NATO Foundation
Defense College

The Russian-Ukrainian conflict as a real-time Internet War (I Part)

Fabio Vanorio

Senior Executive, Italian Ministry of Foreign Affairs and International Cooperation

NATO Defense College Foundation Paper

**DISCLAIMER: views in this paper are expressed in a personal capacity and are in no way attributable to the Italian Ministry of Foreign Affairs and International Cooperation.*

In contrast to the first Gulf War (described as the first to take place in real-time on the mass media), the conflict in Ukraine is the first that is taking place in real-time on the Internet. In a series of briefings, we will illustrate how each technology defined within the so-called "Fourth Industrial Revolution" plays a primary and dominant role in the Russian-Ukrainian clash.

The first topic we will cover is the revolution in intelligence-gathering in the specific Ukrainian context, based on **Big Data originating from OSINT (Open-Source Intelligence) on social media and cyber operations**. In this first part, we will start talking about Intelligence gathering between crowdsourcing and wiper.

Developments in military robotics, autonomy, Machine Learning (ML), and Artificial Intelligence (AI) improve intelligence collection and analysis, facilitate navigation and manoeuvring in high-risk terrain, enable more precise combat targeting, reduce Urban Warfare costs, and enhance the multi-Domain military effectiveness.

In the Ukrainian conflict, though, low-cost smartphones and satellites have often surpassed expensive predictive analytics tools. Web scraping (i.e., Internet data mining) software has also become a priority in every serious intelligence analyst's toolkit.

Smartphone location clusters help identify where soldiers and battle groups are gathered. Traffic data is used to determine the movements of army columns and their directions. At the same time, to safeguard populations, Google has removed user-submitted locations in Russia, Ukraine, and Belarus from its Maps to prevent user-generated pins from being linked to missile attacks.

Real-time analysis carried out on Reddit, Twitch, TikTok, Snapchat, Instagram, Telegram, Twitter, Discord, YouTube has provided detailed images and reports of this conflict, with information scattered on every platform of (live and non-live) streaming, also thanks to HUMINT (Human Intelligence) with coded or encrypted information exchanges through messaging apps.

The result is an information crowdsourcing based on amateur videos combined with official (open and covert) sources of information. The amount of data flowing live (in terms of footage of airstrikes, ground battles, downed Russian helicopters, targeted civilians) is enormous, with tons of social media

accounts dedicated to analysing micro details such as, for example, daily variations in Russian and Ukrainian combat strength, front lines, or equipment losses.

As for the cyber component, since January 2022, a vast series of Denial-of-Service (DoS) attacks (attributed to Russia by the United States) have targeted Ukrainian government agencies, banks, and other companies. In its latest report, the Ukrainian State Service Special Communication, and Information Protection (SSSCIP) reported 65 significant cyberattacks against Ukrainian critical infrastructure between March 23 and March 29 alone, five times higher than in the previous week. Estimates stand at a 200% increase in cyberattacks against the Ukrainian government and army since the beginning of the conflict.

The attacks were directed at rendering computer systems unusable by corrupting data (particularly through the HermeticWiper malware); spreading worms through local networks (particularly through HermeticWizard); and adding a ransomware component to data recovery itself (particularly through HermeticRansom). The three components act synergistically: HermeticWizard as a malware designed to spread HermeticWiper to any potentially vulnerable computer in a network. HermeticRansom as a malware prevented clients from using their data by creating a "smokescreen" to cover further attacks.

The attacks also identified the Internet as a target. Begun on February 24 with a DDoS-type assault that took many modems offline, subsequent malware sent through the network hit Internet communication by overwriting critical data in the internal memory, disseminating damages from Poland to France, and disrupting remote access to thousands of wind turbines in Central Europe. The attack caused a substantial loss of communications in Ukraine in the first hours of the Russian invasion. Last March, malware crippled tens of thousands of modems across Europe, anchoring the attack on U.S.-based Viasat's KA-SAT satellite network used by Ukraine's government and military. The hacked terrestrial network was operated by Skylogic, an Italian subsidiary of Eutelsat, from which Viasat purchased the KA-SAT satellite in April 2021.

Contextually, opposing the Russian interruptions caused by Russia to Ukraine's fibre-optic or cellular communications infrastructure connections, the deployment of Elon Musk's Space X's Starlink network in the early stages of the war (February 28) mitigated its effects. Starlink has provided Internet access at very high speeds and low latency, even during power outages, thanks to a network of thousands of satellites placed in a very Low Earth Orbit (LEO), just 210 miles away. On April 5, a

public-private partnership between the US federal agency USAID and Space X provided 5.000 Starlink terminals to Ukraine to deliver unlimited, bottleneck-free data connectivity.

The situation on the Ukraine side has been just as volatile. A cyber army has been created to support the Kyiv political regime. Several European Union (EU) countries (such as Lithuania, Croatia, Estonia, the Netherlands, Poland, and Romania) have activated a Cyber Rapid Response Team (CRRT) to provide on-site and remote assistance to Ukraine.

The CRRT project belongs to the first wave of EU Permanent Structured Cooperation (PESCO) projects and has been operational since 2019. CRRT was the first of the current 60 PESCO projects to reach full operational capability in May 2021. Cyber experts in a CRRT assist EU member states, institutions, Common Security and Defense Policy missions and operations, and partner countries, contributing to the EU's joint capability to prevent, deter, and respond to cyber threats.

At the same time, Deputy Prime Minister and Minister for Digital Transformation, Mykhailo Fedorov, opened a Telegram channel ("the IT Army of Ukraine") with more than 300 thousand subscribers to provide instructions to volunteers on how to help protect critical infrastructure in Ukraine, but also how to hack into the websites of Russia and its allies.

The choice of Telegram follows the trend of cyber hacktivists present on social media to exchange messages related to weapons and cyber tools. Since the beginning of the war, dozens of groups have been exchanged daily on Telegram tools and information used to coordinate cyberattacks. Ukrainian authorities have also been adept at disseminating content targeting Russians to undermine their morale and strike at Moscow's military prowess, launching Telegram groups with information about captured or dead Russian soldiers and a hotline for concerned Russian parents, amplifying stories of desertion and abandonment of military equipment, and appealing to Russian mothers to prevent their children from joining the war effort.

The "IT Army of Ukraine" is the most visible force in what has become a cyber conflict characterized by a chaotic mix of players, claims of sabotage not always verifiable, and a small number of visible hackers. Despite many claims, few have carried out verifiable attacks. Even for the hacker collective Anonymous, which claimed responsibility for the breach of more than 2.500 websites linked to the Russian and Belarusian governments and state media, banks, hospitals, airports, and businesses, many of these claims have not been directly verifiable.

Such uncoordinated offensive activities by non-state actors, however, risk unforeseeable escalations. The Berlin-based Chaos Computer Club (CCC) has warned hackers against attacking Russian critical infrastructure chaotically and redundantly because it could provide Moscow with the ability to initiate disproportionate retaliation because of misattribution or exploitation.

Fabio Vanorio

Fabio Vanorio is a Senior Executive of the Italian Ministry of Foreign Affairs and International Cooperation serving as a Tech Lead in the Policy Planning Unit of the Public and Cultural Diplomacy Department.

Bibliography

Bajak, Frank. 2022. "Satellite modems nexus of worst cyberattack of Ukraine war." *TechXplore.com.*

Kayyali, Adnan. 2022. "The Role of Digital Technology in the Ukraine War." *InsideTelecom.com.*

Muscat, Sabine and Zora Siebert. 2022. *Laptop generals and bot armies: The digital front of Russia's Ukraine war.* Heinrich-Böll-Stiftung, Germany.

Radoff, Jon. 2022. "The Real-Time Internet War." *Medium.com.*


NATO Foundation
Defense College