# The need for a digital safe haven for Ukraine

**Raquel Jorge-Ricart** | Analyst, Elcano Royal Institute | @RaquelJorgeR

While the stability of the current government and the international order loom large in the conflict in Ukraine, the protection of the country's national security and its people is also paramount. Maintaining control over IT infrastructure, whose effects have grown to permeate all aspects of our lives, is vital. Yet this has received relatively little attention so far and it is important to analyse Ukraine's response capacity if Russia seizes control of its digital infrastructure, alongside the best ways to ensure the protection of its sensitive data, especially in partnership with other countries.

Even when war itself does not arise, the threat nonetheless highlights the vulnerability of critical areas. These include the protection of critical infrastructure that has been digitalised (for example, electrical grids), cybersecurity blueprints for the military command and control (C2) system and access to detailed satellite reconnaissance images to detect movements of troops, arms and people trying to leave the country or looking to enter rural areas.

However, the threat extends beyond military matters and national security. Critical national emergencies can also be caused by public systems losing control of data centres situated throughout a country's territory. Data stored on these sites can include sensitive personal information (for example, social security and civil registration) and information on strategic sectors of the economy. We saw an example of this during Russia's *NotPetya* cyberattack on Ukraine in 2017. The attack used a wiper disguised as ransomware (a type of cyberattack that hijacks a system in exchange for a financial ransom) to target strategic sectors and public agencies, resulting in the irretrievable destruction of all hard drive data and losses of around US$10 billion.

"Critical national emergencies can also be caused by public systems losing control of data centres situated throughout a country's territory."

In the current conflict, Ukraine's government is taking a preventive approach to the defence of its digital infrastructure. The country has sought to anticipate attempts to physically seize control of services, while protecting itself against cyberattacks. Although there have already been some cyberattacks on the country, their scale and the damage they have caused have been relatively small. Ukraine's State Service of Special Communications and Information Protection has drawn up contingency plans and scenarios, involving wiping servers across the country and transferring all sensitive data to Kyiv. There is also the option to move data outside the country, should Russian troops gain control of the capital.

While the country has yet to witness a major cyberattack affecting the foundations of its security system, there have nonetheless been a number of cyberattacks in recent weeks, including distributed denial of service (DDoS) attacks that have taken down official websites. There have also been incursions directly targeting the digital infrastructure of the financial sector, as well as humanitarian aid and emergency response organisations. Multiple actors are involved in the defence against these cyberattacks: the Ukraine cybersecurity contingent, private companies, NATO, the EU and cyber-hacktivists like the Belarusian Cyber Partisans group, which has engaged in the defence of Ukraine's infrastructure and carried out offensive activities against Russian systems.

## Ukraine's current digital defence capacity

Ukraine has stepped up its response to the growing threat of attempts to seize control of its digital infrastructure in recent years, through both national initiatives and cooperation with third parties. However, a number of challenges remain.

First, the current concentration of the country's digital infrastructure in Kyiv is not new and is only temporary. In 2014 the Ukrainian government began centralising its servers and data centres, following the annexation of Crimea and the Donbas region by Russia and separatist groups. This exercise also covered the country's subsea cables. Despite carrying 99% of the world's Internet traffic, the geopolitical dimensions of this strategic component of global security have not been fully explored.

In the case of Ukraine, the Kerch Strait Cable, which connects Ilyich in Russia with Kerch in Ukraine, was commissioned in April 2014, only a month after the annexation of Crimea. Despite its relatively short length (46km), the cable is of strategic importance, having been laid by Rostelecom, Russia's public telecommunications company. Following its annexation, Internet service providers in Crimea began to route traffic with Russia through this cable. Traffic in the rest of Ukraine's territory –under the control of the central government– is routed through other cables connected to countries to the west. In 2014 sources claimed that the cable had been damaged by Russia to shut off access to the Internet; others, however, countered the claim, pointing out that the cable was owned by a Russian company and the absence of data showing outages.

Leaving aside this struggle to shape the narrative, at the material level, the Ukrainian government has brought forward its contingency and protection plans to address vulnerabilities in its digital infrastructure. The EU has played a central role in supporting these efforts. Since 2020 it has supported Ukraine's digital transformation through the EU4DigitalUA programme, under the European Peace Facility. The project has provided €25 million for institutional strengthening, capacity-building of the country's digital infrastructure, improved data interoperability and digital governance, as well as raising awareness of the importance of this issue in the public and private sectors. A telecommunications chapter was also created to allow joint measures under the EU-Ukraine Association Agreement, which was signed in May 2014, just two months after the annexation of Crimea.

What makes this project so innovative is that support for digital transformation is normally channelled through other European platforms, such as the Foreign Policy Instrument

(FPI) of the European Investment Bank or the Directorate-General for International Partnerships (DG INTPA). In this case, however, it has been provided through the Instrument contributing to Stability and Peace (IcSP), with a clear focus on the key role of data security in Ukraine for the European security architecture as a whole. The EU has also activated its Cyber Rapid Response Teams and Mutual Assistance in Cyber Security in an operational context for the first time to provide cyber-support to Ukraine, under its Permanent Structured Cooperation project. It is no coincidence that the initiative is coordinated by Lithuania and that four of the other five participating countries are in Eastern Europe (Croatia, Estonia, Poland and Romania). Consideration is being given to sending a team of between eight and 12 experts to Ukraine, although a final decision has yet to be made.

However, the key question is what happens if Kyiv is seized, along with the country's critical infrastructure. Internal efforts to strengthen IT infrastructure inside the country and the initiation of 'cyber dialogues' between Ukraine and the EU in June 2021 are both necessary steps. Yet the country must go further than just bolstering its IT infrastructure internally with support from other countries.

## Response scenarios

Various scenarios and experiences suggest ways forward for protecting Ukraine's digital infrastructure.

First, it could seek a 'digital safe haven' in a third country. This approach has already been adopted by Estonia, following a major cyberattack on the country's government services by Russia in 2007. The country decided that its digital transformation was so important that it needed to be complemented by a new form of international cooperation, going beyond technical support and encompassing mutual aid. Estonia signed an agreement with Luxembourg to create the world's first data embassy, an Estonian server located outside the country but under Estonian jurisdiction. All the embassy's resources are controlled by the Estonian government. This safe haven aims to guarantee the 'digital continuity' of the State. The security system for cyberattacks and physical crises that threaten the country's digital infrastructure is protected using blockchain technology. This allows the Digital Embassy to provide security copies of data and ensure the operational continuity of core services.

So far, the data embassy model has only been implemented by Estonia and Monaco (also partnering with Luxembourg) and has yet to be widely adopted around the world. The concept of servers as sovereign embassies raises the prospect of modifying the Vienna Convention on diplomatic relations to provide diplomatic support for the hosting of data and IT systems in times of crisis and immunity for the use of data when necessary.

"(…) the data embassy model has only been implemented by Estonia and Monaco (also partnering with Luxembourg) and has yet to be widely adopted around the world."

However, the biggest challenge lies in finding a reliable and stable partner to guarantee the long-term survival of data embassies in the event of a crisis. It is also important to ensure there are no legal restrictions, so that the country of origin of the data can put in place the security level it deems necessary (for example, the Estonian data embassy has the highest level for this type of server).

A second scenario involves relying on the country's diasporas for support. For example, Ireland and Lithuania have sought to leverage ties with citizens living abroad to promote their countries' leadership in artificial intelligence and to boost the security of business agreements and supply chains with other countries.

Thirdly, in 2017 the EU created its Cyber Diplomacy Toolbox, which allows it to implement cybersanctions, subject to unanimity among all Member States. Cybersanctions have yet to be applied in the conflict between Russia and Ukraine although they will only be effective in stopping it when accompanied by defence support on the ground.

To summarise, there can be no doubting that Ukraine's digital infrastructure is vulnerable at this point. The country has so far avoided a major cyberattack but the seizure of data centres would be a national emergency affecting both the protection of people and the country's physical infrastructure and security. In recent years, Ukraine has sought support from other countries, but a digital safe haven is indispensable in case the capital falls.