Michel Dufour : un risque de blackout accru? : les dangers du tout-numérique

Autor(en): **Chambaz, Grégoire**

Objekttyp: **Article**

Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2018)**

Heft 5

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-823410

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-critique*[3]*. 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.

1 Comme le blockchain ou l'intelligence artificielle.

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

3 Ndlr : *Idem.*

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 démontré[4]. 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.

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

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.