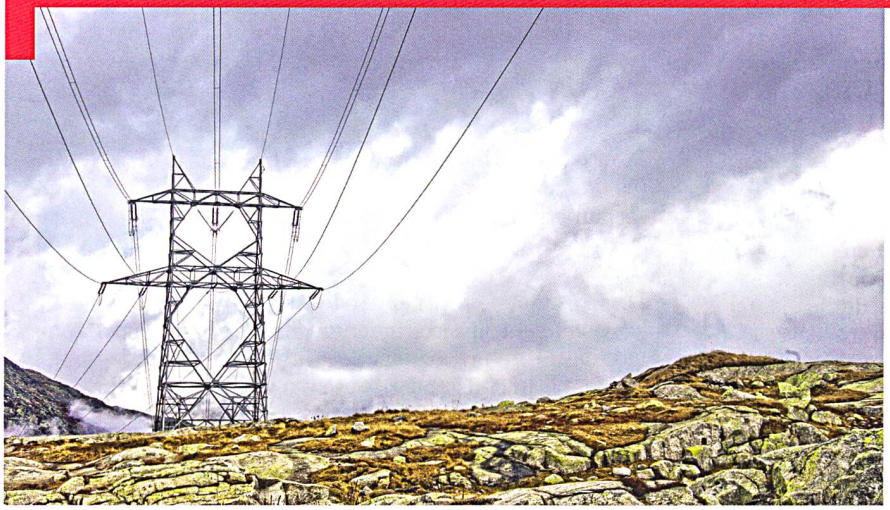
Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: 5

Artikel: Blackout : déclencheurs et mécanismes
Autor: Chambaz, Grégoire
DOI: https://doi.org/10.5169/seals-823405



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 2005[3] 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.

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*.

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 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.

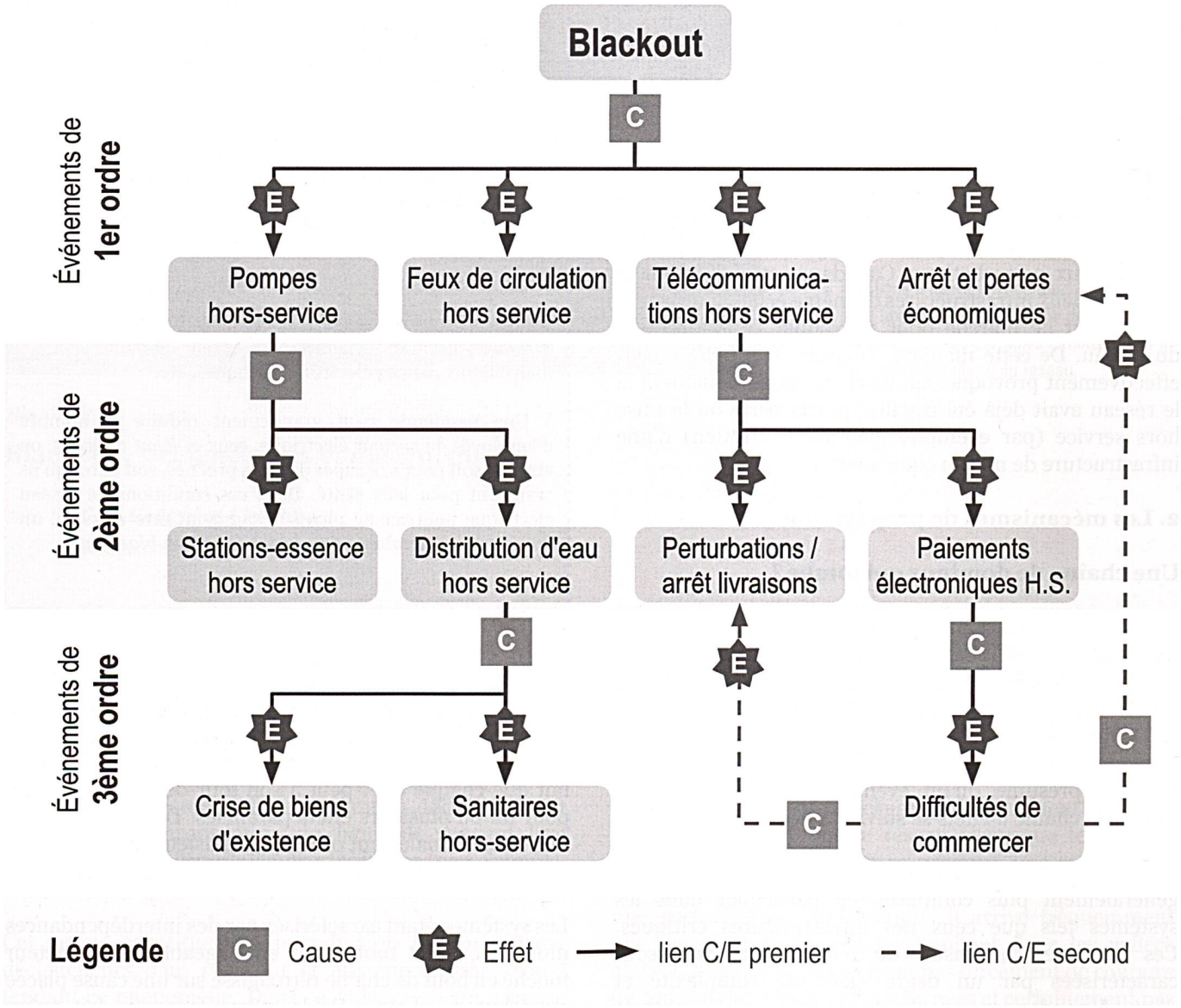
Les systèmes étant caractérisés par des interdépendances multiples, il est tout à fait envisageable qu'un facteur touché en bout de chaîne rétroagisse sur une cause placée en début de chaîne. De la même façon, le fait qu'un événement ne soit pas rattaché à une cause en début de chaîne n'indique pas forcément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