Foreword: War in the Smartphone Age

Dr Matthew Ford, Associate Professor in War Studies, Swedish Defence University

Although rarely linked to warfare, smartphones and their supporting network of communications infrastructures have been incredibly important for shaping our understanding of the wars of the 2010s. From the Sahel to Myanmar and from Somalia to Syria and Iraq, these devices have connected people fighting wars with diasporas that fund them, promoted genocide and shaped warfighting in cities under siege. Connectivity and access to information play a vital role in our daily routines. In critical moments of crisis and conflict it can also mean the difference between life and death.

The smartphone's portability, processing power and capacity to connect to the internet enable individuals to engage with wars wherever they are in the world. As we scroll through our social media feeds, this is happening in previously unimaginable ways. While much of the existing research emphasizes the influence of social media on shaping identities and transforming the politics of representation, the everyday use of smartphones plays a dual role: they both integrate into and drive the unfolding of crises. As such, these devices fundamentally reshape how people perceive, engage with, and respond to the challenges of 21st-century life.

These changes are underscored by the ubiquity of the smartphone. By 2029, for example, the global number of smartphone users is projected to reach 6.4 billion. What sets smartphones apart from similar devices like tablets or laptops is their compact size, ease of use, and portability, enabling a uniquely personal connection with users. This integration extends to a vast ecosystem of wearable connected devices and applications that form part of the Internet of Things. Now smartphones empower us to monitor our health, track loved ones, and purchase goods and services from virtually anywhere. This has revolutionized how we connect with the world and each other.

The speed and scale at which we can now engage online is a function of the smartphone and the information infrastructures that make it work. The smartphone gives its users the capacity to produce, publish, and consume media from one device. With it, events can be witnessed and broadcast globally in an instant, bypassing traditional editorial controls.

Even as these devices have transformed how we interact with each other and our environment, they have increasingly become the source of a contemporary moral panic. In Australia, the government has banned social media for under 16-year-olds. In the UK, parental pressure groups are increasingly vocal about banning smartphones for under 13-year-olds. In part, this reflects how intimately connected we are to our devices; in the way that they shape our behaviour; and how they have become an everyday extension of our lived experience.

Even as our devices are producing moral panic at home, during times of war, the same technologies appear to render the battlefield transparent, turning everyone into a walking sensor. As one of the most advanced sensor technologies available, smartphones can geolocate and transmit metadata that can be used for the purposes of surveillance. Several newspapers have highlighted how the smartphone can be remotely activated and tracked without consent. Some companies even claim the ability to track users based solely on app permissions granted during setup, making everyone an inadvertent participant in a pervasive surveillance network.

Intelligence agencies are intensely wary of politicians and government officials using messaging apps like WhatsApp, leveraging the convenience of instant communication without falling back on 20th century technology like e-mail. However, security agencies mandate strict protocols, requiring smartphones to be stored in secure 'Faraday' lockers during sensitive discussions. This underscores the delicate balance between embracing connectivity in ways that accelerate war with maintaining secrecy and informational security.

The Russo-Ukrainian war represents a particular moment in the evolution of smart devices and their influence on war. Ukrainians have demonstrated how this seemingly ordinary technology is transforming the way society engages with warfare. It is no longer just about civilians using apps to geolocate advancing enemy forces or get alerts about an air attack; the smartphone has become the essential tool for operating the drone, for amplifying propaganda and for helping to identify the enemy.

My focus on the smartphone is not to discount the ongoing importance of artillery, infantry or the more obvious paraphernalia of war. But it is also true to say that the smartphone is sometimes the first and sometimes the last device that soldiers and civilians alike must resort to even as other modes of communication become inoperable or subject to electronic warfare. On so many occasions during the full-scale Russian invasion, the smartphone has saved a military operation even as it has made soldiers more prone to attack.

Given the smartphone's multiple affordances, then, it is understandable why both Ukrainian and Russian armies work to remove these devices from soldiers heading to the front lines. At home, the ease with which critically important military information can be broadcast online – information that might, for example, let the enemy know how effective their bombing campaign had been – explains

why Ukraine's security services are so sensitive about how civilians share footage of the war. And the ubiquity of the device tells us something about why Ukraine's government invests so heavily in digital influence campaigns aimed at shaping global perceptions of the war.

Ukraine's efforts to control information flows underscore the smartphone's power to gather real-time intelligence and disseminate it instantaneously, directly influencing the battlefield as well as the informational and strategic environment. In this context, smartphones are far more than tools for shaping the military's "information domain". They have immediate and tangible impacts on kinetic operations, blurring the lines between information warfare and physical conflict.

The sheer volume of data makes it impossible to make sense of what we are witnessing online without the support of advanced pattern recognition software. Data is no longer thought about in terabytes but in zettabytes, where a zettabyte equals one sextillion (10^{21}) or 2^{70} bytes. Since 2010, the internet has grown from two zettabytes to around 64 zettabytes in 2020. By 2025, some estimates put the quantity of data as reaching 180 zettabytes.

Artificial Intelligence may help us pick out the signal from the noise of data that we are producing, but not everyone has equal access to this technology. This is reshaping digital divides in ways that will reverberate through international politics for decades to come. This process did not start with Russia's full-scale invasion, but the Russo-Ukrainian War is certainly an important step in the ongoing story of digital warfare.

In these challenging media contexts, the chapters in this volume offer important observations that will help readers make sense of what they are seeing on their smartphones. Bearing this in mind, I am extremely pleased to write the forward to this important volume on Digital Warfare as it has been experienced during the Russo-Ukrainian War. Nadiya Ivanenko and Nadia Zasanska should be congratulated for collecting together so many important and revealing contributions from such a highly qualified group of scholars. I am delighted to be associated with the volume which I expect readers will thoroughly enjoy.