Journal of International Relations Diponegoro (JIRUD)
Vol. -, No.-, 2026
ISSN (online): 3063-2684
DOI: 10.14710/jirud.v11i1.58468

Aktivitas Ofensif Rusia Dalam Konflik Ukraina Tahun 2022

Ni Nyoman Dinda Ayudya Putri Kirana[1*], Syaakirah Nur Airin[2], Rania Asweta Hirra[3], Anak Ayu Nindya Rastyrania[4], Najmi Aulia Haritzmi Putri[5]

[1,2,3,4,5] Departemen Hubungan Internasional, Fakultas Ilmu Sosial, Budaya, dan Politik, Universitas Pembangunan Nasional "Veteran" Jawa Timur

Article Info

Article History

Received: 26 April 2026;
Revised: 12 June 2026;
Accepted: 22 June 2026;
Published: 30 June 2026.

How to cite: Kirana, N. N. D. A. P., Airin, S. N., Hirra, R. A., Rastyrania, A. A. N., & Putri, N. A. H. (2026). *Aktivitas Ofensif Rusia dalam Konflik Ukraina Tahun 2022. Journal of International Relations Diponegoro, 11*(1), 117-134. https://doi.org/10.14710/jirud.v11i1.58468

*Email:24044010077@student.upnjatim.ac.id

Abstract

The evolution of digital technology has transformed the dynamics of international conflict, with cyberspace emerging as a fifth strategic domain alongside land, sea, air, and outer space. Although offensive activities in cyberspace are often categorized as "cyber warfare," Thomas Rid (2012) argues that cyber war has never happened in the past, is not taking place in the present, and is unlikely to occur in the future, as politically motivated cyber-attacks are versions of three forms of offensive activity: sabotage, espionage, and subversion. This study aims to analyze forms of offensive activities conducted by Russia in the 2022 conflict with Ukraine using Thomas Rid's conceptual framework. The research employs a qualitative case study approach with secondary data drawn from academic literature, government reports, cybersecurity intelligence publications. The findings indicate that Russia's offensive activities manifested in three forms: sabotage through the deployment of destructive wiper malware targeting Ukrainian government, technical systems; espionage through credential theft campaigns and digital reconnaissance operations conducted by GRU-affiliated groups; and subversion through systematic disinformation campaigns, bot farm amplification, and deepfake technology.

Keyword: Offensive Activity, Sabotage, Espionage, Subversion, Russia–Ukraine Conflict

Abstrak

Perkembangan teknologi digital telah mengubah dinamika konflik internasional, dengan ruang siber muncul sebagai domain strategis kelima di samping darat, laut, udara, dan antariksa. Meskipun berbagai aktivitas ofensif di ruang siber sering dikategorikan sebagai "perang siber," Thomas Rid (2012) berargumen bahwa perang siber belum pernah terjadi di masa lalu, tidak sedang terjadi saat ini, dan kecil kemungkinannya akan terjadi di masa depan karena seluruh serangan siber bermotif politik hanyalah versi canggih dari tiga bentuk aktivitas ofensif, yaitu *sabotage*, *espionage*, dan *subversion*. Penelitian ini bertujuan menganalisis bentuk-bentuk aktivitas ofensif yang dilakukan Rusia dalam konflik dengan Ukraina pada tahun 2022 menggunakan kerangka konseptual Thomas Rid. Penelitian menggunakan pendekatan studi kasus kualitatif dengan data sekunder dari literatur akademik, laporan pemerintah, dan publikasi intelijen keamanan siber. Temuan menunjukkan bahwa aktivitas ofensif Rusia termanifestasi dalam tiga bentuk: *sabotage* melalui penyebaran *wiper malware* destruktif yang menargetkan sistem pemerintahan dan teknis Ukraina; *espionage* melalui kampanye pencurian kredensial dan pengintaian digital oleh kelompok yang berafiliasi dengan GRU; serta subversion melalui kampanye disinformasi sistematis, amplifikasi *bot farm*, dan teknologi *deepfake*.

Keyword: Aktivitas Ofensif, Sabotage, Espionage, Subversion, Konflik Rusia–Ukraina

PENGANTAR

Perkembangan teknologi digital telah mengubah karakter konflik internasional secara mendasar. Ruang siber kini diakui sebagai domain strategis kelima di samping darat, laut, udara, dan antariksa, yang dimanfaatkan negara untuk mencapai kepentingan politik dan militer (NATO, 2016). Dalam konteks ini, berbagai tindakan ofensif yang terjadi di ruang siber sering kali dikategorikan sebagai *cyber warfare*. Namun, Thomas Rid (2012) berargumen bahwa perang siber belum pernah terjadi, tidak sedang terjadi, dan kecil kemungkinannya akan terjadi di masa depan. Menurutnya, seluruh serangan siber yang bermotif politik merupakan bentuk modern dari tiga aktivitas ofensif yang telah lama dikenal, yaitu *sabotage*, *espionage*, dan *subversion*. Ketiga aktivitas tersebut berada di antara kejahatan biasa dan perang konvensional, meskipun tidak memenuhi definisi perang dalam pengertian Clausewitzian, ketiganya tetap memiliki dampak strategis terhadap keamanan nasional suatu negara (Rid, 2012).

Fenomena ini menjadi semakin relevan dalam konteks konflik Rusia–Ukraina yang memasuki fase eskalasi besar pada tahun 2022. Bersamaan dengan invasi militer Rusia ke Ukraina pada 24 Februari 2022, berbagai aktivitas ofensif di ruang siber dijalankan sebagai bagian dari strategi *hybrid warfare* yang terintegrasi dengan operasi militer konvensional. Selama beberapa bulan pertama invasi tahun 2022, insiden gangguan dan kerusakan sistem mendominasi aktivitas ofensif Rusia dengan proporsi 57,4 persen dari total insiden, diikuti operasi *espionage* sebesar 21,3 persen (CSIS, 2023). Pola ini memperlihatkan bahwa aktivitas ofensif Rusia tidak bersifat acak, melainkan terencana dan terintegrasi dengan tujuan strategis yang jelas.

Meskipun konflik Rusia–Ukraina 2022 telah banyak dikaji, sebagian besar penelitian lebih berfokus pada aspek *cyber security* dalam konteks defensif atau mengidentifikasi jenis serangan siber dan dampaknya terhadap keamanan nasional. Penelitian yang secara khusus menganalisis aktivitas ofensif Rusia menggunakan kerangka konseptual Thomas Rid masih terbatas. Oleh karena itu, penelitian ini bertujuan menganalisis bentuk-bentuk aktivitas ofensif yang dilakukan Rusia dalam konflik dengan Ukraina pada tahun 2022 menggunakan kerangka konseptual Thomas Rid sebagai pisau analisis.

Artikel ini menggunakan kerangka konseptual *offensive activity* Thomas Rid (2012) dalam jurnal *Cyber War Will Not Take Place* sebagai landasan analisis. Rid mengklasifikasikan serangan siber bermotif politik ke dalam tiga bentuk , yaitu *sabotage* sebagai upaya yang disengaja untuk melemahkan atau menghancurkan sistem ekonomi maupun militer dengan objek atau sistem teknis sebagai target utama bukan manusia, *espionage* sebagai upaya menyusup ke sistem lawan untuk memperoleh informasi sensitif yang dapat bersifat sosial maupun teknis, serta *subversion* sebagai upaya yang disengaja untuk melemahkan otoritas dan tatanan yang mapan dengan mengikis kepercayaan dan ikatan sosial dalam masyarakat di mana sasaran utamanya adalah cara berpikir manusia bukan sistem teknis. Kerangka ini dipilih karena kemampuannya mengklasifikasikan aktivitas ofensif siber secara komprehensif sekaligus membedakannya dari perang dalam pengertian literal. Penelitian menggunakan metode kualitatif dengan pendekatan studi kasus pada konflik Rusia–Ukraina tahun 2022 serta memanfaatkan data sekunder yang dikumpulkan melalui studi kepustakaan dari jurnal ilmiah, laporan pemerintah, publikasi intelijen keamanan siber, dan media yang kredibel.

TINJAUAN PUSTAKA

Kajian mengenai aktivitas ofensif di ruang siber dalam konteks konflik antar negara berkembang pesat dalam satu dekade terakhir. Nair dan Lakshmikanthan (2023) dalam penelitiannya berjudul *Digital Warfare: Cybersecurity Implications of the Russia-Ukraine Conflict* membahas penggunaan cyber warfare dalam konflik Rusia–Ukraina, termasuk serangan terhadap infrastruktur kritis, teknik serangan yang digunakan, serta dampaknya terhadap keamanan siber global. Penelitian ini memiliki kesamaan dengan artikel penulis dalam pembahasan aktivitas siber Rusia–Ukraina, namun berfokus pada *cyber warfare* dan *cyber security* secara umum, sedangkan artikel penulis secara khusus menganalisis aktivitas ofensif Rusia melalui kategori *sabotage*, *espionage*, dan *subversion* berdasarkan kerangka konseptual Thomas Rid (2012). Willett (2023) dalam penelitiannya berjudul *The Cyber Dimension of the Russia–Ukraine War* membahas dimensi siber dalam perang Rusia–Ukraina 2022 dengan fokus pada efektivitas aktivitas ofensif Rusia, integrasinya dengan operasi militer konvensional, serta perang informasi. Persamaannya terletak pada pembahasan aktivitas ofensif Rusia, sedangkan perbedaannya adalah penelitian Willett mengkaji dimensi siber perang secara umum tanpa menggunakan klasifikasi analitis Thomas Rid.

Moore (2022) dalam bukunya berjudul *Offensive Cyber Operations: Understanding Intangible Warfare* menjelaskan pentingnya membedakan operasi operasi siber ofensif dari konsep *cyber warfare* serta mengklasifikasikannya berdasarkan karakteristik operasionalnya. Penelitian ini sejalan dengan artikel penulis dalam menekankan pentingnya perbedaan bentuk-bentuk aktivitas siber ofensif. Namun, penelitian tersebut berfokus pada pengembangan konsep secara umum, sedangkan artikel penulis mengaplikasikan kerangka Thomas Rid pada kasus konflik Rusia-Ukraina tahun 2022 . Ormrod dkk. (2023) dalam jurnalnya berjudul *Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict* membahas operasi siber ofensif Rusia sebagai bagian dari strategi *hybrid warfare*. Persamaannya dengan artikel penulis terletak pada pembahasan aktivitas ofensif Rusia dalam konflik Rusia–Ukraina 2022 sebagai instrumen strategis yang mendukung tujuan politik dan militer. Perbedaannya penelitian tersebut menganalisis efektivitas operasi siber melalui perspektif *hybrid warfare*, sedangkan artikel penulis secara khusus menganalisis aktivitas ofensif Rusia menggunakan kerangka konseptual Thomas Rid. Thornton dan Miron (2022) dalam artikel jurnalnya berjudul *Winning Future Wars: Russian Offensive Cyber and Its Vital Importance* menjelaskan bahwa Rusia memandang *offensive cyber* sebagai instrumen strategis utama untuk melemahkan dan menetralkan negara-negara NATO melalui operasi *cyber-psychological* dan *cyber-technical*. Persamaannya dengan artikel penulis terletak pada pembahasan aktivitas siber ofensif sebagai instrumen strategis untuk mencapai tujuan politik dan keamanan negara, namun penelitian tersebut berfokus pada doktrin orientasi strategis Rusia terhadap NATO , sedangkan artikel penulis menganalisis implementasi aktivitas ofensif Rusia dalam konflik Rusia-Ukraina 2022 menggunakan kerangka Thomas Rid.

Berdasarkan kajian terhadap penelitian-penelitian terdahulu, terdapat dua kesenjangan penelitian. Pertama, sebagian besar studi membahas aktivitas siber Rusia–Ukraina dalam kerangka *cyber warfare* atau *hybrid warfare* tanpa menggunakan kerangka konseptual yang membedakan bentuk-bentuk aktivitas ofensif secara sistematis. Kedua, belum terdapat penelitian yang secara komprehensif menerapkan kerangka Thomas Rid untuk menganalisis aktivitas ofensif Rusia dalam konflik Rusia-Ukraina 2022. Kebaruan artikel ini terletak pada

penggunaan kerangka konseptual *offensive activity* Thomas Rid (2012) sebagai pisau analisis utama untuk mengklasifikasikan *offensive activity* Rusia ke dalam kategori *sabotage, espionage, subversion.* Melalui pendekatan tersebut, artikel ini menjelaskan bentuk-bentuk aktivitas ofensif Rusia sekaligus menunjukkan bagaimana ketiganya dioperasikan secara terintegrasi dalam mendukung tujuan politik dan militer Rusia selama konflik dengan Ukraina tahun 2022.

METODE RISET

Penelitian ini menggunakan metode riset kualitatif untuk memahami dan menganalisis aktivitas ofensif Rusia dalam konflik Rusia-Ukraina tahun 2022. Penelitian ini menggunakan pendekatan studi kasus sebagai salah satu jenis dalam penelitian kualitatif. Dalam penelitian ini, konflik Rusia Ukraina tahun 2022 dijadikan sebagai kasus utama untuk menganalisis berbagai bentuk aktivitas ofensif yang dilakukan Rusia selama konflik berlangsung. Teknik pengumpulan data dalam penelitian ini menggunakan studi kepustakaan (*library research*), yaitu dengan mengumpulkan data sekunder yang berasal dari jurnal ilmiah, buku, laporan resmi, dan sumber terpercaya lainnya yang relevan dengan topik penelitian. Data yang telah dikumpulkan akan diseleksi dan difokuskan pada aspek yang relevan dengan rumusan masalah, kemudian dianalisis menggunakan kerangka konsep dari Thomas Rid, khususnya dalam kategori *sabotage*, *espionage*, dan *subversion*.

PEMBAHASAN

Bentuk Aktivitas ofensif Rusia dalam Konflik Ukraina 2022

Konflik bersenjata antara Rusia dan Ukraina yang memasuki babak baru pada tahun 2022 tidak hanya berlangsung di medan tempur konvensional, tetapi juga di ruang siber. Fenomena ini menegaskan bahwa perang modern tidak lagi dipahami semata melalui penggunaan kekuatan militer, melainkan juga melalui operasi siber yang mendukung strategis negara. . Untuk menganalisis dimensi tersebut, penelitian ini menggunakan kerangka konseptual Thomas Rid yang mengklasifikasikan aktivitas ofensif di dunia maya ke dalam tiga bentuk, yakni *sabotage*, *espionage*, dan *subversion*. Kerangka ini memungkinkan identifikasi tujuan, metode, dan dampak operasi siber Rusia secara sistematis. Thomas Rid sendiri berpendapat bahwa "perang siber" harus memenuhi tiga unsur: *violent* , *instrumental* , dan *political*, sehingga sebagian besar serangan siber tidak dapat dikategorikan sebagai perang. Namun, konflik Rusia-Ukraina 2022 menunjukkan bahwa operasi siber Rusia dijalankan secara terintegrasi dengan operasi militer konvensional sebagai bagian dari *hybrid warfare,* sehingga ketiga kategori Rid menjadi kerangka relevan untuk menganalisis strategi siber Rusia.

Sabotage

Dalam kerangka yang dikemukakan oleh Rid, *sabotage* dipahami sebagai upaya yang disengaja untuk melemahkan atau menghancurkan sistem ekonomi maupun militer, di mana semua sabotase pada dasarnya bersifat teknis dan objek atau sistem teknislah yang menjadi target utama. Bentuk *sabotage* ini terlihat jelas dalam strategi siber Rusia terhadap Ukraina melalui penggunaan berbagai *wiper malware* yang dirancang untuk menghancurkan data dan

membuat sistem target tidak dapat beroperasi. Salah satu bentuk serangan yang menunjukkan praktik *sabotage* tersebut adalah penggunaan *wiper malware* bernama *WhisperGate* yang muncul pada 13 Januari 2022 dan menargetkan berbagai organisasi pemerintah Ukraina. Serangan ini dikaitkan dengan kelompok *hacker* yang dikenal sebagai Cadet Blizzard, yaitu *hacker* yang berafiliasi dengan Rusia dan memiliki keterkaitan dengan *Russian General Staff Main Intelligence Directorate* (GRU) (Microsoft. 2023).

Kehadiran Cadet Blizzard menunjukkan bahwa aktivitas ofensif siber Rusia telah dipersiapkan bahkan sebelum invasi militer dimulai, dengan menargetkan lembaga pemerintahan dan penyedia layanan teknologi informasi yang berperan penting dalam keberlangsungan negara. Pada Januari 2022, kelompok ini menyebarkan *malware WhisperGate* yang menyebabkan sejumlah situs pemerintah Ukraina, termasuk *Cabinet of Ministers*, *Ministry of Foreign Affairs*, dan platform layanan publik digital Diia, tidak dapat diakses. Serangan tersebut menunjukkan upaya yang terkoordinasi untuk mengganggu berbagai sektor strategis pemerintahan dan pelayanan publik. *WhisperGate* sendiri merupakan *wiper malware* yang dirancang untuk menimpa *Master Boot Record* (MBR) dan menghancurkan file penting pada perangkat korban sehingga sistem tidak dapat beroperasi secara normal. Meskipun memiliki karakteristik yang menyerupai *ransomware*, tujuan utama *malware* ini bukan untuk memperoleh keuntungan finansial, melainkan melumpuhkan sistem dan mengganggu operasional organisasi yang menjadi target (CISA, 2022).

Selain *WhisperGate*, bentuk *sabotage* lain yang menunjukkan eskalasi aktivitas ofensif Rusia adalah penggunaan *wiper malware* bernama *HermeticWiper*. Malware ini digunakan pada 23 Februari 2022, tepat satu hari sebelum invasi militer skala besar Rusia ke Ukraina, yang menunjukkan bahwa serangan siber tersebut merupakan bagian dari operasi yang dirancang untuk mendukung tujuan militer melalui pelemahan infrastruktur digital Ukraina (Kringel, 2022). *HermeticWiper* menargetkan sistem komputer milik bank, kontraktor pemerintah, serta sektor pertahanan, penerbangan, dan teknologi informasi di Ukraina (Rapid7, 2022). Dirancang untuk menciptakan kerusakan permanen, *malware* ini memanipulasi *Master Boot Record* (MBR), mengakses dan merusak struktur data tingkat rendah pada media penyimpanan, serta menghancurkan berbagai file dan partisi sehingga proses pemulihan menjadi sangat sulit bahkan tidak mungkin dilakukan (Hasheresade, 2022; Saade, 2022). Kemampuan tersebut menjadikan *HermeticWiper* sebagai salah satu *wiper malware* dengan tingkat destruktivitas yang tinggi dalam rangkaian operasi siber Rusia terhadap Ukraina.

Fakta yang semakin memperkuat argumen bahwa serangan ini bersifat terencana adalah temuan bahwa *HermeticWiper* memiliki tanggal kompilasi 28 Desember 2021, yang mengindikasikan bahwa serangan ini telah dipersiapkan hampir dua bulan sebelum invasi (ESET, 2022). Hal ini membantah kemungkinan bahwa serangan tersebut bersifat reaktif atau spontan. Dari sisi atribusi, *HermeticWiper* diatribusikan kepada kelompok Sandworm Rusia berdasarkan laporan berbagai pihak dengan tingkat kepercayaan menengah hingga tinggi (Ribeiro, 2025). Sandworm sendiri merupakan unit siber yang berafiliasi langsung dengan intelijen militer Rusia (GRU), yang menegaskan bahwa operasi ini merupakan bagian dari strategi negara, bukan aksi peretas independen (Antoniuk, 2025).

Apabila dibandingkan dengan *WhisperGate*, *HermeticWiper* menunjukkan tingkat eskalasi yang lebih tinggi karena menargetkan ratusan sistem di sedikitnya lima organisasi Ukraina, yang

mengindikasikan adanya persiapan matang dan koordinasi erat dengan operasi militer Rusia. Dalam kerangka Thomas Rid, *HermeticWiper* merepresentasikan *sabotage* yang lebih komprehensif karena bersifat *instrumental* dalam melumpuhkan kapasitas komunikasi dan administrasi Ukraina menjelang invasi, sekaligus *political* karena dijalankan sebagai bagian dari strategi negara yang terkoordinasi. Rangkaian serangan ini kemudian diikuti oleh serangan terhadap jaringan satelit KA-SAT milik Viasat pada 24 Februari 2022, sekitar satu jam sebelum invasi penuh Rusia dimulai. Serangan tersebut menargetkan infrastruktur komunikasi satelit yang menyediakan layanan internet bagi Ukraina dan beberapa negara Eropa lainnya, sehingga menunjukkan integrasi yang jelas antara aktivitas siber dan operasi militer konvensional. Mengingat peran strategis jaringan satelit dalam mendukung distribusi informasi, konektivitas, dan koordinasi berbagai aktivitas penting selama konflik, serangan terhadap Viasat menjadi upaya untuk melemahkan kemampuan komunikasi lawan pada fase awal invasi (CyberPeace Institute, 2022).

Setelah akses tersebut sukses untuk diperoleh, Rusia menyebarkan *malware wiper* bernama *AcidRain* yang dirancang untuk menghapus konfigurasi dan firmware modem satelit sehingga perangkat kehilangan fungsi operasionalnya. Berbeda dengan malware yang bertujuan memperoleh data atau informasi, *AcidRain* menunjukkan karakter destruktif karena fokus utamanya terletak pada perusakan perangkat dan gangguan terhadap keberlangsungan sistem komunikasi. (CyberPeace Institute, 2022; SentinelLabs, 2022). Penggunaan *malware* destruktif dalam serangan ini menunjukkan bahwa Viasat *Attack* tidak hanya berfungsi sebagai operasi gangguan jaringan biasa, namun merupakan bentuk serangan siber yang dirancang untuk melemahkan fungsi infrastruktur komunikasi pada fase awal invasi militer. Dalam konteks konflik Rusia Ukraina, serangan terhadap infrastruktur satelit menjadi penting karena jaringan tersebut berperan dalam mendukung konektivitas dan koordinasi berbagai sektor strategis.

Serangan terhadap jaringan satelit Viasat merupakan bagian dari upaya Rusia untuk melemahkan infrastruktur komunikasi Ukraina pada fase awal invasi. Namun, strategi *sabotage* siber Rusia kemudian meluas ke infrastruktur kritis yang berdampak langsung pada keberlangsungan aktivitas negara dan kehidupan masyarakat, terutama sektor kelistrikan. Salah satu contohnya terjadi pada 10 Oktober 2022 ketika kelompok Sandworm melancarkan serangan *cyber-physical* multitahap terhadap organisasi infrastruktur kritis Ukraina dengan menargetkan sistem kendali industri (*industrial control systems*/ICS) dan teknologi operasional (*operational technology*/OT). Dalam serangan tersebut, Sandworm memanfaatkan teknik *living off the land* (LotL) untuk memicu pemutus arus (*circuit breakers*) pada gardu listrik setelah memperoleh akses ke sistem kendali operasional melalui perangkat lunak *Supervisory Control and Data Acquisition* (SCADA) MicroSCADA yang digunakan untuk mengelola dan memantau infrastruktur kelistrikan dari jarak jauh (Proska et al., 2023).

Dua hari setelah serangan terhadap sistem OT, Sandworm melancarkan tahap kedua operasi dengan menyebarkan varian baru *CaddyWiper* pada lingkungan IT korban untuk memperluas gangguan sekaligus berpotensi menghapus artefak forensik yang dapat digunakan dalam investigasi (Proska et al., 2023). Pola ini menunjukkan kombinasi serangan terhadap teknologi operasional (OT) dan teknologi informasi (IT), pelaku terlebih dahulu memanfaatkan sistem kendali kelistrikan untuk memicu pemutus arus, kemudian menggunakan *CaddyWiper* untuk menghapus data korban dan jejak aktivitasnya pada sistem yang terinfeksi. Penggunaan

kedua metode tersebut mencerminkan upaya sistematis untuk memaksimalkan dampak gangguan sekaligus menghambat respons dan pemulihan pihak Ukraina (Dragos, 2023). Dalam kerangka Thomas Rid, operasi ini merepresentasikan bentuk *sabotage* yang sangat jelas karena bersifat *instrumental*, dilaksanakan beriringan dengan serangan rudal sebagai bagian dari strategi militer terpadu, serta *political* karena dilakukan oleh unit intelijen militer Rusia. Berbeda dengan *WhisperGate* dan *HermeticWiper* yang berfokus pada penghancuran data dan sistem informasi, operasi Sandworm secara langsung menargetkan infrastruktur fisik melalui sistem digital yang mengendalikannya sehingga menghasilkan dampak nyata terhadap layanan publik yang bergantung pada pasokan listrik.

Espionage

Dalam kerangka Thomas Rid, *espionage* merupakan aktivitas ofensif yang bertujuan memperoleh informasi rahasia melalui infiltrasi sistem digital dan pencurian data secara tersembunyi. Dalam konflik Rusia-Ukraina tahun 2022, praktik *cyber espionage* banyak dilakukan oleh kelompok APT28 (*Fancy Bear*), yang berafiliasi dengan Unit 26165 badan intelijen militer Rusia (GRU) (Melella et al., 2024). Kelompok ini menggunakan metode, seperti *phishing email*, eksploitasi kerentanan sistem, *brute force attack*, dan penyebaran malware untuk memperoleh akses ke jaringan target. Setelah berhasil masuk, APT28 mencuri kredensial, memantau komunikasi email, serta mengambil dokumen yang berkaitan dengan pemerintahan dan militer. Untuk menghindari deteksi, mereka memanfaatkan infrastruktur seperti VPN, layanan *hosting* gratis, dan domain sementara, sehingga operasi intelijen yang dijalankan dapat berlangsung secara sistematis dan mempertahankan akses jangka panjang ke dalam sistem target (ANSSI, 2025).

Bukti nyata aktivitas *cyber espionage* yang dilakukan oleh APT28 terhadap Ukraina adalah kampanye serangan siber yang dilakukan sejak invasi Rusia tahun 2022. Serangan siber berawal dari pengiriman email jebakan (*spear phishing)* yang berisi dokumen palsu dengan judul provokatif terkait isu perang nuklir, seperti *"Nuclear Terrorism A Very Real Threat.rtf",* untuk memicu kepanikan target di Ukraina. Serangan ini memanfaatkan celah dari kerentanan Follina (CVE-2022-30190) pada sistem Windows yang tidak membutuhkan aktivitas macro, dimana target berinteraksi dengan dokumen tersebut, sistem akan otomatis mengunduh file HTML berbahaya yang memicu penyalahgunaan protokol *Microsoft Support Diagnostic Tool* (MSDT). Hal ini membuat perintah *PowerShell* berbahaya langsung mengeksekusi *malware* pencuri data untuk memperoleh akses dan mencuri informasi dari sistem target (Stockley, 2022). APT28 juga terdeteksi menggunakan teknik *zero-click* melalui kerentanan Microsoft Outlook (CVE-2023-23397), di mana email berbahaya secara otomatis memicu koneksi ke server penyerang tanpa memerlukan interaksi dari pengguna. Metode ini memungkinkan pencurian kredensial NTLM sehingga pelaku dapat memperoleh akses ke akun dan jaringan internal organisasi target secara diam-diam untuk kepentingan intelijen strategis Rusia.

Di sisi lain GRU Unit 26165 dikenal sebagai 85th Main Special Service Center (GTsSS), merupakan salah satu unit siber di bawah badan intelijen militer Rusia (GRU) yang sering dikaitkan dengan kelompok Fancy Bear, APT28, atau Strontium. Kelompok ini oleh banyak peneliti keamanan siber Barat dianggap sebagai salah satu aktor utama dalam operasi *cyber*

espionage Rusia, sehingga menunjukkan bahwa aktivitas siber negara tersebut tidak dijalankan oleh peretas independen, melainkan telah terintegrasi dalam struktur militer negara (Soldatov et al., 2022). Dalam aktivitas ofensif Rusia, Unit 26165 berperan sebagai fasilitas utama untuk *intelligence gathering*, *digital reconnaissance*, dan pengumpulan informasi strategis guna mendukung kepentingan negara. Berasal dari unit *signals intelligence* (SIGINT) era Uni Soviet, unit ini mengalami modernisasi sejak era 2000-an dan memperkuat kapabilitasnya melalui perekrutan talenta siber dari berbagai jalur profesional (Soldatov et al., 2022).

Keberadaan GRU Unit 26165 menunjukkan bahwa *cyber espionage* Rusia dilakukan secara terorganisasi melalui integrasi antara institusi militer, badan intelijen, dan jaringan pendukung lainnya, sehingga menjadi bagian dari instrumen strategis negara untuk memperoleh keunggulan informasi dalam konflik internasional. Struktur yang terintegrasi ini memungkinkan informasi yang diperoleh melalui dunia maya dimanfaatkan untuk mendukung operasi yang lebih luas, termasuk operasi militer konvensional (Soldatov et al., 2022). Salah satu contohnya terjadi pada 15 Maret 2022 ketika pemerintah Inggris melaporkan bahwa Unit 26165 melakukan *online reconnaissance* terhadap lokasi perlindungan sipil di Mariupol dan Kharkiv. Aktivitas tersebut menunjukkan bahwa *cyber espionage* tidak hanya berfungsi untuk memperoleh akses ke sistem digital, tetapi juga sebagai sarana *intelligence gathering* yang mendukung perencanaan dan pengambilan keputusan operasional di medan perang (Government of the United Kingdom, 2025).

Subversion

Konsep *subversion* dalam kerangka yang dikemukakan Thomas Rid merupakan upaya yang disengaja untuk melemahkan otoritas, integritas, dan tatanan yang telah mapan dengan mengikis kepercayaan, keyakinan, serta ikatan sosial dalam masyarakat, di mana sasaran utamanya adalah cara berpikir manusia, bukan sistem atau perangkat teknis. Dalam konflik Rusia-Ukraina tahun 2022, strategi *subversion* ini terlihat dari penggunaan propaganda, disinformasi, manipulasi media, dan operasi informasi yang dilakukan Rusia untuk membentuk narasi tertentu yang berkaitan dengan Ukraina. Adanya *information war* khususnya dari Rusia terhadap Ukraina yang bertujuan untuk mempengaruhi opini publik, melemahkan legitimasi pemerintah Ukraina, serta membenarkan invasi Rusia melalui penyebaran narasi politik dan propaganda secara masif (OECD, 2022). Hal ini terlihat bahwa ruang siber digunakan Rusia sebagai instrumen strategis untuk mempengaruhi kondisi psikologis dan sosial masyarakat Ukraina maupun komunitas internasional.

Narasi propaganda yang disebarkan Rusia dalam konflik dengan Ukraina tahun 2022 digunakan untuk membangun legitimasi atas invasi yang dilakukan sekaligus membentuk persepsi publik terhadap Ukraina. Rusia menyebarkan berbagai disinformasi seperti klaim bahwa pemerintah Ukraina dikuasai kelompok Neo-Nazi, Ukraina melakukan genosida terhadap masyarakat berbahasa Rusia di Donbas, serta Ukraina merupakan ancaman bagi keamanan Rusia (OECD, 2022). Penyebaran propaganda tersebut dilakukan secara berulang melalui media digital dan platform online agar narasi yang dibangun Rusia dapat mempengaruhi opini publik domestik maupun internasional. Selain itu, aktivitas ofensif Rusia juga dilakukan bersamaan dengan kampanye manipulasi informasi yang menimbulkan kebingungan,

ketidakpercayaan publik, serta melemahkan kepercayaan masyarakat terhadap pemerintah Ukraina (Microsoft, 2022).

Pemanfaatan media digital dan media sosial juga dipakai sebagai sarana penyebaran propaganda serta disinformasi secara luas. Rusia memanfaatkan berbagai platform digital untuk menyebarkan teori konspirasi, berita palsu, dan narasi propaganda untuk mempengaruhi opini publik internasional terkait dengan konflik bersama Ukraina (OECD, 2022). Praktik tersebut juga ditemukan dalam *Meta's Adversarial Threat Report Q3* (2022) yang menjelaskan adanya jaringan operasi informasi dari Rusia menggunakan ribuan akun palsu, Facebook, dan situs berita tiruan untuk menyebarkan narasi pro ke Rusia dan propaganda anti Ukraina. Operasi tersebut dilakukan melalui penyamaran sebagai media independen di Eropa yang kemudian menyebarkan artikel, meme, dan video berisi kritikan untuk Ukraina, dukungan kepada Rusia, serta menyatakan bahwa sanksi Barat terhadap Rusia akan merugikan negara-negara Eropa itu sendiri. Selain itu, ditemukan juga adanya aktivitas *coordinated inauthentic behavior* yang dilakukan secara terstruktur dengan tujuan untuk memanipulasi opini publik melalui Facebook, Instagram, Telegram, Twitter, dan platform digital lainnya (Meta, 2022).

Kremlin menyebarkan disinformasi dan propaganda melalui proksi media untuk membangun "kasus perang" palsu Putin. Kremlin juga memperluas upayanya untuk melemahkan Ukraina dan pengaruhnya di dunia untuk memaksa Ukraina menyerah (Bachman et al., 2023). Pidato Putin pada 24 Februari 2022 memperlihatkan betapa terstrukturnya propaganda yang telah dibangun sejak bertahun-tahun sebelumnya. Narasi "Ukraina adalah agresor" muncul dalam 1.888 artikel sebagai alat tambahan untuk membenarkan perang dan menyangkal tanggung jawab Rusia, dan muncul dalam jumlah besar pada hari-hari setelah klaim pihak separatis dan Kremlin bahwa Ukraina telah menyerang sebuah taman kanak-kanak dan menargetkan tangki klorin (Atlantic Council, 2023).

Sepanjang 2023 Rusia menggunakan seluruh teknologinya untuk menjalankan misi disinformasi termasuk berkoordinasi diseluruh platform media sosial untuk mengeksploitasi opini publik terhadap Barat, melakukan peretasan, dan memalsukan dokumen (Atlantic Council DFRLab, 2024). Rusia telah secara aktif menjalankan operasi disinformasi untuk melemahkan Ukraina setidaknya sejak 2014. Menjelang invasi Ukraina pada Februari 2022, Rusia menggunakan disinformasi dalam bentuk *narrative warfare* untuk membenarkan tindakan militer, menyembunyikan seluruh rencana operasional, dan menolak seluruh tanggung jawab atas invasi (Atlantic Council DFRLab, 2024). Kremlin secara rutin mengubah narasinya untuk mengalihkan perhatian publik dari kegagalan perang dan isolasi politiknya. Mulai dari "Pengepungan Nato", "Denazifikasi", "Desatanisasi", "Mempertahankan Rusia", hingga "Genosida terhadap Donbas" (U.S. Department of State, 2023). Pada Juli 2022 media Russia menyebarkan disinformasi "laboratorium biolabs yang dijalankan AS" yang mengklaim bahwa tentara Ukraina dijadikan subjek eksperimen. Pernyataan-pernyataan ini mengikuti tuduhan yang dibuat pada Maret 2022 oleh Kementerian Pertahanan Rusia bahwa Amerika Serikat mengembangkan "senjata bio etnis" di Ukraina untuk menargetkan etnis Slavia, seperti warga Rusia (U.S. Department of State, 2023). Dalam berbagai publikasi media Rusia lama, sering ditemukan frasa "*na Ukraine*" yang berarti "di atas Ukraina," berbeda dengan "*v Ukraine*" yang berarti "di dalam Ukraina." Perbedaan ini penting, karena Rusia menggunakan "*na*" ketika merujuk pada suatu wilayah dan "*v*" ketika merujuk pada wilayah berdaulat yang merupakan

bagian dari kampanye untuk menghapus wilayah Ukraina (Nastas, 2025). Pasca-invasi, para politisi dan media Rusia menggunakan bahasa untuk melunak-lunakkan realitas tindakan militer. Invasi itu dilabeli sebagai "operasi militer khusus." Salah satu tujuan utamanya, sebagaimana dinyatakan oleh Presiden Vladimir Putin, adalah melucuti senjata dan "meng-denazifikasi" Ukraina (Polegkyi, 2023).

Berbagai bentuk propaganda, disinformasi, dan pengaturan narasi yang dilakukan Rusia memperlihatkan bagaimana informasi digunakan sebagai instrumen strategis untuk mempengaruhi opini publik dan mendukung tujuan politik dan militer, sejalan dengan konsep subversion menurut Thomas Rid yang menekankan bahwa aktivitas ofensif tidak selalu dilakukan melalui serangan terhadap sistem atau infrastruktur digital, tetapi juga melalui upaya mempengaruhi cara berpikir, persepsi, dan kondisi psikologis masyarakat untuk menciptakan situasi yang menguntungkan bagi suatu negara. Dalam konteks tersebut, ruang siber berfungsi tidak hanya sebagai domain teknis, tetapi juga sebagai arena operasi informasi yang semakin efektif seiring perkembangan teknologi dan media sosial yang memungkinkan penyebaran informasi secara cepat, luas, dan sulit dikendalikan.

Salah satu bentuk *subversion* yang terlihat dalam konflik antara Rusia Ukraina tahun 2022 adalah penggunaan *bot farm* dan amplifikasi media sosial untuk memperluas penyebaran narasi pro Rusia. *Bot farm* merupakan jaringan akun otomatis maupun semi otomatis yang dioperasikan secara terkoordinasi untuk meningkatkan visibilitas suatu pesan melalui *retweet* massal, penggunaan hashtag tertentu, komentar berulang, serta interaksi buatan yang dapat meningkatkan popularitas suatu narasi di media sosial. Strategi amplifikasi media sosial kemudian digunakan untuk memperbesar jangkauan pesan agar lebih sering muncul dalam algoritma platform digital, sehingga suatu informasi memiliki peluang lebih besar untuk dilihat dan disebarkan ulang oleh pengguna lain. Kondisi tersebut memperlihatkan bahwa media sosial tidak hanya digunakan sebagai sarana komunikasi, tetapi juga sebagai instrumen untuk membangun pengaruh politik dan membentuk persepsi publik (Shao et al., 2018).

Pemanfaatan *bot farm* dalam konflik Rusia Ukraina menunjukkan bagaimana ruang informasi menjadi bagian penting dari strategi subversion modern. Terdapat penelitian yang menemukan bahwa ada 49.455 pesan pro Rusia di Twitter selama periode Februari hingga Juli 2022 menemukan bahwa pesan-pesan tersebut menghasilkan sekitar 251.000 *retweet* dengan estimasi jangkauan mencapai 14,4 juta pengguna. Penelitian tersebut juga menemukan bahwa sekitar 20,28% akun yang terlibat dalam penyebaran pesan pro Rusia diklasifikasikan sebagai *bot*, serta banyak akun otomatis tersebut dibuat pada tahap awal invasi Rusia ke Ukraina. Temuan ini memperlihatkan bahwa akun otomatis tidak hanya berfungsi sebagai alat penyebaran informasi, tetapi juga sebagai instrumen untuk mempercepat difusi narasi tertentu dan memperluas pengaruh propaganda di ruang digital (Geissler et al., 2023).

Selain penggunaan akun otomatis, strategi subversion digital juga terlihat melalui penggunaan kampanye informasi terkoordinasi, penyebaran disinformasi, dan manipulasi percakapan daring untuk memperkuat narasi yang menguntungkan Rusia. Berbagai laporan menunjukkan bahwa jaringan propaganda pro Rusia memanfaatkan berbagai platform media sosial untuk memperbesar eksposur narasi tertentu sekaligus mengurangi visibilitas informasi yang bertentangan. Dengan demikian, penggunaan *bot farm* dan amplifikasi media sosial dapat dipahami sebagai bentuk subversion dalam aktivitas ofensif modern karena tidak hanya

bertujuan menyebarkan informasi, tetapi juga mempengaruhi persepsi publik, membangun legitimasi narasi tertentu, dan menciptakan dominasi informasi di ruang siber.

Rusia juga melakukan *cyber subversion* melalui pemanfaatan teknologi kecerdasan atau yang biasa disebut dengan *artificial intelligence* (AI) berupa *deepfake*. Teknologi ini digunakan untuk menyebarkan informasi palsu yang memakai tokoh politik seperti Vladimir Putin dan Volodymyr Zelensky. Salah satu kasus yang paling terkenal adalah video *deepfake* Presiden Ukraina Volodymyr Zelensky yang berisi pernyataan agar tentara Ukraina menyerah dan meletakkan senjatanya. Video tersebut disebarkan setelah situs berita Ukraina diretas sehingga terlihat seperti informasi resmi dari pemerintah Ukraina (BBC News Indonesia, 2022). Penggunaan *deepfake* dalam konflik Rusia-Ukraina menunjukkan bahwa manipulasi informasi tidak hanya dilakukan melalui propaganda seperti teks atau gambar, tetapi juga bisa melalui video yang terlihat nyata. Meskipun kualitas video *deepfake* Zelensky dinilai rendah dan mudah diketahui sebagai video palsu, penyebarannya tetap menimbulkan kekhawatiran karena publik pasti kebingungan, menurunkan kepercayaan masyarakat terhadap informasi resmi pemerintah Ukraina, serta masyarakat dapat kesulitan dalam membedakan informasi asli dan manipulasi digital (Pownall et al., 2023).

Analisis Dampak Aktivitas Ofensif Rusia terhadap Ukraina

Aktivitas ofensif siber Rusia dalam konflik Ukraina tahun 2022 tidak hanya menghasilkan kerusakan terhadap sistem digital, tetapi juga menimbulkan konsekuensi strategis yang mempengaruhi kapasitas pertahanan, keamanan informasi, serta ruang informasi Ukraina. Berbagai aktivitas ofensif tersebut menunjukan bahwa operasi tersebut tidak berdiri sendiri, melainkan saling melengkapi untuk kepentingan militer politik selama konflik berlangsung. Oleh karena itu bagian ini berfokus pada analisis dampak yang ditimbulkan oleh aktivitas ofensif siber Rusia terhadap Ukraina.

Dampak *Sabotage* terhadap Kapasitas Pertahanan dan Infrastruktur Ukraina

Aktivitas ofensif dalam bentuk *sabotage* yang dilakukan Rusia dalam konflik Rusia Ukraina 2022 memberikan dampak terhadap kapasitas pertahanan, infrastruktur kritis, serta ekonomi dan sosial Ukraina. Tidak seperti *espionage* yang bertujuan untuk mengumpulkan informasi, *sabotage* lebih menekankan pada penciptaan gangguan dan kerusakan terhadap sistem digital yang mendukung operasional negara. Dalam situasi konflik ini, penggunaan *wiper malware*, serangan terhadap jaringan satelit, hingga gangguan terhadap sistem kelistrikan menunjukkan bahwa ruang siber dimanfaatkan untuk menciptakan disrupsi yang bisa melemahkan kemampuan Ukraina baik sebelum maupun selama perang berlangsung. Hal ini selaras dengan teori yang disampaikan oleh Thomas Rid, dimana tindakan satu arah yang merusak tanpa menghasilkan dialog atau tuntutan yang dapat dinegosiasikan. *WhisperGate dan HermeticWiper* adalah contoh paling jelas dari definisi tersebut.

Salah satu dampak utama dari *sabotage* terlihat pada terganggunya kemampuan pertahanan dan operasional negara Ukraina. Serangan menggunakan *WhisperGate* dan *HermeticWiper* yang menargetkan lembaga pemerintahan, sektor pertahanan, institusi keuangan, serta penyedia layanan publik mengakibatkan gangguan pada berbagai sistem digital dan kehilangan berbagai data penting. Situasi ini memaksa pemerintah Ukraina mengalihkan sumber daya, tenaga ahli, serta kapasitas institusional untuk memperbaiki sistem di tengah

berlangsungnya konflik militer. Situasi ini menunjukkan bahwa serangan ini tidak hanya menghasilkan kerusakan teknis, tetapi juga dapat mengurangi efektivitas negara dalam mempertahankan fungsi administratif dan pertahanannya selama masa perang (Microsoft, 2023).

Selain mempengaruhi kemampuan pertahanan, sabotase juga berdampak besar pada infrastruktur penting Ukraina. Serangan ke jaringan satelit Viasat KA-SAT pada 24 Februari 2022 menunjukkan bahwa infrastruktur komunikasi menjadi target penting untuk mengurangi kemampuan koordinasi suatu negara. Serangan ini berdampak pada sebuah perusahaan energi besar Jerman yang kehilangan akses pemantauan jarak jauh terhadap lebih dari 5.800 turbin angin, serta hampir 9.000 pelanggan penyedia layanan internet satelit di Prancis mengalami gangguan koneksi internet (Viasat, 2022). Perlu dicatat bahwa turbin angin tersebut tidak benar-benar berhenti beroperasi, tetapi kemampuan pemantauan dan pengendalian jarak jauhnya menjadi tidak tersedia akibat gangguan komunikasi satelit (Saade, 2022). Disini, teori dari Thomas Rid terbukti benar, dimana efek sabotase siber merembet jauh melewati target yang diinginkan (*spillover effect*), sesuatu yang tidak mungkin dikontrol seperti misil konvensional. Dampak tersebut menunjukkan bahwa serangan terhadap infrastruktur digital yang modern bisa memiliki efek yang melintasi batas negara dan dapat mengganggu berbagai sektor yang bergantung pada jaringan komunikasi untuk mendukung kegiatan pemerintahan, militer, dan masyarakat sipil (CyberPeace Institute, 2022).

Dampak dari sabotase ini semakin meluas ketika serangan dari Rusia mulai menyasar infrastruktur energi di Ukraina. Operasi *Sandworm* terhadap jaringan listrik menunjukkan bahwa serangan siber saat ini tidak hanya fokus pada merusak data atau sistem informasi, tetapi juga bisa menyebabkan dampak fisik yang nyata berupa pemadaman listrik yang bertepatan dengan serangan rudal masif terhadap infrastruktur kritis Ukraina. Masalah pada jaringan listrik bisa berdampak pada penyebaran energi, mengganggu layanan publik, dan menghalangi aktivitas masyarakat yang bergantung pada pasokan listrik untuk kebutuhan sehari-hari (Proska et al., 2022).

Dampak *Espionage* terhadap Keamanan Informasi dan Kapasitas Strategis Ukraina

Jika sabotage berfokus pada perusakan dan pelumpuhan sistem, maka espionage memberikan dampak yang berbeda karena berorientasi pada pengumpulan informasi strategis yang dapat dimanfaatkan untuk mendukung operasi militer dan pengambilan keputusan. Dalam konflik Rusia–Ukraina, aktivitas espionase memungkinkan Rusia memperoleh akses terhadap data, komunikasi, dan informasi penting milik pemerintah maupun institusi strategis Ukraina (Duguin & Pavlova, 2023). Sesuai dengan konsep Thomas Rid, espionage merupakan tindakan memperoleh informasi secara rahasia tanpa merusak target secara langsung. Meskipun tidak menghasilkan kerusakan fisik yang segera terlihat, informasi yang diperoleh melalui operasi spionase dapat memberikan keuntungan strategis yang signifikan dalam suatu konflik.

Salah satu aktor utama dalam operasi espionage Rusia adalah kelompok APT28 atau Fancy Bear yang diatribusikan kepada Unit 26165 dari *Russian General Staff Main Intelligence Directorate* (GRU). Pada Juni 2022, kelompok ini menjalankan kampanye *spear-phishing* yang memanfaatkan kerentanan Follina (CVE-2022-30190) untuk menyebarkan malware pencuri kredensial bernama CredoMap. Malware tersebut dirancang untuk mencuri kata sandi, *cookie*,

Vol. -, No.-, 2026
ISSN (online): 3063-2684
DOI: 10.14710/jirud.v11i1.58468

dan berbagai informasi yang tersimpan pada peramban seperti Google Chrome, Microsoft Edge, dan Mozilla Firefox, kemudian meng-eksfiltrasi data yang dicuri menggunakan protokol email IMAP ke server yang dikendalikan pelaku (Stockley, 2022). Informasi yang berhasil diperoleh memungkinkan akses lebih lanjut terhadap akun, jaringan, maupun sistem yang digunakan oleh target (Lee, 2025).

Dampak utama dari operasi ini adalah meningkatnya kerentanan institusi Ukraina terhadap infiltrasi dan kebocoran informasi strategis. Dengan memperoleh kredensial pengguna, aktor Rusia dapat mengakses komunikasi internal, dokumen pemerintahan, maupun informasi operasional yang berpotensi memberikan keuntungan intelijen bagi perencanaan militer, sebagaimana dibuktikan oleh kampanye APT28 yang berhasil mengkompromikan lusinan entitas di berbagai negara (Field Effect, 2025). Serangan semacam ini menunjukkan bahwa espionage tidak hanya bertujuan mengumpulkan data, tetapi juga menciptakan *information advantage* yang dapat digunakan untuk memahami kondisi lawan secara lebih mendalam dan memperkirakan respons yang akan dilakukan Ukraina terhadap berbagai operasi militer Rusia.

Dampak *espionage* Rusia juga terlihat pada upaya pengumpulan informasi mengenai dukungan internasional terhadap Ukraina. Unit 26165 diketahui menjalankan kampanye pengintaian terhadap organisasi pemerintah, lembaga pertahanan, penyedia infrastruktur kritis, serta institusi yang terlibat dalam pengiriman bantuan kepada Ukraina, sebagai bagian dari kampanye spionase yang menargetkan bantuan asing untuk Ukraina. Aktivitas ini menunjukkan bahwa informasi mengenai logistik, bantuan militer, serta dukungan internasional dipandang sebagai aset strategis yang dapat membantu Rusia memahami kapasitas pertahanan Ukraina dan jaringan pendukungnya (CISA, 2025). Dengan kata lain, espionage berfungsi sebagai instrumen untuk membangun *situational awareness* yang lebih baik bagi Rusia dalam menjalankan operasi militernya.

Dampak yang lebih serius terlihat dari aktivitas pengintaian yang dilakukan Unit 26165 terhadap lokasi perlindungan warga sipil di Mariupol dan Kharkiv pada 15 Maret 2022. Salah satu target adalah Teater Mariupol tempat warga sipil yang berlindung dari bom Rusia telah melukis kata "anak-anak" di luar dengan harapan melindungi mereka. Keesokan harinya, teater tersebut dihantam serangan udara Rusia yang menewaskan sekitar 600 orang termasuk banyak anak-anak. Dalam konteks ini, cyber espionage tidak lagi sekadar menjadi aktivitas pencarian informasi, tetapi berpotensi berkontribusi terhadap penentuan sasaran operasi militer yang berdampak langsung terhadap keamanan manusia dan keselamatan warga sipil (Government of the United Kingdom, 2025). Oleh karena itu, konflik Rusia–Ukraina memperlihatkan bahwa nilai strategis espionage terletak pada kemampuannya menyediakan informasi yang dapat meningkatkan efektivitas operasi militer, memperkuat pengambilan keputusan, serta memperluas kemampuan negara dalam memahami dan mempengaruhi lingkungan konflik.

Dampak *Subversion* terhadap Persepsi Publik dan Ruang Informasi Ukraina

Praktik *subversion* yang dilakukan Rusia mulai dari adanya propaganda digital, disinformasi, bot farm, amplifikasi media sosial, hingga penggunaan teknologi *deepfake* menunjukkan bahwa ruang siber telah dimanfaatkan sebagai operasi strategis untuk mempengaruhi kondisi politik, sosial, dan psikologis selama konflik berlangsung. Sehingga

praktik yang dilakukan oleh Rusia ini menimbulkan dampak, seperti adanya penyebaran informasi palsu dan manipulasi narasi secara masif menimbulkan kebingungan informasi di tengah masyarakat, serta dapat memperlemah kemampuan publik dalam membedakan informasi yang benar dan salah. Kondisi ini berdampak pada menurunnya kepercayaan masyarakat terhadap media, pemerintah, dan sumber informasi resmi yang beredar selama perang berlangsung (Pownall et al., 2023). Dalam kondisi ini, ruang digital tidak hanya digunakan sebagai media komunikasi, tetapi juga sebagai arena untuk membentuk persepsi publik dan mengendalikan arus informasi selama konflik Rusia-Ukraina berlangsung.

Selain mempengaruhi masyarakat Ukraina, operasi disinformasi Rusia juga berdampak terhadap opini publik internasional. Penyebaran Narasi mengenai Ukraina sebagai negara yang dikuasai Neo-Nazi merupakan ancaman terhadap masyarakat berbahasa Rusia, serta Rusia juga memanfaatkan klaim bahwa adanya tindakan "denazifikasi" untuk membangun legitimasi politik atas invasi yang dilakukan Rusia (OECD, 2022). Penggunaan media digital, situs berita tiruan, dan akun palsu di media sosial juga memungkinkan propaganda tersebut sehingga bisa menjangkau audiens internasional lebih luas. Kondisi seperti ini menyebabkan meningkatnya polarisasi opini publik global karena masyarakat menerima informasi yang berbeda-beda mengenai konflik Rusia-Ukraina, sehingga menimbulkan perdebatan mengenai legitimasi perang, posisi Ukraina, dan keterlibatan negara-negara Barat dalam konflik tersebut (Meta, 2022).

Dampak lain dari praktik *subversion* dari Rusia juga terlihat pada meningkatnya kerentanan ruang informasi digital terhadap manipulasi teknologi penggunaan *deepfake,* bot farm, dan operasi informasi disinformasi secara terstruktur menunjukkan bahwa perkembangan teknologi digital dapat dimanfaatkan untuk memanipulasi informasi dan mempengaruhi persepsi publik di ruang digital. Dilihat dalam jangka panjang, kondisi seperti ini dapat menurunkan tingkat kepercayaan publik terhadap informasi digital secara umum, karena masyarakat menjadi semakin sulit membedakan antara informasi asli, propaganda, atau manipulasi digital (Pownall et al., 2023). Hal ini menunjukkan bahwa aktivitas ofensif tidak hanya menargetkan sistem teknologi atau infrastruktur digital di suatu negara, tetapi juga dapat menyerang psikologis dan sosial masyarakat melalui manipulasi informasi di ruang digital.

Berdasarkan hasil analisis, aktivitas ofensif Rusia dalam konflik Ukraina 2022 termanifestasi secara terintegrasi dalam tiga bentuk utama yang diklasifikasikan Thomas Rid. Sabotage dijalankan melalui wiper malware dan serangan terhadap infrastruktur komunikasi serta energi. Espionage dimanfaatkan untuk memperoleh informasi strategis yang mendukung keputusan operasional militer. Sementara subversion dilaksanakan melalui kampanye disinformasi, bot farm, dan deepfake untuk mempengaruhi persepsi publik. Dengan demikian, aktivitas ofensif Rusia menunjukkan bahwa ruang siber digunakan tidak hanya sebagai alat teknis, tetapi juga sebagai instrumen strategis untuk mendapatkan keunggulan militer, politik, dan informasi sekaligus.

KESIMPULAN

Berdasarkan argumen Thomas Rid, suatu tindakan baru dapat disebut sebagai perang apabila memenuhi tiga unsur sekaligus, yaitu violent, instrumental, dan political. Dalam konflik Rusia–Ukraina 2022, tindakan Rusia di ruang siber lebih tepat dipahami sebagai tiga bentuk

aktivitas ofensif, yaitu sabotage, espionage, dan subversion, karena tidak sepenuhnya memenuhi ketiga kriteria tersebut secara bersamaan. Rusia menyerang infrastruktur penting Ukraina melalui malware, menyebarkan propaganda dan disinformasi untuk mempengaruhi opini publik, serta mencuri informasi strategis pemerintah dan militer Ukraina.

Berdasarkan hasil analisis, bentuk-bentuk aktivitas ofensif Rusia dalam konflik Ukraina tahun 2022 dilakukan secara terintegrasi dan multidimensi sebagai bagian dari hybrid warfare. Menggunakan kerangka Thomas Rid, hal tersebut dijalankan melalui tiga bentuk utama, yaitu sabotage, espionage, dan subversion. Sabotage digunakan untuk melumpuhkan infrastruktur kritis dan kapasitas operasional Ukraina, espionage dimanfaatkan untuk memperoleh informasi strategis dan mendukung kepentingan intelijen, sedangkan subversion digunakan untuk membentuk opini publik melalui propaganda digital dan disinformasi. Namun, aktivitas ofensif ini tidak dirancang untuk berdiri sendiri atau memenangkan konflik secara mandiri. Serangan *HermeticWiper* sengaja diluncurkan tepat satu hari sebelum invasi, serta serangan terhadap satelit Viasat yang dieksekusi hanya satu jam sebelum serangan militer dimulai. Pola ini membuktikan fungsi instrumental siber yang terikat erat dengan lini waktu militer untuk melumpuhkan komunikasi dan administrasi pertahanan Ukraina sesaat sebelum pasukan darat, tank, dan rudal Rusia bergerak masuk. Dengan demikian, konflik ini menegaskan bahwa aktivitas ofensif tidak menggantikan perang konvensional, melainkan berfungsi sebagai instrumen pengganda kekuatan (force multiplier) modern yang terintegrasi penuh dalam mendukung strategi militer dan aktor politik negara secara masif, sebagaimana dijelaskan dalam batasan teori Thomas Rid (Rid, 2012).

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada kedua orang tua, teman-teman, serta seluruh dosen yang telah memberikan dukungan, motivasi, dan bantuan selama proses penelitian dan penulisan artikel ini. Secara khusus, penulis menyampaikan apresiasi kepada Ibu Fadhilah Permata Nira, S.IP.,MA selaku dosen pembimbing atas bimbingan, arahan, dan masukan yang sangat berharga dalam penyusunan artikel ini. Seluruh isi dan tanggung jawab dalam artikel ini sepenuhnya menjadi tanggung jawab penulis.

REFERENSI

Alexander Nastas, C. (2025, June). Justifying Invasion: A Case Study in Russian Propaganda. Retrieved from U.S. Naval Institute website: https://www.usni.org/magazines/proceedings/2025/june/justifying-invasion-case-study-russian-propaganda

Andres Guerrero-Saade , J., & van Amerongen, M. (2022, March 31). AcidRain | A Modem Wiper Rains Down on Europe. Retrieved from SentinelOne website: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

ANSSI. (2025). *TARGETING AND COMPRO- MISE OF FRENCH ENTITIES USING THE APT28 INTRUSION SET ACTIVITIES ASSOCIATED WITH APT28 SINCE 2021*. Retrieved from https://www.cert.ssi.gouv.fr/uploads/CERTFR-2025-CTI-007.pdf

Antoniuk, D. (2025, November 6). Russia's Sandworm hackers deploying wipers against Ukraine's grain industry. Retrieved from Therecord.media website: https://therecord.media/russia-sandworm-grain-wipers

Bachmann, S.-D., Putter, D., & Duczynski, G. (2023). Hybrid warfare and disinformation: A Ukraine war perspective. *Global Policy*, *14*(5). https://doi.org/10.1111/1758-5899.13257

Bateman, J. (2022). Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications. Retrieved from Carnegie Endowment for International Peace website: https://carnegieendowment.org/research/2022/12/russias-wartime-cyber-operations-in-ukraine-military-impacts-influences-and-implications

Bestari, N. P. (2022a, March 18). Mengenal Deepfake yang Minta Tentara Ukraina Buang Senjata. Retrieved June 1, 2026, from CNBC Indonesia website: https://www.cnbcindonesia.com/tech/20220318123220-37-323890/mengenal-deepfake-yang-minta-tentara-ukraina-buang-senjata

Bestari, N. P. (2022b, April 30). Terungkap, Cara Hacker Rusia Hancurkan Siber Ukraina. Retrieved from CNBC Indonesia website: https://www.cnbcindonesia.com/news/20220430134758-4-336211/terungkap-cara-hacker-rusia-hancurkan-siber-ukraina

Burrows, E. (2025, July 18). UK sanctions Russian officers over Mariupol theater bombing and targeting Sergei Skripal's family. Retrieved June 1, 2026, from AP News website: https://apnews.com/article/russia-military-intelligence-sabotage-cyber-attacks-2657fe4b54d93e35f30f4ce3fc2665cb

Burt, T. (2022, April 27). The hybrid war in Ukraine. Retrieved from Microsoft On the Issues website: https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

Calle, M. (2025, August 30). Cyber Warfare in Russo-Ukrainian War. Retrieved from International Relations Review website: https://www.irreview.org/articles/2025/8/28/cyber-warfare-in-russo-ukrainian-war

CyberPeace Institute. (2022). Case Study: Viasat Attack . Retrieved from Protect.ngo website: https://cyberconflicts.protect.ngo/law-and-policy/cases/viasat

Digital Forensic Research Lab. (2024, February 29). Undermining Ukraine: How Russia Widened Its Global Information War in 2023. Retrieved from Atlantic Council website: https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/

Field Effect Security Intelligence Team. (2025, May 22). Russian APT28 targets Western firms supporting Ukraine. Retrieved from Fieldeffect.com website: https://fieldeffect.com/blog/russian-apt28-targets-western-firms-supporting-ukraine

Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian Propaganda on Social Media during the 2022 Invasion of Ukraine. *EPJ Data Science*, *12*(1). https://doi.org/10.1140/epjds/s13688-023-00414-5

GOV.UK. (2025, December 4). Profile: GRU cyber and hybrid threat operations. Retrieved from https://www.gov.uk/government/publications/profile-gru-cyber-and-hybrid-threat-operations/profile-gru-cyber-and-hybrid-threat-operations

Khoirunnisa, K., & Sugiati, C. (2024). Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare. *Jurnal Public Policy*, *10*(2), 138. https://doi.org/10.35308/jpp.v10i2.9026

Lee, G. (2025, August 6). APT28 / Fancy Bear: Russian State Sponsored APT - Threat Actors. Retrieved from Daily Security Review website: https://dailysecurityreview.com/resources/threat-actors-resources/apt28-fancy-bear-russian-state-sponsored-apt/

Messieh, N. (2023, February 22). Narrative warfare. Retrieved from Atlantic Council website: https://www.atlanticcouncil.org/in-depth-research-reports/report/narrative-warfare/

Meta . (2022, November 22). Meta's Adversarial Threat Report, Third Quarter 2022. Retrieved from https://about.fb.com/news/2022/11/metas-adversarial-threat-report-q3-2022/

Microsoft Threat Intelligence. (2023). Cadet Blizzard muncul sebagai pelaku ancaman Rusia yang baru dan berbeda. Retrieved from Microsoft.com website: https://www.microsoft.com/id-id/security/security-insider/emerging-threats/cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor

Milmo, D. (2022, February 28). Facebook takes down Ukraine disinformation network and bans Russian-backed media. Retrieved from the Guardian website: https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram

Moore, D. (2022). Offensive Cyber Operations. Retrieved June 25, 2026, from Google Books website: https://books.google.com/books/about/Offensive_Cyber_Operations.html?id=8Jd8EAAAQBAJ

MSP Threats Security Team. (2022). WhisperGate malware targets Ukrainian government sites. Retrieved from Acronis website: https://www.acronis.com/en/tru/posts/whispergate-malware-targets-ukrainian-government-sites/

Mueller, G. B., Jensen, B., Valeriano, B., Maness, R. C., & Macias, J. M. (2023). Cyber Operations during the Russo-Ukrainian War. *Center for Strategic and International Studies*. Retrieved from https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war

North Atlantic Treaty Organization. (2016). Warsaw Summit Communiqué. Retrieved from NATO.int website: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

OECD. (2022). Disinformation and Russia's war of aggression against Ukraine. *OECD Policy Responses on the Impacts of the War in Ukraine, OECD Publishing*. https://doi.org/10.1787/37186bde-en

Ormrod, A., Ormrod, D., & Slay, J. (2023). Cyber Offensive Operations in Hybrid Warfare: Observations from the Russo-Ukrainian Conflict. *Journal of Information Warfare*, *22*(1), 76–87. JSTOR. https://doi.org/10.2307/27240856

Polegkyi, O. (2023). Russian disinformation and propaganda before and after the invasion of Ukraine. *Rocznik Instytutu Europy Środkowo-Wschodniej*, *21*(1), 91–107. https://doi.org/10.36874/riesw.2023.1.6

Proska, K., Wolfram, J., Wilson, J., Black, D., Lunden, K., Daniel Kapellmann Zafra, D., … Chris Sistrunk, C. (2023, November 9). Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Retrieved from Google Cloud Blog website: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/

Rapid7. (2022, March 4). Russia-Ukraine Cybersecurity Updates | Rapid7 Blog. Retrieved from Rapid7 website: https://www.rapid7.com/blog/post/2022/03/04/russia-ukraine-cybersecurity-updates/

Ribeiro, A., & Ribeiro, A. (2025, May 23). Russian GRU's Unit 26165 conducts two-year cyber espionage on logistics, tech firms using IP cameras, supply chains - Industrial Cyber. Retrieved from Industrial Cyber website: https://industrialcyber.co/cisa/russian-grus-unit-26165-conducts-two-year-cyber-espionage-on-logistics-tech-firms-using-ip-cameras-supply-chains/

Rid, T. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Shao, C., Ciampaglia, G. L., Varol, O., Yang, K.-C., Flammini, A., & Menczer, F. (2018). The spread of low-credibility content by social bots. *Nature Communications*, *9*(1). https://doi.org/10.1038/s41467-018-06930-7

Stockley, M. (2022, June 12). Russia's APT28 uses fear of nuclear war to spread Follina docs in Ukraine. Retrieved from Malwarebytes website: https://www.malwarebytes.com/blog/threat-intel/2022/06/russias-apt28-uses-fear-of-nuclear-war-to-spread-follina-docs-in-ukraine

Twomey, J. G., Ching, D., Aylett, M. P., Quayle, M., Linehan, C., & Murphy, G. (2023). Do deepfake videos undermine our epistemic trust? A thematic analysis of tweets that discuss deepfakes in the Russian invasion of Ukraine. *PubMed*, *18*(10), e0291668–e0291668. https://doi.org/10.1371/journal.pone.0291668

Unit 42. (2023, December 7). Fighting Ursa Aka APT28: Illuminating a Covert Campaign. Retrieved from Unit 42 website: https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/

United States Department of State. (2023, March 23). Disinformation Roulette: The Kremlin's Year of Lies to Justify an Unjustifiable War - United States Department of State. Retrieved from https://2021-2025.state.gov/disarming-disinformation/disinformation-roulette-the-kremlins-year-of-lies-to-justify-an-unjustifiable-war/

Upadhyay, D., & Sampalli, S. (2020). SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. *Computers & Security*, *89*, 101666. https://doi.org/10.1016/j.cose.2019.101666

Willett, M. (2022). The Cyber Dimension of the Russia–Ukraine War. *Survival*, *64*(5), 7–26. https://doi.org/10.1080/00396338.2022.2126193