GLOBAL CRISIS WATCH

ISRM

CENTRE FOR THE STUDY OF WICKED PROBLEMS

CYBER-PHYSICAL VULNERABILITIES IN CRITICAL INFRASTRUCTURE

Editorial Content:
Theodora Posta

20th October 2025

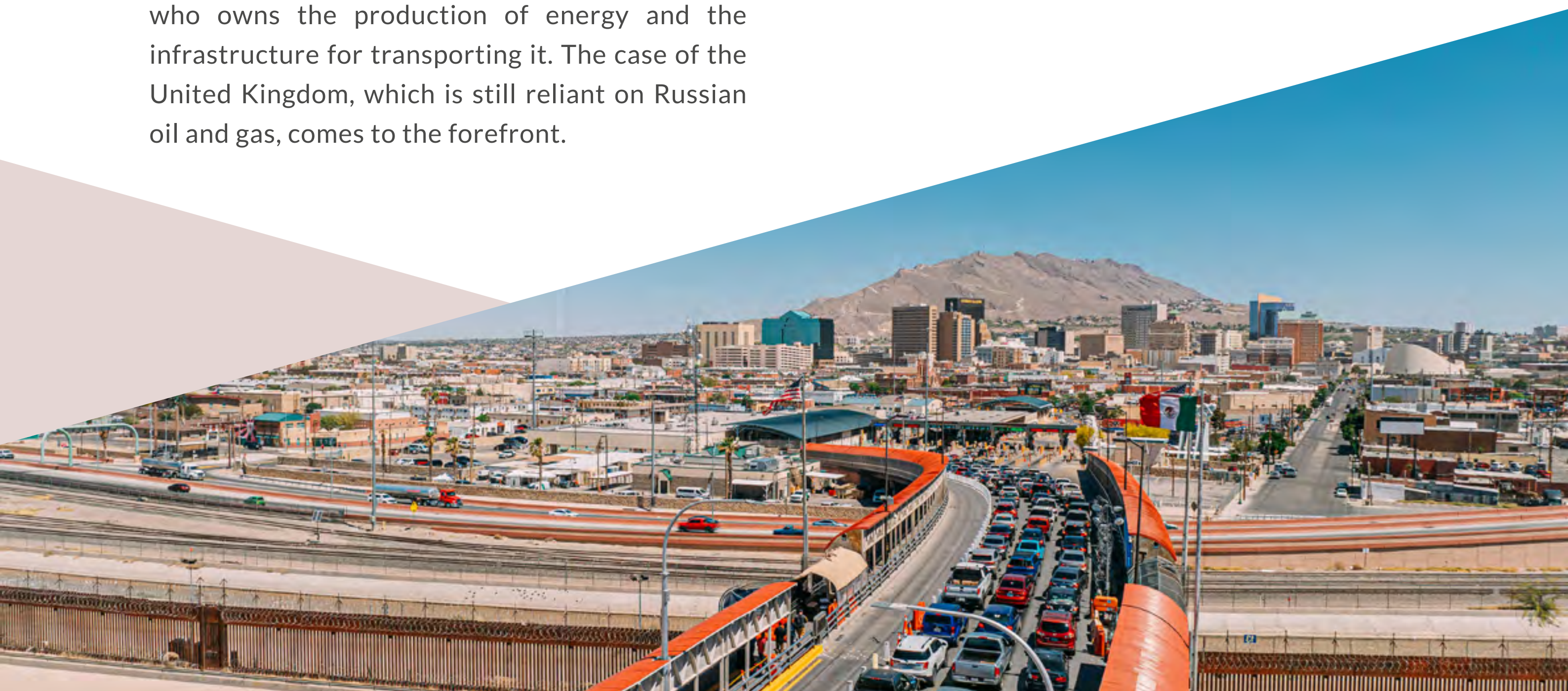
EXECUTIVE SUMMARY

The 372nd edition of the Global Crisis Watch brought into attention the key vulnerabilities of critical infrastructure systems around the world. The underwater cable system connecting different countries, even whole continents, is constantly growing. As an example, according to a 2025 paper by the Carnegie Endowment for International Peace, there are 77 underwater telecommunications cables connecting Africa to the global telecommunications network. These cables are susceptible not only to incidents of sabotage, but also to natural hazards or extreme events, as in the case of Tonga, which lost its sole underwater cable at the beginning of 2022, due to a massive volcanic eruption. Contested land through which support cables run, as in the case of Serbia, brings another layer of insecurity. As easy as it may be to answer these enquiries by depending on global satellite systems for telecommunications, the threat of solar storms puts into perspective a possible overreliance on them.

The discussion also branched towards the current state of risk oversight. As the perspectives on the question of generating energy are increasingly being viewed from a post-climate point of view, the answer must contain the specification of who owns the production of energy and the infrastructure for transporting it. The case of the United Kingdom, which is still reliant on Russian oil and gas, comes to the forefront.

The transition to renewable energy is staggered by the path dependency on exploiting natural fossils, as highlighted by the recent talks between American President Donald Trump and British PM Keir Starmer. Moreover, the optimisation of systems has raised a series of questions regarding risk reporting, particularly in the debate over quarterly versus annual reporting, which touches upon the issue of transparency.

The ubiquitous embedment of infrastructures, from energy systems to online shopping, reframes the critical vulnerability of such assets: one failure may lead to the collapse of the entire system, with examples ranging from the cyberattack sustained by the British retailer Marks & Spencer to the outage of Heathrow Airport. The push for disruptive innovation, as is the case with generative AI, further showcases the abyss in which countries may plunder themselves, if prioritisation for essentialism is not being taken into consideration accordingly.



INTRODUCTION

The infrastructures of today can be best described as a cascading effect of complex systems. Complexity brings robustness, as well as resilience, but it also brings fragility. By definition, the more complex the system is, the higher the likelihood of systemic failure, which brings upon cascading consequences. As systems become more complex, two problems emerge. The first of them is the outsourcing of management: decision-making is done at the lowest cost, with little to no regard for safety. The second problem is the rush to market, as it has been seen in many cases of cutting-edge technologies, from cryptocurrencies to ChatGPT. Rather than testing a complete technology, a company may instead market the beta version and have it learn from its own mistakes as it is being commercially used.

One of the most important questions that arises in these situations, is that of who owns the problem in case of failure. It can even be argued that the avoidance of responsibility had been built in, as the liability has been partitioned among too many services to keep count. In the face of such obfuscation, regulations should serve as a pillar of stability; however, the market bemoans that attempts at regulations, as is the case with the European Union trying to manage AI, stifles innovation. Thus, the cycle continues, as deregulated markets are unpredictable, and unpredictability is a fertile territory for risk. On the contrary, this should pose as a matter of concern not only for local or national governments, but also to stakeholders, who have the duty to stay informed, in order to understand the fragile link between critical, physical infrastructure and global telecommunications systems.

KEY ISSUES

A MATTER OF CRITICAL NATIONAL INFRASTRUCTURE: UNDERWATER TELECOMMUNICATION CABLES

As of the last couple of years, we have started to see a rising willingness of state actors to take hostile action against underwater cables. It is difficult to accept claims that undersea cables are damaged by anchors dragging across the ocean floor, as the positions of these cables are broadly mapped and known to mariners. Furthermore, it can be argued that such actions are easy to undertake, not only because civilian ships are being used for them (recently, by a Chinese ship affecting Samoa), but because underwater cables are almost impossible to protect thoroughly.

In a report authored by the Joint Committee on the National Security Strategy of the British Parliament, dated September 19, 2025, it is recommended that the Government of the UK turn its attention towards its system of underwater telecommunications cables, over which “security vulnerabilities abound”. Incidents of civilian vessels – supposedly used by adversaries – dragging anchors over the seabed, thus damaging the cables, are just one example of the security risks Britain is currently objectifying its critical infrastructure.

Moreover, the communication aspect is not the only one that would incur damage; the cables are also used to generate power for the United Kingdom. Given these factors, the country is in a situation where it cannot guarantee its own self-reliance for providing energy and electricity.

But malicious actions taken by state forces, under the guise of civilian ships, aren’t the only factors that need to be taken into consideration, when discussing the vulnerability of underwater cables: environmental factors need to be included as well. An example which has been pinpointed during the discussion is that of Tonga, which lost its sole underwater cable at the beginning of 2022 due to a massive volcanic eruption. The disaster left the island nation isolated in all matters pertaining communication and the private company Starlink, owned by American oligarch Elon Musk, took advantage of this.

THE RISE OF GLOBAL SATELLITE SYSTEMS

The wonder of the telegraph, which connected various points of the world starting from the 1840s to the middle of the 20th century, can be argued as to be the reason why physical security is still at the forefront of discussion regarding communications. However, as more recent developments have shown, logical protection came to be understood as just as important as the physical one. The need to protect communication lines isn't anything new, but because of the loss of touch in terms of their functionality – as well as their loss of visibility in the world around us, since the rise of satellites – policymakers seem to be unaware of the large variety of risks. For example, cyberattacks can easily disable communication lines without even getting close to them.

A lot of the global systems, which we are dependent on, are privately-owned. Starlink is a prime example of this: Ukraine, a state engaged in war that uses this satellite internet service, could have its use best described as tumultuous. For that reason, Elon Musk ordered its shutdown of areas including Kherson, in late September 2022. The decision, which came to be reported only in July 2025 by Reuters, showcased the immense accumulation of power in the hands of a single company. As the world is seemingly becoming more of a multipolar space, rather than one governed by a sum of great powers, countries with no satellite capability will arrive to a reality of being left behind technologically or, at worst, being left in the dark, physically. The idea of being self-reliant is becoming increasingly important in such a globalised world.

A compelling aspect of new technology is the opportunity to take a leap from zero capabilities to world-leading ones in a much shorter timeframe than was the case in the past. In the case of mobile technology, for example, it can be argued that Kenya is ahead of the United Kingdom in terms of integration of such technology into how a society is run.

INABILITY TO TEST FAILURE IN EMBEDDED INFRASTRUCTURE

In April, Marks & Spencer, a British retailer, disclosed that it had been the victim of a ransomware cyberattack, which forced it to shut down automated ordering and stock systems. The company only began taking online orders again in June, after admitting that some customer data was indeed stolen during the attack. This event underlined a major issue of embedded infrastructures: their vulnerabilities to failures, which target the entire system. Within modern systems, the simple act of shutting down everything for testing becomes near impossible — and thus, analysis can only be built upon unpredictable events. It can be argued that a certain degree of redundancy has to be retained in order to avoid single points of failure. However, there are also cases when not even a backup responds accordingly: the Heathrow Airport outage, caused by the failure of one substation, is one of those.

POST-CLIMATE PERSPECTIVES ON THE QUESTION OF GENERATING ENERGY

Fuel and power security is absolutely critical to national security. Given this fact, Donald Trump's advice to Keir Starmer during their most recent joint press conference, that of 'drill, baby, drill', in reference to the deposits of oil and gas in the North Sea, can come across as innocuous. The problem is that such an action would hinder the transition to renewable energy, as Starmer pledged in its case before the meeting. There is a very delicate balance that has to be kept between producing power and controlling the costs for the regular citizen. Moreover, the United Kingdom still imports Russian oil and gas, which makes it dependent on another country controlling the flow of its own energy. Besides the obvious security risks this fact poses, it is also crucial to follow the trail back on who provides the energy and the infrastructure, at large, in the case of such economic partnerships.

LANDLOCKED COUNTRIES IN THE WESTERN BALKANS: THE CASE OF SERBIA

As Serbia is a landlocked country, any of the underwater cables connected to its grid would have to land at the coast of another country. A good example is the underwater electricity cable between Italy and Montenegro, stretching over 400 kilometers, mostly under the Adriatic Sea, connecting the Balkans to the wider European energy network. A small outage on a Mediterranean cable, which took place in 2020, briefly reduced the flow of power to Montenegro, which in turn affected the regional grid. As repairs are costly and take a lot of time, this further proves the point that modern infrastructure, as invisible as it sometimes is, can default to a domino effect that has consequences on large areas of land. Even more, there are not only cyber and physical risks that have to be considered, but also the issue of the land itself through which the supporting power lines pass through, as some are privately-owned or even contested.

THE CURRENT STATE OF RISK OVERSIGHT

A critical self-awareness of all possible risks, as essential as it is, seems to have been pushed to the background in the current era of risk oversight. Disasters and failures become the victims of mere prioritisation over regular affairs. Returning to the example of Tonga, the underwater cable took 18 months to fix, mostly because the ships that were appointed to the task had been booked for months, if not even years, in advance. As those ships were regularly used for transporting oil or gas, another point can be made about the resilience of a country if, given an exceptional scenario, it would have to rely on its own supply without any new deliveries.

According to the International Energy Agency, for example, in the case of Australia, the state should have 90 days' worth of liquid fuel. However, more recent estimates cut down that time period to 42 days, as Australia is absolutely reliant on the Singapore Terminal. If a tsunami were to take place in the Indian Ocean, on the side of the Strait of Malacca, the country would lose access to the Singapore-Johor Terminal. Overreliance on satellite systems is not a safe bet, either. In May 2024, a major solar eruption occurred, and Starlink was reserved in announcing how many satellites had been damaged. American forces admitted that 500 satellites have been maneuvered to avoid said storm — which was not even considered to have been a major one.

The optimisation of systems has brought forward a series of questions regarding risk reporting. The US Securities and Exchange Commission is in the process of deciding whether companies will be required to publish quarterly or annual reporting. On the one hand, they argue that transparency would be lost in the process of producing annual reports. On the other hand, the advocates for quarterly reports argue that executives would be able to look at the bigger picture and focus on the long-term goals. In reality, there is a bias towards employing enterprise risk management systems, because companies do not see them as valuable or, even further. They see them as a liability that would plummet their stocks. The rush towards performing only to achieve key performance indicators is also the cause of why decision-making boards tend to be homogenous: the voices that tend to be favoured are those of lawyers or accountants.

A lack of standardisation when it comes to which position owns the responsibility for the design of a risk register is another issue encountered within the private sector. It has been discussed that, in the end, such a standardisation will have to be decided upon by companies at large, instead of coming from the policymakers. This situation might affect the state of the rule of law in some countries, as absolute power is being essentially handed directly to the financial sector, which would not only have the ability to shape all business continuity models, but also lobby for their applicability. The EU regulation regarding the mandatory position of a Data Protection Officer in all private companies is an isolated exception when considering the global scene at large.

AI INFRASTRUCTURE TRIGGERS RESOURCE MANAGEMENT VULNERABILITIES

Generative AI has the real possibility of becoming the newest disruptive innovation, which will push those who do not conform to it onto obsoletion. The momentum lost by Kodak and its own digital cameras bears resemblance to companies that are opposing the AI boom. Matters are further complicated by the fact that, nowadays, all forms of critical infrastructure are intertwined, from the energy sector to that of transportation and telecommunication. To serve as an example, the increased number of data and support centres serving the AI sector is dependent on clean water, at least of the potable standard. The water needed to cool down the centres also requires vast amounts of electricity, before being treated as wastewater. Policymakers, at least in the United Kingdom, seem to be more concerned about budgeting the massive reservoirs needed to handle the water, rather than the question of equity posed by the strained water system, which should serve its direct consumers, first and foremost.

CONCLUSIONS & RECOMMENDATIONS

Overall, it is important to emphasise the urgent need to reshape what is considered essential and what is not. As with the example of bandwidth, which can be relieved by shutting down applications that require massive amounts (such as YouTube), a similar concept has to be found when it comes to electricity, as a whole. The opposite of a risk register, an asset register, would include exploits which companies are prepared to compromise. This model could be transposed to the public sector, as well: data centres are drawing upon considerable amounts of resources out of national assets. In such cases, a question of prioritisation will most likely arrive, as to relieve the pressure put upon resources.

Redefining liability is, finally, another crucial step to consider in the attempt to address exposure. Decision-making boards tend to diverge, in this case, given the example of the UK, where liability is not given appropriate attention, in comparison to the US. Its priority should be immediate, as without responsibility, drawing upon inadequate conclusions becomes a fruitless task.