BAB II

DINAMIKA PERANG SIBER RUSIA-UKRAINA HINGGA KEMUNCULAN NORTH ATLANTIC FELLA ORGANIZATION (NAFO)

2.1 Perang Siber antara Rusia dengan Ukraina

Dalam memahami kemunculan serta peran NAFO sebagai aktor non-negara dalam perang informasi Rusia-Ukraina, penting untuk terlebih dahulu meninjau latar belakang dan sejarah panjang dari perang siber yang berlangsung antara kedua negara tersebut. Perang siber antara Rusia dan Ukraina bukanlah fenomena yang tiba-tiba muncul pada saat invasi militer besar-besaran tahun 2022 lalu. Sebaliknya, ia merupakan bagian dari konflik yang telah berlangsung lama, bahkan sebelum aneksasi Krimea oleh Rusia pada tahun 2014.

2.1.1 Akar Awal Konflik Siber

Perang siber antara Rusia dan Ukraina memiliki akar historis yang dalam, jauh sebelum eskalasi militer pada 2022. Apabila dilacak jauh, hubungan kedua negara telah diliputi ketegangan sejak runtuhnya Uni Soviet pada 1991. Setelah kemerdekaannya, Ukraina mewarisi banyak infrastruktur ekonomi dan digital yang sebelumnya dikontrol secara terpusat dari Moskow, menciptakan ketergantungan besar terhadap sistem komunikasi, energi, dan keamanan siber Rusia. Kondisi ini membuka peluang bagi Rusia untuk melakukan berbagai infiltrasi ke jaringan informasi Ukraina, baik untuk tujuan intelijen maupun manipulasi politik jangka panjang.

Pada awal 2000-an, perang siber belum begitu diperhitungkan sebagai ancaman strategis. Namun, seiring waktu, Rusia mulai mengembangkan dan menggunakan teknik-teknik siber, terutama sebagai instrumen propaganda dan disinformasi untuk memperkuat pengaruh politiknya di negara-negara bekas Uni Soviet, termasuk Ukraina. Salah satu strategi yang dominan digunakan adalah memanfaatkan jaringan *troll*, *bot*, serta media sosial untuk menyebarkan narasi politik pro-Kremlin dan melemahkan integritas informasi publik di Ukraina.

Menurut Munk (2024), sejak sebelum 2014, Rusia sudah menggunakan berbagai bentuk propaganda daring, serangan siber, serta manipulasi informasi untuk mengontrol persepsi masyarakat Ukraina dan global tentang hubungan kedua negara. Rusia secara aktif membangun narasi palsu yang menggambarkan Ukraina sebagai negara yang lemah, korup, dan cenderung ke arah ekstremisme, yang digunakan sebagai pembenaran tindakan-tindakan politik dan militer berikutnya. Praktik ini kemudian semakin intensif menjelang dan setelah Revolusi Euromaidan (2013-2014), ketika rakyat Ukraina menggulingkan pemerintahan Viktor Yanukovych yang pro-Rusia dan menuntut pendekatan yang lebih dekat dengan Barat (Tejasuar & Hanura, 2022).

Selain memanfaatkan media sosial dan jaringan *troll*, Rusia juga terlibat dalam serangkaian operasi siber untuk melemahkan institusi strategis Ukraina. Bahkan sebelum invasi Krimea tahun 2014, institusi

Ukraina seperti bank, media, serta lembaga pemerintah sering mengalami serangan siber berskala kecil hingga menengah berupa gangguan layanan (*Distributed Denial of Service/DDoS*) atau infiltrasi sistem yang menyebabkan kerugian finansial dan hilangnya kepercayaan publik terhadap institusi tersebut. Serangan ini tidak sekadar bertujuan sabotase, tetapi juga sebagai bagian dari upaya sistematis melemahkan kapasitas pertahanan digital Ukraina, sebagai persiapan serangan-serangan besar berikutnya.

Periode sebelum invasi Krimea pada tahun 2014 merupakan fase kritis dalam sejarah konflik siber ini, ketika Ukraina mulai menyadari pentingnya memperkuat kapasitas pertahanan siber nasionalnya. Sebagai respons terhadap ancaman ini, Ukraina mulai berusaha membangun pertahanan digital yang melibatkan aktor negara maupun non-negara. Dalam periode tersebut, strategi Rusia beralih dari pendekatan pasif menjadi aktif dalam perang informasi, di mana manipulasi opini publik melalui berita palsu, meme, dan kampanye digital yang agresif menjadi metode utama. Perang informasi secara bertahap berkembang menjadi salah satu elemen penting dari keseluruhan konflik antara Rusia dan Ukraina, yang kemudian menjadi sangat jelas ketika konflik meletus secara militer pada 2014.

Narasi sejarah ini menunjukkan bahwa akar perang siber Rusia-Ukraina berawal jauh sebelum invasi Krimea, dengan manipulasi informasi dan infiltrasi digital yang telah menjadi bagian dari hubungan

kedua negara selama bertahun-tahun. Pemahaman akan konteks historis ini penting untuk menjelaskan kemunculan aktor-aktor baru, seperti komunitas NAFO, yang berperan dalam melawan narasi dominan Rusia di ruang siber selama invasi besar-besaran yang terjadi kemudian.

2.1.2 Tahun 2014: Titik Balik Eskalasi Siber

Invasi Rusia ke Krimea pada Februari-Maret 2014 menjadi momentum penting dalam sejarah konflik siber berskala internasional. Invasi ini tidak hanya menandai eskalasi konflik militer tradisional antara Rusia dan Ukraina, tetapi juga menampilkan secara nyata bagaimana dunia siber dimanfaatkan secara efektif sebagai medan perang baru oleh Rusia untuk mencapai tujuan politik dan militer strategisnya. Berbagai operasi siber yang kompleks diluncurkan oleh Rusia sebelum, selama, dan setelah proses pendudukan Krimea, sebagai bagian integral dari strategi "*hybrid warfare*" yang kemudian banyak diteliti oleh pakar keamanan internasional.

Andrew Jenkinson (2023) menguraikan bahwa serangan siber Rusia pada 2014 diatur secara sistematis, bukan tindakan impulsif atau spontan. Menurutnya, Rusia telah sejak lama menanam *malware* canggih seperti BlackEnergy dan Sandworm ke dalam sistem infrastruktur vital Ukraina, yang bertujuan jangka panjang untuk melemahkan kapasitas pertahanan digital negara ini. BlackEnergy, misalnya, mulai terdeteksi secara intensif menjelang akhir 2013 dan awal 2014, ketika Ukraina dilanda ketegangan politik akibat Revolusi Euromaidan. Malware ini

digunakan untuk menginfiltrasi dan mengganggu sistem perbankan, pemerintahan, serta media Ukraina. Jenkinson juga mencatat bahwa Sandworm secara efektif berhasil menyerang infrastruktur kritis, seperti jaringan listrik Ukraina, meski dampak terbesarnya baru terasa setahun kemudian pada serangan pemadaman listrik 2015.

Serangan-serangan awal ini menunjukkan pola yang jelas: Rusia secara metodis melemahkan ketahanan sistem digital Ukraina sebelum tindakan militer nyata di lapangan dimulai. Invasi Krimea sendiri disertai dengan kampanye disinformasi masif, yang menggunakan berbagai platform digital untuk menyebarkan narasi palsu yang mendukung intervensi militer Rusia. Menurut Tine Munk (2024), Rusia secara agresif memanipulasi media sosial dengan menggunakan jaringan *troll*, akun *bot*, dan situs berita palsu yang pro-Kremlin. Narasi utama propaganda ini menggambarkan pemerintahan baru Ukraina sebagai hasil kudeta ilegal yang didukung oleh kelompok neo-Nazi ekstremis yang didanai Barat, sehingga memberi legitimasi moral bagi Rusia untuk "melindungi" populasi berbahasa Rusia di Krimea.

Kampanye propaganda digital Rusia juga bertujuan menciptakan kebingungan, mengurangi kepercayaan publik, serta perpecahan internal di antara warga Ukraina, sehingga melemahkan respons efektif pemerintah Ukraina terhadap invasi Krimea. Operasi-operasi ini terbukti berhasil dalam menciptakan kebingungan informasi, yang memperlambat respons pemerintah dan meningkatkan ketidakpastian

masyarakat tentang situasi sebenarnya di lapangan. Jenkinson (2023) menyebutkan bahwa operasi siber yang dilancarkan Rusia di Krimea merupakan gabungan yang canggih antara operasi intelijen digital, sabotase infrastruktur, serta *psy-ops* (operasi psikologis) yang bertujuan melemahkan moral nasional.

Di sisi lain, invasi Krimea 2014 juga mendorong respons aktif dari warga sipil Ukraina secara spontan melalui internet. Seperti diungkapkan oleh Tine Munk (2024), warga Ukraina mulai menggunakan meme sebagai bentuk perlawanan terhadap dominasi narasi Rusia. Meme menjadi alat ekspresi politik, protes kreatif, serta sarana menyatukan solidaritas masyarakat sipil yang merasa tidak memiliki cukup kekuatan untuk melawan agresi militer secara langsung. Meme seperti "Putin Khuilo" (Putin Idiot) muncul dan viral di berbagai platform, menjadi ekspresi populer perlawanan masyarakat sipil Ukraina terhadap pendudukan Rusia. Dalam konteks ini, perang siber mulai menampilkan bentuk baru dari perang informasi yang tidak hanya dilakukan negara, tetapi juga melibatkan partisipasi spontan warga sipil sebagai aktor non-negara dalam perjuangan mereka.

Operasi-operasi siber dan disinformasi yang terjadi di Krimea pada 2014 juga memberi pelajaran penting bagi komunitas internasional tentang efektivitas *hybrid warfare* Rusia. Dampak nyata dari perang siber ini menegaskan bahwa ancaman terhadap negara tidak lagi hanya bersifat fisik, tetapi juga digital dan psikologis. Menurut Jenkinson (2023),

serangan di Krimea merupakan salah satu contoh paling awal di mana operasi siber secara efektif menjadi bagian integral dari strategi militer Rusia, digunakan secara sengaja untuk melemahkan kemampuan lawan sebelum konflik fisik dimulai.

Peristiwa ini juga menandai pergeseran paradigma perang modern, dari yang semula hanya fokus pada medan tempur fisik menjadi medan tempur digital yang sama pentingnya. Ukraina, yang sebelumnya kurang siap dalam menghadapi serangan siber berskala masif ini, segera mulai meningkatkan pertahanan digital nasionalnya. Ukraina mulai bekerja sama dengan berbagai komunitas internasional, perusahaan teknologi global, serta mengembangkan berbagai kebijakan keamanan siber untuk merespons ancaman digital yang semakin meningkat.

2.1.3 Eksperimen dan Intensifikasi Serangan (2015-2021)

Periode tahun 2015 hingga 2021 merupakan fase penting dalam evolusi konflik siber antara Rusia dan Ukraina, di mana Rusia secara nyata mulai bereksperimen dengan melancarkan serangan siber berskala besar dan terorganisir. Serangkaian operasi siber yang diluncurkan selama periode ini memperlihatkan bahwa Rusia tidak sekadar menguji kemampuan teknisnya, melainkan secara strategis menggunakan serangan digital sebagai bagian dari kampanye politik dan militer yang lebih luas terhadap Ukraina.

Menurut Andrew Jenkinson (2023), tahun 2015 menjadi titik awal serangan yang lebih canggih dan destruktif oleh Rusia, terutama dengan

serangan terhadap jaringan energi nasional Ukraina. Pada Desember 2015, *malware* BlackEnergy yang sebelumnya telah disisipkan dalam infrastruktur digital Ukraina digunakan secara efektif untuk melumpuhkan sistem listrik, menyebabkan pemadaman besar-besaran di wilayah Ivano-Frankivsk, dengan lebih dari 230.000 warga kehilangan akses listrik selama berjam-jam. Serangan ini menjadi peristiwa bersejarah dalam perang siber karena untuk pertama kalinya dalam sejarah, suatu negara berhasil menggunakan serangan siber untuk mematikan secara fisik infrastruktur vital negara lain. Menurut Jenkinson, serangan ini tidak hanya bertujuan sabotase, tetapi juga memiliki tujuan psikologis untuk menurunkan moral nasional serta mengintimidasi pemerintah Ukraina.

Setelah keberhasilan BlackEnergy pada 2015, Rusia semakin berani dalam mengembangkan operasi-operasi siber lanjutan. Serangan yang paling terkenal terjadi adalah pada Juni 2017 dengan kemunculan *malware* NotPetya, yang mulanya menyamar sebagai *ransomware* tetapi sebenarnya dirancang untuk menghancurkan data tanpa kemungkinan pemulihan. NotPetya menyebar dari Ukraina ke berbagai perusahaan multinasional seperti Maersk, Merck, dan FedEx, menyebabkan kerugian ekonomi global sebesar lebih dari 10 miliar dolar AS (Jenkinson, 2023). Serangan ini kembali membuktikan bahwa Ukraina bukan hanya target utama dari agresi siber Rusia, tetapi juga menjadi "laboratorium" di mana

Rusia bereksperimen dengan berbagai teknik perang siber yang kelak bisa digunakan terhadap negara lain.

Selain serangan teknis yang destruktif, Rusia juga mengintensifkan penggunaan propaganda digital dan kampanye disinformasi selama periode ini. Tine Munk (2024) mencatat bahwa antara 2015 hingga 2021, Rusia semakin masif memanfaatkan media sosial, *bot*, *troll farms*, serta jaringan influencer digital untuk menyebarkan narasi palsu tentang Ukraina. Narasi yang disebarluaskan melalui operasi ini antara lain menggambarkan Ukraina sebagai negara gagal, dikuasai kelompok radikal, serta rezim boneka Barat yang tidak memiliki legitimasi politik. Kampanye ini bertujuan melemahkan kredibilitas pemerintah Ukraina baik di dalam maupun luar negeri, sekaligus melemahkan solidaritas internasional terhadap perjuangan Ukraina.

Operasi siber yang dijalankan oleh Rusia dalam periode ini juga semakin canggih secara teknis. Menurut analisis Jenkinson (2023), kelompok peretas Rusia seperti Sandworm Group dan Fancy Bear (APT28) mulai secara intensif bereksperimen dengan berbagai teknik baru, seperti *advanced persistent threats* (APT), *zero-day exploits*, serta serangan terhadap *supply-chain* (rantai pasokan). Serangan *supply-chain* yang menargetkan *software* akuntansi Ukraina, M.E.Doc, dalam kasus NotPetya menjadi contoh nyata bagaimana Rusia menggunakan teknik

infiltrasi secara diam-diam melalui perangkat lunak yang secara luas digunakan oleh berbagai instansi strategis.

Menanggapi ancaman ini, Ukraina pun secara aktif memperkuat pertahanan sibernya dengan melibatkan komunitas internasional, NATO, dan perusahaan teknologi global. Menurut Munk (2024), perang siber yang semakin intens ini turut memicu munculnya respons dari masyarakat sipil, terutama dalam bentuk perlawanan kreatif melalui meme di media sosial. Warga Ukraina secara aktif mulai menggunakan meme sebagai alat kritik dan perlawanan terhadap propaganda Rusia. Meme juga menjadi bagian penting dari upaya masyarakat sipil dalam membangun narasi alternatif dan menjaga moral nasional, khususnya dalam kondisi tekanan politik dan sosial yang tinggi.

Dari sudut pandang strategis, eksperimen Rusia selama periode 2015 - 2021 menunjukkan bagaimana operasi siber digunakan tidak hanya sebagai senjata teknis, tetapi juga sebagai instrumen politik yang bertujuan melemahkan negara lawan secara internal, menciptakan polarisasi sosial, serta mengurangi dukungan internasional terhadap Ukraina. Eksperimen Rusia ini terbukti efektif dalam merusak kepercayaan publik terhadap pemerintah Ukraina, sekaligus menunjukkan potensi perang siber sebagai ancaman keamanan global yang nyata dan serius (Jenkinson, 2023).

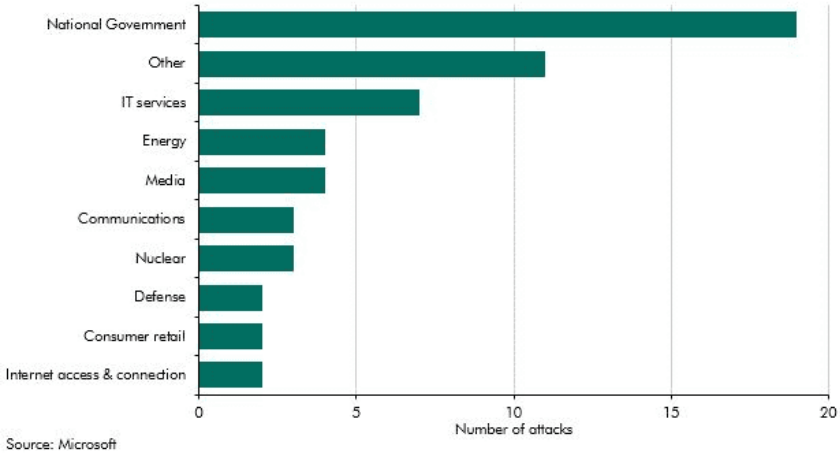
Pada saat yang sama, Ukraina juga mulai menyadari pentingnya perang informasi sebagai arena strategis dalam konflik modern.

Pemerintah Ukraina mulai secara aktif menggunakan media sosial dan meme sebagai instrumen kontra-propaganda, sementara warga sipil secara organik membentuk komunitas-komunitas daring yang secara spontan mendukung perjuangan negara mereka di dunia digital. Fenomena ini merupakan bentuk perlawanan sipil modern yang mengandalkan platform digital sebagai medium utama perjuangan politik, sekaligus memperkenalkan konsep *memetic warfare* sebagai bentuk baru dari perlawanan masyarakat terhadap agresi digital negara lain.

2.1.4 Invasi Tahun 2022 dan Eskalasi Perang Informasi Digital

Invasi militer Rusia terhadap Ukraina pada 24 Februari 2022 menjadi puncak eskalasi konflik siber yang telah berlangsung bertahun-tahun antara kedua negara. Sejak hari-hari pertama invasi, Rusia mengintegrasikan serangan siber berskala besar dengan serangan militer konvensionalnya. Berbeda dengan invasi Krimea 2014, invasi tahun 2022 memperlihatkan skala yang jauh lebih masif, dengan berbagai serangan digital yang secara simultan menargetkan layanan pemerintah, infrastruktur kritis, sistem komunikasi, layanan perbankan, hingga media

nasional Ukraina sebagaimana dicatatkan oleh grafik 2.1 yang memuat laporan Microsoft di bulan April tahun 2022.



Grafik 2.1 Sektor yang terdampak dari serangan siber Rusia sejak invasi di tahun 2022
Sumber: Microsoft, 2022

Andrew Jenkinson (2023) mencatat bahwa Rusia melancarkan gelombang serangan DDoS (Distributed Denial of Service) masif sejak beberapa hari sebelum invasi dimulai. Serangan ini melumpuhkan situs-situs pemerintah, bank-bank besar seperti PrivatBank dan Oschadbank, serta layanan komunikasi penting yang menyebabkan kepanikan publik dan gangguan signifikan terhadap pelayanan publik Ukraina. Dalam beberapa kasus, serangan ini juga disertai infiltrasi sistem yang bertujuan mencuri data sensitif, menghapus database penting, serta menciptakan kerusakan permanen pada berbagai sistem teknologi informasi negara

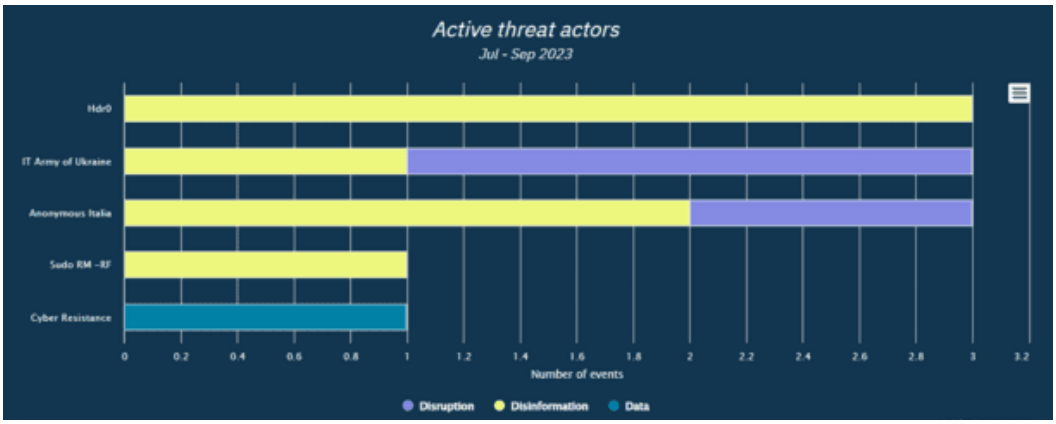
Selain serangan DDoS, Rusia juga menggunakan malware penghapus data (wiper malware) seperti HermeticWiper, WhisperGate, dan CaddyWiper yang ditemukan oleh perusahaan keamanan siber global pada awal invasi. Malware-malware ini secara sengaja dirancang untuk

menghancurkan sistem data tanpa peluang pemulihan, menyebabkan hilangnya informasi sensitif milik pemerintah, bank, serta institusi strategis lainnya. HermeticWiper, misalnya, terdeteksi pada 23 Februari 2022 yang hanya beberapa jam sebelum invasi militer dimulai telah terjadi kerusakan data yang parah pada berbagai instansi pemerintah Ukraina (Jenkinson, 2023).

Sebagai respons, Ukraina juga melancarkan berbagai bentuk serangan balik digital yang efektif. Pemerintah Ukraina secara resmi melibatkan komunitas siber internasional, khususnya kelompok *hacker* global seperti Anonymous yang secara terbuka menyatakan "perang siber" terhadap Rusia sejak awal invasi. Dalam beberapa hari pertama invasi, Anonymous berhasil melumpuhkan atau merusak ratusan situs pemerintah Rusia, termasuk website resmi Kremlin, Kementerian Pertahanan Rusia, serta berbagai situs media pemerintah seperti Russia Today (RT) dan Sputnik. Selain itu, mereka juga membocorkan data sensitif dari lembaga pemerintah Rusia ke publik secara *online* sebagai bentuk dukungan terhadap Ukraina (Jenkinson, 2023).

Selain melibatkan aktor internasional, pemerintah Ukraina melalui unit sibernya juga aktif dalam serangan siber ofensif. Menurut Jenkinson (2023), Ukraina mengembangkan strategi pertahanan yang disebut "IT Army of Ukraine," yakni sebuah komunitas digital yang didirikan oleh pemerintah Ukraina dan terdiri dari para sukarelawan IT dan keamanan siber global untuk melawan Rusia di ruang digital. IT

Army of Ukraine bertanggung jawab atas berbagai serangan balasan yang menargetkan infrastruktur digital Rusia, termasuk bank, perusahaan teknologi, platform transportasi publik, serta media massa pro-pemerintah. Berdasarkan laporan analisis di grafik 2.2 oleh Cyber Peace Institute bulan Juli hingga September 2023, terdapat 13 insiden serangan siber yang ditujukan kepada negara Rusia, tiga insiden di antaranya diidentifikasi dilakukan oleh IT Army of Ukraine.



Grafik 2.2 Aktor Pro-Ukraina yang melakukan serangan terhadap Rusia di bulan Juli-September 2023
Sumber: (Cyber Peace Institute, 2023)

Di samping serangan teknis, kampanye disinformasi berskala besar juga dijalankan secara bersamaan oleh Rusia. Narasi sentral yang berusaha diangkat dalam kampanye disinformasi ini adalah menggambarkan Ukraina sebagai negara yang dikuasai kelompok ekstremis neo-Nazi yang menindas minoritas Rusia, dan menuduh Barat, khususnya NATO dan Amerika Serikat sebagai penghasut konflik bersenjata di dunia. Narasi ini secara strategis digunakan untuk memberikan legitimasi moral atas tindakan militer Rusia dengan dalih "membebaskan" Ukraina dari dominasi kelompok ekstremis. Kampanye

ini dijalankan secara intensif melalui media sosial seperti Telegram, Facebook, Twitter, TikTok, serta kanal propaganda resmi Kremlin seperti RT dan Sputnik, yang menyebarkan berbagai konten seperti video palsu, gambar yang dimanipulasi, serta berita bohong.

Sebagai sebuah contoh, di bulan Maret 2022, sebuah video palsu yang dibuat dengan teknologi *deepfake* menunjukkan Presiden Volodymyr Zelenskyy yang menyerukan tentara Ukraina untuk menyerah tersebar hingga viral di media sosial. Walaupun video ini berhasil diklarifikasi dan dibantah oleh pemerintah Ukraina dengan cepat, insiden tersebut menunjukkan bagaimana Rusia menggunakan kombinasi teknologi dan manipulasi digital untuk menciptakan kebingungan, melemahkan moral tentara dan masyarakat Ukraina, serta menciptakan disorientasi informasi global (Munk, 2024).

Tidak tinggal diam, Ukraina juga melancarkan perang informasi digital sebagai bagian dari strategi pertahanannya. Berbeda dengan narasi Rusia, narasi Ukraina yang disebarluaskan melalui platform digital berusaha menggambarkan negara ini dengan simbol heroisme, perlawanan, demokrasi, dan kebebasan yang sedang melawan agresi otoriter Rusia. Melalui akun resmi lembaga pemerintah seperti Kementerian Pertahanan Ukraina di X, Ukraina secara aktif menyebarkan meme, video heroik, cerita keberanian sipil, serta mengabadikan momen-momen perlawanan sipil yang kemudian terkenal

seperti peristiwa Pulau Ular atau Snake Island, di mana prajurit Ukraina menolak menyerah kepada kapal perang Rusia.

Selain itu, narasi heroisme Ukraina diperkuat dengan penggunaan media sosial oleh presidennya sendiri, yakni Volodymyr Zelenskyy yang aktif dalam menyampaikan pesan secara langsung kepada masyarakat global melalui video-video pendek di Instagram dan X. Berbagai unggahannya menunjukkan bahwa ia berusaha membangun citra diri sebagai pemimpin yang sederhana namun memiliki keberanian. Tentu hal ini ia lakukan untuk menarik simpati publik internasional, menciptakan kontras tajam dengan propaganda Rusia yang menggambarkan pemerintahan Zelensky sebagai pemerintahan yang pengecut dan lawak.

Intensifikasi perang informasi digital juga memaksa Ukraina untuk merespons melalui penguatan strategi komunikasi digitalnya. Pemerintah Ukraina dengan cepat memanfaatkan media sosial untuk melawan propaganda Rusia, menyediakan informasi *real-time* yang akurat, serta memastikan bahwa disinformasi yang disebarkan Rusia dapat dengan segera diklarifikasi. Akun-akun media sosial resmi pemerintah Ukraina secara aktif digunakan untuk menyebarluaskan narasi tandingan dan memerangi penyebaran hoaks dari pihak Rusia.

Respons Ukraina terhadap perang informasi juga melibatkan elemen sipil secara spontan yang mendukung narasi heroisme tersebut. Menurut penilaian Munk (2024), rakyat Ukraina berperan aktif dalam

menyebarkan cerita dan video nyata tentang perlawanan mereka terhadap Rusia, yang secara efektif melemahkan propaganda Rusia sekaligus memperkuat solidaritas global terhadap perjuangan Ukraina. Fenomena ini menunjukkan bahwa serangan misinformasi dan disinformasi Rusia mendapatkan upaya perlawanan yang tidak kalah masif dan cukup terkoordinasi dari warga sipil Ukraina sendiri.

2.1.5 Munculnya Aktor Non-Negara dalam Ranah Siber: NAFO dan Gerakan Global

Konflik siber antara Rusia dan Ukraina tidak hanya melibatkan aktor negara, tetapi juga menarik perhatian dan partisipasi aktif dari berbagai aktor non-negara dalam arena digital. Invasi Rusia ke Ukraina pada tahun 2022 mempercepat munculnya aktor-aktor baru ini, baik dari kalangan komunitas siber global, peretas independen, maupun kelompok aktivis yang secara sukarela terlibat dalam perang informasi. Kehadiran mereka memperlihatkan bahwa konflik modern telah berubah secara signifikan, di mana masyarakat sipil dan aktor non-negara memiliki peran sentral dalam mempengaruhi dinamika perang informasi.

Sebelumnya, telah disebutkan tentang kelompok Anonymous dan Ukrainian IT Army, yang merupakan aktor non-negara yang membantu Ukraina dalam melancarkan operasi siber terhadap Rusia. Sementara, pihak pro-Rusia juga memiliki aktor non-negara pula seperti Killnet dan XakNet untuk mengimbangi dukungan global Ukraina. Kedua kelompok ini melakukan serangan terhadap infrastruktur digital negara-negara yang

memberikan dukungan kepada Ukraina, seperti Amerika Serikat, Inggris, dan negara-negara NATO. Melalui platform Telegram, Killnet secara terbuka mengklaim bertanggung jawab atas berbagai serangan terhadap infrastruktur digital yang mereka lancarkan terhadap negara-negara Barat. Hal tersebut mereka lakukan sebagai bentuk protes terhadap apa yang mereka anggap sebagai dukungan agresif Barat terhadap Ukraina (Jenkinson, 2023).

Di samping kelompok peretas, perang informasi ini juga menampilkan peran penting dari kelompok sipil yang secara spontan terbentuk di media sosial, salah satunya adalah komunitas North Atlantic Fella Organization (NAFO). Berbeda dengan Anonymous yang lebih teknis dalam serangannya, NAFO menggunakan meme dan humor sarkastik sebagai senjata untuk melawan propaganda Rusia di media sosial. Kehadiran NAFO mencerminkan fenomena baru di mana masyarakat sipil global menggunakan media sosial sebagai sarana perlawanan narasi secara aktif, terkoordinasi, dan efektif (Munk, 2024). NAFO bisa menciptakan narasi tandingan terhadap disinformasi Rusia dengan cara-cara yang kreatif, yang pada akhirnya membantu membangun solidaritas internasional terhadap Ukraina.

Kemunculan berbagai aktor non-negara ini menunjukkan bahwa perang siber Rusia-Ukraina telah menjadi fenomena global yang melibatkan berbagai lapisan masyarakat, tidak lagi terbatas pada militer resmi dan institusi negara. Dalam konflik ini, aktor non-negara

menunjukkan kemampuan signifikan dalam mempengaruhi narasi global, membantu mempertahankan integritas informasi, sekaligus menandai pergeseran signifikan dalam bentuk-bentuk perjuangan politik modern. Fenomena ini sekaligus memperlihatkan tantangan baru dalam studi hubungan internasional dan keamanan global, yakni bagaimana masyarakat sipil dapat secara efektif terlibat dalam konflik geopolitik melalui arena digital.

2.2 Struktur dan Organisasi NAFO

North Atlantic Fella Organization (NAFO) adalah komunitas berbasis internet yang awalnya terbentuk secara spontan sebagai reaksi terhadap invasi militer Rusia ke Ukraina pada tahun 2022. Organisasi ini berawal dari fenomena meme internet, khususnya sebagai bentuk pelesetan dari NATO (North Atlantic Treaty Organization), dengan tujuan menyindir sekaligus memberikan dukungan terhadap Ukraina. Ikon meme yang menjadi identitas NAFO adalah anjing Shiba Inu, yang dipilih secara humoris untuk merepresentasikan kelompok ini. Istilah “Fella” sendiri merupakan istilah gaul dari “fellow” yang merujuk pada persahabatan atau solidaritas dengan Ukraina.

Menurut Tine Munk (2024), kemunculan NAFO menandai perkembangan baru dalam konteks perang siber dan informasi digital, di mana aktor non-negara secara terorganisir mengambil peran penting dalam mempengaruhi persepsi publik global melalui media sosial. NAFO pada mulanya merupakan komunitas daring yang terdesentralisasi dan terbentuk

secara organik, yang kemudian berkembang menjadi gerakan media sosial yang cukup terstruktur, dengan aktivitas utamanya meliputi produksi dan distribusi meme politik untuk melawan narasi propaganda Rusia. NAFO dapat digambarkan sebagai kelompok non-kombatan yang bertempur menggunakan *keyboard* dari rumah mereka dan bertindak secara independen untuk mendorong berlanjutnya perang sekaligus menyebarkan ketakutan kepada para pengguna internet lain, khususnya terhadap musuh mereka.

NAFO mulai dikenal secara global setelah meme yang mereka produksi viral di berbagai platform media sosial seperti Twitter (X), Reddit, Discord, dan Facebook. Meme-meme ini biasanya berupa humor sarkastik atau satir politik yang ditujukan untuk merendahkan citra militer Rusia serta mempertanyakan kredibilitas narasi yang dibangun oleh Kremlin tentang invasi ke Ukraina. Menurut Jenkinson (2023), kemampuan NAFO untuk memanfaatkan meme sebagai alat propaganda tandingan membuat organisasi ini berhasil mendapatkan perhatian luas dari komunitas internasional, termasuk mendapat liputan dari media besar seperti The Economist, yang menyoroti efektivitas NAFO dalam perang informasi.

NAFO merupakan komunitas dengan keanggotaan yang bebas dan ini memungkinkan anggotanya yang berasal dari berbagai negara untuk bergabung dengan mudah dan cepat dalam melakukan koordinasi secara daring. Di *platform* media sosial X, NAFO tercatat diikuti oleh sebanyak 118 ribu pengguna, sementara di *platform* Discord, mereka memiliki anggota sebanyak 6.942 pengguna. Hal tersebut dikarenakan karakteristik lingkungan digital

yang berisi kelompok/individu yang berasal dari luar Ukraina, bukan hanya warga Ukraina itu sendiri saja. Maka dari itu juga, latar belakang anggota NAFO juga sangat beragam, mulai dari pengguna media sosial biasa, *influencer* digital, hingga individu yang ahli dalam desain grafis, keamanan siber, dan komunikasi politik (Munk, 2024). Selain itu, individu-individu di balik NAFO kebanyakan menggunakan bahasa Inggris, baik itu untuk berkomunikasi maupun membuat meme. Pemilihan bahasa ini berkontribusi juga pada kemampuan mereka untuk menjangkau audiens yang lebih luas, mengingat bahasa Inggris merupakan salah satu bahasa yang sering digunakan, sehingga pesan yang ingin disampaikan dalam meme dapat dipahami dengan lebih mudah (Johais & Meis, 2024). Tidak ada hirarki formal yang ketat di dalam NAFO, namun setiap anggota dapat berkontribusi dengan bebas dalam memproduksi atau menyebarkan meme.

Gambar 2.3 Profil X NAFO
Sumber: (@Official_NAFO, 2025)

Salah satu aspek penting dalam sejarah perkembangan NAFO adalah bagaimana organisasi ini secara konsisten mengeksploitasi momen-momen penting dalam konflik Rusia-Ukraina untuk memperkuat narasi tandingan. Misalnya, ketika Ukraina melakukan serangan balik atau berhasil merebut kembali wilayah yang sempat diduduki Rusia, meme dari NAFO segera tersebar secara luas untuk mempromosikan kemajuan Ukraina sekaligus mengejek kegagalan militer Rusia. Dengan cara ini, NAFO turut berperan dalam mempengaruhi opini publik global dengan menampilkan narasi alternatif yang menguntungkan bagi Ukraina.

Munculnya NAFO dalam perang siber Rusia-Ukraina menunjukkan pergeseran signifikan dalam dinamika perang modern, di mana aktor non-negara menggunakan teknologi dan media sosial untuk memainkan peran aktif dalam peperangan informasi, sekaligus menjadi contoh nyata bagaimana budaya internet, yakni meme dapat digunakan secara efektif sebagai alat politik dalam konflik internasional kontemporer.