Structure of New Critical Infrastructure

For much of the modern era, the term "critical infrastructure" evoked a familiar picture: power plants, electricity grids, oil and gas pipelines, bridges, airports, ports, railways, water systems, telecommunications networks and major government facilities. These were tangible assets, fixed in a particular place, owned or controlled by identifiable institutions and protected mainly through physical security, redundancy and emergency response.

That picture no longer captures the systems modern societies depend on. Infrastructure has become an ecosystem of physical assets, digital networks, data, software, satellites, cloud platforms, artificial intelligence, energy systems, financial networks, logistics chains and human expertise. Some of its most important components are invisible. Some sit thousands of miles from the populations that rely on them. Others are privately owned, globally distributed or governed by automated processes. Failure in one part of the system can move rapidly through several sectors and across national borders.

The critical infrastructure of the next decade should therefore be understood less as a list of facilities than as a network of essential functions and dependencies.

Policy has begun to catch up. The European Union's Critical Entities Resilience Directive defines resilience as the ability to prevent, protect against, respond to, resist, mitigate, absorb, accommodate and recover from disruption. It covers energy, transport, banking, financial-market infrastructure, health, water, digital infrastructure, public administration, space and food. A United States national security memorandum likewise describes critical infrastructure as physical and virtual systems whose incapacity could have a debilitating effect on national security, economic security, public health or safety. The critical infrastructure of the next decade should therefore be understood less as a list of facilities than as a network of essential functions and dependencies.

TEMURI YAKOBASHVILI
Contributor

Ambassador Temuri Yakobashvili distinguishes himself as an accomplished leader in government, crisis management, and diplomacy. As the founder of TY Strategies LLC, he extends advisory services globally. A pivotal figure in co-founding the Revival Foundation, aiding Ukraine, and leading the New International Leadership Institute, Yakobashvili held key roles, including Georgia's Ambassador to the U.S. and Deputy Prime Minister. With the rank of Ambassador Extraordinary and Plenipotentiary, he is a Yale World Fellow, trained at Oxford and Harvard. As a co-founder and chair of the Governing Board of the Georgian Foundation for Strategic and International Studies, he actively contributes to global media discussions on regional security. His significant contributions have merited the Presidential Medal of Excellence.

From Assets to Essential Functions

The central change is conceptual. Traditional infrastructure policy asked which facilities were critical. The more useful question now is which functions must continue when individual facilities fail. A hospital is a critical facility, but it cannot operate without electricity, telecommunications, water, medicines, transport, payment systems and cloud-based medical records. A power plant depends on software, fuel, communications, specialized components and, in many cases, satellite-based positioning and timing. A financial institution may own little heavy infrastructure and still become incapacitated when it loses cloud services, data connectivity or trusted digital identity.

> ***Criticality is shifting from the asset to the service, and from the service to the chain of dependencies that keeps it alive.***

Criticality is shifting from the asset to the service, and from the service to the chain of dependencies that keeps it alive. Aybars Tuncdogan argues that highly digitalized economies face a condition of "mass criticality": a widening set of cloud, identity, software and communications providers can now become indispensable to many sectors at once. The point is not that every component deserves the same protection. Governments must understand which combinations of failure would interrupt an essential function.

This changes the unit of analysis. Risk cannot be measured only at the perimeter of a plant, port or ministry. It must also be traced through suppliers, communications links, data services, maintenance contractors and specialized personnel. The CISA resilience playbook maps this problem through dependencies, cascading failures and recovery planning. That is a more realistic model than treating each sector as a separate fortress. Tomorrow's infrastructure will resemble an interconnected nervous

system: distributed, adaptive and difficult to divide into neat administrative boxes.

Digital, Data and Space Infrastructure

The boundary between physical and digital infrastructure has nearly disappeared. Electricity grids are software-controlled. Water systems depend on industrial control systems. Airports rely on interconnected databases, communications and automation. Ports use digital logistics platforms; factories run through industrial Internet-of-Things networks; financial infrastructure is overwhelmingly digital. A cyberattack can produce physical damage, while sabotage of a cable, data center or satellite link can cause digital disruption. Cybersecurity is no longer an added layer of protection. It is part of infrastructure engineering itself.

> ***Cybersecurity is no longer an added layer of protection. It is part of infrastructure engineering itself.***

That convergence has expanded the attack surface. A modern facility may contain thousands of sensors, controllers, cameras, wireless connections, remote-management tools, and third-party software components. Each adds capability, but each can also become an entry point. The practical consequence is uncomfortable: a facility can be physically intact and functionally unavailable. Security planners must protect the flow of commands and information as seriously as they protect walls, gates and machinery.

Data must now be treated as infrastructure in its own right. Data centers, cloud platforms, internet exchange points, domain-name systems, satellite networks and fiber-optic cables perform functions once associated with roads, ports and electricity grids. NATO reports that more than 95% of global internet traffic passes through undersea cables. Those cables carry financial, commercial and governmental information on a scale that makes them strategic assets. Protection must cover not only where data is stored, but how it moves, who controls it, how it is authenticated and what happens when it becomes unavailable or untrustworthy.

The same logic extends above the Earth. Satellites underpin communications, navigation, weather forecasting, agriculture, logistics, disaster response, financial transactions and military operations. Dava Newman, Pascale Ehrenfreund and Peter Martinez observe that space systems are converging with terrestrial infrastructure and digital services. Positioning, navigation and timing signals provide an invisible foundation for transport, telecommunications, finance and energy. Commercial constellations such as Starlink have also shown the value of distributed satellite communications when terrestrial networks are attacked or interrupted. Infrastructure protection now extends vertically, from underground cables and pipelines to orbital systems.

AI, Autonomy and Distributed Systems

Artificial intelligence may have the greatest effect on the architecture of critical infrastructure. It can monitor complex systems continuously, identify unusual electricity consumption, detect suspicious network activity, analyze satellite imagery, anticipate equipment failure, and flag abnormal maritime movement. Digital twins can model how an attack, natural disaster, or technical failure would move through a network before the event occurs. NIST shows how those models can help manufacturers identify cyber vulnerabilities and test defensive responses without placing live operations at risk.

The advantage is speed. Instead of waiting for an operator to notice a failure, an AI-enabled system can detect abnormal behavior, isolate a compromised component, and shift demand to another part of the network. That capability matters in systems where seconds determine whether a local fault becomes

a national outage. Yet the same dependence creates a new class of vulnerability. If infrastructure increasingly relies on AI, an adversary may attack the data, sensors, or algorithms that guide the system rather than the machinery itself.

> ***The challenge is thus not only to protect infrastructure with AI, but to protect AI as infrastructure.***

The Department of Homeland Security's safety framework identifies risks from AI-enabled attacks, attacks on AI systems, and failures caused by deploying AI in critical functions. Training data can be poisoned, sensors manipulated, and automated decisions deceived. The challenge is thus not only to protect infrastructure with AI, but to protect AI as infrastructure. Human expertise remains indispensable, particularly when automated systems confront conditions outside their training or when operators must decide whether a signal is genuine.

At the same time, infrastructure is becoming more autonomous and more distributed. Electricity grids will increasingly balance supply and demand automatically. Drones will inspect pipelines, bridges, power lines and offshore installations. Robots will perform dangerous maintenance, smart buildings will regulate energy use and autonomous vehicles will interact with intelligent transport systems. Solar generation, batteries and microgrids can produce electricity locally; edge computing can process data closer to users; distributed manufacturing can reduce dependence on distant factories. The International Energy Agency finds that a more decentralized Ukrainian electricity system can improve security and resilience. Distribution does not remove risk, but it can deny an adversary a single decisive target. Governments will have to protect thousands of interconnected nodes rather than one enormous installation.

War, Recovery and Allied Resilience

If technology is redefining what critical infrastructure is, war is showing how it must be protected. Ukraine has become the clearest laboratory. For decades, efficiency encouraged centralization: large power stations, major transport hubs and consolidated databases offered economies of scale. Precision missiles, inexpensive drones and persistent cyber operations have exposed the security price of that concentration. A transformer or substation may take months to replace, while a comparatively cheap drone can damage it in seconds. The defender can spend millions protecting an installation against a threat that costs a fraction of that amount.

> ***A transformer or substation may take months to replace, while a comparatively cheap drone can damage it in seconds.***

Ukraine's response has combined air defense with smaller generating units, mobile power, distributed energy resources, emergency generators, local storage and alternative supply arrangements. It has also announced underground weapons-production facilities to reduce the vulnerability of fixed industrial sites. Yet the deepest lesson is not concealment. It is recovery. The International Energy Agency documents repeated attacks on the Ukrainian energy system and the need for repairs, spare equipment, emergency logistics and international support. Repair crews, engineers and replacement transformers have become strategic capabilities.

> ***The governing question is no longer whether every attack can be prevented. It is how quickly a failure can be detected, contained and repaired.***

Eva Sula describes Ukraine as a continuity laboratory, where survival depends on restoring services

while attacks continue. That is the practical meaning of resilience. Complete invulnerability is impossible against cyberattack, sabotage, extreme weather, technical failure and war. Systems must instead absorb shocks, provide essential services at a reduced level, isolate damage, recover quickly and learn from failure. The governing question is no longer whether every attack can be prevented. It is how quickly a failure can be detected, contained and repaired.

War also reveals that infrastructure is a battlespace, a weapon and a source of strategic leverage. Much of it is privately owned. Telecommunications networks, cloud platforms, ports, online marketplaces, data centers and energy facilities often sit outside direct government control. The Associated Press reported the disruption of Wildberries, Russia's largest online retailer, after a Ukrainian cyberattack, illustrating how privately operated digital services can become wartime economic targets. Governments cannot manage this environment alone; military institutions, intelligence services, regulators, operators and technology companies need permanent mechanisms for sharing warnings and coordinating recovery.

The conflict surrounding Iran adds a wider geographical dimension. The U.S. Energy Information Administration estimates the enormous volume of petroleum products moving through the Strait of Hormuz, a chokepoint whose disruption can affect shipping, insurance, prices, supply chains and inflation far beyond the immediate theatre. Criticality is no longer necessarily national. A subsea cable, semiconductor plant, LNG terminal, pipeline, port or shipping route may be part of another country's critical infrastructure even when it lies outside that country's jurisdiction.

Infrastructure is also increasingly allied infrastructure. A country's resilience may depend on electricity interconnectors in neighboring states, foreign semiconductor plants, commercial cloud providers, allied satellites, maritime routes and international supply chains. A NATO study argues that critical-infrastructure security is an enabling condition for collective defense. Alliances will therefore have to defend not only territory and populations, but also the networks that allow forces, economies and public services to function.

Georgia: What to Protect and How

Georgia is a particularly relevant case because its strategic importance outweighs its physical size. Its geography places it at the intersection of the Black Sea, the South Caucasus, and European and Central Asian transport, energy, and communications networks. Pipelines, electricity connections, ports, railways, roads and telecommunications systems serve domestic needs, but they also carry regional trade, energy and data. For Georgia, critical infrastructure is both national and international.

Black Sea security, energy diversification and the development of the Middle Corridor are raising the value of resilient Georgian infrastructure. Batu Kutelia and Vasil Sikharulidze explain that Georgia's place in Black Sea connectivity gives it a strategic role in linking Europe with the South Caucasus and Central Asia. That opportunity comes with exposure. A disruption in a Georgian port, railway, energy link or digital route can produce effects well beyond Georgia's borders, while a foreign failure can interrupt essential services inside the country.

The answer is not to protect every asset equally. Batu Kutelia argues for protecting systems and functions rather than isolated objects, with adaptability and resilience built into planning. Georgia should identify the services that must survive, map their cross-sector dependencies and decide what minimum level of operation is acceptable during a crisis. The strongest investment may be a second route, a stock of spare equipment, a trained repair team or a manual fallback procedure rather than another wall around a facility.

Alessandro Lazari and Nana Tabagua recommend a clearer national framework for critical-infrastructure security and resilience in Georgia, aligned with European practice and supported by cooperation between the state and private operators. That framework should connect risk assessment with redundancy, secure digital systems, emergency power, alternative telecommunications routes, diversified transport connections and rapid repair. It should also define how government shares threat information with companies that operate essential services.

> ***For a small country, the objective is not to build the largest infrastructure system. It is to build one that is difficult to paralyze.***

For a small country, the objective is not to build the largest infrastructure system. It is to build one that is difficult to paralyze. Distributed energy, modular services and cross-border interconnection can reduce single points of failure, but only if institutions can coordinate under pressure. Georgia will also need agreements for mutual assistance, replacement equipment, cyber response and continuity of transport and communications. Those arrangements cannot be improvised after a crisis begins.

If Georgia provides secure and resilient energy, transport and digital connectivity, its infrastructure becomes a strategic asset for Europe and the wider region. That result depends on embedding the country more deeply in European and Euro-Atlantic economic, political and security systems. Georgia cannot meet every demand of future infrastructure resilience alone. Its advantage lies in becoming a reliable node in a larger network: connected enough to matter, diversified enough to endure and organized well enough to recover ■