18 October 2023

PERSPECTIVES

The Growing Use of Scamming Techniques and Social Media on the Battlefield

By David Kirichenko

As warfare evolves from sticks and stones to nuclear armaments and beyond, digital tools like scamming and social media offer novel and significant impacts on the battlefield. New digital tactics, techniques, and procedures (TTPs) developed by Ukraine in response to Russia's February 2022 incursion mark the beginning of social media warfare, characterized not just by cyber confrontations but how the digital translates into action on the battlefield. The use of digital platforms will only grow and further expose how these technologies can both aid and compromise military efforts in modern warfare. Russia's experience with Ukrainian-leveraged digital assets serves as a cautionary tale for both individuals and militaries about the perils and possibilities inherent in our connected world.

As irregular warfare (IW) gains prominence in modern military strategy, the role of digital tools like social media and cyber-enabled scamming cannot be overstated. Social media platforms serve as an ideal ecosystem for executing a wide range of IW activities, from disinformation campaigns aimed at sowing division among enemy lines to civil-military operations that gauge public sentiment and build community relations. In the digital world, the battlefront's traditional geographic confinement disappears and the environment is persistently dynamic.

Digital tools are particularly potent for small-scale, non-state actors who might not have the resources for traditional warfare but can nevertheless exert a significant impact through well-coordinated online campaigns, such as Ukrainian activists who use scamming techniques to convince Russians to firebomb their own military offices. In the age of IW, the power dynamics on the battlefield are no longer solely determined by physical might; the impact of influence and information will continue to grow and allow for certain aspects of warfare to be crowdsourced, with ordinary civilians taking on a more prominent role in the era of irregular warfare.

The challenges faced by Ukraine on the battlefield have provided invaluable lessons for military strategists regarding conventional warfare and the future of war. "Once the war is over, we will definitely write a textbook," proclaimed Vice-Admiral Oleksiy Neizhpapa, the head of Ukraine's Navy, "And we'll send it to all the NATO military academies." Ukraine is already applying many recently learned lessons with new digitally-enabled TTPs. The West, including and beyond NATO, can learn much from Ukraine's social media application of irregular warfare in their ongoing war with Russia.

Romance and espionage: how online dating apps betrayed Russian soldiers

Since Russia's full-scale invasion of Ukraine, Russian soldiers have revealed information from their Tinder dating app profiles to AI-generated fake profiles of Ukrainian women. Some soldiers inadvertently disclosed their tactical locations through images while seeking companionship. One woman ingeniously employed two Tinder accounts, setting a different location near the border for each account and, referencing the difference between locations of shared matches, "triangulate(d) the exact locations of her matches." As a result, she reported over seventy such profiles, and their locations, to Ukrainian authorities.

Ukrainian hackers devised a ruse using fake profiles of appealing women across multiple social media platforms, such as Telegram, to ensnare Russian soldiers stationed near Melitopol. According to the Financial Times, the Russian soldiers were persuaded to share photos of themselves on duty. Upon receiving these images, the hackers pinpointed their origin to a secluded Russian military base near Melitopol in southern Ukraine. This intelligence was subsequently relayed to the Ukrainian military, leading to an assault on the base days later.

On Russian Navy Day in July 2023, Ukrainian hackers targeted Russian sailors by sending them a video with good "wishes" via messaging apps. According to the Ukrainian military's Main Directorate of Intelligence (HUR), these videos depicted Ukrainian drones and missiles attacking Russian warships, including the Moskva cruiser. In addition to any potential psychological impact of the footage, the message contained malware that provided the hackers with access to the sailors' phone data, subsequently transferring confidential information to Ukrainian servers. Most sailors unwittingly expressed gratitude before opening the deceptive video.

Activists use scamming techniques to target Russia military infrastructure and offices

Russian officials attribute a series of fire-bombings at their recruitment centers to "phone scammers" who specifically target the elderly to attack Russian army recruitment offices. According to Russian intelligence services, scammers target vulnerable citizens "who found themselves in difficult circumstances and are easy to influence." By convincing them to take out a loan or share their bank details, they are subsequently convinced to attack a recruitment office in an attempt to recover their losses. For example, in Russian-occupied Crimea, scammers duped a schoolteacher into throwing a flammable object at a recruitment office. Similarly, in St. Petersburg, a 66-year-old woman was lured into taking out a loan with the false promise that her debt would be cleared if she attacked a recruitment office with a Molotov cocktail. Digital scammers do not only target the elderly. Teenagers in Russia, who claim they are not aware of who their financier may be, were recruited via social media to ignite railway junction boxes in exchange for money.

The rising significance of open-source intelligence (OSINT)

In August 2022, the Wagner group faced an attack in Popasna, Ukraine. A local pro-Russian journalist inadvertently revealed the Wagner base's location through images shared on Telegram. One such image, now removed, disclosed the base's exact address. Armed with this information, Ukrainian forces demolished the site. A Ukrainian official hinted that the strike's precision was possibly aided by the shared Telegram images. This incident epitomizes how social media-derived open-source intelligence (OSINT, information procured from public sources) is strategically leveraged in the ongoing Russo-Ukrainian war.

When location-based apps lead to physical attacks

In March 2017, a Royal Navy member's run inside His Majesty's Naval Base, Clyde (HMNB Clyde), a high-security base housing the UK's nuclear deterrent, was tracked via the Strava app, leading to concerns about revealing sensitive military locations. Research has shown that data from fitness apps might inadvertently reveal the locations of hidden military bases by mapping consistent exercise patterns and patrol paths within or around such bases. These apps, which often connect to devices such as Fitbits and Garmin watches, allow users to log their exercise routes. A feature designed for friendly competition might unintentionally expose the precise activities and identities of staff within high-security military zones.

In July 2023, data from the app turned deadly. A Le Monde report from July 11, 2023, suggests that Strava may have inadvertently played a role in the assassination of Captain Stanislav Rzhitsky. The Russian officer was ambushed and killed on July 10, 2023, in a park in Krasnodar, Russia. Rzhitsky formerly led a submarine - a submarine implicated in a 2022 strike on the Ukrainian city of Vinnytsia that resulted in 27 civilian deaths.

Rzhitsky's leadership role in this act made him a target for Ukrainian intelligence. Le Monde disclosed that Rzhitsky was a regular Strava user, often sharing his routes. The consistency in his routes led to speculation that his killers might have used the app to predict his movements on the day of his assassination. Strava's user agreement highlights that unless data sharing settings are restricted, user activity can be accessed by anyone online, including details like distance, runtime, and maps of routes.

Diia, a Ukrainian government app originally designed to facilitate access to public services, was repurposed for wartime efforts. It enables Ukrainians to both report the presence of Russian soldiers in their vicinity and manage tasks like uploading tax returns, renewing passports, or providing students with bus fare discounts. Among its features is the "e-Enemy" function, which lets Ukrainian citizens relay information about Russian troop movements, providing invaluable data to the Ukrainian military for strategizing their defense and countermeasures.

The evolving face of modern warfare

Carl von Clausewitz's *On War* posits that, while the fundamental nature of war remains constant in the human experience, its execution or character is ever-changing. He viewed war as a complex social activity and in the 21st century, our interconnectedness expands our connectivity to war as individuals through the digital realm. The increasing democratization of warfare, facilitated by technology, is shifting the focus towards the role of ordinary civilians, like the women who set up virtual "honey traps" using dating apps to get Russian soldiers to reveal their location. As digital tools continue to enter the fray, regular citizens will assume an even more important role in today's warfare.

This metamorphosis of warfare, propelled by the digital age, underscores the urgent need for a comprehensive reevaluation of how we in the West approach conflict in the 21st century and ensure we apply lessons from the Russo-Ukrainian war. The battlefield is no longer confined to physical terrain; it now includes the vast, interconnected realm of the internet, where each click or post could be as consequential as any traditional military maneuver.

Therefore, it is vital for the Western alliances and NATO to adapt and develop new strategies that respond to this evolving threat landscape - the next compromised service member could be a NATO soldier who accidently leaks vital information on social media to our adversaries. In an all-out war, it could be our own populations that are targeted by scammers to attack military offices. We must learn lessons early on from the digital irregular warfare we are seeing in the Russo-Ukrainian war and begin strategizing new approaches to protect ourselves. We must develop an understanding of how to leverage these tools more effectively in the future.

About the Author:

David Kirichenko is a freelance journalist, researcher and Eastern Europe expert. David can be found on the social media platform X @DVKirichenko.

The views expressed are those of the author(s) and do not necessarily reflect the official position of the Department of Defense, Defense Security Cooperation Agency, or the Center for Irregular Warfare.