12 November

Lessons from the telecoms frontline

What wartime Ukraine taught us about running critical infrastructure in systemic crisis

By Yuriy Kurmaz, CEO of Ukrtelecom

When the full-scale invasion of Ukraine began, every business theory and strategic plan was subjected to the ultimate stress test. For a national telecommunications operator like Ukrtelecom, this was not a theoretical exercise. We learned that managing a business in chaos can become a new reality, and the lessons are universal. War is an extreme proxy for any systemic crisis—a pandemic, a natural disaster, a financial collapse—that can shatter the foundations of ”business as usual”. What follows are the principles we’ve forged under daily russian physical and cyber attacks.

Commercial telecommunications networks aren't designed for wartime operations. Yet here we are, nearly four years into the full-scale war, maintaining connectivity for millions of households, the Armed Forces of Ukraine, and critical infrastructure. The principles we've developed for technologies and processes offer a blueprint for any organization facing extreme disruption.

When cyber warfare becomes business as usual

Since the full-scale invasion began, we've faced relentless cyber attacks from russian hackers. The numbers tell the story: in just the first quarter of 2024, we blocked over 20 million external unauthorized attacks on our web applications.

In order to protect critical network infrastructure and not interrupt services to the Armed Forces we have sometimes been forced to temporarily restrict internet access to private users and business customers. It's far from ideal to deny service to paying customers, but sometimes resilience means making painful decisions to protect what matters most.

The cyberattacks we’ve faced exposed a critical vulnerability many organizations might encounter: the convergence of IT and telecommunications cores. When these systems aren't properly isolated, a breach in one domain cascades catastrophically across the entire infrastructure. Proper network segmentation between IT and operational technology systems and networks is a crucial security control. In simple terms: imagine if a hacker breaking into your office email could also shut down your factory floor. That's the risk of converged networks without proper segmentation.

Power makes data flow

russia quickly learned that if you cannot break the network with code, you can try to break it by cutting the power. But fiber-optic networks, particularly GPON (Gigabit Passive Optical Network) architecture, have an unexpected advantage: they can maintain connectivity even during blackouts. The passive nature of fiber optics means signals travel without requiring power at every node along the way. In wartime, this architectural feature became a lifeline.

We turned power independence into a market differentiator, even trademarking "Power Independent Internet" and creating a landing page where households could verify whether their home connection would survive blackouts. This is not a marketing gimmick; it is an architectural advantage rooted in our deployment of GPON technology. Blackouts seemed uniquely relevant to Ukraine's circumstances—until power outages hit Cannes during the Film Festival and shut down Spain last summer. Perhaps power independence isn't just a wartime concern after all.

Principles for Operating in Chaos

From the challenges we faced in cyber, power and other domains we've developed five principles which guide us well.

First, **lead your people**. When the crisis hit, our first message to our 6,000 employees was not a business directive, but a human question: "Are you and your close ones safe?". In an environment of fear and disinformation, leadership must be the single source of truth. We ensured every employee had the tools to stay connected, from VPNs to groups on messengers like WhatsApp which could operate while our systems were under attack.

Second, **serve your community**. Our message to customers was simple: "We are here with you". We made the decision to maintain frontline services even if customers could not pay their bills, while asking those who could to please do so. This transforms a transactional relationship into a trust-based one, building loyalty that will outlast any crisis.

Third, **fortify your ecosystem**. The mantra "no competition during the war" became the Ukrainian telco business reality. We shared network resources with our rivals because national connectivity was a matter of collective survival. We started to demand that our critical suppliers be as resilient as we are, and their technology choices, like using distributed cloud solutions, must reflect the physical reality of missile attacks and blackouts.

Fourth, **embrace adaptive resilience over rigid planning**. Standard disaster recovery plans assume disasters affect you while the rest of the world functions normally. They're useless when everyone faces the same catastrophe simultaneously. We shifted to situation-driven management. But one lesson stands out for any telco: automate your organization and processes to swiftly stop business operations on occupied or compromised physical sites. When the Ukrainian army liberated Kherson, we found russian operator equipment installed in our central office. No disaster recovery plan could have anticipated that scenario—but having the capability to remotely erase router configurations and licenses meant we could sever physical links before they compromised the network.

Fifth: **fix the roof when the sun is shining**. Automation, redundancy, and cybersecurity deserve a guaranteed fraction of every year's capital expenditure program, regardless of immediate profit calculations. In stable times, this seems excessive. In a crisis, it's the difference between survival and collapse.

The universality of crisis

We operated a commercial, civilian telco network under daily missile and cyber threat. That’s unusual — but the vulnerabilities it revealed are not. We hope no other teleco faces the challenges we've endured. Commercial networks aren't designed for war but the lessons from operating one under fire have universal applications. Because in our interconnected world, the question isn't whether your organization will face a crisis - it's whether you'll be ready when it arrives.