



Fight against Fraud

- *Mathematical tools* -

A "fraud" is of course of juridical nature : a person may or may not have the rights to some document (such as a passport), or be entitled to some help (such as health, employment, and so on). So, one might expect that all checkings must be individual, and must concern the authenticity of all documents presented by the person. This topic, apparently, does not require any mathematics.

But this is not quite so ; indeed, thousands of organizations and millions of persons are concerned, so one cannot check all demands individually. There is a clear need for automatic tools, which will characterize in a simple and robust manner all profiles which may result in frauds. Such tools rely on mathematics. The concerned profiles will then be checked more thoroughly.

We see that these mathematical tools have a preliminary role : they allow a first, quick, treatment. They must be as efficient as possible : detect true frauds, but not too many false alarms (people who would be identified as fraudulent, though they are not). False alarms is a major concern in such a case.

Mathematical tools will allow two kinds of investigations :

- Self-coherence of all informations given by the applicant

Here, we have to check that all the informations provided are coherent between themselves : one date should be after another, the various locations mentioned are compatible, and so on. In any application, the information provided cannot be "random".

- Coherence with other demands

Here, we have to check that we did not receive hundreds of demands, all with the same name, coming from the same small village, or all with the same address, or all with the same data, whatever these data must be.

The search is made upon the existence of identical, replicate, fields in the databases ; this is allowed by all the laws in all countries and does not carry any restriction to individual rights.

All these tools we just mentioned are purely deterministic : they consist in computer treatment, usually extractions from databases and comparisons of fields, according to several criteria. But they can be completed by probabilistic tools, which will allow to characterize "average profiles" of the persons who apply, on all the parameters one wants to consider (age, residence, place of birth, time of the year, and so on). One can then detect any person who differs too much from the average profile, according to a predefined threshold.

Qualifying deterministic tools is rather simple ; things are harder with probabilistic tools, if one wants them to be useful. Inside a given organization, such tools should not be constructed by the statisticians who are employed by the organization itself, for two main reasons :

- The usual statistics of the organization incorporate the fraud, which may be quite ancient ;
- The statisticians who are employed by this organization see the present project as a criticism of their work.

So, the fight against fraud must be done from the Chairman's authority, or by the Inspectors or Controllers, if they exist. Those who have done the work cannot be those who check it : this is an old piece of wisdom !

Our achievements

They also concern the search for "vulnerabilities" in a system. All titles are in French.

1. Le niveau de préservation des disciplines scientifiques. Secrétariat Général de la Défense Nationale (Premier ministre), 1998.
2. Analyse des besoins en cryptologie. Secrétariat Général de la Défense Nationale (Premier ministre), 1998.
3. Contre-mesures anti-torpilles : scénarios d'utilisation. Service des Programmes Navals, Direction des Systèmes d'Armes, DGA, 2000.
4. Missiles et torpilles à courte portée : les problèmes que pose la prolifération. Le concept de "bouclier local". Secrétariat Général de la Défense Nationale (Premier ministre), 2000.
5. La protection du patrimoine scientifique du Ministère de la Défense. Secrétariat Général de la Défense Nationale (Premier ministre), 2001.
6. Discrimination des leurres par les missiles munis d'un autodirecteur infrarouge. Etat Major de l'Armée de l'Air, Cellule d'Analyse, de Simulation et d'Innovations, en cotraitance avec Matra BAe Dynamics, 2001-2002.
7. Le Bouclier Local : préétude de faisabilité concernant l'ensemble des technologies susceptibles d'être utilisées pour protéger un navire contre une attaque terroriste à courte portée (roquette, missile). Service des Programmes Navals, DGA, 2002.
8. La protection de l'information par tatouage. Secrétariat Général de la Défense Nationale (Premier ministre), 2002.
9. Analyse des vulnérabilités d'un réseau numérique domestique, pour Thomson Multimedia et Canal + Technologies, 2002-2003.
10. Les exportations de matériel sensible et la prolifération. Délégation aux Affaires Stratégiques, Ministère de la Défense, 2002-2003.
11. Recensement des formations universitaires relatives aux domaines sensibles. Service des Recherches et Etudes Amont, DGA, 2003-2004.
12. Le Bouclier Naval : protection d'un navire de surface contre une attaque terroriste à courte portée. En cotraitance avec Thales Naval France, Thales Systèmes Aéroportés et TDA Armements, la SCM étant responsable de la faisabilité du système complet. Service des Programmes Navals, DGA, 2004-2009.
13. Analyse des vulnérabilités d'un système d'archivage électronique, pour CDC-Arkhinéo, 2006.
14. Analyse des vulnérabilités dans le processus de délivrance d'un passeport biométrique. Agence Nationale des Titres Sécurisés, 2008.
15. Détection de données aberrantes dans des bases de données. Nuclear Energy Agency (OCDE), 2010.