

Ecran-titre de l'émission spéciale de la SRF sur le blackout, le 2 janvier 2017.

Blackout

Introduction au dossier « blackout »

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Blackout. Ce mot emprunté à l'anglais fait référence à l'obscurité totale après l'extinction des feux. Durant la Seconde Guerre mondiale, le blackout décrivait les mesures de précaution des belligérants. La nuit, aucune lumière ne devait donc être visible de l'extérieur afin d'éviter que les aviateurs ennemis ne s'en servent pour se repérer.

Aujourd'hui, *blackout* est employé pour décrire des effets similaires, mais involontaires. Il s'agit des conséquences d'une rupture de l'approvisionnement en électricité. Cette rupture peut durer quelques minutes, quelques heures, voire quelques jours. Les ruptures de courte durée ont des conséquences limitées. Les ruptures de moyenne et longue durée ont des conséquences étendues.

En Suisse, le *blackout* est un des risques majeurs pour le pays. Cependant, c'est un risque encore trop peu connu. Dans ce cadre, la RMS consacre un long dossier à ce risque. Ce dossier a pour ambition de :

- Sensibiliser au risque de blackout et ses conséquences ;
- Inviter à considérer les vulnérabilités de nos sociétés modernes ;
- Fournir aux lecteurs des connaissances afin de se préparer à ce risque ou de s'y prémunir ;
- Et donner aux personnes qui le souhaitent la possibilité de sensibiliser à leur tour d'autres personnes.

Le dossier est structuré comme suit :

- Page 37 : un premier court article explique les raisons pour lesquelles le risque de blackout est un « super-risque » ;
- Page 38 : un second article synthétise les déclencheurs et mécanismes d'un blackout ;
- Page 42 : un troisième article dresse le portrait de l'évolution des conséquences blackout de quelques heures à plusieurs jours ;
- Page 49 : un premier entretien aborde l'évolution de la perception du blackout dans les cantons romands et comment celui-ci s'est notamment retrouvé au premier rang ;

- Page 52 : un second entretien couvre la problématique mal connue du vieillissement du réseau électrique suisse et comment celui-ci pourrait augmenter les risques de blackout ;
- Page 55 : un troisième entretien explore les conséquences du *blackout* et de la pénurie d'électricité (un risque lié), sur l'économie et la population et comment l'Office fédéral de la protection de la population suggère d'agir face à un tel risque ;
- Page 59 : un quatrième entretien aborde l'évolution générale des risques et ouvre plusieurs perspectives sur les risques futurs, en particulier ceux liés à la société numérique et comment ils peuvent accroître le risque de *blackout* ;
- Page 62 : la conclusion du dossier pose la question du chemin parcouru et encore à effectuer, aborde quelques interrogations en suspens et appelle à la contribution.

Ce dossier n'aurait pas vu le jour sans le soutien du Colonel EMG Alexandre Vautravers ainsi que de l'accueil, la patience et la guidance de Michel Dufour, Philippe Bettens, Jacques Audergon, Stefan Brem, Pascal Äbischer et Charles-Louis Notter. En outre, que l'ensemble des correcteurs et relecteurs¹ ayant contribué à la lisibilité, l'intelligibilité, et la pertinence de ce dossier soient profondément remerciés.

G.C.

¹ Par ordre alphabétique (nom de famille) : Christophe Achte, Pascal Blachier, Sophie Crampe, Isabelle De Keyzer, Christine DH, Anne Saunier-François, Jean-Pierre Gaussens, Pierre Lanéry, Louise Lapierre, Jacques Chartier-Kastler, Rodolphe Meyer, Corentin Neuffer, Anne-Laure Spa, Luc Taesch, Vadim Turpyn et Julien Perrochet.

Le blackout, un «super-risque»: Une explication par la criticalité

En quoi le risque de *blackout* est-il si singulier? Avant tout, il s'agit d'un risque directement lié à un secteur critique, ce qui n'est pas le cas d'une pandémie ou d'une crise économique. Ce secteur critique, c'est l'approvisionnement en électricité. En effet, sans électricité, nos sociétés ne pourraient pas fonctionner. Si elles peuvent se permettre de se passer quelques jours de pétrole, une coupure de courant les affecte immédiatement.

Comment cela se fait-il? Pour deux raisons principales. La première, c'est que l'électricité irrigue tous les autres secteurs et infrastructures critiques. Ceux-ci sont pratiquement incapables de fonctionner sans elle. La deuxième raison, c'est que le *blackout* paralyse les deux secteurs critiques les plus importants après l'électricité, à savoir les télécommunications et les systèmes d'information. Sans eux, la coordination devient très difficile, surtout lors d'une situation de crise comme celle d'une coupure de courant.

Cette centralité de l'électricité a été mise en évidence en 2010 dans un rapport de l'Office fédéral de la protection de la population (OFPP) sur la criticalité des secteurs critiques¹. L'OFPP y définit la criticalité comme «l'importance relative d'un secteur critique en fonction des effets que son arrêt ou sa destruction auraient pour l'économie et la population».²

1 Stefan Brem et al, *Schlussbericht Kritikalität der Teilsektoren*, Programm Schutz Kritischer Infrastrukturen, Bundesamt für Bevölkerungsschutz, 11.9.2010, 21 p.

2 Traduction libre de l'auteur.

Dans ce cadre, le rapport effectue une évaluation qualitative (sur quatre degrés: 0, 1, 2, 3) de l'importance de chaque secteur critique par rapport aux autres.³

Les résultats font apparaître la centralité de l'approvisionnement électrique, touchant plus de secteurs que tout autre et provoquant le plus d'effets sur l'ensemble (voir tableau ci-dessous⁴). Les systèmes d'information et les télécommunications passent respectivement en deuxième et troisième position. À l'inverse, les secteurs les plus vulnérables à l'arrêt des autres sont les services de secours et hôpitaux.

En conséquence, la criticalité de l'approvisionnement électrique détermine le *blackout* comme le risque plus important et motive sa qualification de «super-risque».

G. C.

3 L'évaluation a été conduite au moyen d'une consultation étendue d'experts issus de l'économie et de la Confédération.

4 A des fins de lisibilité, le tableau présenté ici est une version légèrement remaniée du rapport de 2010. Seuls les secteurs critiques les plus importants figurent. L'évaluation qualitative de la criticalité des secteurs demeure fidèle au rapport, seuls changent les coefficients relatifs. De plus, un coefficient de dépendance a été ajouté afin d'identifier les secteurs particulièrement vulnérables.

Évaluation d'une sélection de secteurs critiques par l'OFPP. Chaque case indique la criticalité du secteur placé en ligne sur celui situé en colonne. Les numéros des cases renseignent de la force de cette criticalité (0 : pas criticalité, 4 : criticalité la plus forte). Le coefficient de criticalité indique l'importance relative d'un secteur pour l'ensemble. Le coefficient de dépendance signale la vulnérabilité relative d'un secteur par rapport à tous les autres.

Lire le tableau

	Approvisionnement électrique	Systèmes d'information etc.	Télécommunications	Transport routier	Systèmes automatisés etc.	Banques et services financiers	Internet	Approvisionnement pétrolier	Radiodiffusion et médias	Traitement des eaux usées	Approv. en eau potable	Produits pharmaceutiques	Services d'urgence	Transport aérien	Approvisionnement gazier	Hôpitaux et soins médicaux etc.	Approv. alimentaire etc.	Coefficient de criticalité	Nb de secteurs touchés
Approvisionnement électrique	3	3	1	3	3	3	2	3	3	3	2	2	2	1	3	2		40	16
Systèmes d'information et réseaux	1	3	1	3	3	3	0	2	1	2	1	1	2	2	0	2	1	27	14
Télécommunications	2	2	1	3	3	3	1	2	0	1	0	0	3	2	1	2	0	26	13
Transport routier	1	1	1	1	0	0	2	2	1	1	1	2	3	1	1	1	2	19	14
Systèmes d'instrumentation et de surveillance	2	2	2	1	1	0	1	0	1	2	1	0	1	2	0	1	1	17	12
Banques et services financiers	2	1	2	0	0	1	2	1	0	1	0	0	1	1	1	1	3	14	11
Internet	0	2	2	0	2	2	0	2	0	1	0	0	1	1	0	1	1	14	9
Approvisionnement pétrolier	0	0	0	3	0	0	0	0	0	1	0	0	2	3	0	0	2	9	4
Radiodiffusion et médias	0	0	1	1	2	1	0	0	0	1	1	0	2	0	0	1	0	10	8
Traitement des eaux usées	0	0	1	0	0	1	0	1	0	1	1	0	1	1	0	2	0	9	8
Transport ferroviaire	0	0	0	0	0	0	2	1	0	0	1	0	1	0	0	2		5	4
Approvisionnement en eau potable	1	0	1	0	0	0	0	0	1	0	0	1	0	0	2	0		6	5
Produits pharmaceutiques	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	3	0	5	2
Services d'urgence	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	3	3
Transport aérien	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	1	2	2
Approvisionnement gazier	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
Hôpitaux et soins médicaux	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
Approvisionnement en denrées alimentaires	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Coefficient de dépendance	9	11	16	10	14	14	10	10	15	7	14	8	7	22	17	4	20	15	
Nb de secteurs dépendants	6	6	9	8	6	7	4	6	9	5	10	6	5	13	11	4	12	9	



Une ligne à haute tension dans les Alpes. La mise hors service d'une seule de ces lignes peut suffire dans certaines circonstances à provoquer une chute du réseau.

Blackout

Blackout : Déclencheurs et mécanismes

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Dans quelles circonstances un *blackout* peut-il se produire? Cette question est importante à plus d'un titre: la compréhension du déclenchement et de la propagation d'un tel phénomène peut contribuer à mieux s'y préparer, à limiter une partie de ses effets, voire à le prévenir. De plus, les connaissances acquises dans cette étude peuvent être appliquées ailleurs. En effet, les mécanismes à l'œuvre dans le déclenchement et, surtout, la propagation du *blackout* peuvent être transposés dans l'étude d'autres secteurs (par exemple, les systèmes informatiques).

Cet article constitue une introduction aux principaux déclencheurs d'un *blackout* et aux mécanismes sous-tendant ce phénomène. Dans ce cadre, ce texte propose une courte synthèse de la littérature spécialisée sur le sujet. Une première partie porte sur les déclencheurs, suivie d'une seconde abordant les mécanismes généraux et d'une troisième partie consacrée à la thématique des interdépendances ainsi que des problématiques que ces dernières soulèvent.

1. Les déclencheurs

Des causes multiples

Les ruptures d'approvisionnement électrique peuvent se produire par de multiples causes. La littérature spécialisée en identifie jusqu'à 300 différentes. Elles ont toutes en commun d'endommager ou de paralyser les infrastructures de production, de transport ou de consommation de l'électricité. On peut ranger ces causes en trois catégories :

- Les catastrophes naturelles ;
- Les catastrophes techniques ;
- Les risques ou menaces d'origine humaine.

Si, jusqu'à aujourd'hui, les catastrophes naturelles ont été la cause la plus fréquente de ruptures de courant, cela pourrait changer à l'avenir. En effet, selon des spécialistes

du secteur électrique, les estimations des futures causes de *blackout* se partagent à moitié entre les facteurs naturels et techniques et les risques et menaces humains (cyberattaques et attentats en tête).¹

Une résilience variable

Il ne suffit pas qu'une des causes précédemment évoquées se manifeste pour que le réseau électrique tombe. En effet, un *blackout* ne peut se produire que si le réseau n'est pas en mesure de continuer à fonctionner malgré une perturbation. Par exemple, il arrive fréquemment que des poteaux électriques tombent dans les vallées alpines, mais ils ne provoquent pas forcément de coupure de courant dans les zones concernées et certainement pas de *blackout* à l'échelle nationale.

En effet, les réseaux électriques sont construits autour d'une architecture en « n-1 », c'est-à-dire que leur fonctionnement est garanti si un des éléments du réseau est mis hors service.² Concrètement, cela signifie qu'en cas d'interruption d'un transformateur, les autres transformateurs de même échelon doivent pouvoir sans problèmes continuer d'approvisionner en électricité l'ensemble du territoire. Cela s'applique également aux lignes à haute tension, etc.

Un autre facteur important est la vulnérabilité des infrastructures critiques, c'est-à-dire leur fragilité. Par exemple, la perturbation qui a causé l'interruption de la circulation des trains en Suisse en 2005³ s'est propagée dans les lignes de téléphone du réseau ferroviaire, jusqu'à

¹ Sur ce sujet, consulter l'entretien de Jacques Audergon dans ce dossier.

² Ce choix est économique. En effet, les infrastructures doivent être amorties en 30 à 35 ans. Il serait possible d'accroître ce degré, mais cela serait plus onéreux.

³ À savoir, la déconnexion de la sûreté automatique en Suisse centrale de la ligne de transport des CFF reliant Amsteg à Rotkreuz.

trouver un point vulnérable et se diffuser à l'ensemble du réseau. Par définition, le risque qu'une infrastructure s'effondre est proportionnel à sa fragilité. Et si deux infrastructures fragiles de même échelon tombent, une situation de blackout peut se déclarer, indépendamment de la robustesse des autres infrastructures.

Dans ce sens, il ne suffit pas que le réseau soit capable de fonctionner en mode dégradé, encore faut-il s'assurer que les infrastructures critiques soient le moins vulnérables possible aux perturbations. Car, dans cette situation, il suffit que deux infrastructures de même échelon ne soient pas en état de marche pour provoquer l'effondrement du réseau. De cette manière, la chute d'un pylône peut effectivement provoquer un blackout, mais seulement si le réseau avait déjà été fragilisé par la perte ou la mise hors service (par exemple, pour de l'entretien) d'une infrastructure de niveau équivalent.

2. Les mécanismes de propagation

Une chaîne de dominos qui tombe ?

On emploie régulièrement la métaphore des dominos « qui tombent » pour décrire le mécanisme de propagation des effets d'un *blackout*. Pourtant, cette métaphore pourrait être trompeuse. C'est la conclusion de Gianluca Pescaroli et David Alexander, deux chercheurs sur le sujet. Ils reprochent à la métaphore d'être trop simpliste. Cette dernière présume qu'un événement initial déclenche toute une chaîne d'effets se suivant linéairement.

Or, indiquent Pescaroli et Alexander, la réalité est généralement plus complexe, en particulier dans les systèmes tels que ceux des infrastructures critiques. Ces dernières, à l'instar du réseau électrique, sont caractérisées par un degré élevé de complexité et d'interdépendances avec d'autres systèmes.⁴ De plus, la nature de ces systèmes est non linéaire, ce que ne reflète pas la métaphore des dominos : des petits changements peuvent en provoquer d'autres, de plus en plus grands, générant ainsi des effets d'amplification potentiellement exponentiels et difficilement envisageables *a priori*.⁵

Une définition plus adaptée : Les cascades d'effets

Dans ce cadre, Pescaroli et Alexander proposent de

Principales catégories de causes de déclenchement d'un *black-out* (sélection)

Catastrophes naturelles

Inondations, neige, vagues de chaleur, tempêtes de glace, vent et tempête solaires, pandémies*, etc.

Catastrophes techniques

Surcharge du réseau, explosions ou accidents industriels (voire nucléaires), problèmes techniques et informatiques, etc.

Risques ou menaces d'origine humaine

Sabotage, attentats, cyberattaques, erreur humaine, malveillance, armes électromagnétiques, etc.

* Une pandémie peut grandement réduire le nombre d'employés du secteur électrique, ceux-ci étant malades, ou absents soit pour s'occuper de leurs proches, soit parce qu'ils craignent pour leur santé. Dans ces conditions, le réseau électrique pourrait ne plus suffisamment être encadré, un facteur de vulnérabilité pouvant mener à un *blackout*.

substituer le concept de cascade d'effets à la métaphore des dominos. Une cascade d'effets est une séquence d'événements multiples et non linéaires. Elle se distingue principalement de la chaîne d'effets des dominos par le fait que chaque effet peut à son tour devenir une cause pour un ou plusieurs effets parallèles. De cette manière, une cause initiale peut provoquer plusieurs effets, ceux-ci devenant des causes pour d'autres effets et ainsi de suite.

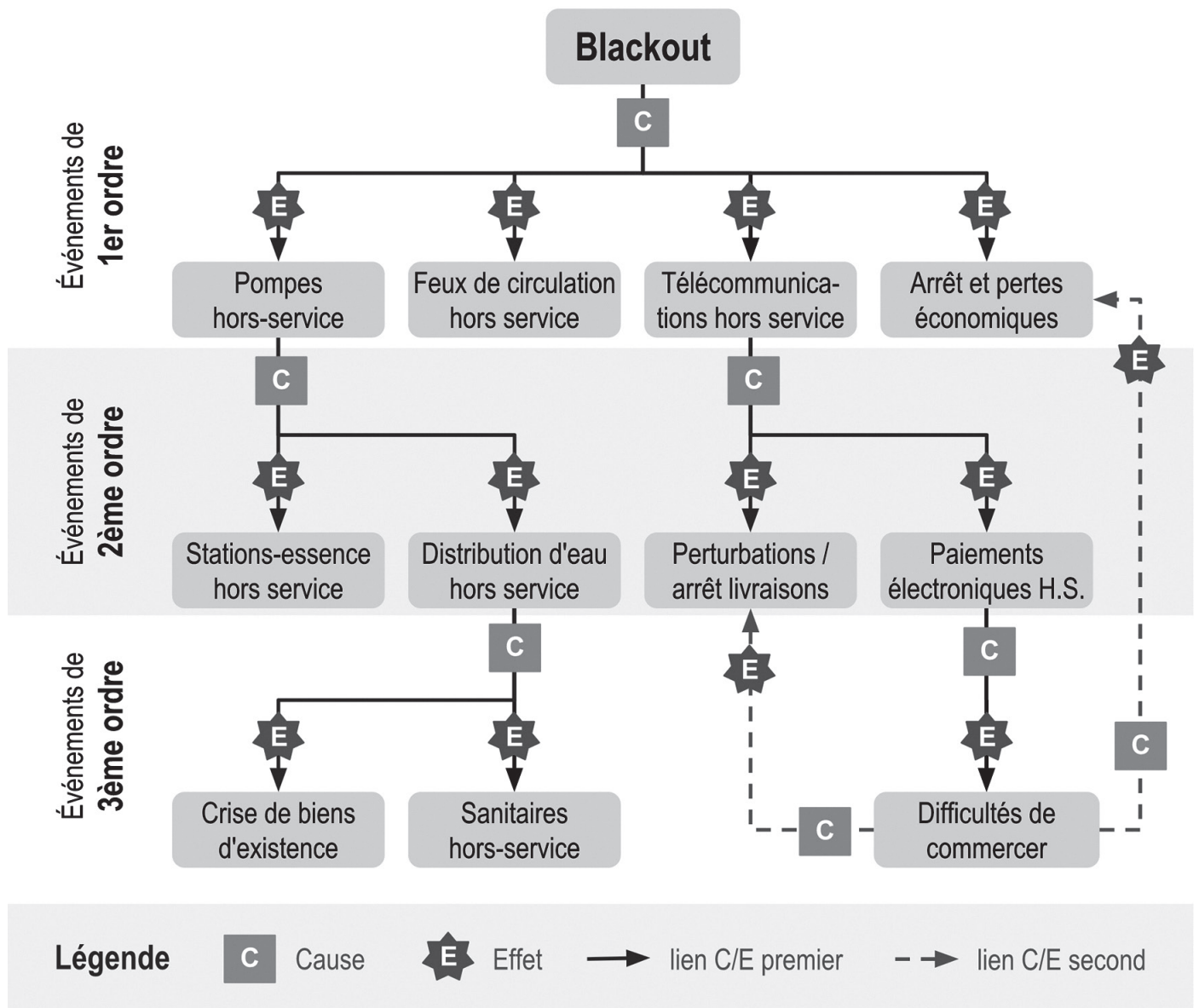
Les systèmes étant caractérisés par des interdépendances multiples, il est tout à fait envisageable qu'un facteur touché en bout de chaîne rétroagisse sur une cause placée en début de chaîne. De la même façon, le fait qu'un événement ne soit pas rattaché à une cause en début de chaîne n'indique pas forcément que celui-ci est moins dangereux, bien au contraire.

Par exemple, dans le cas d'un *blackout*, la cascade d'effets de l'arrêt des télécommunications (événement de premier ordre) illustre bien ces interdépendances multiples. Cet arrêt a pour conséquences (entre autres) de perturber, voire de suspendre les livraisons et d'interrompre les paiements électroniques (événements de second ordre). Cet arrêt rend le commerce très difficile (événement de troisième ordre) et accentue un autre événement de premier ordre : un ralentissement économique et les pertes associées.

Pour continuer, une interruption de courant a pour conséquence (parmi d'autres) d'arrêter les pompes (de n'importe quel type) et les feux de circulation (événements de premier ordre). Immédiatement, l'arrêt des pompes ne semble pas être directement dommageable. Pourtant, cet arrêt met les stations-service hors d'usage, un développement beaucoup plus préoccupant (événement de second ordre).

⁴ Cette complexité et ces interdépendances peuvent s'expliquer par la difficulté à saisir l'ensemble des interactions à l'intérieur d'un système ainsi que la vulnérabilité de ces systèmes aux instabilités provenant de l'extérieur.

⁵ Par exemple, lors d'un *blackout*, la majorité des systèmes de cuisson sont mis hors service. Des individus peuvent alors recourir à des réchauds à gaz, des grills ou aux cheminées. Dans ces circonstances, il est très probable que certains provoquent des départs de feu. La problématique serait bénigne si les pompiers pouvaient intervenir. Mais ceux-ci sont, d'une part, difficiles à joindre (les téléphones ne marchent plus) et, d'autre part, peut-être incapables d'éteindre le feu, les bornes incendies n'étant plus alimentées (les pompes assurant la pression dans les conduites ne fonctionnent plus). Ainsi, un blackout peut être un facteur d'augmentation de la fréquence et de l'intensité des incendies. Cet exemple fournit une bonne illustration de conséquences s'amplifiant mutuellement et *a priori* difficilement prévisibles.



Exemple de représentation (indicative et non exhaustive) des cascades d'effets pouvant se produire après un blackout.

L'effet retard : Une surprise potentielle

Une autre caractéristique des cascades d'effets est qu'elles peuvent s'étaler dans le temps. Ainsi, une chaîne causale peut sembler s'interrompre, alors que ses effets sont simplement retardés. Les cascades d'effets intègrent bien cet aspect réel — et déterminant — du délai entre la cause et son effet. La durée de l'arrêt est dépendante de la capacité à durer, c'est-à-dire de la période pendant laquelle l'infrastructure en question dispose de suffisamment de ressources pour assurer son autonomie.⁶

Ainsi, lorsque l'alimentation de secours des antennes de téléphonie mobile se déclenche suite à une interruption de courant, on pourrait penser que celles-ci sont résilientes. Mais la réalité est plus complexe. La résilience de ces antennes dépend de leur capacité à assurer les télécommunications jusqu'au rétablissement de

l'alimentation électrique générale. L'autonomie minimum des antennes est de 30 minutes. Aussi, si la durée de la panne dépasse cette période (jusqu'à huit heures selon les antennes), celles-ci excèdent leur capacité d'autonomie et cessent d'émettre.

Ainsi, le degré de résilience des infrastructures critiques (notamment leur capacité à durer) a un rôle déterminant dans la propagation des cascades d'effets.⁷

Les infrastructures critiques disposant d'une longue autonomie sont plus susceptibles d'être prémunies longtemps de conséquences négatives et participent ainsi à élever le degré de résilience (physique et temporel) de l'ensemble d'un secteur. À l'inverse, les infrastructures critiques à faible autonomie fragilisent l'ensemble d'un secteur et contribuent de la sorte à la propagation rapide de perturbations, comme lors d'un *blackout*.

⁶ A cet égard, un des problèmes du modèle économique « just-in-time » est justement de réduire les stocks pour diminuer les coûts, mais cette pratique rend les systèmes plus vulnérables.

⁷ Cela s'applique également aux terminaux nécessaires à l'exploitation d'un service, comme les téléphones mobiles le sont pour la téléphonie mobile.

Type de service	Terminaux	Nœuds de commutation	Réseaux principaux	Capacité à durer du service
Téléphonie fixe (analogue)	Heures	Heures	Semaines	Heures
Téléphonie fixe (digital, VoIP)	Aucune	Heures	Semaines	Aucune
Téléphonie mobile	Jours	Heures	Semaines	Heures
Internet (internet mobile)	Aucune (heures)	Heures	Semaines	Aucune (heures)
Radio & télévision	Aucune	Jours	Jours	Aucune
Radio (receveurs indépendants)	Semaines	Semaines	Semaines	Semaines

Autonomie moyenne des services et infrastructures de télécommunications et des technologies de l'information sans alimentation électrique. Ce tableau fournit une bonne illustration de la manifestation de l'effet retard.

La vulnérabilité : Un critère déterminant

Un autre facteur à prendre en compte est la vulnérabilité. Déjà abordée dans la partie sur les déclencheurs du blackout, cette notion est centrale pour comprendre le degré de résilience des systèmes critiques. Dans le cas des infrastructures de télécommunications et des technologies de l'information, certains composants de ces systèmes disposent d'une très large autonomie. Plus leur importance nationale est élevée, plus leur alimentation de secours leur permet de durer. Cette disposition est pertinente en cas de coupure locale d'électricité, car le fonctionnement de ces systèmes est impératif à l'échelle nationale.

En revanche, dans le cas d'un *blackout* à large échelle, c'est l'autonomie des composants les plus faibles qui détermine le degré de résilience de l'ensemble du système. Par exemple, si les grands axes et les carrefours de communication d'internet disposent d'une autonomie respective de plusieurs semaines et de plusieurs heures, c'est la rupture de l'alimentation des routeurs (et ordinateurs) qui rend le système inutilisable. Exprimé autrement, ce sont les composants les plus fragiles d'un système qui sont déterminants dans la propagation des effets et dans la résilience de l'ensemble.

La criticité : Une mesure du degré de dangerosité des interdépendances

La criticité est un concept important pour identifier l'exposition d'un élément dans un système aux cascades d'effets. Mise à jour par les physiciens Per Bak et Kan Chen, la criticité peut être définie comme la mesure du degré d'interdépendances d'un système. En particulier, la criticité rend compte du degré de connectivité de ces interdépendances, à savoir leur capacité à diffuser des perturbations dans un système.

Dans un système dit « sous-critique », une perturbation externe ne produit que des dégâts localisés et mineurs, car les composants du système sont faiblement liés entre eux, voire pas du tout. En revanche, dans un système dit « sur-critique », une perturbation, même mineure, se diffuse dans une grande partie du système en occasionnant des dégâts significatifs, voire en détruisant certains composants.

Plus la criticité est forte, plus la probabilité que des effets

en cascade se diffusent d'un système à un autre, ou d'une infrastructure critique à une autre augmente. Ainsi, en cas de blackout, une société ayant des interdépendances réduites entre ses différents secteurs critiques sera moins affectée qu'une société fortement interdépendante comme celle des pays dits développés. Ainsi, les dégâts seront nettement plus importants dans le cas d'une société ultraconnectée.

Conclusion

Le *blackout* est un phénomène complexe dont la dangerosité fait consensus parmi les experts. Celle-ci est notamment le produit des interdépendances de nos sociétés et de ses infrastructures critiques. Dans ce cadre, il est dans l'intérêt de la sécurité de chercher à limiter ces interdépendances. Pour terminer, les concepts introduits dans cet article pour analyser le *blackout* gagneraient à être transposés à l'étude d'autres secteurs critiques et risques les affectant. La question est ouverte : où cette entreprise a-t-elle déjà été effectuée ? Sinon, où devrait-on s'y atteler ?

G. C.

Remerciements

Merci à Michel Dufour et Jacques Audergon pour leurs informations, conseils et relecture attentive.

Bibliographie indicative

- Per Bak and Kan Chen « Self-Organized Criticality », Scientific American, vol. 261, n° 1, janvier 1991, pp. 46–53.
- Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch et Ulrich Riehm, *What happens during a blackout: Consequences of a prolonged and wide-ranging power outage*, Office of Technology Assessment at the German Bundestag (Technology Assessment Studies Series), 2011, 260 p.
- Gianluca Pescaroli and David Alexander, *A definition of cascading disasters and cascading effects: Going beyond the 'toppling dominos' metaphor*, Planet@Risk, volume 2 (3), Global Risk Forum GRF Davos, 2015, pp. 58–67.
- Gianluca Pescaroli and David Alexander, *Critical infrastructure, panarchies and the vulnerability paths of cascading disasters*, Natural Hazards, volume 82, n° 1, 2016, pp. 175–192.
- Gianluca Pescaroli et al., *Cascading Impacts and Escalations in Wide-Area Power Failures*. UCL IRDR and London Resilience Special Report 2017-01, Institute for Risk and Disaster Reduction, University College, London, 2017, 16 p.



Les effets du *blackout* de 1977 sur l'éclairage de la ville de New York.

Blackout

Blackout : Les conséquences en heures et en jours

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

A quoi un article sur les conséquences d'un blackout¹ peut-il bien servir ? Cette interrogation appelle plusieurs constats. Le premier est que sans connaissance claire d'un enjeu, il est difficile de se positionner de façon informée. Le deuxième est que la population a peu, voire pas de connaissance sur la thématique et l'interprète comme un non-danger. Le troisième est que sans information ni sensibilisation, la préparation à un danger ne se fera pas d'elle-même.

La question « que se passe-t-il durant un *blackout* ? » forme le fil rouge de ce texte. Elle est secondée par deux autres interrogations : « le chaos peut-il s'installer ? » et « si oui, à partir de quand ? » À cet effet, cet article présente une synthèse des conséquences d'un *blackout* sur une large zone dans un milieu urbain moderne. Le scénario présenté suppose que l'aire touchée est trop importante pour que de l'assistance extérieure lui parvienne. Ce choix se justifie, d'une part, par la volonté de présenter toutes les cascades d'événements² possibles après l'arrêt de l'approvisionnement en électricité et, d'autre part, de souligner la vulnérabilité d'une société privée d'électricité. Dans ces circonstances, le scénario couvre l'ensemble du spectre des conséquences possibles et ne reflète donc pas les possibles effets atténuateurs des interventions extérieures.

En raison d'une trop grande variabilité des scénarios possibles au-delà d'une certaine durée et d'un manque de données, le texte ne couvre que les conséquences des premières heures jusqu'à huit jours après. Parmi celles-ci, on peut distinguer les perturbations, arrêts ou dégâts d'ordre technique, qui relèvent d'un enchaînement mécanique prévisible, des réactions de la société dans son

ensemble, qui appartiennent à la conjecture jugée la plus probable par les experts.

Quatre sources ont été retenues pour cette synthèse : le rapport de l'Office de l'évaluation technologique du parlement allemand³ (la référence en la matière), le roman « *Blackout* » de Marc Elsberg⁴ (considéré comme vraisemblable par les spécialistes des risques), un rapport de l'Institut de réduction des désastres et du risque de Londres⁵ et des discussions avec des spécialistes des analyses de risque.

En sus d'une synthèse des conséquences concrètes, cet article met en évidence les principaux domaines et secteurs touchés ainsi que les effets principaux d'un blackout. Il se structure ensuite en fonction des conséquences rangées en six périodes de temps. Enfin, le texte finit sur une évaluation critique des sources et des conséquences du *blackout*.

Introduction

Les effets d'une rupture de courant sont graduels. Ils diffèrent considérablement selon la durée et la temporalité du blackout. Les ruptures de courant en hiver ont des conséquences bien plus sévères qu'en été. Selon les infrastructures et les services touchés, les coupures se produisant en journée ont des effets plus chaotiques que pendant la nuit, ou inversement. Dans tous les cas, les domaines et secteurs suivants sont

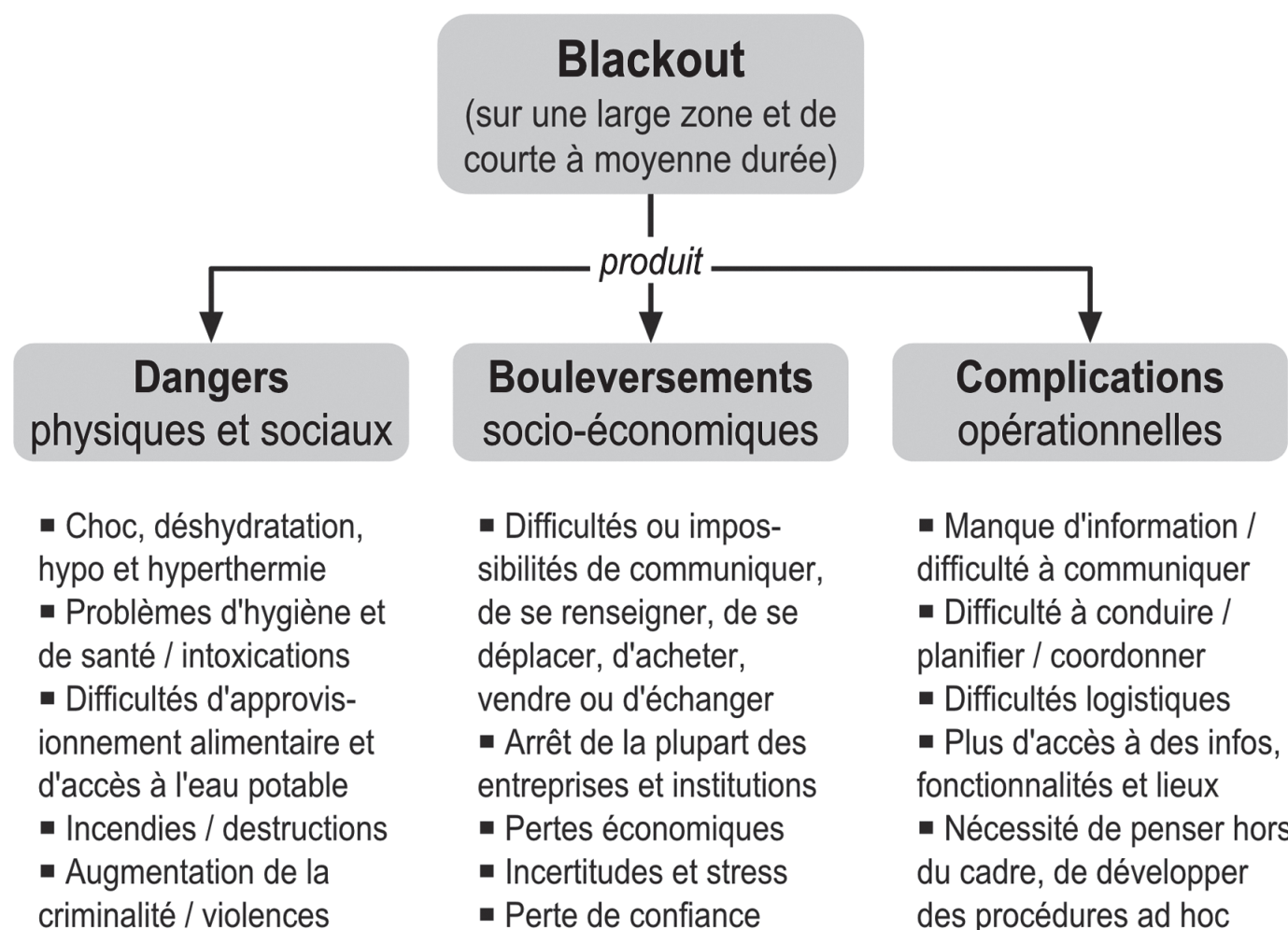
¹ Par *blackout*, on entend une interruption de l'alimentation en courant électrique d'une à plusieurs journées sur une large zone. Une panne de courant de quelques heures sur une aire limitée n'est pas à considérer comme un *blackout*.

² À ce sujet, lire l'article « *Blackout* : déclencheurs et mécanismes » dans ce dossier.

³ Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch et Ulrich Riehm, *What happens during a blackout: Consequences of a prolonged and wide-ranging power outage*, Office of Technology Assessment at the German Bundestag (Technology Assessment Studies Series), 2011, 260 p.

⁴ Marc Elsberg, *Blackout*, Piranha Editions, 2015, 475 p.

⁵ Gianluca Pescaroli et al., *Cascading Impacts and Escalations in Wide-Area Power Failures. UCL IRDR and London Resilience Special Report 2017-01*, Institute for Risk and Disaster Reduction, University College, London, 2017, 16 p.



Principaux effets d'un blackout de plusieurs jours sur une société moderne en milieu urbain.

impactés à divers degrés :

- Transport et trafic : réseau routier, réseau ferroviaire, trafic aérien ;
- Télécommunications et technologies de l'information : téléphonie fixe et mobile, internet et *data centers*, médias (radio, télévision, presse) ;
- Approvisionnement : alimentation, eau potable, traitement des eaux usées ;
- Santé : hygiène, production et acheminement de médicaments, prestations de soin, élimination des déchets ;
- Finance, banques et assurances : services bancaires, paiements électroniques, bourse ;
- Autorités : gestion de crise, services d'urgence et forces armées.

On peut classer les principaux effets d'un *blackout* en trois catégories : les dangers physiques et sociaux, les bouleversements socio-économiques et enfin, les complications opérationnelles. Celles-ci s'appliquent particulièrement aux organisations devant demeurer opérationnelles en tout temps, comme les services d'urgence et les autorités (voir illustration).

La compréhension du développement temporel d'un blackout révèle des interdépendances insoupçonnées

et permet de mieux saisir les conséquences de ces implications. Dans ce but, le texte présente ci-dessous le déroulement d'un blackout en six périodes successives : immédiatement après un blackout, de deux à huit heures, de huit heures à 24 heures, de 24 heures à sept jours et à partir huit jours.

Immédiatement après un blackout

Tous les systèmes nécessitant une alimentation électrique, mis à part ceux bénéficiant d'un approvisionnement de secours,⁶ cessent de fonctionner instantanément après l'interruption de courant. Le réseau routier est rapidement touché par des perturbations, surtout en milieu urbain. L'arrêt des feux de circulation crée la confusion. Cette situation est aggravée par le fait que les véhicules électriques sans alimentation auxiliaire, notamment les bus et les trams à caténaires, sont immobilisés sur les routes.

De ce fait, le nombre d'accidents de circulation augmente, alors que la congestion complique l'arrivée des services de secours. De plus, l'interruption du courant signifie que

⁶ Cet approvisionnement peut prendre deux formes : une génératrice ou des batteries dont le démarrage ou l'enclenchement est automatique après la coupure de courant.



Les artères de la ville de New York après la soirée du *blackout* de 1965. La ville demeure animée et ordonnée et plusieurs centaines de milliers de personnes rentrent chez elles à pied.

les pompes des stations essence ne fonctionnent plus et un nombre croissant d'automobilistes sont immobilisés en conséquence. Les passagers des transports publics sont soit bloqués, soit mis en retard. En fonction de la présence ou non de tunnels sur les tronçons, les autoroutes peuvent être fermées. En effet, l'absence de ventilation et d'éclairage dans les tunnels conduit à leur fermeture pour des raisons de sécurité. Cette fermeture rallonge les trajets et temps de parcours. Le trafic ferroviaire est également immédiatement touché.⁷ La grande majorité, voire la totalité des trains s'arrête (en fonction de la prévalence des locomotives diesel). Si, lors de l'interruption de courant, certains trains sont en gare, d'autres se retrouvent à l'arrêt dans des tunnels ou des tronçons ouverts. Très rapidement, l'ensemble du trafic restant doit cesser pour raisons d'encombrement ou de sécurité.

Dans le secteur des télécommunications, les téléphones fixes numériques, internet et la télévision sont mis immédiatement hors d'usage. Les communications mobiles peuvent être maintenues entre 30 minutes et 8 heures, en fonction de l'alimentation d'urgence des antennes. La téléphonie fixe (analogique) pourrait également demeurer opérationnelle plusieurs heures après un blackout.⁸ A l'exception des récepteurs autonomes (à pile/batterie ou embarqués comme dans les véhicules), la réception (ou transmission) radio cesse également de fonctionner.

Initialement, les centrales d'urgence disposent d'une alimentation électrique ininterrompue. Elles sont rapidement débordées par les appels provenant de personnes en détresse (par exemple bloquées dans les ascenseurs) ou victimes d'accidents (notamment de circulation). Dans le même temps, le réseau téléphonique

⁷ En Suisse, les CFF disposent de leur propre réseau électrique pour l'alimentation électrique des locomotives. Même si celui-ci n'était pas touché par un blackout, les systèmes de contrôle et de commande du réseau ainsi que l'alimentation électrique des gares sont raccordés au réseau standard et ne fonctionnent donc plus. De ce fait, le trafic doit cesser pour des raisons de sécurité.

⁸ Mais en Suisse, la Confédération a décidé de remplacer ce système par la téléphonie VoIP (numérique).

mobile devient saturé, à mesure qu'une partie de la population essayait de joindre ses proches pour s'informer. Cette explosion du nombre d'appels et la saturation du réseau compliquent l'organisation et l'accès aux services de secours. Il est possible que l'allongement des délais occasionné par la situation ait des conséquences mortelles.

Les commerces sont vite dépassés par la situation, surtout ceux sans éclairage naturel. Les systèmes de réfrigération, de sécurité et les portiques automatiques cessent de fonctionner. Même les enseignes disposant d'alimentation électrique de secours rencontrent des problèmes. En effet, avec l'arrêt des télécommunications, les terminaux de paiement par carte ne sont plus utilisables. De plus, les distributeurs automatiques ne marchent plus. Cette situation génère des tensions étant donné que la majorité de la population ne dispose que de peu, voire plus du tout d'argent liquide.

Les premières difficultés auxquelles les hôpitaux doivent faire face sont d'ordre organisationnel, avec des problèmes de télécommunications et une augmentation des admissions aux urgences. Disposant d'une alimentation électrique de secours, la plupart des services hospitaliers sont maintenus dans l'immédiat. La situation est plus aiguë dans les maisons de retraite, où l'arrêt de certains appareils peut rapidement impliquer le décès de certains patients. Les pharmacies connaissent les mêmes difficultés que les commerces.

Le secteur bancaire n'enregistre pas ou peu de perturbations immédiates, compte tenu de ses préparations préalables. Tant les données que le trafic de données financières ne sont pas touchés. Le trafic de paiements est maintenu, même s'il n'est généralement plus possible d'y accéder depuis un réseau externe au secteur bancaire. Les opérations des banques centrales ne sont pas affectées et les échanges européens peuvent en principe continuer. C'est également le cas des bourses, qui peuvent continuer leurs opérations avec un minimum de perturbations. La plupart des succursales (celles de grande et moyenne taille) disposent d'une alimentation électrique ininterrompue et mettent en œuvre leurs *business continuity plans*. En revanche, les petites agences connaissent les mêmes problèmes que les commerces.

2 à 8 heures après

La situation sur les routes évolue peu et les accidents y sont toujours aussi nombreux. La congestion urbaine tend cependant à se réduire, surtout à l'approche de la nuit. Dans les zones urbaines, les véhicules abandonnés, en particulier bus et trams, commencent à être évacués. Le trafic demeure élevé sur les autoroutes sans tunnels. Le transport routier de longue distance n'est initialement pas affecté par la coupure de courant. De plus en plus de camions doivent s'arrêter ou faire demi-tour parce qu'ils ne peuvent pas accéder à leur destination (en particulier en zone urbaine) ou parce que la marchandise ne peut plus être réceptionnée.

Les personnes à court d'essence ne peuvent plus solliciter leurs proches et restent livrées à elles-mêmes. Cette

situation est délicate, en particulier si le *blackout* a lieu en hiver. Ce problème est à mettre en relation avec l'impossibilité pour une partie des travailleurs de rentrer chez eux ou de se rendre à leur travail. Se déplacer en voiture devient compliqué puisqu'il n'est plus possible de faire le plein de carburant. Le nombre de véhicules abandonnés augmente.

Sur les rails, la plupart des trains et métros ont désormais été évacués. Les gares, qui s'étaient fortement remplies, commencent à se vider. Les compagnies ferroviaires parviennent partiellement à se réorganiser et à dégager les voies au moyen de locomotives diesel. Dans les commerces, une partie des enseignes passent à la gestion manuelle de la vente, certes plus lente, mais permettant de continuer leurs activités. Les produits réfrigérés commencent à s'avaries, dans les commerces et ailleurs. La plupart des systèmes de chauffage ou de climatisation sont à l'arrêt.

L'approvisionnement en eau commence en revanche à rencontrer des problèmes. Une partie des pompes ne dispose plus d'alimentation électrique d'urgence et cesse de fonctionner. Les autres infrastructures nécessaires au bon acheminement de l'eau (traitement de l'eau, systèmes de contrôle à distance) sont compromises si elles ne disposent pas d'alimentation de secours. Là où la pression est encore suffisante dans les canalisations, ou là où les bassins de rétention sont encore suffisamment remplis, obtenir de l'eau est encore possible. Les premières zones à ne plus être desservies en eau sont les plus éloignées géographiquement des pompes ou les plus en hauteur. Outre les problèmes d'hydratation, cette situation implique l'arrêt du bon fonctionnement des toilettes.

Le secteur hospitalier continue d'enregistrer une affluence considérable, en particulier en raison des accidents provoqués par le *blackout*. Les centres de dialyse ne disposent généralement pas d'alimentation électrique de secours et doivent fermer. Les services d'urgence voient la pression graduellement diminuer à mesure que le trafic se fluidifie, mais commencent à avoir des problèmes de communication, car les émetteurs-récepteurs fixes ne sont plus alimentés.

Le système d'évacuation des eaux usées connaît des problématiques similaires à celles du réseau de distribution d'eau. Les installations d'épuration des eaux qui ne disposent pas d'alimentation électrique d'urgence cessent de fonctionner. En conséquence, des dépôts de matière fécale et d'urine commencent à s'accumuler.

Dans le secteur bancaire, les agences qui avaient pu demeurer ouvertes continuent de fonctionner. En fonction des circonstances, certains établissements sont exploités sous la protection de la police. Le retrait d'argent aux guichets est toujours possible, même si les files d'attente s'allongent. Pour les individus ne pouvant se rendre en agence, le manque d'argent liquide commence à poser des problèmes.



Eclairage aux chandelles la soirée du *blackout* de New York en 1965. L'ambiance est à ce stade décontractée et amusée.

8 à 24 heures après

Sur les routes, le trafic diminue de même que le nombre d'accidents. Une partie des routes et des accès demeurent cependant bloqués. Mis à part les tronçons fermés pour raisons de sécurité, les autoroutes demeurent relativement peu affectées. En revanche, la situation des personnes bloquées sur les autoroutes et n'ayant pas été récupérées par leurs proches devient de plus en plus précaire. Dans les gares, la plupart des opérations ont cessé. Les stations sont pratiquement vides.

Les supermarchés encore ouverts le sont en fonction de la lumière disponible. La police doit intervenir dans certains d'entre eux parce que les clients n'ont pas d'argent liquide pour payer leurs achats. L'alimentation de secours des entrepôts cesse de fonctionner ou approche ses limites. L'industrie agricole est touchée par les premiers dégâts. Dans les fermes laitières, les exploitations sans alimentation d'urgence doivent traire les vaches à la main. Dans le cas où la traite ne pourrait pas être effectuée, les vaches laitières risquent l'infection, et à terme, la mort.

Les conditions d'exploitation du réseau de distribution d'eau, déjà fortement affecté, se dégradent encore. Dans les stations d'épuration, la température optimale ne peut plus être maintenue dans les bassins chimiques. L'eau stagnante pose des problèmes d'hygiène. Dans les hôpitaux, les perturbations requièrent une adaptation des plans d'urgence. L'électricité encore disponible est affectée aux départements prioritaires. Les cuisines cessent de fonctionner. Tous les patients qui ne nécessitent pas un traitement urgent ou peuvent rentrer à domicile sont renvoyés chez eux. Dans le même temps, les personnes auparavant bloquées dans les ascenseurs, trains, ou autres sont secourues par les services d'urgence. Une partie est redirigée vers les hôpitaux en raison de leur état de choc, de déshydratation ou d'hypothermie. La plupart des nouveaux patients arrive par ses propres moyens ou ceux de ses proches. Les personnes médicalement dépendantes sont amenées dans les hôpitaux par leur famille ou par les services de proximité. Dans les pharmacies sans alimentation de



Pour ceux qui ne peuvent pas rentrer chez eux, s'éclairer et se chauffer devient nécessaire. Ici, un groupe d'hommes brûle des journaux dans une poubelle lors de la nuit soirée du *blackout* de New York en 1965.

secours, les médicaments réfrigérés se réchauffent et deviennent inutilisables. Les clients nécessitant ces médicaments sont redirigés vers les hôpitaux. La situation des hôpitaux devient délicate. Dans les maisons de retraite, la température peut devenir dangereuse pour les résidents. Cette situation nécessite de transférer une partie des patients dans les hôpitaux ou de les confier à leurs familles.

Le secteur bancaire continue de fonctionner. Les guichets sont encore ouverts et on peut encore retirer de l'argent. Les files d'attente s'allongent encore. L'exploitation des dépôts et des investissements par le public est stoppée. Seuls les prêts extrêmement urgents sont encore accordés. Les processus critiques sont toujours assurés, mais les communications bancaires ne fonctionnent plus que sur des lignes dédiées. Si cela est possible, les préparations de délestage des opérations à une agence en dehors de la zone affectée sont effectuées.

24 heures à 7 jours après

Le trafic routier baisse fortement pour deux raisons : la pénurie de carburant et la fermeture de la plupart des commerces, entreprises et établissements publics. De la sorte, le nombre d'accidents décline fortement. Les moyens de transport non motorisés, comme le vélo, sont de plus en plus employés. Les transports en commun mettent en place des lignes opérées par des bus diesel sur des parcours prioritaires. La gestion du carburant devient critique, y compris pour les autorités. Le transport de marchandises baisse fortement et les camions encore en circulation sont affectés prioritairement à la distribution de biens de première nécessité.

La situation sur le rail s'améliore sensiblement. Les tronçons et tunnels précédemment fermés sont rouverts une fois que la situation de blackout est estimée durer plus longtemps. Cette mesure permet la circulation prudente

de quelques trains, en particulier pour le transport de marchandises. La plupart des employés ne se rend pas au travail, à part là où ils savent avec certitude que leur présence est indispensable. La plupart des individus demeure à domicile. Des centres d'accueil sont ouverts pour les personnes à risque, notamment si la température extérieure est trop basse ou trop élevée.

La plupart des entrepôts alimentaires cessent leurs opérations dans les deux premiers jours. Les supermarchés encore ouverts se vident dans les deux à cinq jours. Comme la plupart des individus ne peuvent plus cuisiner, la demande en denrées alimentaires se focalise sur les produits de base pouvant être consommés facilement. Des distributions d'urgence de biens de première nécessité sont organisées, mais elles n'atteignent pas forcément toute la population. Sans ravitaillement, la plupart des ménages épuisent leurs réserves en moyenne entre trois (milieu urbain) et sept jours (milieu rural).

Un marché noir apparaît où des produits avariés sont vendus. Des individus consomment des produits alimentaires avariés et doivent se rendre à l'hôpital. Les personnes disposant de réchauds à gaz, de cheminées ou de grills y recourent. Certains provoquent des départs de feu, qui sont particulièrement difficiles à éteindre étant donné que les bornes incendies ne sont plus alimentées.

Dans l'industrie agricole, les pertes s'accumulent. Les stocks prêts à la vente ne peuvent pas être livrés. Dans ces conditions, les stocks, le bétail et les plantations sous serre peuvent se dégrader sous l'effet des températures. Les bœufs, porcs et poulets résistent aux perturbations, mais celles-ci occasionnent stress, agressivité et cannibalisme animal.

Cinq jours après le blackout, les générateurs de secours des infrastructures critiques arrivent au bout de leurs réserves. Là où l'approvisionnement en eau fonctionnait encore, il s'arrête. Les bassins de rétention se vident définitivement. Les opérations d'épuration des eaux usées aussi. Dans les toilettes, l'accumulation d'urine et de matières fécales commence à poser des problèmes d'hygiène. Les hôpitaux ne sont pas tous équipés pour faire face à ce problème. En outre, ceux-ci manquent de plus en plus de matériel et de médicaments. Seules les opérations les plus prioritaires sont encore effectuées. L'énergie encore disponible est rationnée.

Dans le secteur bancaire, la délivrance de prêts n'est plus possible. Dans le même temps, les paiements planifiés sont encore exécutés. En fonction de la perception de la durée du blackout, les demandes de retrait en liquide peuvent grandement varier. Si la population estime que le courant sera bientôt rétabli, les retraits demeurent modérés. Dans le cas contraire et si les agences ne peuvent pas se réapprovisionner en liquide, les guichets ferment les uns après les autres. Cette situation peut parfois virer au chaos et la police doit intervenir (si elle est disponible). Les agences se recentrent sur le maintien des processus critiques et leur transfert à l'extérieur de la région affectée. Les banques ne pouvant pas le faire se préparent

Période	Perturbation	Types de risques/dangers (mentionnés le plus tôt où ils peuvent se manifester)
0-2 heures	Stupéfaction	Accidents, difficultés de déplacement et d'appel aux services de secours, personnes coincées
2-8 heures	Confusion	Stress, choc, pénurie d'eau, pénurie de carburant, stress monétaire, décès (personnes assistées)
8-24 heures	Détérioration	Hypo et hyperthermie, immobilisation, fermeture de commerces, heurts sur moyens de paiement
2-4 jours	Dégradation	Incendies, pénurie alimentaire et de fournitures médicales, intoxications, fermeture bancaire
5 à 7 jours	Désorganisation	Marché noir, épuisement du personnel d'urgence et des alimentations de secours, agressivité
8 jours et plus	Désagrégation	Effondrement des structures d'intervention et de soin, repli communautaire, pillages, violences
?	Désintégration	Soif/faim/maladies, prédation individuelle ou collective, dégradation terminale des infra critiques

Tableau synoptique de l'évolution d'une situation de blackout et risques/dangers associés

à de lourdes pertes. Les bourses disposent toujours d'une alimentation de secours et les échanges de titres peuvent se poursuivre, mais avec une baisse de régime.

7 jours et plus

Sur les routes, le trafic est réduit au minimum. Le transit sur les autoroutes décline fortement. Le risque de se retrouver coincé sur les routes agit comme un puissant dissuasif pour les individus qui peuvent encore circuler. Dans ces circonstances, une sélection de tunnels critiques est rouverte au public, même si la ventilation ne fonctionne pas. Le transport ferroviaire continue d'opérer à régime très limité. Des tronçons restreints et quelques stations sont rouverts pour les passagers.

Dans le domaine de la santé, la situation est catastrophique. Les hôpitaux manquent de tout et ne peuvent plus prendre de nouveaux soins en charge, voire assurer les soins en cours. Des départements entiers sont fermés. Là où c'est possible, les patients sont transférés vers des zones non affectées. Dans le cas où cette éventualité n'est pas envisageable, le personnel médical se retrouve dans des situations délicates le confrontant à des dilemmes éthiques. Sans renfort de l'extérieur, les hôpitaux et organisations d'urgence arrivent aux limites de leurs capacités, alors qu'une partie de leur personnel ne vient plus travailler.

Presque toutes les pharmacies sont désormais fermées. La production et la livraison de médicaments deviennent des enjeux centraux. L'insuline vient à manquer pour les diabétiques, mettant ces personnes en danger. Il est possible qu'à ce stade, un marché noir des produits pharmaceutiques se mette en place. Les personnes nécessitant une dialyse commencent à se trouver en danger mortel. Dans cette situation, l'effondrement de l'ensemble du système médical de la zone affectée devient probable : il dépend des réserves à disposition, de la pression de la population et de l'aide reçue de l'extérieur.

Si les autorités n'arrivent pas à couvrir les besoins de base de la population, des mouvements de foule, des émeutes sont à prévoir. L'augmentation de la criminalité aussi. Les ménages qui le peuvent fuient la zone affectée s'ils ne l'ont pas déjà fait. Si l'aire touchée est trop étendue pour en sortir, des logiques communautaires peuvent se mettre en place.

Evaluation

La présentation du déroulement d'un *blackout* sans fin définie et sans réception d'une aide extérieure permet de mesurer le considérable risque que ce scénario représente. Les problèmes posés par l'interruption de l'alimentation électrique sont multiples, non-linéaires et peuvent s'amplifier de plusieurs manières. Dans ce sens, un scénario de *blackout*, même limité à une journée, met clairement en évidence la vulnérabilité de nos sociétés à une rupture d'approvisionnement d'un bien critique. Quelques jours après une rupture de l'alimentation électrique, le scénario souligne comment, en l'absence de réserves, les biens de base sont épuisés et les problèmes de liquidité paralysent la société. Poussé à une semaine, le scénario de *blackout* indique le peu de résilience et d'adaptabilité de nos sociétés dépourvues d'électricité.

Tout le long de ce déroulement, les perturbations augmentent, passant de la stupéfaction à la désagrégation (voir tableau). La question se pose : que peut-on faire ? La tournure chaotique que prennent les événements dès le milieu de la première semaine indique que les services d'urgence et les autorités sont très rapidement débordés, désorganisés, dépassés et ensuite épuisés. Cette situation n'est pas « gérable » et pourrait à terme mener à un effondrement terminal de la société. Cependant, la situation pourrait devenir bien plus grave ou arriver bien plus rapidement. Trois éléments viennent appuyer cette éventualité :

- Les deux documents de référence principaux sont vieux : sept ans. Durant cette période, bien des techniques et usages ont changé. Ainsi, plusieurs nouveaux risques ne sont pas représentés⁹ ;
- Des discussions avec des spécialistes de risques reprochent à ces documents d'être trop optimistes. Pour eux, la situation pourrait virer au chaos bien avant le délai de huit jours. L'absence de considération de cette possibilité les préoccupe ;
- Enfin, tant le rapport de l'Office de l'évaluation technologique du parlement allemand que le roman « Blackout » passent totalement sous silence l'immense problème du rétablissement et reconstruction du réseau, qui pourrait prendre plusieurs semaines à plusieurs mois, voire des années dans certains cas. Ce

⁹ Notamment les « nouveaux risques », tels que décrits dans l'entretien de Michel Dufour dans ce dossier.

problème devrait fortement détériorer une situation déjà très fragile. Toutes les implications du délai nécessaire à la pleine reconstruction du réseau ne sont pas bien connues et les conséquences mesurées.

Conclusion

Le risque de *blackout* est élevé. Sa gravité est fortement sous-estimée, en partie en raison de l'absence de connaissance de l'ensemble des conséquences de la matérialisation de ce risque. Il est de la responsabilité des décideurs, des acteurs compétents et de la société dans son ensemble d'œuvrer à sa prévention ou à la constitution d'une résilience sociétale pour en limiter les impacts. Toutefois, il est possible que ces derniers soient plus importants qu'anticipés. Dans ce cadre, il est dans l'intérêt de se préparer adéquatement face à ce risque, notamment en établissant des stratégies, procédures et stocks permettant d'assurer des prestations minimales pendant un tel scénario. Enfin, il serait nécessaire d'évaluer les vulnérabilités apparues depuis sept ans et ainsi d'effectuer une mise à jour complète d'un scénario de blackout tenant compte de celles-ci. Car sans information pertinente, pas de préparation appropriée.

G. C.

Des passants passent la nuit du 11 septembre 1965 dans une gare lors du *blackout* à New York. L'ambiance est moins décontractée et l'inconfort rend la situation déjà pénible. Et ce n'est que le premier jour.



Roman : *Blackout*

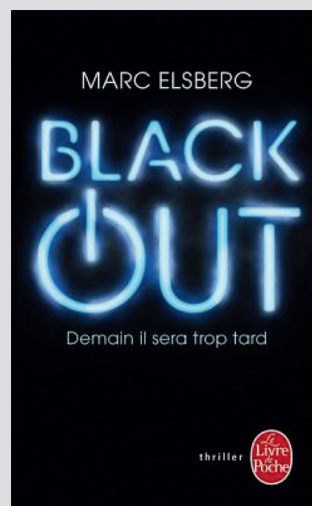
« Le confort matériel augmente. Le courant vient directement de la prise. Depuis des générations. Les gens n'y font même plus attention ! C'est normal pour eux. » Alors, quand un groupe de cyberanarchistes réussit à paralyser le réseau électrique européen, ses habitants sont forcés de reconnaître leur dépendance à ce bien critique. Rapidement, les besoins de base ne sont plus assurés. L'Europe plonge dans un chaos graduel, sans assurance d'en sortir. Il fait noir au propre comme au figuré : « l'obscurité » s'imisce dans la vie des Européens.

Deus ex machina oblige, les *hackers* sont finalement arrêtés, et l'électricité est en partie rétablie deux semaines après. Mais l'Europe a échappé de peu à un effondrement terminal. Cette trame, c'est celle du roman « *Blackout* » de l'auteur allemand Marc Elsberg. Signé en 2012, « *Blackout* » est un *thriller* d'anticipation, mais pas de science-fiction. En effet, Marc Elsberg a effectué une longue recherche avant la rédaction de l'ouvrage et interviewé une multitude d'experts. Il en ressort un scénario réaliste sur la thématique des vulnérabilités des réseaux électriques contemporains et des sociétés modernes aux ruptures d'approvisionnement en électricité.

Au-delà de l'aspect frénétique de la recherche de l'origine de la coupure de courant et des aspects romancés du récit, « *Blackout* » constitue un avertissement de la fragilité des modes de vie occidentaux et du modèle d'approvisionnement « juste-à-temps ». « *Blackout* » s'affirme comme une critique de la logique du profit sur celle de la sécurité et de la foi aveugle en la technique. La panne initiale est d'ailleurs provoquée par le piratage de trois compteurs électriques individuels supposément « smart », entraînant la chute des réseaux. La puissance des infrastructures et réseaux techniques est alors anéantie.

Aujourd'hui, réaliser presque toutes les tâches quotidiennes nécessite de l'électricité. Les infrastructures critiques ne sont pas ou peu protégées contre une interruption du courant et, plus grave, elles partagent toutes des logiciels de gestion similaires « SCADA », qui les rendent plus vulnérables à une attaque informatique coordonnée. Dans ce cadre, « *Black-Out* » constitue une invitation à reconsidérer l'emprise de l'électricité dans nos vies et du modèle d'approvisionnement « juste-à-temps ». Car « demain, il sera trop tard ».

Marc Elsberg, *Blackout, Demain il sera trop tard*, Le livre de poche, 2016, 552 p.





Blackout

Jacques Audergon : Evolution de la perception du risque de blackout de 2004 à 2018

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Jacques Audergon est ingénieur EPFL en Génie civil. Il dispose de plus de 48 ans d'expérience dans le domaine. Au début des années 2000, il se spécialise dans l'analyse de risques et, en particulier, de celui du *blackout*. Dans cet entretien, Jacques Audergon analyse pour la RMS le risque de blackout en perspective de ses quinze ans d'expérience. Il résume l'évolution de la perception du risque de *blackout* depuis le début du nouveau millénaire, analyse les facteurs de cette évolution et enfin livre sa perception du risque et comment celui-ci devrait être pris en compte. S'il fallait résumer cet entretien en un message, c'est que le risque de *blackout* doit être considéré avec le plus grand sérieux.

Revue militaire suisse: Depuis 2004, vous accompagnez les cantons romands dans leurs analyses de risques. Comment la perception du risque de blackout a-t-elle évolué depuis?

Jacques Audergon: La perception du risque de blackout a surtout évolué chez les électriciens, ceux-ci exerçant une influence prépondérante sur l'analyse des risques dans le domaine de l'approvisionnement électrique. En 2004, la posture des représentants du secteur électrique suisse était empreinte de très grande prudence. On admettait la possibilité de petites coupures, mais pas d'interruption de l'alimentation électrique à grande échelle. En quinze ans, bien des choses ont changé. Les scénarios de blackout national, voire européen, ne sont plus exclus.

Par exemple, en 2004-2005, lors de l'analyse des risques pour le canton de Fribourg, le blackout faisait partie des scénarios envisagés. Celui-ci avait été accueilli par les cadres du secteur électrique avec beaucoup de scepticisme. Finalement, un compromis avait été trouvé sous la forme d'une panne touchant le Canton pendant 24 heures avec probabilité d'occurrence moyenne d'une fois par 5'000 ans.

Lors de l'analyse des risques du canton de Vaud trois ans plus tard (2006-2008), les électriciens admettaient déjà un changement d'appréciation: un scénario de blackout européen d'une certaine durée n'était plus exclu. Il était toutefois considéré comme un cas extrême avec une probabilité d'occurrence de l'ordre d'une fois par 2'000 ans. En revanche, un scénario de crise énergétique extrême entraînant une pénurie électrique sévère (réduisant l'offre de 50%) pendant plusieurs semaines — en particulier pendant l'hiver — était estimé pouvoir se produire une fois tous les 500 ans. Cette évaluation plaçait alors la pénurie en deuxième risque le plus important pour la population.

Deux ans plus tard, dans le cadre de l'analyse des risques pour le canton du Valais (2010), les électriciens admettaient la possibilité d'un blackout européen d'une semaine, avec une probabilité d'occurrence de l'ordre d'une fois tous les 1'000 ans. L'évaluation de ce scénario extraordinaire a alors contribué à placer ce risque en septième position.

Quatre ans plus tard, lors de l'analyse des risques pour le canton de Neuchâtel (2014), le scénario d'un blackout européen d'une durée d'une semaine était admis, avec un temps de retour estimé à 400 ans, plaçant ce risque en cinquième position. Dans le même temps, le scénario de pénurie électrique sévère (réduisant l'offre de 50%) pendant six mois était estimé pouvoir se produire avec une probabilité d'occurrence d'une fois tous les 500 ans. Ce risque représentait alors le deuxième risque le plus important pour le Canton.

Aujourd'hui, l'actualisation de l'analyse des risques pour le canton de Genève vient de se terminer (2018). Pour la première fois, la possibilité d'un blackout européen d'une durée de trois jours constitue le premier risque pour le canton, avec une probabilité d'occurrence d'une fois par 100 ans. Inspiré du scénario moyen développé par

Risque	Année (et canton)	Aire	Durée	Probabilité	N° du risque
Pénurie (de 50 % pour tous sauf 2014 : 30 %)	2004-5 (Fribourg)	Suisse	1 mois	1x / 100 ans	2
	2006-8 (Vaud)	Suisse	3-4 mois	1x / 500 ans	2
	2010 (Valais)	Suisse	6 mois	1x / 500 ans	6
	2014 (Neuchâtel)	Suisse	6 mois	1x / 500 ans	2
	2018 (Genève)	Europe	6 mois	1x / 500 ans	4
Blackout	2004-5 (Fribourg)	Canton	24 heures	1x / 5000 ans	9
	2006-8 (Vaud)	Europe	2 semaines	1x / 2000 ans	7
	2010 (Valais)	Europe	1 semaine	1x / 1000 ans	7
	2014 (Neuchâtel)	Europe	1 semaine	1x / 400 ans	5
	2018 (Genève)	Europe	3 jours	1x / 100 ans	1

Tableau synthétique de l'évolution de la perception des risques liés à la pénurie ou panne électrique par les différents cantons romands de 2004 à 2018. Si la perception du risque de pénurie a peu évolué, l'appréhension du risque de blackout est passée de la neuvième à la première place.

l'Office fédéral de la protection de la population (OFPP)¹ le scénario genevois est limité à trois jours, mais touche toute l'Europe. Les analyses de risque du canton du Jura sont en cours. Dans ce cadre, il est possible que les estimations évoluent encore.

RMS: On passe d'une estimation d'un blackout de 24 heures à trois jours (voire une semaine), et d'un temps de retour de 5000 à 100 ans. Comment expliquez-vous cette évolution? Quels facteurs auraient pu contribuer à la prise en compte du risque?

J.A. : Plusieurs facteurs peuvent expliquer cette évolution. Je relèverais l'incertitude sur l'avenir de la production électrique, le risque de cyberattaques, les évaluations du risque de blackout par l'OFPP et enfin, les exercices de conduite stratégiques nationaux. Il me semble difficile de dire lequel de ces facteurs est le plus important. La réalité est probablement plus nuancée, ces facteurs agissant en conjonction et se renforçant mutuellement. Il est également possible que le roman de Marc Elsberg « Blackout » (paru en 2012)² ou l'émission spéciale (six heures) de la télévision Suisse-Allemande sur le sujet en janvier 2017 ait pu influencer les évaluations les plus récentes.

Tout d'abord, les débats sur l'avenir du nucléaire, puis la décision d'arrêter ce moyen de production électrique, la difficulté de construire de nouvelles installations hydroélectriques ou thermiques (à gaz) ont rendu les électriciens circonspects sur l'avenir. De ce fait, l'approvisionnement électrique ne peut plus être considéré garanti et des pannes électriques à très grande échelle semblent ne plus relever de l'impossible.

Ensuite, les électriciens ont graduellement pris conscience de la fragilité et de la saturation du réseau européen avec les blackouts italien du 28 septembre 2003 (57 millions de personnes touchées) et européen du 4 novembre 2006 (15 millions de personnes affectées). Même si la Suisse

n'a pas connu de blackout, des pannes importantes ont eu lieu. Le 22 juin 2005, une panne géante affecte le réseau dédié des CFF. Le trafic ferroviaire est bloqué de 18 à 5 heures du matin. 100'000 personnes se retrouvent bloquées dans les trains. N'oublions pas non plus la panne du 22 février 2010 qui frappe Lausanne pendant deux heures. Cette panne a marqué les esprits en Suisse romande. Puis, la situation de l'hiver 2015-2016 a souligné le peu de marges du réseau électrique suisse. La situation était particulièrement critique. Il s'en est fallu de peu pour que l'Office fédéral de l'approvisionnement économique (OFAE)³ déclenche les plans de rationnement électrique.⁴

Parallèlement à cette prise de conscience, l'intensification des tentatives de pénétration des hackers a mis en évidence les vulnérabilités des systèmes de commande. L'épisode de stuxnet (2009) a achevé de démontrer qu'avec suffisamment de ressources et de temps, aucun système — y compris ceux de la branche électrique — n'est définitivement protégé. Ces éléments ont contribué à un changement de perception quant à la fiabilité des systèmes de commande et de contrôle face au risque de piratage informatique, ce dernier pouvant conduire à des pannes organisées. Ndlr : sur ce sujet, lire l'entretien de Michel Dufour dans ce dossier.'

Le 13 octobre 2014, l'OFPP, dans le cadre de l'analyse nationale des dangers, a convié une quarantaine d'experts et de responsables des principales branches économiques suisses sur la question du blackout⁵. J'y ai participé. À

³ Ndlr : la RMS a consacré un article à l'OFAE et aux stocks stratégiques suisses. Voir Grégoire Chambaz et Julien Perrochet, « Stocks stratégiques et approvisionnement économique du pays », *Revue militaire suisse*, 5/2017, 7p.

⁴ Le 2 décembre 2015, les réacteurs nucléaires de Beznau I et II sont momentanément à l'arrêt. De plus, le niveau des barrages est particulièrement bas. La situation fait craindre le pire. L'organisation de gestion du réseau de transport, Swissgrid et l'État-major fédéral de gestion de crise ABCN sont réunis. La décision de rationner n'est pas prise, mais la situation demeurera critique une partie de l'hiver en raison du niveau des barrages.

⁵ Notamment, des représentants de Swissgrid, des CFF, de la Migros, des banques, de l'Office fédéral de l'environnement et d'autres offices fédéraux.

¹ Ndlr : Pour plus de précisions sur ce scénario, se référer à l'entretien de Stefan Brem dans ce dossier.

² Ndlr, l'édition du livre en français : Marc Elsberg, *Blackout*, Piranha Editions, 2015, 475 p.

l'issue de la séance d'échanges et de présentations, un vote a été organisé à bulletin secret pour déterminer l'évaluation moyenne de la probabilité d'un blackout de trois jours touchant un grand nombre de cantons.⁶ Le résultat du vote a été : une fois par 40 ans.

Enfin, deux exercices de conduite stratégique incluant le thème blackout ont été menés en 2009 et en 2014. Ils s'inscrivent dans la volonté des autorités de pouvoir réagir et conduire lors d'une interruption de l'alimentation de courant. Le premier exercice était organisé par la Chancellerie fédérale et testait les états-majors de crise et la rapidité des flux d'information entre la Centrale nationale d'alarme (CENAL), les organes de conduite cantonaux et les exploitants de réseau. Le deuxième exercice a été organisé par le nouvellement créé Réseau national de sécurité (RNS), avec un scénario comportant une panne d'électricité à grande échelle. Plus vaste, ce second exercice, intitulé ERNS14, a testé la gestion de crise et la communication entre la Confédération, les cantons ainsi que les exploitants de réseau et de certaines infrastructures critiques. (Un prochain exercice incluant la thématique blackout est prévu 2019).

Si les exercices de conduite stratégique indiquaient que le risque de blackout est pris très au sérieux par la Confédération, la préoccupation des autorités a été clairement soulignée par le discours de Guy Parmelin à l'occasion du 11^e Congrès suisse de l'électricité le 12 janvier 2017. Le Conseiller fédéral y déclarait : les exercices de conduite stratégique sont indispensables pour exercer les organes compétents, car « la panne généralisée ou la pénurie d'électricité ne relèvent pas de l'utopie ».

L'ensemble de ces différents facteurs a probablement participé d'une façon ou d'une autre à la prise en compte du blackout comme une thématique centrale. Cela semble le cas à la fois pour le secteur électrique suisse et pour les autorités, qu'elles soient cantonales ou fédérales.

RMS: A la lumière des éléments qui précèdent, comment évaluez-vous le risque de blackout? Quels autres éléments devraient être pris en compte pour s'en protéger?

J.A. : Premièrement, le réseau électrique européen étant interconnecté, un blackout peut toucher tous les pays européens, y compris la Suisse, même si notre pays n'a pas connu jusqu'à ce jour un tel événement. Ce point n'est généralement pas suffisamment pris en compte, même si les analyses de risques des cantons et de la Confédération le reconnaissent.

Deuxièmement, l'accroissement grandissant des interconnexions et interdépendances, notamment informatiques, provoque une augmentation exponentielle de la vulnérabilité de nos sociétés. Le développement à plein régime de l'internet des objets constitue un danger pour la résilience de nos sociétés, en particulier face au risque de blackout. Face à ces développements, peu semblent conscientiser les dangers que cette situation implique.

Portrait express

Après des études d'ingénieur en génie civil, Jacques Audergon travaille pendant cinq ans dans un bureau spécialisé dans les grands barrages. En 1974, il devient directeur de la succursale de Fribourg d'un bureau de génie civil. Sept ans plus tard, il fonde le bureau d'ingénieurs Geimesa, spécialisé dans les systèmes énergétiques et les techniques du bâtiment. Parallèlement, il poursuit une carrière militaire comme officier de renseignement d'artillerie. Après avoir pris sa retraite en 2011, Jacques Audergon continue ses activités de conseil en nom propre.

Parmi ses réalisations, figurent la conception, la construction et l'expérimentation d'un des premiers véhicules électriques avec moteurs dans les roues (Mobilec, 1981-1989) ainsi que la réalisation de l'analyse des risques des cantons de Fribourg, Genève, Neuchâtel, Vaud et du Valais. Depuis, 2009, Jacques Audergon est également responsable de l'organe intercommunal de conduite en cas de catastrophe de la Haute Sarine Rive Droite (Fribourg).

Dans une optique stratégique, des acteurs étatiques, voire non étatiques, peuvent maintenant frapper à distance, cela sans engager de moyens conventionnels. Ainsi, ils peuvent mettre un adversaire à genoux en paralysant ou détruisant ses infrastructures vitales et en particulier son approvisionnement électrique.⁷ S'il semble qu'aujourd'hui tous les électriciens ont pris conscience du sérieux de ce risque, cela est-il le cas de nos institutions de sécurité, à l'instar de l'armée ?

Troisièmement, il ne faudrait pas oublier les risques « humains ». Il s'agit concrètement des risques découlant de la négligence, des vulnérabilités propres dont l'adversaire pourrait prendre avantage (avec du social engineering) ou encore de la malveillance. Ce dernier cas est probablement plus difficile à admettre pour les exploitants de réseaux qu'une cyberattaque, mais le risque est pourtant bien réel. Compte tenu de la nature actuelle du réseau, le déclenchement d'une panne par un employé mécontent occupant un poste névralgique est de l'ordre du techniquement possible. Notons que dans un tel cas, l'ampleur de la panne devrait rester limitée. On ne peut toutefois exclure qu'une conjugaison d'événements puisse déboucher sur un véritable blackout.

En guise de conclusion, j'aimerais user d'une métaphore. Si l'eau est un élément vital et indispensable à l'humanité, l'électricité est devenue un élément essentiel des sociétés développées. C'est en quelque sorte le sang de nos sociétés modernes. Ce constat semble également partagé par le chef du DDPS dans son discours du 12 janvier 2017. Dans ce cadre, il est de notre responsabilité d'assurer que ce sang puisse circuler et que ses artères demeurent ouvertes.

Propos recueillis par Grégoire Chambaz

6 Ndlr: Il s'agit du « scénario moyen » de l'OFPP. Celui-ci est détaillé dans l'entretien de Stefan Brem, dans ce dossier.

7 Ndlr: sur ce sujet, consulter l'entretien de Michel Dufour dans ce dossier.



Blackout

Philippe Bettens : Vieillissement du réseau électrique suisse et risque de *blackout*

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Philippe Bettens est ingénieur en Génie électrique et spécialiste du transport de l'électricité. Il dispose de plus de 35 ans d'expérience dans le domaine et d'une connaissance particulière des infrastructures électriques nationales. Dans cet entretien, Philippe Bettens dresse le tableau de l'état du réseau électrique suisse. Plus précisément, il cartographie l'évolution des enjeux de sécurité du réseau et des acteurs de cette sécurité. A travers des observations factuelles et une analyse d'expert, Philippe Bettens livre à la RMS son évaluation des risques liés au réseau électrique suisse. Dans ce cadre, il estime plausible le risque de *blackout*, notamment en raison du vieillissement des infrastructures.

RMS : Pour le citoyen moyen, le réseau électrique suisse semble garantir la fourniture d'électricité. Selon votre expertise, cela correspond-il à la réalité ?

Philippe Bettens : Si on se réfère à la communication destinée au citoyen, l'approvisionnement apparaît effectivement comme garanti. Or cette communication ne traite pas (ou rarement) du réseau, dont la vocation est seulement d'acheminer cette électricité. Pourtant, je constate que le réseau et les infrastructures qui le composent n'évoluent guère, alors que le contexte ne cesse de se modifier.

Ce réseau électrique est une infrastructure affectée par des limites de capacité et de durée de vie. Il peut être considéré en deux parties : le réseau de transport et de répartition (l'équivalent des autoroutes et des routes cantonales) et le réseau de distribution (les routes et chemins communaux). Le réseau de transport et de répartition comporte les postes de transformation et les lignes à haute tension (dont la majorité est aérienne). Il assure l'approvisionnement national et régional en électricité. Le réseau de distribution est constitué des lignes à moyenne et basse tension (en zone urbaine, la plus grande partie est souterraine). Il assure la distribution de l'électricité aux consommateurs.

Mes analyses se concentrent particulièrement sur le réseau de transport et de répartition. Elles tendent à conclure que son état est aujourd'hui préoccupant. Cette infrastructure devient vétuste et les risques associés sont grandissants, comme la corrosion des supports métalliques ou des implantations immobilières qui entravent des projets de renouvellement ou d'extensions. A mes yeux, l'état du réseau de distribution est moins alarmant. Les installations correspondantes sont nettement moins coûteuses et leurs besoins en (re) construction sont donc plus faciles à satisfaire.

RMS : Vous disposez de quarante ans d'expérience dans le domaine. Cette situation a-t-elle toujours été la norme ? Si non, quels ont été les changements majeurs ?

PB : À la fin du 20^e siècle, le secteur électrique suisse se saisissait des problèmes qui se présentaient et les résolvait. Les responsabilités étaient plutôt bien définies et plutôt bien assumées. On renouvelait le réseau à haute tension et on l'étendait là où cela était jugé nécessaire.

L'ouverture du marché de l'électricité, décidée en 1999 et entrée en vigueur en 2009, a opéré un changement de paradigme fondamental. Pour l'avoir vécu de l'intérieur, je dirais que cela a surtout engendré un climat de grande incertitude. Concrètement, on a assisté à une véritable chute des investissements consacrés aux renouvellements et extensions. De plus, les infrastructures à l'échelon de transport ont été en quelque sorte expropriées et la société nationale Swissgrid, a été créée pour gérer ces dernières. C'est un fait sans précédent dans notre pays et, dans le milieu, cela a fait l'effet d'une révolution.

De fait, toute la chaîne a été impactée : des constructions approuvées ont été reportées ; des projets en cours ont été retardés ou arrêtés ; les demandes d'autorisations de construction ont décliné¹ ; les remises en cause des études

¹ Notamment au vu de l'adversité rencontrée par les requérants dans les procédures d'approbation d'une nouvelle ligne à haute tension,

préliminaires se sont multipliées ; et les planificateurs ont été confrontés par leur hiérarchie ou leurs partenaires à une avalanche de remises en question et de doutes.

Aujourd'hui, un fond d'incertitudes malsaines demeure. Ainsi, l'infrastructure électrique suisse vieillit et — par la force des choses — se dégrade continuellement. Par exemple, la dernière ligne à haute tension dont j'ai dirigé le remplacement accusait l'âge de 70 ans. Au train où vont les choses, cela va devenir monnaie courante. La problématique est officiellement connue, mais officiellement n'est pas une priorité. Combien temps cette situation pourra-t-elle durer sans conséquences dommageables ?

RMS: Aujourd'hui, quels sont les acteurs responsables de la sécurité du réseau? Quels problèmes rencontrent-ils ?

PB: En Suisse, les échelons de transport et de répartition de l'alimentation électrique comprennent une vingtaine de propriétaires et d'exploitants. Leurs intérêts sont à présent principalement concentrés en dehors du domaine strict de l'infrastructure d'acheminement de l'électricité. Les conditions-cadres suffisantes n'apparaissent pas réunies, aux yeux de beaucoup, pour assurer les investissements nécessaires. Par exemple, plusieurs propriétaires et exploitants affichent publiquement que c'est essentiellement par des activités de service qu'ils financent les dividendes versés à leurs actionnaires. Cependant, ces services ne font pas partie de leur activité historique — pour ne pas dire leur raison d'être —, à savoir l'approvisionnement d'une collectivité en électricité, y compris la construction et l'entretien des infrastructures pour acheminer cette électricité.

En outre, plusieurs autres acteurs sont apparus dans le nouveau système d'exploitation du réseau, mis en place lors de l'ouverture du marché de l'électricité. La régulation correspondante est complexe. Dans ce cadre, un peu moins de dix ans après, la répartition des responsabilités entre les différents acteurs n'est pas toujours bien établie. Quoi qu'il en soit, cette situation fait apparaître un manque de coordination, de leadership et de vision d'ensemble à long terme.

Mes contacts avec des acteurs du domaine ont mis une évidence une gêne et un malaise croissant à évoquer la sécurité du réseau. Ce phénomène est à associer avec un autre, à savoir le refus grandissant de mes interlocuteurs d'engager leur responsabilité ou leur nom par rapport à des informations sur l'état du réseau. Par exemple, j'ai récemment sollicité un organisme parapublic pour une enquête sur la question. Celui-ci a refusé de s'associer à la démarche par crainte de conséquences politiques. Cette situation laisse songeur.

RMS: Vous mentionnez la réduction drastique des investissements dans le réseau électrique. Quels sont les effets de cette diminution de moyens ?

PB: A la fin des années 1980, nous disposions d'une

des processus conflictuels par nature.

Portrait express

Après des études en ingénierie électrique, Philippe Bettens travaille pour les acteurs de l'économie électrique suisse. Ses premiers postes se situent tout d'abord dans le secteur privé : ingénieur de projet, chef de projet, puis responsable de ceux-ci en tant que maître d'ouvrage. Vingt-cinq ans plus tard (en 2007), il rejoint l'Office fédéral des transports en tant que collaborateur scientifique. Il entre ensuite en 2012 comme spécialiste de lignes à haute tension à Swissgrid, la nouvelle société propriétaire et gestionnaire du réseau électrique suisse de transport.

Depuis 2016, il exerce une activité indépendante. Philippe Bettens est également l'auteur de plusieurs publications techniques sur la sécurité, la gestion et la planification du réseau électrique.

bonne vingtaine de prestataires suisses pour monter des pylônes ou mettre en place des mâts en béton. Aujourd'hui, ceux qui subsistent se comptent sur les doigts de la main. C'est un exemple de perte de ressources, de savoir-faire et d'autonomie pour entretenir, moderniser, renouveler voire étendre une infrastructure qui est essentielle. À présent, les grands projets en cours doivent inmanquablement recourir à des prestataires étrangers.

Au-delà de la tendance au non-renouvellement des installations techniques, la législation encadrant ces renouvellements se modifie. Les lois, les règlements et la jurisprudence évoluent dans un sens qui ne cesse d'être défavorable à l'entretien ou l'expansion nécessaires du réseau. Plusieurs récentes planifications de l'aménagement du territoire ne semblent simplement pas prendre en compte la nature vitale des installations électriques. Ces conditions sont une source d'inquiétude légitime.

RMS: La situation ne semble pas optimale. Dans l'idéal, comment le réseau électrique devrait-il être géré ?

PB: Avant tout, la discussion devrait s'effectuer sur une base factuelle, même si cette situation est désagréable. Le vieillissement du réseau devrait être abordé de front. Une grande partie du réseau est à rénover. Certes, cet effort de réalisme suppose du courage politique, mais la situation me semble l'exiger.

Ensuite, la relance d'une planification à long terme est d'un intérêt public manifeste. C'est une question de bon sens. Cette planification pourrait être marginalement inexacte, mais, comme « la prospective, c'est remplacer l'incertitude par l'erreur », disposer d'un plan est préférable à son absence. A cet égard, la nouvelle loi² adoptée en décembre 2017 par le parlement ne va pas dans la bonne direction. Elle s'aligne sur l'horizon de planification de l'aménagement du territoire : 15 ans.

² Loi fédérale du 15 décembre 2017 sur la transformation et l'extension des réseaux électriques, voir <https://www.admin.ch/opc/fr/federal-gazette/2017/7485.pdf>

Cette durée n'est pas adéquate pour des infrastructures qui s'amortissent généralement sur 30 ans et qui sont construites pour 50, 70 ou 80 ans.

RMS: La situation est-elle grave au point que la Suisse puisse connaître un *blackout*? Quels sont les risques?

PB: La situation me semble relativement grave et pourrait le devenir plus encore. Si la tendance au vieillissement n'est pas inversée, le réseau haute tension va inévitablement s'affaiblir et présenter de plus en plus de vulnérabilités. Dans ce contexte, un *blackout* pourrait se produire. Je ne saurais affirmer où se situent les premiers risques.

RMS: Dans ce cadre, quelle serait la durée d'un *blackout* potentiel? Est-ce qu'une interruption de courant d'une semaine est plausible?

PB: J'ai connu de l'intérieur le *blackout* d'un canton entier. Les exploitants avaient fait preuve d'une grande débrouillardise. En une demi-journée, le réseau avait pu être partiellement rétabli dans la région concernée. Aujourd'hui, nous pouvons continuer à compter sur les compétences très pointues des responsables d'exploitation. Mais la situation en 2018 est sensiblement différente de celle d'il y a vingt ans en deux points: premièrement, l'infrastructure 50 à 400 kV (le réseau de lignes à haute tension) a peu évolué, donc est de moins en moins adaptée. Deuxièmement, les exploitants sont contraints de poser de plus en plus de câbles souterrains, notamment pour éviter des procédures d'approbation interminables. Or, si une ligne électrique aérienne peut (la plupart du temps) être provisoirement rétablie en quelques heures, il en va tout autrement pour les réparations de câbles électriques souterrains. De ce fait, on peut s'attendre à ce que la restauration du réseau prenne plutôt quelques jours.

RMS: Vous mentionnez le risque de *blackout* comme non négligeable. Comment la problématique est-elle perçue et traitée par les institutions du secteur?

PB: L'économie électrique suisse et ses relais au sein des administrations fédérales et cantonales ont toujours bénéficié de structures de gestion de crises. J'en ai encore eu la confirmation tout récemment. Ainsi, il ne faut pas douter que l'anticipation des effets d'un *blackout* mobilise des moyens et du personnel. Ces efforts se concentrent toutefois sur les « effets » et non les « causes ». Pourtant, c'est bien la résolution ou l'atténuation des origines du problème qui pourrait réaliser les progrès les plus significatifs dans la réduction des risques. Mes analyses indiquent cependant que ces préoccupations passent au second plan, si elles ne sont pas purement et simplement négligées... et que des spécialistes de la communication s'affairent pour rassurer certaines autorités et la population.

RMS: Quelle est la vision du problème par les entreprises du secteur? Quelles mesures prennent-elles? Estiment-elles le risque au sérieux?

PB: Les entreprises du secteur font actuellement face à

beaucoup d'interrogations. Les renvois de responsabilités sont très fréquents. En outre ces entreprises consomment depuis des années leur réserves, les « marges de dimensionnement ».³ Les décideurs actuels sont logiquement tentés de prolonger cette situation pour deux raisons: d'une part, l'état du réseau est relativisé par rapport aux défis à relever dans le domaine de la production, de l'achat ou de la vente d'électricité et, d'autre part, la situation juridique n'incite pas, voire entrave, le renouvellement et l'extension du réseau.

RMS: Qu'en est-il au niveau des autorités? Que font-elles? Reconnaittent-elles le danger?

PB: Bien des autorités et leurs administrations me semblent plus préoccupées par la maîtrise de leur communication que par la résolution de la problématique de fond. De plus, leurs actions ne me semblent pas toujours suffisamment coordonnées. Certaines pratiques, par exemple au sein de l'Office fédéral de l'environnement, laissent perplexe. En effet, dans une procédure d'approbation d'une nouvelle ligne électrique, l'office en question a récemment produit deux prises de positions contradictoires. Or, la Confédération a la responsabilité de procéder à des pesées d'intérêts et de trancher le cas échéant. La pratique que je rapporte contribue en tous cas directement à la lenteur des procédures, donc au phénomène de vieillissement du réseau.

Un autre exemple de manque de coordination est l'ordonnance sur la protection contre le « rayonnement non ionisant »⁴ (ORNI). L'ORNI a pour principale conséquence d'accroître les distances entre les installations électriques et les lieux fréquentés par des personnes. Concrètement, la complexité de l'ordonnance complique les procédures et pose des problèmes multiples lorsqu'il faut concevoir ou modifier une infrastructure. L'élaboration, puis la mise en vigueur de l'ORNI sont emblématiques d'un comportement en « cavalier seul », en l'occurrence de l'Office fédéral déjà évoqué. Cette ordonnance aurait pu susciter une importante coopération entre aménagistes du territoire et électriciens. Les directives de son application auraient pu occasionner des rencontres entre ces deux corps de métier et traiter des problèmes avant leur émergence.

..... Suite en page 58

³ Les marges de dimensionnement désignent ici les marges de planification et de sécurité établies avant l'ouverture du marché de l'électricité, lorsque s'opérait une véritable planification à long terme.

⁴ Le rayonnement non ionisant considéré par l'ORNI correspond au champ électrique et au champ magnétique produits par bon nombre d'installations électriques.



Blackout

Stefan Brem : La pénurie d'électricité et le *blackout* dans l'analyse nationale des dangers

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Stefan Brem est docteur en sciences politiques. En tant que directeur de la section d'analyse des risques et de coordination de la recherche à l'Office fédéral de la protection de la population (OFPP), il dispose de plus de 10 ans d'expérience dans le domaine. Dans le cadre de son mandat, Stefan Brem a coordonné l'Analyse nationale des dangers, une étude établissant 32 fiches individuelles de risques pouvant toucher la Suisse. Parmi ces risques figurent la pénurie d'électricité et le *blackout*. Dans cet entretien, Stefan Brem décrypte pour la RMS les enjeux de ces deux risques pour la Suisse. En particulier, il livre la version de l'OFPP d'un scénario de possible *blackout* et des dangers associés. Enfin, il conclut en faisant le résumé des possibles mesures de prévention à l'échelle nationale, cantonale et individuelle.

RMS: Dans l'analyse nationale des dangers, l'OFPP envisage les risques de pénurie d'électricité et de panne électrique. De quoi s'agit-il exactement?

Stefan Brem : La pénurie d'électricité et la panne électrique peuvent avoir de graves conséquences. Ces deux notions sont souvent confondues alors que leur nature et les mesures qu'elles appellent diffèrent significativement. C'est pourquoi l'OFPP les distingue dans l'analyse nationale des dangers :

- *La pénurie d'électricité y est définie comme une inadéquation entre l'offre et la demande d'électricité. Cette situation peut se produire en raison d'une réduction des capacités de production, de transport ou d'importation. Elle peut durer de plusieurs jours à quelques semaines, voire plusieurs mois ;¹*
- *La panne d'approvisionnement électrique (ou « la panne d'électricité ») y est caractérisée par l'inter-*

ruption de l'approvisionnement en électricité à la suite de dommages aux infrastructures de transport ou de distribution, de problèmes de production ou de dysfonctionnements du système de gestion. Lorsqu'un réseau d'approvisionnement s'est entièrement effondré, on parle de « blackout ».

RMS: Quelles seraient les principales conséquences d'une pénurie électrique, notamment sur le plan de la sécurité?

SB : En cas de pénurie, l'approvisionnement d'une part importante des consommateurs finaux (par exemple) n'est plus assuré. Des interruptions de l'alimentation peuvent alors se produire. Afin d'éviter des coupures de courant à large échelle pendant la pénurie, des mesures de rationnement sont introduites pour équilibrer la production et la demande.

L'OFPP identifie plusieurs scénarios de pénurie d'électricité dans l'analyse nationale des dangers. Parmi ceux-ci, le scénario majeur consiste en une réduction de 30 % de l'approvisionnement en électricité durant plusieurs mois en hiver. Les conséquences de ce scénario sont graves et porteraient significativement préjudice à l'économie et à la population. Les dommages encourus sont estimés à plus de 100 milliards de francs.

En outre, ce scénario requiert une adaptation des mesures de sécurité. En effet, il deviendra difficile, voire impossible de joindre les services d'intervention² dans les régions touchées par la pénurie en raison des perturbations affectant les réseaux téléphoniques (fixes et mobiles). Dans ce cadre, on peut s'attendre à une recrudescence du sentiment d'insécurité dans la population. L'accroissement des cambriolages et les agressions ponctuelles pourraient accroître ce phénomène et faire chuter la confiance de la population envers les autorités.

¹ Cette situation peut notamment se produire lorsque le niveau des cours d'eau et des barrages est bas et que par conséquent, la production hydroélectrique est insuffisante. Cette situation peut également contraindre les centrales nucléaires de diminuer leur production par manque d'eau de refroidissement ou alors d'eau trop chaude.

² Ndlr : les organisations « feux bleus ».

Portrait express

Après des études en histoire, sciences politiques, droit public et droit international, Stefan Brem entreprend une thèse en sciences politiques à l'Université de Zürich. Dans ce cadre, il séjourne une année à l'Université Georgetown à Washington, avant d'obtenir son doctorat en 2003. De 2003 à 2007, Stefan Brem rejoint le Centre pour la politique internationale de sécurité (aujourd'hui la Division politique de sécurité) du DFAE comme collaborateur scientifique.

Depuis lors, il dirige la section d'analyse des risques et de coordination de la recherche à l'OFPP au sein du DDPS. Les tâches de cette unité sont multiples : mettre en œuvre la stratégie nationale de protection des infrastructures critiques ; procéder périodiquement à une analyse nationale des risques ; et aider les cantons à effectuer leurs propres analyses des dangers et leurs planifications prévisionnelles.

RMS : Dans ce cadre, comment l'OFPP aborde le blackout ?

SB : Plusieurs facteurs et événements d'intensité variable peuvent provoquer une panne d'électricité. De petites pannes se produisent régulièrement. En principe, ces pannes ne durent que quelques minutes ou quelques heures et ne causent pas de graves dommages. Toutefois, des interruptions plus grandes peuvent se produire, que cela soit par panne subite ou effondrement du réseau à la suite d'une pénurie d'électricité. Cette situation provoque des graves conséquences pour l'ensemble des clients dépendants d'un approvisionnement en électricité : les infrastructures vitales et critiques, l'économie et la population. Sans électricité, notre société est paralysée.

RMS : Quels sont les principaux scénarios envisagés et les risques associés ?

SB : L'analyse nationale des dangers établit plusieurs scénarios d'intensité différente parmi de nombreux développements envisageables. Ils ne font pas office de prévision, mais permettent d'envisager différentes conséquences et ainsi de s'y préparer de manière adaptée. Ces scénarios sont au nombre de trois :

- **Scénario « important » :** un blackout d'une journée sur un territoire de la taille d'un canton moyen et le rétablissement de la situation en une journée. Dans ce scénario, les infrastructures touchées sont les lignes à moyenne tension et le réseau n'est pas physiquement endommagé ;
- **Scénario « majeur » :** une interruption de courant de deux à quatre jours en été dans plusieurs cantons, y compris dans de grandes zones urbaines. Ce cas de figure pourrait toucher un grand nombre d'infrastructures critiques et jusqu'à 1,5 million de personnes. Dans ce scénario, le réseau à haute tension est endommagé et nécessite deux à trois jours de réparation être rétabli. Le retour à la normale est progressif et peut prendre plus d'un mois. L'OFPP estime le risque que ce scénario se produise à une fois tous les trente ans ;
- **Scénario « extrême » :** un blackout national de cinq à sept jours en plein hiver. Ce cas de figure envisage des dommages importants aux infrastructures du réseau de haute tension et aux organes de commande. Trois à quatre semaines seraient nécessaires pour rétablir progressivement le réseau. Le retour total à la normale pourrait prendre plusieurs mois.

RMS : Quels seraient les principaux secteurs affectés par un blackout en Suisse ?

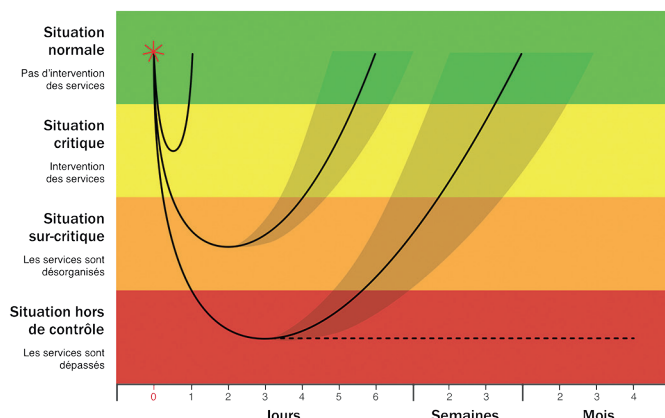
SB : Avant toute considération, il faut rappeler qu'en cas de survenue d'une panne d'électricité, ni sa durée, ni l'ampleur des dégâts occasionnés ne peuvent être anticipées. Une panne d'approvisionnement électrique de plusieurs jours à plus d'une semaine toucherait tous les domaines de la vie quotidienne, travail et loisirs compris. Les services vitaux, comme les communications, la circulation de l'argent ou encore l'approvisionnement en combustibles et en carburants seraient sérieusement perturbés.

RMS : Dans le cas de la survenue d'un blackout d'intensité « majeure », quels dangers pourraient en découler ?

SB : Dès le début de la panne, les systèmes d'alimentation électrique sans interruption (ASI) et les groupes électrogènes s'enclenchent de manière à ce que les systèmes essentiels continuent de fonctionner. De cette façon, les entreprises et organisations disposant de tels systèmes continuent leurs opérations. C'est le cas des centres de calcul et des sièges des grandes banques ainsi que des hôpitaux (en grande partie). En revanche, les systèmes électroniques, de communication, d'éclairage, etc. cessent brusquement de fonctionner dans les entreprises et organisations sans ASI. Dès que la panne est caractérisée comme un blackout, les entreprises renvoient leur personnel à la maison.

Le premier jour, la situation des transports est difficile. Les trains ne roulent plus. Si les CFF disposent de leur propre réseau électrique, le contrôle du trafic ferroviaire et des aiguillages dépend du réseau public. Des bus de remplacement sont mis en place, mais les temps d'attente sont longs pour les voyageurs. Sur les routes, le chaos règne. Les trams et les trolleybus sont immobilisés sur les routes et bloquent de ce fait le trafic. Les feux

Les trois différents scénarios de l'OFPP et leurs conséquences. Notez qu'un quatrième scénario appartient à l'ordre du possible, à savoir une désintégration terminale de la société suite des trop grands dommages et une incapacité à rétablir le réseau, et donc les services.



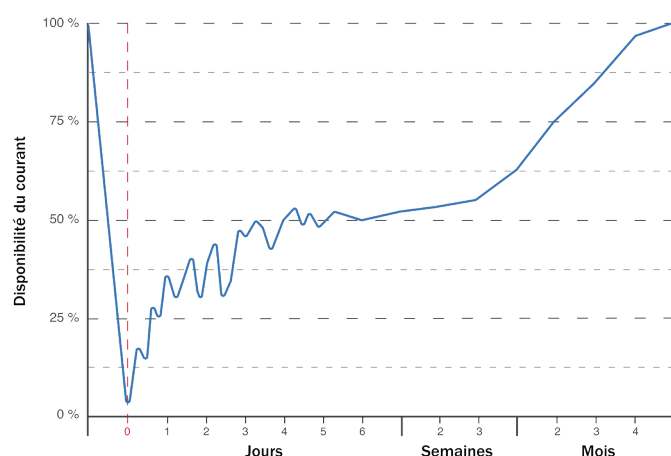
de circulation ne fonctionnent pas. Pour des raisons de sécurité, les tunnels sont fermés. Les accidents se multiplient. Le deuxième jour, la situation commence à s'améliorer sur les routes. Cependant, l'essence commence à manquer, les pompes des stations-service ne fonctionnant plus.

Chez l'habitant, les réfrigérateurs et congélateurs ne fonctionnent plus. La chaîne du froid est rompue et la nourriture commence à s'avaler, un phénomène aggravé en été. Sans électricité, la cuisine s'effectue à gaz ou au feu de bois. Cette situation entraîne par négligence plusieurs incendies ou intoxications au gaz. Les ménages n'ayant pas constitué de réserves se retrouvent vite à court de provisions. Les magasins ayant encore de la nourriture à vendre se vident. Seuls les paiements en espèces ont désormais cours, les caisses enregistreuses et les lecteurs de cartes bancaires ne fonctionnant plus. Pourtant, peu d'argent liquide circule, car les distributeurs de billets sont également hors service.

Dans les premières minutes après l'interruption de courant, les centraux téléphoniques des organisations d'urgence sont fortement sollicités pour des accidents, des ascenseurs bloqués, des altercations dans les commerces (en raison de l'impossibilité d'encaisser), etc. En raison du chaos de la situation et des appels d'urgence, le réseau téléphonique mobile est rapidement surchargé après l'interruption de courant. Toutefois, le nombre d'appels diminue progressivement au bout d'une demi-heure, car l'ASI de la majorité des antennes ne fonctionne plus. La majorité des personnes affectée ne peuvent alors plus communiquer par téléphone, mis à part celles qui disposent encore de téléphones fixes analogiques³.

La panne des systèmes informatiques et de communication complique fortement le travail des forces d'intervention. Après quelques heures, les autorités parviennent tout de même à informer et à conseiller la population par points d'informations, haut-parleurs ou encore par radio. Toutefois, seules les radios à piles ou à capteur solaire fonctionnent encore. La pression médiatique augmente. Les organisations de secours interviennent depuis l'extérieur de la région touchée. Elles mettent place des postes de distribution de nourriture et surtout d'eau. En effet, l'approvisionnement en eau et l'évacuation des eaux usées sont partiellement hors service. Afin de prévenir les pillages et d'autres actes criminels, la police mobilise toutes ses ressources et met en place des patrouilles régulières. Des policiers supplémentaires sont dépêchés en soutien par les cantons voisins.

Après le premier jour, plusieurs individus consomment de la nourriture avariée et sont intoxiqués en conséquence. Les secours arrivent trop tard pour quelques blessés ou malades, les organisations d'intervention n'étant pas joignables et/ou les appareils maintenant leur survie étant à l'arrêt. Les autorités et les organisations d'intervention mettent à disposition des hébergements



Représentation schématique (indicative, non exhaustive) de la disponibilité du courant électrique avant, pendant et après un *blackout*. Notez que le rétablissement et la remontée du réseau peuvent prendre plusieurs semaines à plusieurs mois.

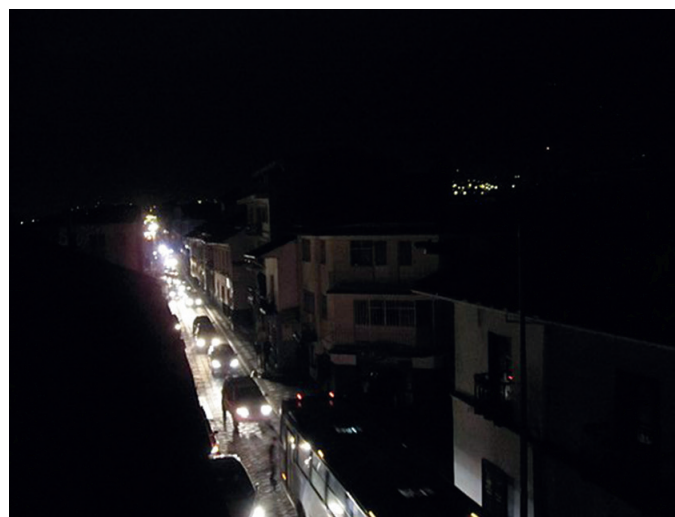
de secours (par exemple des abris de la protection civile) pour les personnes nécessitant une prise en charge. Même après le rétablissement de l'électricité, la situation n'est pas encore maîtrisée. Quelques jours, voire quelques semaines, sont encore nécessaires pour que la situation se normalise.

RMS: Dans la perspective d'un blackout, comment la population peut-elle se préparer de façon à subir le minimum de dommages?

SB: Chacune et chacun devrait prendre des dispositions en prévision d'une catastrophe ou d'une situation d'urgence. La plupart des mesures recommandées peuvent s'appliquer à un large éventail de cas de figure. Chaque ménage devrait disposer de provisions pour pouvoir s'alimenter plusieurs jours sans électricité. À cette fin, une réserve de denrées alimentaires pouvant se conserver sans réfrigération est indispensable (par exemple, les conserves). De plus, l'OFPP recommande de stocker neuf litres d'eau par personne par jour⁴ (pour

4 Ndlr: cela correspond, pour une semaine de consommation, à 252 litres pour une famille de quatre personnes.

La ville de Quito en Equateur après les grandes pannes de 2017.



3 Ndlr: Non dépendant d'une alimentation électrique externe.

l'hydratation, la cuisine et l'hygiène). Disposer d'un plan en cas d'urgence est par ailleurs fortement recommandé. Ce concernant, une check-liste et d'autres informations utiles sont disponibles sur www.alertswiss.ch.

RMS: Dans cette perspective, quelles préparations et quelles actions les entreprises peuvent-elles effectuer lors d'une coupure d'électricité?

SB: Il est important que les compagnies d'électricité révisent leurs processus, vérifient leurs points faibles et le cas échéant, prennent les mesures nécessaires pour éviter des pannes à grande échelle. L'OFPP recommande aux exploitants d'infrastructures critiques (adduction d'eau, télécommunications, transports, etc.) de vérifier et d'améliorer leur résilience⁵ face à des coupures d'électricité et d'autres risques importants (comme les cyberattaques). Il faut notamment vérifier si elles disposent d'emplacements redondants et consolider leurs principaux processus en tenant compte du risque de pénurie d'électricité. Dans ce sens, l'Office fédéral de l'approvisionnement économique du pays (OFAE)⁶ a édité une brochure regroupant des conseils utiles, notamment pour les PME.

RMS: Enfin, que font les cantons et la Confédération pour se préparer à un tel cas?

SB: La Confédération et plusieurs cantons ont élaboré des planifications préventives en cas de panne de courant à grande échelle (KATAPLAN). La planification de la Confédération a été mise à jour pour la dernière fois en 2011. En outre, le réseau national de sécurité a exercé la Confédération et les cantons en 2014 dans un scénario de pénurie d'électricité de longue durée. Les enseignements en gestion de crise de cet exercice ont été traduits en 16 recommandations, elles-mêmes transposées en 42 mesures. La plupart de celles-ci ont été mises en œuvre depuis et feront l'objet de vérifications lors de prochains exercices. Manque encore: des systèmes de communication sécurisés pour les autorités et un réseau intégral de suivi de la situation. Ces moyens feront l'objet d'un débat au niveau politique ces prochains mois.

RMS: Pour terminer, comment la population pourrait-elle aider l'OFPP avant, pendant et après un blackout?

SB: Tout d'abord, une recommandation technique. En cas de blackout, la règle d'or est la suivante: débrancher tous les appareils fonctionnant sur le réseau. Une fois

⁵ La résilience est un concept fondamental pour la protection des infrastructures critiques et la lutte contre les catastrophes à l'heure actuelle. Il s'agit de définir ce qu'il faut protéger (personnes, biens, infrastructures, etc.), de connaître la vulnérabilité et d'identifier les menaces. On prendra ensuite des mesures adéquates pour éviter les dommages (capacité de résistance), maintenir autant que possible les fonctionnalités (capacité d'adaptation) ou les rétablir au plus vite (capacité de régénération). Une protection complète repose aussi bien sur des mesures prises par les pouvoirs publics (p. ex. les organisations de crise intégrale, les systèmes de communication sécurisés), les acteurs économiques (protection des infrastructures critiques) et les individus (préparation personnelle).

⁶ Ndrl: la RMS a consacré un article à l'OFAE l'année dernière. Voir Chambaz, G. et Perrochet, J., « Stocks stratégiques et approvisionnement économique du pays », RMS 2017/5.

que le courant est rétabli, réenclencher progressivement les appareils, afin d'éviter une surcharge du réseau. Pour le reste, les mêmes consignes s'appliquent que pour les autres catastrophes. Il ne faut utiliser les voies de communication et les routes qu'en cas de nécessité.

Ensuite, pour les autorités, la meilleure aide, c'est celle qu'elles n'ont pas à apporter. Dans ce cadre, la population devrait s'intéresser aux dangers et prendre les dispositions recommandées par les autorités, et ce dès aujourd'hui. Les personnes déjà informées peuvent sensibiliser leur entourage. Les individus et familles qui prennent se préparent à subvenir à leurs besoins pendant quelque temps⁷ — et peut-être ceux de leurs voisins — déchargent significativement les autorités et les services d'intervention. En cas de blackout, ces derniers ont déjà fort à faire pour rétablir la situation et venir en aide aux personnes vulnérables.

Propos recueillis par Grégoire Chambaz

⁷ Ndrl: L'OFPP recommande 3 à 4 jours.

Suite de la page 54

Pourtant, à ma connaissance, rien n'a été mis sur pied. Le résultat est un durcissement sans équivalent des conditions-cadres propres à l'infrastructure électrique en Suisse: les exigences y sont cent fois plus contraignantes que ce qui se pratique dans les pays environnants. Ainsi et en se prévalant du principe de précaution, l'ORNI peut expliquer une partie du retard que nous prenons dans le renouvellement d'un élément essentiel pour la qualité de vie et le bien-être économique que connaît notre pays.

RMS: Votre analyse se concentre sur des problèmes potentiels. Quelles solutions pourraient changer la situation?

PB: J'ai déjà évoqué un besoin de réalisme, de bon sens et de probable nécessaire courage au plan politique. Fondamentalement, la situation pourrait enregistrer une amélioration très claire si les dysfonctionnements liés à la complexité de l'organisation du marché de l'électricité étaient traités à la hauteur de l'enjeu. Une gouvernance adaptée apparaît comme une condition préalable à toute amélioration: les responsabilités devraient être rassemblées là où elles sont trop fractionnées. De mon point de vue, la coordination doit être significativement renforcée là où le nombre de parties prenantes s'est multiplié. Peut-être qu'un changement à la tête du département fédéral de l'énergie donnera à ces perspectives une occasion de se concrétiser.

Propos recueillis par Grégoire Chambaz



Blackout

Michel Dufour : Un risque de *blackout* accru ? Les dangers du tout-numérique

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Michel Dufour est docteur en physique. Il dispose de plus de 35 ans d'expérience dans le domaine des études globales de risques. Spécialiste des risques pour la Confédération, il a principalement œuvré à l'élaboration des analyses globales de risques et la construction de plusieurs exercices de conduite stratégique. Il exerce actuellement comme expert pour le Département fédéral de la Défense, de la protection de la population et des sports, notamment dans le domaine des risques numériques. Dans cet entretien, Michel Dufour livre dans un premier temps son analyse de l'évolution de la nature des risques depuis les années 80 et cartographie de nouveaux risques peu, voire encore inconnus de nos jours. Dans un second temps, il décrypte les impacts de cette cartographie sur le risque de *blackout*, pour finir par en tirer les conséquences pour la politique de sécurité suisse.

Revue militaire suisse : Vous étudiez les risques depuis près de 40 ans. Quelle a été l'évolution de l'appréhension des risques ? Leur perception a-t-elle toujours été à la hauteur de leur gravité ?

Michel Dufour : Je distingue l'évolution suivante dans la perception des risques. Pendant la guerre froide, le risque majeur se situait dans le domaine militaire avec le péril nucléaire. La chute du mur de Berlin n'a pas fait disparaître ce risque, mais a mis en évidence les risques liés aux domaines économiques, technologiques, environnementaux, politiques et sociaux. Cela a marqué une rupture fondamentale.

Depuis le milieu des années 1990, la Confédération dispose d'une cartographie très complète de ces risques. La plupart de ceux-ci se sont matérialisés depuis à divers degrés : les pandémies, le terrorisme, les migrations non contrôlées, le changement climatique, etc. A-t-on oublié la crise de l'UBS ? Cette crise avait déjà été envisagée par la Banque Nationale en 1996 dans le rapport « Risikoprofil Schweiz ». Ce rapport décrivait pour la

première fois le spectre complet des risques auxquels la Suisse est exposée, mais n'a jamais été distribué pour des raisons politiques.

Aujourd'hui, à l'agenda politique, on trouve les risques globaux représentés par le changement climatique, l'épuisement des ressources et la pollution de l'air, de l'eau des sols. Si la perception actuelle de ces risques correspond assez bien à leur gravité, la volonté politique d'y faire face est encore insuffisante. Si aucune action suffisante n'est prise, ces risques pourraient à terme bouleverser la planète, et avec elle, la Suisse.

RMS : Dans l'immédiat, quels sont aujourd'hui les risques les plus importants pour la Suisse ?

M.D. : Dans l'immédiat, les trois risques les plus importants pour la Suisse sont le *blackout*, la pandémie, ou l'éclatement d'une nouvelle bulle financière. Le délai de préalerte face à ces trois risques est court, voire nul. La Suisse n'a pas encore connu de *blackout* grave, mais aujourd'hui, ce risque est devenu l'un des plus probables et les plus graves.

Une pandémie grave pourrait toucher la moitié de la population (active) en Suisse aurait des effets désastreux. Cependant, une pandémie légère survenant dans une situation dégradée, par exemple en cas de pénurie d'énergie, pourrait également avoir des effets désastreux. En 2005, la Confédération avait effectué un exercice de conduite stratégique sur le thème de la pandémie. Lorsqu'une pandémie a éclaté en 2009, la Suisse était bien préparée. Par chance, cette pandémie était de faible gravité et a pu être rapidement maîtrisée.

La crise financière de 2008 a été une crise importante, mais les effets en cascade ont pu être majoritairement évités. Il n'est pas certain qu'on parvienne à limiter aussi bien les effets d'une nouvelle crise financière. Jusqu'ici, ces risques sont assez bien connus dans l'ensemble, mais

Portrait express

Après des études de physique à l'EPFL et une thèse à l'Université de Berne, Michel Dufour entre en 1977 au Département militaire fédéral (aujourd'hui le DDPS) comme collaborateur scientifique spécialisé dans la prospective technologique. Il collabore aussi dès 1983 au lancement des études globales de risques à l'Office central de la défense (OCD), office supprimé en 1999. En sus, il participe en 1996 et 1997 à l'élaboration et au suivi du premier exercice de conduite stratégique sur la vulnérabilité de la société de l'information.

En 2001, il devient consultant indépendant, mais continue à travailler comme coach pour la Confédération. Parmi ses mandats figurent l'accompagnement du domaine cyberdéfense et durant dix ans la formation à la gestion de crise de la Chancellerie fédérale. À ce titre, il participe à la préparation et à la conduite et à l'évaluation des exercices de conduite stratégique « blackout » en 2009 et « cyberattaque contre la Suisse » en 2013. Depuis lors, il intervient comme expert au DDPS dans le domaine des cyberrisques.

le passage au tout-numérique pourrait changer la donne.

RMS: En quoi le passage au tout-numérique est-il problématique?

M.D.: Le passage au tout-numérique est une révolution dont on a encore de la peine à saisir l'ensemble des contours et à évaluer toutes les conséquences. En Suisse, les risques du passage au tout-numérique sont largement sous-estimés. L'économie s'est engouffrée dans le tout-numérique et cherche avant tout à générer du profit, les questions de sécurité venant ensuite (si elles viennent). Les politiciens se profilent sur la « Suisse 4.0 » sans véritablement savoir vraiment de quoi il retourne et quels sont les risques associés. C'est seulement maintenant que certains cercles spécialisés commencent à prendre en compte les dangers liés au tout-numérique.

Le problème du passage au tout-numérique est qu'il est présenté comme inévitable. On promet l'amélioration des services et de la productivité avec l'avènement de la société de l'information. Parallèlement, on affirme que si la transition numérique n'est pas effectuée, on risque d'être laissé sur le côté. On ne se pose pas la question de ce qui serait souhaitable pour la société et en quoi le numérique pourrait y répondre. Le discours dominant est plutôt: « passez au numérique, c'est dans l'esprit du temps », indépendamment des implications et conséquences que ce passage implique.

Cet état d'esprit pose un danger pour la sécurité. Il produit une fuite en avant dans de nouvelles technologies dites « disruptives », ¹ c'est-à-dire capables de perturber le fonctionnement actuel de la société. Face aux immenses sommes qu'on promet ou alloue pour le passage au tout-numérique, la logique du profit l'emporte définitivement sur celle de la sécurité. A-t-on oublié le principe de précaution? On adopte alors ces technologies sans mesurer

les risques auxquels elles sont associées, ou alors en ne réfléchissant pas suffisamment sur la manière dont on veut les encadrer. De cette façon, les risques aujourd'hui identifiés comme majeurs pourraient prochainement être dépassés par de nouveaux risques numériques, ou alors être amplifiés par eux.

RMS: Quels sont ces nouveaux risques? Quels dangers posent-ils?

M.D.: En sus des cyberrisques déjà connus (pénétration informatique, piratage, vol d'identité, etc.), on peut regrouper les risques liés à la société numérique en trois catégories principales.

La première catégorie de risques couvre les effets liés l'explosion d'objets connectés, ce qui ajoute une couche de vulnérabilité informatique. En effet, il devient très difficile, sinon impossible d'assurer que l'ensemble de ces objets soient convenablement protégés face à des cyberattaques. De ce fait, le nombre de vecteurs d'attaque potentiels s'accroît considérablement et on peut s'attendre une augmentation significative de la vulnérabilité des organisations et individus, notamment par le piratage, le vol de données ou encore la surveillance non consentie.

La deuxième catégorie de risques englobe les dangers liés à l'hyperconnectivité. L'accroissement des interdépendances entre les différentes infrastructures critiques, services vitaux et prestations indispensables expose la société de plus en plus aux événements en cascade.² De petites perturbations peuvent provoquer des dégâts considérables. Cette situation est aggravée par le fait que depuis quelques années, la connectivité de la société est passée d'un état sous-critique à un état sur-critique³. Concrètement, cela veut dire que si un des éléments centraux est mis hors service, une partie, voire la totalité de la société peut tomber avec, comme lors d'un blackout. C'est un danger redoutable dont personne ne parle.

La troisième catégorie concerne les dangers liés à la conservation de la mémoire. Ces risques semblent moins immédiats, mais leur dangerosité menace notre système de civilisation. En effet, le passage au tout-numérique implique la numérisation de toute l'information, alors qu'il n'existe pas encore de supports durables. L'information doit alors être copiée périodiquement d'un support sur un autre, ce qui est très coûteux et ce qui consomme beaucoup d'énergie. Il faut envisager de devoir perpétuellement migrer les données.

L'abandon du papier expose nos sociétés à une perte définitive d'information en cas d'effacement des données numérisées ou si les lecteurs appropriés ne sont pas disponibles. Ainsi, le passage de la mémoire reposant sur des supports analogiques à des supports numériques rend nos sociétés bien plus vulnérables aux événements ou aux menaces catastrophiques.

² Ndlr : Sur ce sujet, consulter également « Blackout : déclencheurs et mécanismes » dans ce dossier.

³ Ndlr : Idem.

¹ Comme le blockchain ou l'intelligence artificielle.

En résumé, il me semble que dans les circonstances actuelles, le passage au tout-numérique représente plus de dangers que d'opportunités. C'est un constat probablement aujourd'hui impopulaire. Mais on constate bien que les nouveaux risques numériques augmentent considérablement les vulnérabilités de nos sociétés, voire sapent leur capacité de résilience après un effondrement. Et dans une société « tout-numérique », la perspective d'un blackout devient effrayante. Est-ce vraiment un risque auquel nos sociétés sont d'accord de s'exposer ?

RMS : Cela est préoccupant. Pouvez-vous décrire comment ces risques sont liés à celui de blackout ?

M.D. : Le risque de blackout augmente proportionnellement à l'accroissement de l'hyperconnectivité. Depuis quelques années, les cyberattaques ciblent les infrastructures vitales et les réseaux électriques en particulier. Ces attaques ont pour objectif de pénétrer au sein des systèmes de commande et d'en prendre le contrôle. Une fois les infrastructures sous contrôle, il est facile de paralyser les infrastructures critiques d'un pays à distance. C'est par exemple ce qui s'est produit en 2007 en Estonie.

Il est également possible d'endommager, voire de détruire ces infrastructures à distance. Une expérience en 2010 aux USA l'a clairement démontré⁴. En 2015, une cyberattaque a pris le contrôle d'une centrale électrique en Ukraine et a provoqué un blackout pendant 24 heures. Dans ces conditions, « éteindre » un pays à distance ne relève plus de la science-fiction. Ces développements sont très inquiétants, cela d'autant plus qu'avec l'augmentation des vecteurs d'attaque (précédemment mentionnés), la vulnérabilité à une telle éventualité s'accroît considérablement.

Dans ce cadre, la question en Suisse n'est pas de savoir si des pirates ou un État sont en mesure de pénétrer les systèmes de commande et d'en prendre le contrôle, mais de savoir quand et quels dégâts ils pourraient infliger. Ainsi, le blackout ne constitue plus seulement un risque, mais aussi une menace. La capacité à s'en protéger ou à y faire face ne relève alors plus seulement de la sécurité intérieure, mais aussi de la défense extérieure. Qui a conscience cet état de fait en Suisse ?

Mais il y a plus inquiétant encore : avec la fuite en avant dans le tout-numérique et la course vers l'hyperconnectivité, notre société passe, comme on l'a déjà dit, d'un état sous-critique à un état sur-critique dans lequel des perturbations mineures pourraient avoir des conséquences majeures. Dans ce cas, indépendamment d'une cyberattaque, le système pourrait s'effondrer spontanément.

⁴ L'expérience s'est déroulée sur une centrale électrique vouée à la démolition. Le gouvernement américain a mis un spécialiste informatique au défi de pénétrer cette centrale à distance et d'y causer un maximum de dégâts. Le spécialiste est parvenu à prendre le contrôle d'un générateur d'électricité. Il en a fait ensuite brusquement varier la vitesse (ralentissement et accélération saccadés), jusqu'à ce que l'échauffement de la machine provoque un départ de feu. Ce départ de feu s'est transformé en incendie, puis s'est étendu aux autres génératrices et enfin à la centrale. Concrètement, cette expérience prouve qu'on peut non seulement paralyser, mais aussi détruire à distance (!) une centrale électrique par des moyens cyber.

RMS : Dans ces conditions, que nous reste-t-il de notre souveraineté ? Faudrait-il revoir la politique de sécurité ? Quel pourrait être le rôle de l'Armée ?

M.D. : Ces changements — en particulier l'arrivée des technologies disruptives — sont en train de bouleverser tous les secteurs de la société. La connaissance de ces nouveaux risques devrait être diffusée auprès des autorités, de l'économie et de la population. Il serait temps d'ouvrir une grande concertation nationale. Les questions suivantes devraient être posées : « où-allons-nous ? », « la direction actuelle du changement est-elle souhaitable ? », « où souhaitons-nous réellement aller ? » et « quels moyens donnons-nous pour atteindre cette direction ? »

En outre, les nouveaux risques vont évidemment affecter la politique de sécurité. Or avec la rapidité de l'évolution actuelle, les rapports de politique de sécurité sont vite dépassés. Les derniers exercices de conduite stratégique ont démontré la grande difficulté de la conduite en situation dégradée : pas d'électricité, pas de télécommunications, pas de conduite. L'Académie suisse des sciences techniques (SATW) a esquissé des pistes qui vont dans ce sens. Il conviendrait de les développer.

Face aux crises de demain, comme un blackout, la défense relève avant tout de la gestion de crise. Le rôle de l'Armée est d'abord subsidiaire. Ses contributions les plus pertinentes seraient alors le maintien de l'ordre et l'aide à la conduite civile, par exemple en établissant de lignes de communication sécurisées.

Enfin, la politique de sécurité, c'est beaucoup plus qu'une politique de défense élargie. Le concept de défense générale, abandonné en 1999, s'inscrivait dans cette idée. Les infrastructures vitales telles que l'énergie électrique et les télécoms en faisaient partie. Compte tenu des circonstances, il conviendrait de reprendre ce concept et de le mettre à jour.

Propos recueillis par Grégoire Chambaz



Une salle de surveillance et de commande du réseau électrique suisse.

Blackout

Conclusion du dossier « *blackout* »

Cap Grégoire Chambaz

Rédacteur adjoint RMS+

Même si le risque de *blackout* est désormais à l'agenda d'un plus grand nombre d'acteurs et qu'on peut se féliciter que plus de communication soit effectuée sur le sujet, du chemin reste à parcourir en matière de sensibilisation, de prévention et de protection. Comme une rupture de courant prolongée n'est jamais survenue en Suisse, il est possible que les politiques ou les décideurs n'aient pas pleinement conscience du problème ou de toutes ses implications. Même parmi les organisations aux prises avec le risque de *blackout*, certaines actions laissent dubitatif sur leur connaissance des conséquences directes et indirectes de ce risque. Par exemple, les Forces motrices bernoises proposent dans une de leurs dernières communications de se renseigner sur... leur site internet en cas de coupure de courant.

Quoi qu'il en soit, pour une partie des personnes mobilisées dans la réalisation de dossier, la prise en compte du risque d'un *blackout* est significativement sous-estimée. D'après eux, l'éventualité d'un *blackout* de longue durée ne relève pas de l'impossible et son potentiel de destruction n'est pas adéquatement mesuré. Après plus d'une semaine sans courant, « un effondrement partiel ou total de la société » est à considérer, déclarent-ils. Dans ces conditions, la combinaison du non-renouvellement des infrastructures et des risques issus du tout-numérique (entre autres) représente une bombe à retardement. Pourra-t-on la désamorcer à temps ?

Réduire le risque ?

Comment réduire le risque ? Le risque zéro n'existe pas, ou plus. Mais il est possible de diminuer l'exposition au risque. Dans ce sens, ce dossier constitue une première étape d'une réduction du risque : la sensibilisation. Dans le registre politique, la seconde étape serait naturellement de se pencher sérieusement sur ce risque et, en particulier, sur la thématique du vieillissement du réseau électrique.

Cela implique des changements législatifs que le parlement saura probablement arbitrer, mais cela se fera-t-il à temps ? Quoi qu'il en soit, ces modifications législatives ne seront pas suffisantes sans investir massivement et rapidement dans la modernisation dudit réseau. En outre, les autorités pourraient encourager les entreprises, les services de l'Etat et les consommateurs à reconstituer des stocks, de manière à être plus résilients en cas de rupture d'approvisionnement.

Perspectives

Ce dossier se termine avec un sentiment d'inexploré. En effet, la thématique du *blackout* est — bien évidemment — interconnectée avec une quantité d'autres sujets dont ce dossier a uniquement gratté la surface. Parmi ceux-ci figurent la problématique de la lente reconstruction du réseau après un *blackout* et les dangers électromagnétiques (tempêtes solaires et armes électromagnétiques). La RMS consacrera prochainement des entretiens à ces thématiques.

Une autre interrogation demeure : quelle est la capacité de l'Armée à résister à un *blackout*, et a fortiori aux armes électromagnétiques ? Peut-on mobiliser ? Quelles prestations pourrait-elle fournir ? Peut-on défendre sachant que l'adversaire peut provoquer une panne de courant en Suisse ? La RMS a cherché d'obtenir des réponses auprès des personnes compétentes, mais sans succès.

Invitation

Enfin, ce dossier se clôt avec une invitation à toutes les personnes voulant contribuer à la politique de sécurité — et particulièrement à la prise en compte du risque de *blackout* — à diffuser ce dossier ainsi qu'à échanger sur la question. Les courriers peuvent être adressés à la RMS.

G. C.