Digital Immunity: An Intreaging Metaphor

George F. Hurlburt
STEMCorp
ghurlburt@change-index.com

Abstract - Over recent decades, many have postulated a parallel between the human immune system and hypothetical digital immune systems as a means to enhance dynamic cybersecurity. The human immune system works at many levels. At a conscious level, senses serve much as sensors in an Internet of Anything (IOA). Much like the skin protects against many microscopic invaders, procedural measures block malware. Just as innate immune system cells exist to devour hostile cells on contact, sensitized bots may someday serve a similar function. As the human immune system becomes more microscopic, however, it gains levels of sophistication permitting the adaptive immune system an ability to recognize, catalog and recall materials that are "not self". This capability permits an ability to prevent subsequent attacks alt the molecular level. It is the very definition of "not-self" that compounds digital immunity. Despite remarkable advances in Network Science which offers odds of statistically conquering relevant sustained attacks on "not-self" elements in computational environment, the human adaptive immune system has not yet been duplicated.

Keywords - Complex adaptive systems, immune systems, digital immune system, Network Science, self, not-self, pathogen, malware

The human being exemplifies a network of complex networks. Many separate biological systems harmonize simultaneously at many levels to yield a thriving human individual, capable of lifelong learning. Fascinatingly, mental frames of reference differ from individual to individual, because each possesses unique memories. Learning and memories extend all the way to the molecular level. Because of this deeply embedded recollection capacity, novel pathogens that would otherwise threaten existence are regularly identified and extinguished – silently and autonomously.

The human immune system, about which much remains to be known, represents a multi-layer, diverse, distributed, autonomous, dynamic and adaptive system of systems capable of protecting the body from all manner of invaders. It its core, the human adaptive immune system is capable of learning and recalling at the level of specific chemical receptors and electrostatic charges. This level of distinction is important, as some estimate 10^{14} different bacterial, fungal or protozoan agents exist among the 10^{13} natural cells in the human body.[1] This "normal flora" of often helpful microbes, however, discounts debris, foreign particles or viruses, which can become toxic if they are able to overwhelm the human immune system. This brings the foreign element count to an estimated 10^{16}.

As humans shape their tools, there is a nascent resemblance to human internal workings. Some might compare computer networks to the human nervous system, noting that both share memories and transmit data, often to control remote phenomena. Some have even gone so far as to suggest that computers and the networks upon which they operate can be endowed with immune systems of their own. As mankind approaches the age of the Internet of Anything (IoA), legitimate cybersecurity concerns mount. But can a digital immune system metaphor withstand the cybersecurity demands surely to arise from the IOA?

The concept of a digital immune system to satisfy deepening cybersecurity concerns took root three decades ago. The notion first surfaced in 1986, when Farmer, et al broached the idea that neural networks had a similarity to an immune system. They further suggested that the immune system might be viewed as a computational system.[2] By the 1990's through the early 2000s, a number of Artificial Immune Systems (AIS) appeared as a result of funded research projects.[3] Many however, faced insurmountable scalability barriers. This work fell into literal, metaphysical and modeling approaches.[4] The literal school attempted directly exploit the principles of immunity. The metaphysical school praised the immune system to perfect indirectly related optimization schemes. The modelers attempted to segregate the notion of "self" from "non-self" in computational systems via mathematical and computational models. Alas, however, most of this effort predated a growing appreciation of Network Science. Might Network Science become a digital immunity game changer?

Growing from Complexity Theory, as the Internet continues to mature, Network Science is all about how things relate. Amazingly, across all disciplines, vast network configurations are becoming evident as perceptions change to accommodate this new mathematical connectivity paradigm. Network Science, the study of how all manner of living and inanimate things are connected, offers workable mathematics to attach metrics to to what is otherwise nonlinear, highly

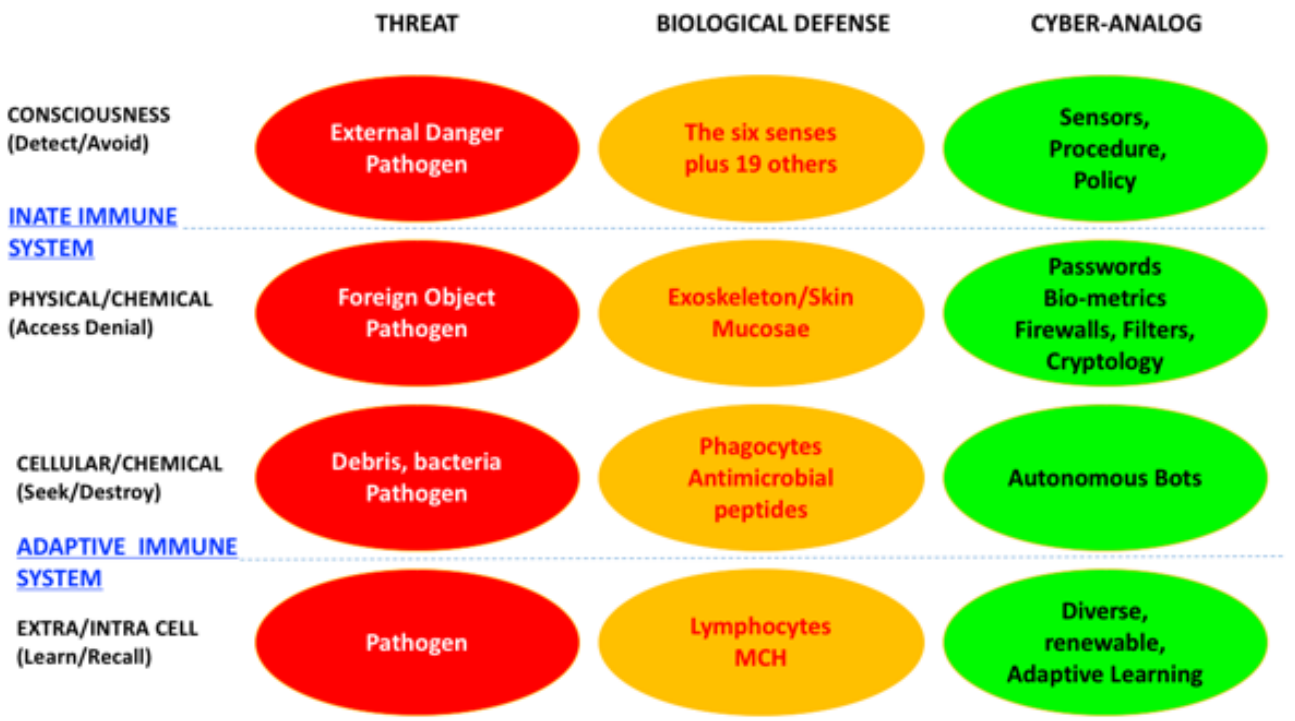

Figure 1: Correspondence between threats, biological defenses and potential cyber-analogs

dynamic, and irreducible. Might this new basis of knowledge add to the immune system dialog?

To answer this question, it is necessary to dive deeper into the human immune system which is actually a multi-layered system of systems. Figure 1 depicts the correlation between threats, human immune defenses and potential cyber-analogs as described in the following paragraphs. The figure rather simplistically considers the layers of the human immune system to draw analogous cybersecurity parallels.

In an ethereal sense, one could argue that human consciousness may be viewed as a preliminary line of defense. Enabling knowledgeable responses, such as using hand sanitizers, covering a sneeze in flu season, taking proven vaccines or actively practicing no touch policies and performing safe burial in Ebola stricken regions, goes a long way towards protection from contracting or spreading harmful pathogens. The five primary human senses, plus at least 18 other human senses[5], all serve as early warning systems for the health conscious individual.

Using a computational immune system metaphor, an array of specialized sensors, coupled with timely policies and sound procedures offer a similar conscious awareness in the realm of computational networks. Sensors, an endemic element of the IOA, can be calibrated to provide early warning for denial of service and other organized external attacks.[6] Given that most all systemic operational environments regularly morph over time, proactive policy and aligned procedure are essential conscious management techniques. Such continuously learned, incremental techniques will become essential to sound cybersecurity management. They must flow with the dynamic systems environment where key components, including entire networks, often come and go. They must also be compatible with all components of the cyber-immune system, meaning that they must exhibit network characteristics including percolation of bottom up standards. The days of meaningful system accreditation and effective management by periodic isolated, voluminous and comprehensive system snapshots are long gone. Security must be consciously managed in the moment, not by pounds of outdated paper documentation.

The human immune system, however, really starts with the exoskeleton. Skin, the largest of the human organs, effectively blocks invasive diseases. Inside many body cavities, secreted mucus filters unwanted particles and organisms from reaching vital internal organs. Ph and temperature regulation further limits organic breeding grounds for many potential diseases. Physical barriers are the first and a highly effective line of defense in human beings. It is a part of what is termed the innate immune system.

Again, using the computational metaphor, use of access controls such as strong passwords, bio-metric recognition, role based access verification, firewalls, cryptology and other discriminatory filtration methods all serve to control access. They prohibit a high percentage of unwanted users, bit streams and malware (computational pathogens) from penetrating the system. Good cyber–security practice dictates that whenever possible these access controls be used in tandem. Two factor authentication, enforcing combined fingerprint recognition and passwords for example, significantly reduce risk of unauthorized access. Likewise, solid encryption practices protect data from meddlesome activity while in transit or at rest.

The human innate immune system also operates internally on a smaller scale. This component of the innate immune system circulates specialized class of cells called phagocytes, including large white blood cells, that can identify and devour foreign objects, debris and bacteria on contact. Other antimicrobial peptides (proteins) serve as internally generated antibiotics.

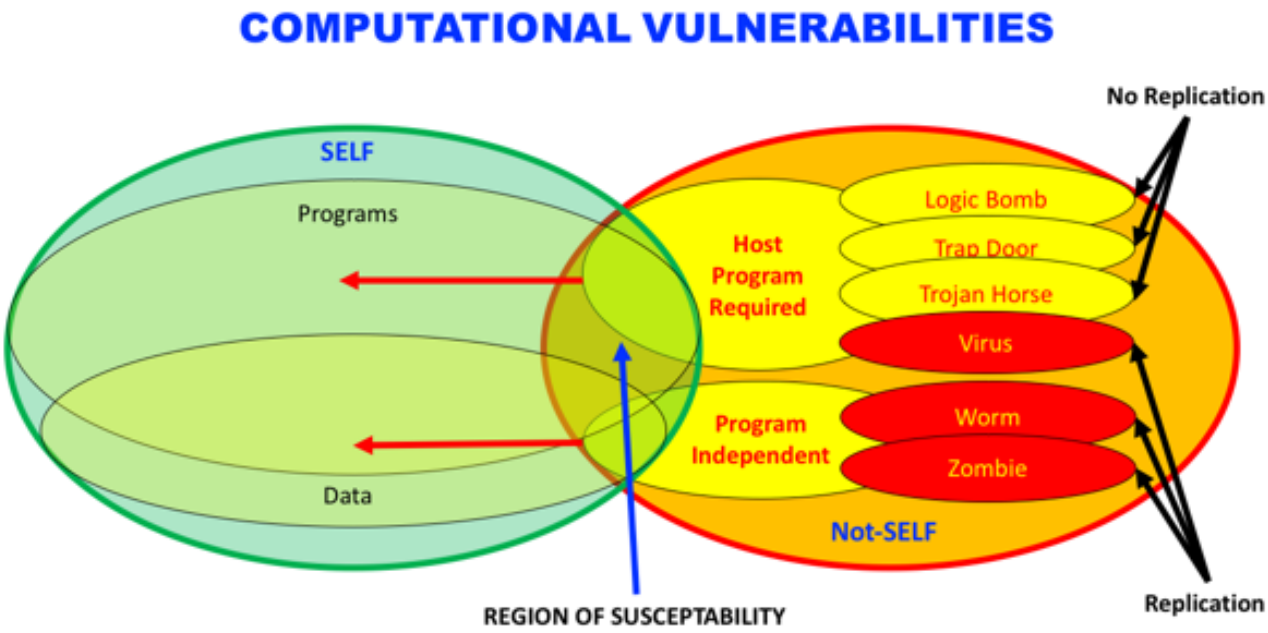

Figure 2: Distinctions between "Self" and "Non-Self" in computational systems

Returning again to the computational metaphor, it is reasonable to expect to develop and launch autonomous bots or agents which freely circulate to remove foreign threats. Oblivious to "self", these designer bots would be trained to identify and eliminate threats, unassociated fragments and other "digital debris" that constitute "not-self" computational components.

This becomes very murky, however, as the distinction between digital "self" and "not-self" is seldom straightforward, especially in dynamic computational environments. Worse, non-replicating logic bombs, trap doors and Trojan horses, frequently embedded in existing programs, would naturally be considered a part of "Self", as they are a part of the installed base. This suggests that independent agents must either be highly adaptive, which rapidly bloats them, or designed to operate at a base level, relegated to performing routine defragmentation in the background. Further compounding the problem, the practice of, stockpiling vulnerable signatures for quarantine or quarantining unknown signatures, is likely too costly a resource and performance drain to survive in large networked environments. For replicating threats, agents may be able to effectively seek the incidences of rapid redundancy and stem the tide of rapidly multiplying patterns. While attractive theoretically, however, the overall notion of autonomous intelligent agents would seem to require further research before they may be fully deployed analogous to their presumed biological counterparts. Figure 2 examines the nature of threats that emerge from "non-self" to negatively affect "self".

Finally, the adaptive immune system, operating at the cellular level within humans, is triggered by innate immune responses. Simply speaking, the adaptive immune system, generates cells called lymphocytes, a type of small white cell, that circulate in the blood stream and the lymphatic system. Lymphocytes are automatically rejected upon formation in the thymus and bone marrow, if they show affinity to normal human cells. This principle of clonal selection means that lymphocytes are generated such that they cannot attack own their host's cells. Otherwise, autoimmune responses would be commonplace. Totally unaware of "self", they exist to trigger attacks on anything that is "Not self". In the identification of "not-self", known as negative selection, lymphocytes must possess some level of discriminatory capability. At any given time, some 2 $x10^{12}$ lymphocytes are in circulation within a given human being.[7] They live only a few days, meaning that they are constantly refreshed with new randomly configured cells optimized by clonal selection and capable of negative selection. This means that at any given time, there is less than 100% coverage against all foreign materials in any given individual.

Should a known pathogen arrive, specialized lymphocyte subclass memory cells retain the signatures from previous attacks. When triggered, these cells can generate a secondary immune response by calling for rapid production of disease attacking effector cells. When a new pathogen arrives, other specialized naive cells trigger effector cells to rapidly amass against it in a primary immune response. This learning experience also initially generates new memory cells. Thus, while coverage is less than 100%, a principle known as Danger Theory triggers cellular distress calls to which a phalanx of specialized adaptive immune system cells may be summoned to respond. This response also applies to viruses multiplying within existing cells via specialized peptides known as Major-Histocompatibility Complex (MHC) molecules which attack foreign materials within infected cells.

The actual array and interaction of cells in the adaptive immune system is, of course, far more intricate and complex than rather simplistically described above. Thus, the human adaptive immune system, operating autonomously at both intra and extra-cellular levels represents a truly distributed complex adaptive network capable of both learning and emergent behavior.

From the computational viewpoint, this level of controlled interaction is what would need to be developed

systemically. Imitation of the adaptive immune system would require a learning system capable of fully discriminating between "self" and "not-self". This must be accomplished over the course of time and regardless of constant variation in the operating environment borne of network dynamics, software changes, operational modifications, scale variations, or data volume, velocity and variety. Its autonomous agents would further be able to exercise discriminatory negative selection against threats represented as undesirable patterns that it has learned or novel patterns associated with zero-day attacks.

Early postulated organizing principles for a digital immunity architecture include:1) distribution with no centralized control, 2) multiple layers of defense, 3) diversity among immune systems and the systems they protect, 4) disposability of any individual component without loss of effect, 5) autonomy without external control, 6) adaptability to recognize old patterns and detect new ones, 7) no separate secure layer operating on the premise that everything is vulnerable, 8) dynamic in both space and time, 9) identity by behavior through system calls, 10) imperfect detection at any point in time and 11) engaged in a game of large numbers where many pathogens can be replication simultaneously.[8] This list, drawn up just as awareness of networks was growing is telling, as it clearly outlines an architecture for a man-made complex adaptive network. In the case of a digital immune system, the network architecture must be suited for dynamically managing cybersecurity.

In many ways, such an architecture may well become a blueprint for the IOA itself, suggesting a shift from deterministic design to development of non-deterministic systems approach to architecture. As exemplified by a hypothetical digital immune system, any IOA system may well have to interact globally and harmoniously with other equally independent systems in order to perform a useful function. To that extent, the systems are autonomous, but well bounded within the environment in which they are intended to operate. Applied Network Science offers some hope that such systems may be designed and fielded in time to prevent the feared cybersecurity meltdown.

Despite the virtues of the human immune system, it is intuitive that mankind still contracts diseases, epidemics are real and 100% pathogen detection and eradication is not possible within the scope of any natural immune system. Indeed, great variation exists whereby one person may fall from some deadly disease and the next person is hardly affected. Likewise, it is safe to assume, so far as the immunity metaphor holds up in the computational world, that some malware will create epidemic losses, not all computationally intense systems will be totally immune to some overwhelming attack or there will never be 100% coverage against yet to be devised zero-day attacks.

It is safe to conclude, however, that the outer layers of immunity defense are essential as they serve to block the majority of potentially deadly attacks. Assuming good conscious effort, these layers can be implemented and dynamically enforced today. It is also safe to assume that the deeper layers are not quite ready for prime time without a far deeper understanding of how to translate what is known about the immune system into actionable complex adaptive software capable of mimicking how human immunity discriminates, learns recalls and triggers offences. To that end, the goal of building a working digital immunity architecture still remains elusive, yet tantalizing for its elegance.

References

[1] Alberts B.; Johnson A,; Lewis J,; et al., Molecular Biology of the Cell. 4th edition, New York: Garland Science; 2002.

[2] Farmer, J.D.; Packard, N.H. and Perelson A.S.; "The immune system, adaptation, and machine learning.', Physica D, 22:187–204, 1986.

[3] Dasgupta, D.; Ji, Z.; Gonzalez, F., "Artificial immune system (AIS) research in the last five years", Evolutionary Computation, 2003. CEC '03. The 2003 Congress on (Volume:1)

[4] Cohen, I.R. Tending Adam's Garden: Evolving the Cognitive Immune Self., Elsevier Academic Press, 2000.

[5] "Senses" Wikipedia: The Free Encyclopedia. Wikimedia Foundation, Inc. August 2015. Web. 23 Oct. 2015.

[6] Sun, H.F.; Li, Y.; Yang, Y.C.; Feng, L.; and Zhang H., "A Security Scheme Research of the Internet of Things Based on the SA/NIA Architecture", Advanced Materials Research, Vol. 320, pp. 291-296, Aug. 2011

[7] Ibid reference 1.

[8] Somayaji, Anil; Hofmeyr, Steven; and Forrest, Stephanie; "Principles of a Computer Immune System", NSPW '97 Proceedings of the 1997 workshop on New security paradigms, Pages 75-82, ACM New York, NY, USA ©1997

George Hurlburt is chief scientist at STEMCorp, a nonprofit that works to further economic development via adoption of network science and to advance autonomous technologies as useful tools for human use. He is engaged in health informatics and course development. He sits on the Editorial Board of IT Professional and is a member of the Board of Governors of the Southern Maryland Higher Education Center. Contact him at ghurlburt@change-index.com.