

# **Immunology and the survivability of mission critical cyber-based systems**

Benoit MOREL, Department of Engineering and Public Policy  
Carnegie Mellon University Pittsburgh, Pa 15213  
bm1v@andrew.cmu.edu

*Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security. (From: Presidential White paper: PDD 63, May 22, 1998)*

“Controlling a complex system is difficult, even under the best of circumstances. Whether or not human operators are involved, the geographic scope and the speed at which an National Infra-Structure operates mean that assembling a current and consistent view of the system is not possible. The control theory that characterizes the operation of such systems (if known at all) is likely to be fraught with instabilities and to be highly nonlinear”<sup>1</sup>.

Most of what is known about critical infrastructure vulnerability is based on isolated events. In absence of rigorous scientific studies it is hard to know what vulnerabilities are the most significant. A more rigorous study of existing data would certainly improve the situation. But only the real experience with large-scale interlinked networks could provide really useful information.

This means that unavoidably we will have to go through a phase where the envelope is being pushed, and new unforeseen vulnerabilities will emerge, to which a speedy response will be needed.

---

<sup>1</sup> F. Schneider, S. Bellovin, A. Inouye “Critical Infrastructure you can trust”, 26<sup>th</sup> annual Telecommunication Policy Research Conference (1998)

Not only should that response be efficient and protective but out of this evolutionary experience an “efficient” architecture for cyber-security should emerge. Efficient architecture implies:

1. Being able to respond to any attack, while preserving as much functionality as possible.
2. Having the ability to address as wide a spectrum of attacks as possible. That includes new forms of attacks, since one has to assume that whatever defense has been developed, attackers will try new ways of attacking.
3. A way to limit somewhat the spectrum of possibility is to identify a design, which limits the options to the attackers, while maintaining the complexity of the system.
4. The system should be integrated in such a way that it is not a serious load and does not impede the overall system.

This is a tall order, but not unprecedented: the immune system can be construed as an example of that<sup>2</sup>. In the words of S.A. Hofmeyer and S. Forrest<sup>3</sup>: “The biological immune system provides a compelling example of a massively-parallel adaptive information-processing system, one which we can study for the purpose of designing better artificial systems. It exhibits many properties that we would like to incorporate into artificial systems: It is diverse, distributed, error tolerant, dynamic, self-monitoring (or self-aware) and adaptable. These properties give the immune system certain key characteristics that most artificial systems today lack: robustness, adaptivity and autonomy.”

More complex systems have naturally more vulnerabilities. The spectrum of vulnerability to intruders is different as are the requirements on the response. The cyber-security of large integrated systems is far more complex than the already challenging security of individual computers or small networks. In the same way, the survivability of organisms involving several organs, interlinked, like mammals is a much larger challenge than simpler organisms. The immune system of complex organisms has to mount a precisely tailored response against a large variety of threats from the vast world of parasites, viruses or bacteria while preserving as much of the functionality of the organism.

What can the study of the immune system teach about the survivability of critical infrastructures?

The immune system of living organisms (from plant to mammals) is the result of millions of years of biological co-evolution between the organisms and a very active and changing microbial environment. The immune system reflects the degree of complexity of the organisms. In the animal kingdom, it goes from the relatively simple (sponge) to the very complicated in the case of the mammals.

In passing it may be worthwhile (because it may have relevance for cyber-security) to point out that some basic features are shared across all organisms. “The implications of [immunological mechanisms] uniting insects, mammals and plants are far reaching, especially considering that the last common ancestor of these diverse groups was

---

<sup>2</sup> *Artificial Immune systems and Their Applications*, D. Dasgupta, editor, Springer 1998

<sup>3</sup> S.A. Hofmeyer and S. Forrest: Architecture for an Artificial Immune System, Univ. New Mexico Preprint, 2000.

probably unicellular.”<sup>4</sup> This seems to confirm the conjecture that evolution proceeds “by experimentation and then by standardization”<sup>5</sup>.

The comparison between the immune systems of the different organisms reveals a fundamental difference of architecture between vertebrates and invertebrates. The invertebrates have only a so-called “innate” system. The vertebrates have in addition an “adaptive” system<sup>6</sup>.

Because the human body is far more complicated, immune responses used by simpler organisms like insects would do too much harm to be protective. A much more precisely tailored immune response is required. This is the function of the “adaptive response”.

In cyber-security, there is no equivalent to the “adaptive” system, at least not yet. Our degree of advancement is the equivalent of the “innate” system. The protection of large integrated cyber-networks requires the cyber-equivalent of an “adaptive system”. What that means concretely is not obvious, although it certainly suggests far more reliance on artificial intelligence, as far more information would have to be processed and circulated.

In immunology, the adaptive response is not a substitute for the innate response. It is triggered by the innate response. What the adaptive response does is to counter the antigen in such a way that the functions of the organism are affected as little as possible. This involves a large amount of information processing and distribution within the immune system and the use of effectors far more subtle and specific than used by insects for example.

In complex organisms, the innate system is the biological equivalent of Intrusion Detection System (IDS). Intrusion detection uses very similar mechanisms across species: organisms as different as insects and mammals use the same kind of receptors: the “Toll-like receptors”<sup>7</sup>.

When the organism has an adaptive system, i.e. in the case of the vertebrates, after the first detection and identification of a challenge has been accomplished by the innate system, the adaptive response is triggered. The first significant event of the adaptive response is the interaction between the T-cell and a class of special cells that invertebrates do not have, the Dendritic cells, whose function is to recruit the T-cells. The interaction between these two classes of cells is referred to as the “cognate” interaction or the immunological synapse. This is in recognition of the fact that a lot of information is actually exchanged between the two sets of cells. Then during the adaptive response, the T-cells act as processors and distributors of information.

A cyber-security equivalent of that would require the introduction of new tools, in addition to the existing IDS. These new tools would consist in specific programs

---

<sup>4</sup> Wilson I, Vogel J, Somerville S. Signaling pathways: a common theme in plants and animals? *Curr Biol* 1997;7:r175–r178.

<sup>5</sup> Gould SJ. *The Flamingo Smile*. London: Penguin, 1985.

<sup>6</sup> A misconception is to believe that the famous self-non-self recognition belongs only to the adaptive response. Self/non-self recognition plays an important role in the initiation of the adaptive response. But it is not specific to it. Self/non-self distinction also occurs in the innate response. The so-called “danger” signal can also be based on a self-non-self discrimination.

<sup>7</sup> Medzhitov, R., Preston-Hurlburt, P. & Janeway, C. (1997) *Nature (London)* **388**, 394-397

activated when there is a suspicion and which interactively with the IDS would analyze (autonomously) the challenge.

The immune system then has a phase during which the innate response mounts a provisional response to the antigen, trying to control its progression by killing as much of it as possible. (This uses cells called macrophage, neutrophils, NK-cells and the like). In parallel the adaptive system proceeds to a detailed analysis of the antigen and prepare a response. A possibility is that some B-cells are made to improve the quality of their antibodies to make them as selective to the antigen and effective against it as possible. When such antibodies exist, they are released in the blood stream. The adaptive response can take other forms. They tend to be exquisitely selective, efficient and designed to minimize the collateral damage on the organism.

Organisms like mammals are extremely complex integrated systems with non-linear controls. They have potentially instabilities that, in most cases, are not triggered by the immune response. So little is understood about this whole world that it is difficult to assert with confidence what is the reason for that. It seems safe to assume that the architecture of the system has an important role. The immune system is very distributed. Its action tends to be local. The properties of the immune system are not the same in all tissues. There is little if any central control. Furthermore, “when the survival of the individual is at stake, nature will rarely allocate this function to a single mechanism”<sup>8</sup>. I.e. there is an element of redundancy.

One blatant, obvious major impediment to design a cyber-security system that ensure a high degree of survivability for a very large inter-linked network, which emulates, even remotely the immune system, is the lack of experience and information.

A system will have to be fielded with a limited knowledge of what challenges it should be able to face. A lot of learning will take place in the first phase. Human beings by necessity will be given a very central role at least in the beginning. Not only does this imply that the system will be at the mercy of human errors, but it should be designed having in mind in the long term the possibility or desirability to reduce the role of humans.

There is a certain prudence in emulating as much of the architecture of the immune system as possible at the beginning, before we know better. This means distributed architecture, working in having an increased amount of information being gathered routinely during the operation of the system, and circulated to a monitoring system. The threat and defense will have to co-evolve. The system should be designed in a way somewhat emulated also from living organism, where the coupling between the components do not introduce a wealth of new vulnerabilities difficult to contend with.

At the institutional level, it is possible that the organization should be in contrast with the architecture of the system. I.e. to make sure that the integrated system will be as distributed as possible, with couplings well designed, a central agency should be in charge of the integration and be a watchdog.

---

<sup>8</sup> Du Pasquier, L., “The evolution of the immune system”, in *Fundamental immunology*, 4<sup>th</sup> Edition, W. Paul, 198 Lippincott-Raven Publication