

Supporting an ally: What can the tech world do in response to Russia's invasion of Ukraine?

As Russia began its invasion of Ukraine in the early hours of February 24th, many in Britain started to think about how support could be lent to the Ukrainians. What has been done, what is being done, and what can be done by the tech sector to support Ukraine?

As Russia began its invasion of Ukraine in the early hours of February 24th, many in Britain started to think about how support could be lent to the Ukrainians.

Those who do not work within the tech sector may not know that Ukraine has a thriving tech and startup ecosystem. It is a country of entrepreneurs. Kyiv is home to over 1000 successful startups and creative companies. It is also home to UNIT.City, the largest entrepreneurship and innovation park in Eastern Europe.

In 2021, Ukraine registered its fourth unicorn company. By 2025, the Ukrainian tech industry was projected to value \$10B. Vladimir Putin's invasion was designed, in part, to disrupt Ukraine's free-market economy. Entrepreneurship is a characteristic of democracies, and is threatened by autocrats.

Technological innovation, funding rounds, and capital expansion lose their relevance under the pressure of an invading foreign power. Yet, those who work within a tech ecosystem, regardless of its geographical location, are minded to support their Ukrainian peers, for the ethos and ideals of technological innovation and entrepreneurship are under threat.

So what has been done, what is being done, and what can be done by the tech sector to support Ukraine?

How the tech industry can support humanitarian aid

Launched by *Tech To The Rescue*, a 'voluntary movement of tech companies' that helps global humanitarian organisations 'implement digital solutions to scale up their influence', *#TechForUkraine* is a new campaign hoping to connect Ukrainian nonprofits with *technology companies*.

Supporting a rich tapestry of pre-existing Ukrainian charities and social impact organisations, *#TechForUkraine* hopes to allocate tech companies who can provide cybersecurity, communication and information sharing, and public health aid.

The *Ukrainian Volunteer Service* and *NGO Kamyanytsya Austria* have already joined the *#TechForUkraine* campaign, calling for support from the international technology industry.

In the build-up to the conflict, some companies with offices in Ukraine took the unprecedented decision to relocate staff and families. Cloud-based web development service, Wix, which offers simplified website design for users, *offered* its 1000-strong Ukrainian team temporary relocation to Turkey. Other international tech companies, such as San Francisco-based SaaS mobile marketing analytics company AppsFlyers, announced plans to relocate Ukrainian employees, but it is unclear whether this was achieved before the invasion took place.

Protecting against disinformation

In 2022, online documentation of geopolitical events is a double-edged sword. On one hand, rolling news and instantaneous messaging promote equality of access to information. Yet the same technology can be wielded for malignant purposes, intending to distort actuality and distribute false information.

Indeed, Twitter, YouTube, and even TikTok are being used by the governments and militaries of Ukraine, Russia, and neighbouring countries to distribute information, opinion, and propaganda.

With an eye towards posterity, and the future prosecution of participants in the invasion, certain individuals are turning to technologies to archive evidence that has been posted online.

Issie Lapowsky, writing in *Protocol*, discusses recent Web3 startup *Arweave*, who are encouraging users to archive online evidence relating to the Russian invasion of Ukraine on the blockchain.

A critical discussion on the ethical issues around the permaweb is needed, though perhaps here isn't the appropriate place.

The fear is that online evidence may be wiped by Big Tech in a broad-brush attempt to remove disinformation. Twitter has already apologised for *suspending*, in error, the accounts of users posting video footage of Ukraine over the past week.

However, most platforms are also implementing personalised security measures for users. Nathaniel Gleicher, head of security policy at Facebook, outlines *here* the steps the platform is taking to protect Ukrainians. Facebook has enabled a profile 'lock', enabled through a single click, that prevents individuals from accessing the personal information of non-friends, and is a security tool that was similarly deployed in Afghanistan in August 2021.

Looking forward

The military-invasion of a sovereign democracy on European soil should be an anachronism. Though suspected, and heavily predicted, there was an inability to believe in a Russian invasion of Ukraine until it happened.

Modern warfare in the Western world does not follow a blueprint. Sophisticated cyber-attacks have already been *deployed* by Russian hackers against Ukraine. In retaliation, there have been calls to deny Russian access to SWIFT, the international interbank financial communications system, *disabling* Russia's oil and gas trade. This is a new type of war.

The role that tech will play in it is yet to be determined. It is itself a complex ecosystem that will be both antagonist and ally.

For now, support can be most effectively delivered through verified aid networks, open channels of communication can be utilised to support Ukrainians, and encouragement should be directed toward the Russian people,

most of whom are similarly caught up in an unwanted war, to stand up in protest against their President.

Article by JAMIE WALKER