk., 2024; Willett, 2022). Serangan ini berdampak pada kelangsungan berbagai aktivitas krusial masyarakat maupun pemerintah Ukraina. Meskipun demikian, efektivitas teknis ancaman *malware* Rusia (baik *ransomware* maupun *Wiperware*) menurun dari waktu ke waktu karena Ukraina secara proaktif terus menambal celah kerentanan, mengumpulkan intelijen ancaman siber (*cyber threat intelligence*) dan menganalisisnya, serta meningkatkan keamanan IIV dari ancaman siber (Arnold dkk., 2024; Swallow, 2023; Willett, 2022).



Gambar 1. Temuan 9 Jenis Wiperware pada Invasi Rusia terhadap Ukraina tahun 2022
Sumber: Arnold dkk. (2024)

Ancaman *malware Industroyer* yang digunakan Rusia sejak tahun 2016 terhadap Ukraina telah berkembang melalui pemaduan *malware* tersebut dengan ancaman *Wiperware* ketika Rusia menginvasi Ukraina tahun 2022 untuk mengganggu fungsionalitas pembangkit-pembangkit listrik di Ukraina dalam rangka melemahkan ketahanan nasional Ukraina.

Salah satu jenis *wiperware*, yaitu AcidRain, juga digunakan Rusia sebagai senjata siber secara terpadu dengan serangan DDoS terhadap Viasat, penyedia komunikasi internet satelit utama bagi Ukraina dan banyak negara Eropa lainnya (Carlo & Obergfaell, 2024; Vedorchak, 2024; Arnold dkk., 2024; Broeders & Sukumar, 2024; Koval dkk., 2023). Ancaman ini ditujukan untuk mengacaukan komunikasi pasukan Ukraina di medan perang (Arnold dkk., 2024; Broeders & Sukumar, 2024). Terlepas dari ancaman siber yang dilancarkan Rusia terhadap Viasat, Ukraina berhasil kembali terhubung ke jaringan komunikasi satelit berkat dukungan terminal satelit seluler Starlink yang disediakan oleh SpaceX dan dibiayai oleh pemerintah Amerika Serikat (AS) (Arnold dkk., 2024).

Pengembangan Kebijakan Pelindungan IIV dari Ancaman Siber Berdasarkan Pengalaman Empiris Konflik Rusia-Ukraina

Salah satu aspek pembelajaran penting dari konflik Rusia-Ukraina bagi kebijakan pelindungan IIV terhadap ancaman siber adalah keniscayaan redundansi dan ketahanan dalam merancang IIV. Upaya preventif, mitigasi serta penguatan daya tahan IIV saat menghadapi ancaman siber merupakan faktor kunci untuk memastikan keberlangsungan fungsi-fungsi IIV yang menyangkut hajat hidup masyarakat serta layanan publik yang esensial. Peningkatan redundansi dan ketahanan IIV terhadap ancaman siber tidak cukup hanya dengan menata dan merancang sistem dan komponen sarana prasarana cadangan (*backup*), tetapi juga perlu diiringi dengan kemampuan untuk beradaptasi dan pulih dengan cepat dari insiden siber (*recovery* dan *continuity*). Penguatan redundansi untuk

keberlangsungan IIV saat mengalami ancaman siber juga perlu dilakukan melalui desain subsistem IIV yang terdistribusi dan terdesentralisasi sehingga sulit untuk diserang secara bersamaan menggunakan bentuk-bentuk ancaman siber serta dapat dipulihkan dengan cepat jika salah satu subsistem atau komponen mengalami serangan.

Konflik ini juga menyoroti pentingnya kesiapsiagaan dan kemampuan respons dalam menghadapi ancaman siber, khususnya kemampuan untuk mendeteksi, menganalisis, dan merespons serangan siber secara cepat dan efektif. Dihadapkan pada kompleksitas dan kecepatan penyebarluasan serangan siber, maka kemampuan respons yang cepat dan efektif sangat penting untuk dibangun dalam rangka mencegah, membatasi, dan mengisolasi serangan siber terhadap IIV beserta dampak yang ditimbulkannya. Pembangunan kemampuan ini memerlukan teknologi deteksi, analisis, dan mitigasi ancaman yang canggih, proses bisnis yang mengedepankan kecepatan koordinasi dan respons antara tim tanggap insiden siber dengan pengelola sistem dan subsistem IIV yang mengalami serangan dan berpotensi terimbas dampaknya, serta pelatihan dan pengembangan kapasitas para pemangku kepentingan yang terkait dengan proses tersebut. Selain itu, latihan dan simulasi respons terhadap berbagai skenario serangan siber juga perlu dilaksanakan secara berkala untuk menguji dan meningkatkan kesiapsiagaan pihak pengelola IIV dan tim tanggap insiden siber serta mengevaluasi proses bisnis yang telah dirancang sebelumnya agar efektivitas pelaksanaan respons insiden siber dapat ditingkatkan secara berkelanjutan.

Berdasarkan contoh-contoh ancaman siber pada konflik Rusia-Ukraina yang telah dijelaskan di atas, beberapa bentuk ancaman siber pada konflik tersebut memiliki dampak tumpahan terhadap negara-negara lain di berbagai belahan dunia. Fenomena ini memberi pelajaran bagi banyak negara agar mewaspadai dan meningkatkan perlindungan serta kesiapsiagaan terhadap potensi penyebarluasan ancaman siber yang telah terjadi di suatu negara. Dalam hal ini, diplomasi siber dan kerja sama internasional dalam menghadapi ancaman siber lintas negara juga menjadi semakin penting dalam membangun kewaspadaan dan kapasitas bersama dalam membendung dan merespons penyebarluasan ancaman siber lintas negara. Kewaspadaan yang tinggi dan respons yang efektif memerlukan koordinasi dan kolaborasi internasional yang kuat, khususnya dalam hal berbagi informasi ancaman siber yang berkembang di berbagai belahan dunia dan berpotensi menyebar luas ke banyak negara beserta strategi penanggulangannya.

Pelajaran lain yang dapat diambil dari konflik Rusia-Ukraina adalah pentingnya inovasi dan adaptasi terus-menerus dalam menghadapi lanskap ancaman siber yang senantiasa berkembang. Sebagaimana telah dijelaskan sebelumnya, varian-varian ancaman malware *Notpetya* serta *Wiperware* terus dikembangkan oleh Rusia sehingga menjadi semakin canggih dari waktu ke waktu. Oleh karena itu, riset dan pengembangan inovasi teknologi keamanan siber harus dilakukan secara berkelanjutan, mulai dari teknologi untuk menunjang proses pengumpulan informasi intelijen, deteksi, hingga respons terhadap ancaman siber. Pengalaman empiris dari konflik Rusia-Ukraina juga menunjukkan pentingnya pembangunan kemampuan siber nasional yang mandiri dengan tingkat ketergantungan serendah mungkin terhadap sumber daya siber negara lain. Ketergantungan pada negara lain dapat memunculkan kerentanan tambahan, terutama pada situasi konflik

ketika sumber daya siber negara lain sulit diakses untuk mendukung penanggulangan ancaman siber. Pengembangan industri keamanan siber domestik dan investasi di bidang pendidikan dan pelatihan keamanan siber merupakan prioritas strategis untuk meningkatkan kemandirian kapasitas suatu negara dalam melindungi IIV dari ancaman siber.

Konflik Rusia-Ukraina juga menyoroti pentingnya penguatan kerja sama antara pemerintah, sektor swasta, dan masyarakat pada bidang siber dalam mencegah dan menghadapi ancaman siber terhadap IIV. Pengalaman empiris konflik Rusia-Ukraina sebagaimana telah dijelaskan pada bagian sebelumnya menunjukkan bahwa berbagai aktor non-negara, mulai dari perusahaan swasta hingga komunitas masyarakat, memiliki peran yang sangat signifikan dalam pelindungan IIV terhadap ancaman siber. Oleh karena itu, pelembagaan dan penguatan kolaborasi lintas pemangku kepentingan di bidang keamanan siber IIV perlu dijalin dan dibangun sedini mungkin guna mempersiapkan unsur-unsur kekuatan nasional yang mampu menghadapi berbagai potensi situasi ancaman siber terhadap IIV di masa depan secara terpadu.

SIMPULAN

Konflik Rusia-Ukraina telah memberi bukti empiris mengenai pentingnya pelindungan IIV dari ancaman siber. Pengalaman empiris konflik tersebut menunjukkan kecenderungan dominasi pola ancaman siber yang menyasar ketersediaan layanan dan data serta informasi pada IIV. Pembelajaran penting yang diperoleh dari konflik tersebut bagi pengembangan kebijakan pelindungan IIV terhadap ancaman siber adalah perlunya penguatan redundansi dan ketahanan dalam desain IIV, peningkatan kesiapsiagaan dan kemampuan respons dalam menghadapi ancaman siber, pembangunan kemandirian kemampuan siber nasional, serta pengembangan kerja sama lintas pemangku kepentingan di bidang siber yang melibatkan sektor swasta dan masyarakat secara aktif. Aspek-aspek pembelajaran tersebut perlu tercakup dalam pengembangan kebijakan pelindungan IIV terhadap ancaman siber, terutama pada situasi konflik.

DAFTAR PUSTAKA

Albakjaji, M., & Almarzoqi, R. (2023). The Impact of Digital Technology on International Relations: The Case of the War between Russia and Ukraine, *Access to Justice in Eastern Europe*, 6(2): 8-24.

Anakhov, P., Zhebka, V., Popereshnyak, S., Skladannyi, P., & Sokolov, V. (2023). *Protecting Objects of Critical Information Infrastructure from Wartime Cyber Attacks by Decentralizing the Telecommunications Network*. Workshop on Cybersecurity Providing in Information and Telecommunication Systems II (CPITS-II), Kyiv, Ukraina 26 Oktober 2023.

Arnold, K., Pijpers, P., Ducheine, P., & Schrijver, P. Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War. In: Rothman, M., Peperkamp, L., & Rietjens, S. (Eds). (2024). *Reflections on the Russia-Ukraine War*. Belanda: Leiden University Press.

Aviv, I., & Ferri, U. (2023). Russian-Ukraine armed conflict: Lessons learned on the digital ecosystem, *International Journal of Critical Infrastructure Protection*, 43: 100637.

Brantly, A. F., & Brantly, N. D. (2024). The Bitskrieg That was and wasn't: The Military and Intelligence Implications of Cyber Operations during Russia's War on Ukraine, *Intelligence and National Security*, *39*(3): 475-495.

Broeders, D., & Sukumar, A. (2024). Core Concerns: The Need for a Governance Framework to Protect Global Internet Infrastructure, *Policy & Internet*, 16(2): 411-427.

Carlo, A., & Obergfaell, K. (2024). Cyber Attacks on Critical Infrastructures and Satellite

Communications, *International Journal of Critical Infrastructure Protection*, 46: 100701-100708.

Done, W. D. (2023). The Information Technology Army of Ukraine and Cyber Warfare Doctrine, *Journal of Strategic Security*, 16(4): 15-33.

Fedorchak, V. (2024). *The Russia-Ukraine War: Towards Resilient Fighting Power*. London: Routledge.

Gall, M., Gall, J., & Borg, R. (2007). *Educational Research: An introduction*, 8th edition. New York: Pearson Education.

Harknett, R. J., & Smeets, M. (2022). Cyber Campaigns and Strategic Outcomes, *Journal of Strategic Studies*, 45(4): 534-567.

Koval, M., Ivashchenko, A., Telelym, V., Sæther, T., Fedianovych, D., Uvarova, T., ... & Pavlikovskyi, A. (2023). *Theoretical and Applied Aspects of the Russian-Ukrainian War: Hybrid Aggression and National Resilience*. Ukraina: Technology Center PC.

Lin, H. (2022). Russian Cyber Operations in the Invasion of Ukraine, *The Cyber Defense Review*, *7*(4): 31-46.

McCrory, D. (2020). Russian Electronic Warfare, Cyber and Information Operations in Ukraine: Implications for NATO and Security in the Baltic States, *The RUSI Journal*, 165(7): 34-44.

Pagnacco, A. (2021). *Critical Information Infrastructure Protection: Between Cybersecurity and Policymaking*. Italian Conference of Cybersecurity, Roma, Italia 7–9 April 2021.

Petraeus, D. & Roberts, A. (2023). *Conflict: The Evolution of Warfare from 1945 to Ukraine*. New York: Harper.

Sai, R. L. P., & Kumar, T. P. (2019). Reverse Engineering the Behaviour of NotPetya Ransomware, *International Journal of Recent Technology and Engineering*, 7(6S): 574-578.

Song, U., Hur, G., Lee, S., & Park, J. (2024). Unraveling the Dynamics of the Cyber Threat Landscape: Major Shifts Examined through the Recent Societal Events, *Sustainable Cities and Society*, 103: artikel 105265.

Swallow, R. C. (2023). Considering the Cost of Cyber Warfare: Advancing Cyber Warfare Analytics to Better Assess Tradeoffs in System Destruction Warfare, *The Journal of Defense Modeling and Simulation*, 20(1): 3-37.

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War, *Survival: Global Politics and Strategy*, 64(5): 7-26.