Hybrid menaces and the safety, security and resilience of transportation networks in the digital era

Antoine-Tristan Mocilnikar,
Ministry of the Environmental Transition and Solidarity, Ministry of the Cohesion of Territories and Relations with Local Authorities

Abstract:
In a context of technological proliferation and an open economy, the transportation industry's relation with the problems of safety and security and with the actions of local authorities is complex. Resilience provides a methodology for handling this situation. In this sector (or other sectors) of the economy, digital technology creates new risks for activities and the parties involved. At a time of "hybrid menaces", the questions related to safety and security are being decompartmentalized, since they entail what amounts to a global security. What tools does resilience offer us? Resilience is systemic: given the many interdependent relations, it must be designed on a global scale. The priority is to identify all risks and time frames, and take account of territorial logistics. This means reinforcing our ability to anticipate and manage. It implies an integrated approach for optimizing transportation that simultaneously takes into account the economic, social, financial and digital aspects of safety and security as well as a form of territorial governance based on a multiparty dialog for anticipating and monitoring current changes and those to come.

The question of transportation crops up in a context of economic liberalization and technological expansion. The issues of safety and security are part of this new context. Transportation follows up on the rationale of liberalization in some respects and, in most other respects, advances in this direction. The liberalization of freight transportation by road occurred a good while ago at the European level. Reforms in France and the EU are now stimulating competition in rail traffic. Competition has recently been introduced between taxi services; and busses will be fully open to competition in a few years. We are in a Schumpeterian period of economic liberalization. Interactions between transportation, security, safety, and regional actions bring to light a complex field.[1]

Meanwhile, major events related to safety and security in the transportation industry have drawn attention to this problem area.

From 31 May to 10 June 2016, an unprecedented climatic episode closed a major controlled-access highway (A10 northwest of the city of Orléans), a strategic infrastructure in the French highway system. Owing to exceptional precipitation, water stagnated in pools spanning the highway at four points on a section several kilometers long. Hundreds of vehicles were blocked

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites have been consulted in September 2019.

between the zones under water (up to 1.4 meters deep). The forces of the concession-holder and the army had to be mustered to evacuate nearly 250 people and provide them accommodations. At the time, it was not clear whether the highway could be used again; but the concession-holding company undertook major repairs.

In July 2018, a fire at RTE's substation in the Montparnasse railway station in Paris affected train traffic for a week. This event drew attention to the linkage between energy and transportation, and set it in the light of global security. Major investments have to be made to eliminate such potential domino effects in basic infrastructures everywhere in France.

In September 2018, the collapse of the motorway bridge in Genoa, Italy, reminded us that big investments in highway maintenance are becoming a burden on our societies. The French Ministry of the Environmental Transition and Solidarity published in July 2018 the audit of French highways (those under public management) made by Nibuxs and IMDM. The findings were a cause of concern, but not catastrophic: 17% of highways and 7% of bridges are structurally damaged and should be repaired; and 30% need more maintenance or major repairs. With a budget in 2037 equal to the total of budgets over the past ten years, 62% of our roadways would fall into poor repair (29% in 2017), and 6% of bridges would be "out of service". If we continued spending yearly €666 million till 2022, an investment of €1.3 billion per year would then have to be made till 2037 for the highway system to return to its current state. Meanwhile, a joint study has exposed, in particular, the impact of climate change on infrastructures (CEREMA & CARBONE 4 2018).

Starting in November 2018, the "yellow vests" set up several road blocks and even filtered the vehicles allowed through, an action that seriously affected trucking. Members of this movement attacked toll booths, even demolished a few. A highway police station, a center for supervising urban traffic and logistic platforms were destroyed. Demonstrators were a danger to bridges, and they made brief incursions in train stations and trespassed on tracks. Some of them might have wanted to manipulate the news.

Let us felicitate the three American heros who, on 21 August 2015, foiled the Islamic State's attack on the train (Thalys 9364) connecting Amsterdam and Paris. And let us remember Mauranne and Laura, assassinated on Sunday, 1 October 2017, at the Saint Charles train station in Marseille in an attack claimed by the same organization.

Resilience, an aspect of the management of emergencies, catastrophes and immediate reactions, can provide a methodology for coping. However its global conception in the Rockefeller Foundation's[2] sense refers to all time scales, including coping in the long run. Let us start by examining the momentum imparted by the digital revolution before addressing the question of a strategy for safety and security and then defining the toolbox provided by resilience.

Digitization and the use of data

As this issue of *Annales des Mines* shows, using data, information systems and digital platforms radically alters the transportation sector, where vehicles and containers, as well as their uses, are being digitized. Systems communicate with each other and the rest of the world. Dematerializing shipping documents, orders and information fits in with the generalized use of digital technology on terminals and on board vehicles (shipping and handling operations).

[2] The program "100 Resilient Cities", launched by the Rockefeller Foundation in 2013, seeks to form a network of resilient cities that better stand physical, social and economic stresses. See, forthcoming, CEREMA *Villes et stratégies de résilience. Enseignements du programme 100 Resilient Cities*.

By using masses of data, relevance is improved; control, improved; and confidence, reinforced. The agility associated with this “flattening” of organizations increases efficiency. Whereas a private car is used only 1% of the time, digital technology will make “automobiles-as-a-service” possible. Infrastructures, too, are underused, with a peak load but 3% of the time. Some trucks circulate empty, while others wait days on end to be processed by customs.

The efficiency of transportation should be significantly improved thanks to digital technology. A better electronic use of data would generate a value ranging from $720 to $920 billion per year worldwide in transportation alone (MANYIKA *et al*. 2013). A key to mastering climate change is to better manage transportation. Accounting for a quarter of the CO_2 emitted in the world, transportation is the second source of greenhouse gas emissions (following the production of energy and electricity). As data and artificial intelligence are put to use, the velocity of data processing will increase; and we shall be better able to detect key elements in transportation, predict trends, react and make thought-out decisions as a function of our current objectives.

The scope of activities affected covers a wide range of fields: optimization of the size, mix and sharing of networks; management of both supply and demand; optimization of maintenance and maintenance schedules; calculation of the cost of congestions; optimization of a fleet of vehicles; improved, more efficient procurement services; reports and assisted decision-making; accident prevention; the evaluation of best practices; conception of value; sobriety in construction; implementation and strategy; optimization of technology; rollout decisions; optimization of labor and recruitment; allocation of capital based on risks; optimization of the rollout of smart networks; optimization of energy efficiency, scheduling; procurement and management of stocks; and planning operations. As it brings more opportunities, this revolution will better synchronize supply and demand in all fields of activity. This concerns short-term (*e.g.*, congestion), middle-run (*e.g.*, scheduling vehicles) and long-term (*e.g.*, choice of an infrastructure or even an industry) topics.

As in other sectors of the economy, digitization introduces new risks for transportation and those involved in it. Information systems, a potential gateway for cyberpiracy, should be made secure. In June 2017, a major cyberattack was launched against Maersk, the world leader in shipping; and ransomware blocked reservation services in the ports of Rotterdam, New York and Mumbai for several hours (GREENBERG 2018). Among the menaces taken ever more seriously are the theft of merchandise and control over vehicles. Hackers have managed to divert local data flows from sensors in smart vehicles that were not sufficiently encrypted.

At a time of hybrid menaces, safety and security tend toward global security

Security in transportation encompasses all the actions undertaken to protect against unlawful acts (violence, theft, depredations or uses of the logistic chain to fraudulently ship materials, equipment or human beings) the property of operators (whether infrastructures or means of transit), their personnel and the freight hauled. The work of safety involves the operators and, more broadly, all stakeholders — the state and local authorities as well as clients and users, whether firms or individuals. Safety refers to technical malfunctions not deliberately caused by human beings.

Menaces are evolving, becoming hybrid as advantage is taken of synergies between players and activities. The tools used range from fake profiles on the social media to espionage and disinformation, from manipulations to attempted fraud, from sophisticated cyberattacks to the outright use of force, not to forget the full range of intermediate actions. Hybrid tools of influence can be used separately or together depending on the nature of the target and hoped-for results. To cope with these hybrid menaces, the means adopted must be dynamic too, and adapted to remain in phase with these threats. This fight entails designing new means of defense in anticipation of the attacks to come.

To handle problems of security in practice, and on the basis of the defense code and of the program act for the armed forces, the public administration has, along with operators, produced many a text, such as the SAIV documents on vital sectors, including transportation (SGDSN 2016). A new phrase — operators of essential services (OSE) — emerged in 2018 from the EU’s NIS directive on the security of network and information systems. Provisions about the transportation sector also figure in Vigipirate and the other plans for interventions adapted to each type of risk: on land, NRBC (nuclear, radiological, biological or chemical), or via computers (Piranet). These elements are adapted to the territory covered (PRIME MINISTER’S OFFICE 2018).

Safety and security correspond to problems long considered to be separate. The disciplines historically associated with them have evolved separately. The concept of risk is fundamental in both safety and security. Evaluating a menace is radically different depending on whether it stems from criminal intent or an accident. In the case of security, the origin of the menace to be evaluated is, by definition, beyond the control of analysts and covers a vast range of possibilities. In the case of safety, it is less hard to characterize dangers, and the number of scenarios to take under consideration can usually be reduced to a set probabilities that is limited but sufficient to be deemed significant. In matters of security, the menace is potentially intelligent and adaptative. It might target a system’s points of vulnerability and even the countermeasures and defensive reactions whereas, in matters of safety, the menace does not dynamically interact with points of vulnerability.

To pursue this idea: once the dangers related to safety are identified, they are often thought to be relatively stable over time, and an adapted approach is to use standard scenarios. In the case of security, the profiles, motivations and means of the attacking forces evolve faster and less foreseeably, since they depend on several factors. The “race” between the forces of attack and of defense thus tends toward instability and impels these factors. Scenarios have to be updated much more frequently.

Though different, security and safety share substantial points that, gradually identified, have already inspired thoughts from the methodological, technological and architectural viewpoints. For instance, approaches based on a fault tree analysis or a strategy of in-depth defense, which combines several types of countermeasures that are complementary and independent, work in matters both of safety and of security.

Though different, safety and security have to converge. Their separation still had a meaning when they had separate subjects of concern, but this is no longer so. When safety and security requirements and measures are applied to the same systems, friction might arise between the two. Let us take a simple example to illustrate this. A system for automatically closing doors could be programmed to leave the door open in case of an incident related to safety but to lock the door in case of an incident related to security. Since the two do not fully converge, a minimal requirement is to build better models of interactions between the two and of their interdependencies. This is the condition for controlling all the risks threatening transportation and for optimizing the resources devoted to design solutions and conduct operations. Safety and security tend toward global security.

A safety and security strategy centered on the idea of resilience

A strategy of resilience takes all risks into account: the economic risk, the difficulty of using infrastructures due to congestion, and risks related to the climate, pollution and noise. Nor should we forget the physical risks related to criminal intent, terrorism and hostile foreign governments, not to mention the social and political risks and the risks related to governance. Technical risks, though still present of course, are not the only risks to be analyzed. Questions of resilience arise for long-term planning and emergency management. When there are floods, people have to be evacuated. When technological risks trigger emergencies, people have to be evacuated too; and transportation is part of a resilient response. All levels of the national territory have to be involved, one not being more important than another. On the contrary, they have to be embedded. Individuals, consumers, citizens, students, teachers… are the major actors in governance, a governance that creates resilience.

A white book on national defense has defined resilience in public administrations as the willingness and ability to withstand the consequences of an aggression or a major catastrophe and then rapidly reestablish the capacity of institutions, the society and the economy to function normally, or at least in a socially acceptable way (MALLET 2008).

Resilience refers to what is systemic in contrast to what is sectoral. It must be understood globally owing to interdependencies (especially in the networks underlying our societies). In this respect, we already have a long experience, since the end of the 1970s. Let us take as example road safety. From a systemic approach, it is not just drivers who are responsible, there are also those who build highways, who make cars, who write regulations… each party has a part in the lack of safety on our roads. Starting in 1972, the management of road safety in France was overhauled. The relevant services in various ministries (Interior, Transportation, Public Works, Education) were better coordinated. A battery of measures ensued, ranging from education in primary and middle schools, to the adoption of a point system for drivers' licenses and including programs for drivers guilty of traffic violations. Measures were also taken to improve infrastructures, reduce the speed limit, make better signs, more strictly enforce traffic laws and, too, raise the safety level for vehicles and passengers.

The first, decisive point is time. The relation between an infrastructure and its uses calls for resilience. It took time before strategies for infrastructures and for their uses could be worked out together. Over time, we came to realize the need for a full view, geographically and territorially based. In the short and middle runs, building infrastructures will still be important, but much slower. In other words, the time for adding infrastructures is and will be slow while the time for using them is and will be exponential. Electric scooters, autonomous vehicles, flying taxis and, above all, the "sharing" platforms signal major shifts. These various tools impart a momentum to the operation of our infrastructures. The logic of resilience in the short, middle and long terms must cope with two forms of "temporality". The pivotal time for resilience is the management of emergencies and catastrophes and the launching of immediate reactions, and then the return to normalcy, the post-crisis phase and reconstruction. Standardization, certification, prevention, preparation and monitoring will always occur upstream. Questions of resilience are for long-term planning and crisis management.

The second point is territorial. The concept of interconnections is essential to resilience. Rural areas are to be studied in interconnection with metropolitan areas; and vice-versa. Territorial subdivisions and decentralization have a history. Their governance has evolved significantly over the past forty years. The recent emphasis placed on decentralization in transportation is worth noting; and major changes can still occur.

The priority is to identify all risks, all forms of “temporality”, and to understand the “territorial logic”. This is what global security means (PRÉVENTIQUE 2019). These elements implement resilience.

In all, we must reinforce our ability to anticipate and steer changes and adaptations. The idea is to optimize transportation thanks to an integrated approach that takes account, altogether, of the economic, social, financial and digital issues related to safety, security and governance, from a geographically-based perspective in a multiparty dialog that leads us to foresee and monitor the changes under way and to cope. The big challenge is to steer territorial subdivisions, big or small, while leaving none behind. This means immediately achieving a level of performance and, even more, reformulating fundamentals and reconstructing itineraries that can make sense, consolidate cohesion and allow for collective successes.

References

CEREMA & CARBONE 4 (2018) *Analyse des risques liés aux événements climatiques extrêmes sur les infrastructures et services de transport, note de synthèse méthodologique et exemple d’application*, 3 May. The conspectus is available at
http://www.carbone4.com/de-plus-vers-resilience-reseaux-de-transport-face-changement-climatique-analyse-de-risque-reseau-de-dir-mediterranee/.

GREENBERG A. (2018) “The untold story of NotPetya, the most devastating cyberattack in history”, *Wired*, 31 May, available at
https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

MALLET J.C. (2008) *Défense et Sécurité nationale. Le Livre blanc* (Paris: Odile Jacob & La Documentation Française) 402p. available at
https://www.ladocumentationfrancaise.fr/docfra/rapport_telechargement/var/storage/rapports-publics/084000341.pdf.

MANYIKA J., CHUI M., GROVES P., FARRELL D., VAN KUIKEN S. & DOSHI E.A. (2013) *Open Data: Unlocking Innovation and Performance with Liquid Information*, October (New York: Mckinsey Global Instiute Report), 116p. available at
https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Open%20data%20Unlocking%20innovation%20and%20performance%20with%20liquid%20information/MGI_Open_data_FullReport_Oct2013.ashx.

MINISTRY OF THE ENVIRONMENTAL TRANSITION AND SOLIDARITY [MTES] (2018) “Réseau routier national non concédé: résultats d’audits”, a report by the audiors NIBUXS & IMDM for the ministries of the Environmental Transition and Solidarity and of Transportation, 10 July, 8p. available at
http://www.ecologique-solidaire.gouv.fr/sites/default/files/2018.07.10_dossier_reseau_routier,pdf.

PRÉVENTIQUE (2019) *Les Premières Assises de la sécurité globale des territoires*, special issue of *Préventique*, 162, January, available via
http://www.preventique.org/Preventique_Securite/securite-globale-des-territoires-assises-de-lyon-162.

PRIME MINISTER’S OFFICE (2018) “Plan d’action contre le terrorisme”, 13 July, 36p., available at
https://www.gouvernement.fr/sites/default/files/document/document/2018/07/dossier_de_presse_-_plan_daction_contre_le_terrorisme_-_13.07.2018.pdf.

SGDSN (2016) “La sécurité des activités d’importance vitale”, 18 March, 4p., available at
http://www.sgdsn.gouv.fr/uploads/2016/10/plaquette-saiv.pdf.