Informatique et vulnérabilité

Maurice Guini

L'emploi de l'informatique, déjà largement répandu, est appelé à se généraliser dans toutes les branches de la Défense, de la Production - contrôle de processus industriels ou conception et fabrication assistées par ordinateurs -, et de la Gestion. Cette étude très succincte, tend à démontrer que, plus se généralise l'emploi de l'informatique, plus la sécurité et l'économie d'un pays deviennent vulnérables.

Toutefois, cette constatation ne doit pas être un prétexte pour condamner ou limiter l'emploi inéluctable de l'informatique, mais doit suggérer et mettre en oeuvre une législation, des méthodes et des dispositifs de sécurité, pour pallier cette situation, qui faute de mesures de précaution urgentes et adéquates, risque de devenir catastrophique.

Vue générale

Les cas de fraudes sur ordinateurs, bien que graves, sont réparables et font l'objet de poursuites en justice. En revanche, du fait de l'emploi de l'informatique, la vulnérabilité de la Défense et de l'Economie du Pays - ses installations militaires, son appareil de production comme ses circuits monétaires ou commerciaux -, est à la fois plus profonde et plus subtile.

Cette faiblesse s'est révélée, en France comme dans plusieurs pays industrialisés, par des incidents graves, de caractère accidentel, criminel ou terroriste qui ont fait l'objet d'analyses mais dont il semble que l'on n'ait pas tiré toutes les conséquences.

L'accès aux dispositifs de contrôle et de commande par ordinateurs, d'installations vitales telles que Centrales d'Energie (nucléaires ou conventionnelles), Usines de Transformation (raffineries, métallurgie, produits chimiques), Noeuds de Transports (aéronautiques, ferroviaires ou routiers), réseaux d'alimentation (en carburants, en eau ou en électricité), s'effectue par fils pilotes, par satellites ou par faisceaux hertziens.

La neutralisation des dispositifs ou des codes de verrouillages même redondants, suivie d'instructions de manoeuvres inappropriées, peut provoquer à la fois mort d'hommes et destruction d'un matériel essentiel et coûteux. Leur remplacement pourrait exiger des mois sinon des années. (Annexe 1 : quelques exemples d'accidents criminels provoqués).

La mise hors service d'ordinateurs de gestion - des grands services publics, banques, Sécurité Sociale,

chèques postaux, organisation portuaire, transports de voyageurs et de marchandises -, pourrait provoquer des pertes matérielles considérables et, si elle se prolonge, la dislocation de l'économie.

Enfin, la mise en mémoire sur ordinateur de données confidentielles et vitales ou de calculs et de programmes de fabrication, facilite et encourage l'espionnage militaire et industriel. (Annexe 2 : exemples de vols criminels de données).

Facteurs de vulnérabilité

L'analyse des facteurs, qui la provoquent et qui l'aggravent, permet une meilleure appréhension de la vulnérabilité de notre société, qui résulte de l'emploi de l'informatique. Un caractère inhérent à l'informatique est sa forte concentration géographique et fonctionnelle :

- Concentration géographique, qui oblige à installer les grands centres de calculs près de grands centres d'utilisation et de décision, et là où se recrute une main-d'oeuvre hautement qualifiée. En France, dans la capitale bien entendu, dans les villes universitaires, au voisinage des grands ensembles industriels, économiques et financiers (le dispatching de l'E.D.F., les centres de calcul de la S.N.C.F., les bureaux de gestion des banques, des compagnies d'assurances, des ports et des aéroports).

- Concentration fonctionnelle imposée par le traitement intégré des données. En cas d'actions militaires ou terroristes, des secteurs complets de l'économie risquent d'être facilement et complètement paralysés.

Par ailleurs, la Télématique est née et s'est développée avec la nécessité d'interconnecter les centres de calculs entre eux et avec les terminaux d'utilisation. Cette interconnexion s'opère par fils pilotes, par faisceaux hertziens ou par satellites, causes graves de faiblesse et de faillibilité. En effet, la destruction ou la mise hors service d'un centre important et bien choisi de la chaîne entraînerait des perturbations sur l'ensemble du réseau, malgré les redondances et les voies parallèles de secours.

Le péril est encore plus sérieux, car tous ces réseaux sont des voies d'accès pratiquement libres vers les ordinateurs, soit pour le retrait illicite d'informations, soit pour l'injection d'ordres ou de données incorrectes, qui pourraient endommager le matériel ou fausser le traitement des programmes. Enfin, de graves perturbations, provoquant l'arrêt des communications et du fonctionnement de certaines installations, peuvent résulter d'explosions nucléaires à haute altitude (effet d'impulsion éléctromagnétique).

Problème de la Main-d'œuvre

L'informatique exige un personnel restreint hautement qualifié et indispensable. Des arrêts de travail des informaticiens peuvent donc être la cause de perturbations aux conséquences incalculables.

Placé aux points névralgiques de la Défense et de l'Economie du pays, ce personnel ne fait pourtant l'objet d'aucune déontologie, en ce qui concerne les fraudes, le secret des données, la sauvegarde du matériel et la continuité du fonctionnement. Avec la généralisation de l'informatique, cette lacune devient profondément inquiétante. En cas de guerre ou de prises d'otages

terroristes, le remplacement d'une main-d'oeuvre hautement qualifiée serait difficile sinon impossible. La main-d'oeuvre pose en outre un autre problème au premier abord paradoxal. Habitué à opérer en permanence avec l'extraordinaire machine qu'est l'ordinateur, le personnel risque de se trouver dans le désarroi, s'il vient à en être accidentellement privé. En cas de destruction de l'outil informatique, le contrôle, la commande ou la gestion de l'appareil de Défense ou de Production encore intacts, pourraient s'avérer impossible.

Propositions succinctes

Afin de mesurer la gravité et l'ampleur du problème, il serait souhaitable que les autorités compétentes organisent des manoeuvres de pannes simulées, successivement dans divers secteurs clés de l'Economie : au dispatching de l'E.D.F., aux centres de gestion de la Sécurité Sociale, aux centres de triage de la S.N.C.F., sur les aéroports, dans les banques, les ports, la vente des billets de chemin de fer, les réservations de places d'avion, etc. Les informations recueillies seraient mises sur modèles et traitées par ordinateurs. On en tirerait sans doute de précieux enseignements.

Certaines mesures pourraient néanmoins être mises à l'étude immédiatement :

- Création d'une Commission Technique Nationale ou Européenne, chargée d'analyser la situation, dans son ensemble, et de faire ses recommandations.

- Création d'une Commission Parlementaire destinée à compléter la législation sur l'information, les archives, la déontologie de la profession, les règles de sécurité, les règlements d'emploi des ordinateurs

(par exemple la nécessité d'un permis d'emploi, analogue au permis de conduire), etc.

- Création obligatoire dans tous les grands services publics d'un département : Sécurité - Informatique.

- Normalisation des règles de sécurité informatique et construction d'un appareillage adéquat, destiné à la mise en oeuvre et au contrôle de ces règles.

Conclusions

Ce qui précède mériterait de faire l'objet d'une analyse détaillée systématique et méthodique de la vulnérabilité qu'introduit l'emploi de l'informatique. Comme pour chaque nouvelle situation, évolution sociale ou politique, découvertes médicales ou scientifiques, progrès technologiques et industriels, il serait vain de condamner des états de fait, du reste irréversibles. L'évolution de nos sociétés vers le progrès et le mieux-être a toujours été fondée sur la science, la raison et l'expérience. Le problème existe et ses solutions ne nécessitent aucune découverte fondamentale ou percée technologique. "Science d'où prévoyance, prévoyance d'où action".

Maurice GUINI
B.Sc (Eng.) Ingénieur de systèmes