Introduction

Yves CORREC
DGA/DCE/CELAR
BP7, 35998 Rennes Armées
France

yves.correc@dga.defense.gouv.fr

There is little doubt that information systems have gradually become the electronic brain and nerves of our modern (best possible??) world, thanks to the so-called silicon revolution of the last half century.

While making a biological analogy, one must bear in mind that these systems can be disrupted by computer attacks, just the same way our neurocortical functions can be impaired by the use of very small quantities of the right (neurotoxic) stuff. On the path of evolution, computer systems are currently mutating from the fortress model to the living being model: At dawn of computer history, expensive systems were dedicated to critical high value functions, and their protection was quite simple. Tomorrow, pervasive computing will extend our capabilities up to shockingly high levels: our brand-new computer-aided washing machine, or emergent Network Centric Warfare concepts are faint early beginnings. But security will become a correspondingly trickier concern, and rely on complex mechanisms. Yet an evolution of this magnitude must go through intermediate stages, with smaller and smaller interconnected fortresses… A fairly good view of the present stage can be found in the IATF (Information Assurance Technical Framework) document, issued by the NSA.

What can be said about the threat? The publicized threat is on line hacking of computers, with strong underlying assumptions of connectivity and restricted targets… The actual threat is unfortunately related to more physical assets (political, economical, military) and their potential value for the foe, through the whole spectrum of available means. In this present chapter of mankind history, we are just transposing usual human behaviour in a new space. It will require an evolution of security concepts and tools to keep it civilized.

IATF information infrastructure model connects local computing environments through enclave boundaries and networks. Some of them are classified, and accordingly protected. The others are not. Classified networks are supposedly designed to support noble functions, and carry confidential information (a paper legacy). Hard regulatory constraints often result in hardened more or less dedicated systems. But we cannot be unaware of some discretionary aspects of homologation and classification processes. Unclassified networks on the other hand deal with everything else, with a strong need for availability and integrity of the services. COTS software and hardware are widely used in both cases (with some precautionary measures –GOTS- for classified networks) for evident economical reasons.

The existence of various (and secure of course) gateways between all our networks must then be acknowledged, to conclude they are in fact part of a weakly segmented technical continuum. This blurred boundary between classified and unclassified networks calls for a common technological framework, including the full set of security mechanisms (protection, deception, IDS, monitoring & analysis, etc). In this respect, unclassified networks may be considered as a testbed for advanced technologies.

Paper presented at the RTO IST Symposium on "Adaptive Defence in Unclassified Networks", held in Toulouse, France, 19 - 20 April 2004, and published in RTO-MP-IST-041.

Let us now think of the security engineering process, as set out in IATF. A key component is effectiveness assessment, which unfolds in operational effectiveness (required functionalities) and security matters (risk analysis). These concepts are unfortunately too often opposed (security versus capability). The question can be settled if we are able to quantify security, but this very problem has long been some sort of a security Holy Grail…

So we cope now with the strong current trend towards ubiquituous computing, and a basically ill-posed problem, by using a nice combination of technology and organization, which we grant more empirical faith than theoretical proofs. Possible improvements may come from a more systematic use of models, allowing for a better understanding of systems behaviour in an operational environment. We give a simple example of a layered model accounting for a better definition of infowar concepts (cyberwar analysis grid) and subsequent works (deriving attack paths from the so-called foe's hopscotch).