Infrastructure Recovery through Resilience Stress Testing in Ukraine

In light of major system disruptions, such as the COVID pandemic, supply chain interruptions, and geopolitical conflict, the need to evaluate resilience — the capability of systems to rebound from disruption — has never been more pressing. However, the foundation for resilience science remains underdeveloped, particularly in the context of repeated external shocks. This project puts Ukraine at the forefront, leveraging its distinct digital services sector, which simultaneously faces compounded risks due to repeated external attacks (shocks). We aim to validate the hypothesis that the recovery and resilience of systems under threats can be quantified via stress-testing of interconnected networks representing systemic their functions. Our proposed Resilience-Recovery Under Attack (RRUA) framework aspires to quantitatively explore distinct system response stages to diverse shocks. We employ a multi-faceted methodology combining network science, resilience analytics, explainable AI (xAI), and digital twin technologies. This integrated approach seeks to redefine systemic recovery modeling and adaptation of interconnected infrastructure across Ukraine, benefiting from the knowledge of our proposed international partnership in USA, Ukraine, Poland, Estonia, and Lithuania. This project will utilize a three-pronged approach: refining RRUA using data-rich analyses at DFW airport, testing it in Poland, Estonia and Lithuania testbeds, including human behavior components of vulnerability, and jointly integrating RRUA within Ukraine's cyber and energy infrastructure systems in the presence of dynamic threats and variable data. Success could revolutionize Ukraine's prospects for recovery, positioning it as a global example for resilience strategies. Additionally, our project recognizes the imperative to connect Ukrainian scientists with Western colleagues as geopolitical tensions have isolated the nation's scientific community. It aims to unify Ukrainian scientists within an international research and response community, cultivating vast collaboration and knowledge-sharing.

The IITIS PAN team will focus on creating mathematical models and computer simulations to show how various systems, such as communication and energy networks, cope after major failures or disasters. This will help us better understand how to restore normal functioning to systems after various types of catastrophes. Within the project, these models will be generalized in goal (1) to capture the recovery of the system after a collapse with transient-state analysis showing how the system behaves through the recovery (2) to represent the recovery scenarios for a large variety of distributed systems, from telecommunication networks and energy grids to the transportation systems or other life-essential infrastructures. We want to understand how critical systems like phone networks, power grids, and airports get back on their feet after major disruptions. This will help us predict what to expect in different crisis situations, from small glitches to major failures.

To test our models, we will use real-world data and a variety of scenarios, including those related to war situations. For example, we will evaluate what happens when too many devices try to come online at the same time after a power outage, causing a digital 'traffic jam.' We'll create realistic 'what-if' scenarios using computer simulations and real data, including information from before and during wars. We will employ discrete event models to explore the effects of simultaneous failures in multiple critical network elements, leading to a global outage. Next, we will juxtapose synthetic data with real-world data related to infrastructure attacks in Ukraine. Specifically, we will integrate data from the Phukov Institute concerning the pre-war energy grid topology and updates from the Ukrainian Ministry on system changes during the war. When it comes to figuring out where attacks might have happened, we'll use public information like NASA's Black Marble project, which can give us a rough idea of where explosions have occurred . We plan to take our computer models even further by including how vital services like energy, water, and transportation could be affected by attacks. In the last step, the machine learning techniques will be used to identify the correlation between different system factors (such as, e.g. network topology, recovery times of infrastructure components, and redundancy of elements) on the recovery time.