The current issue and full text archive of this journal is available at
www.emeraldinsight.com/1460-1060.htm

Using biological models to improve innovation systems

The case of computer anti-viral software

John Rice
Adelaide Graduate School of Business, The University of Adelaide, Adelaide, Australia, and
Nigel Martin
School of Business and Government, University of Canberra, Canberra, Australia

Abstract

Purpose – A strong and fast-cycle innovation system has been developed to counter the ongoing threat of computer viruses within computer systems employing vulnerable operating systems. Generally, however, the innovative applications that develop in response to each generation of computer virus can be seen as a reactive, rather than proactive, critical response. The paper seeks to present a critique of the innovation system that has emerged to combat computer viruses by comparing it with its natural system namesake, the human anti-viral immune system. It is proposed that the relevance of this analogy extends beyond this case to innovation systems more generally.

Design/methodology/approach – This paper discusses the biological theory related to the human body's immune system and how immune systems might be mimicked in the development of security systems and anti-virus software. The paper then outlines the biomimicry framework that can be used for scoping the development and features of the security systems and software, including the population of the framework segments. The implications of biomimetic approaches in the wider innovation management literature are discussed.

Findings – Some commercial security products that are undergoing evolutionary development and current research and development activities are used to augment the biomimetic development framework and explicate its use in practice. The paper has implications for the manner in which the objectives of innovation systems are defined. There is implicit criticism of linear models of innovation, that by their nature ignore the recursive and/or adaptive processes evident in natural systems.

Originality/value – This is the first paper, to the best of the authors' knowledge, that discusses the application of natural systems and biomimetics to broaden the scope of innovation process design, and link its findings back to the wider innovation literature.

Keywords Information systems, Data security, Computer viruses, Software tools, Innovation

Paper type Conceptual paper

1. Introduction

The creation of innovative products and services, or the adoption of innovative internal processes, is generally a complex and important challenge for all organisations. Rothwell (1992) has emphasised that this process has grown more complex in response to accelerating technological and market-based challenges, with traditional linear views of innovation (i.e. invention driven or market-pull) making way for more fuzzy and non-linear systems of organisational innovation response to market, technological and organisational stimuli (McAdam, 2005). More recently, there has been an emerging

European Journal of Innovation Management
Vol. 10 No. 2, 2007
pp. 201-214

1460-1060
DOI 10.1108/14601060710745251

emphasis on network openness as a determinant of innovation performance (Laursen and Salter, 2006).

Nonetheless, innovation process models have traditionally been characterised as highly linear, involving the creation of knowledge, the transformation of this knowledge into new applications and the commercialisation of these applications to market requirements (Pavitt, 2004). Where innovations systems models have emerged and have become popular, they have tended to address the complex interactions between system participants (within network, regional and national aggregations). A far less prevalent application of systems approaches in the innovation literature has been the examination of the recursive processes that occur within the fundamental problem solving arena of innovation (Leydesdorff and Etzkowitz, 1998).

In this paper, we explore the potential application of complex, biological systemic processes in the improvement of the innovation system and processes in a highly technical field. One of the most dynamically emergent technological product offerings in the global economy, bar none, is the suite of products available to counter the debilitating and/or destructive impacts of computer viruses (Balthrop *et al.*, 2004). The prevalence of computer viruses and other forms of "malware" (unauthorised and contaminant software designed to infiltrate and/or damage a computer or computing system) has been the cause of untold economic and other harm since its inception in the mid-1980s. In its wake, the growth of such malicious applications has spawned an industry intent on providing computer users with a variety of defences and cures for the viral-borne ills.

Anti-virus software vendors generally provide protection for their customers within hours of the virus being detected. Service provision ranges from applications available to single users, through to network-based applications tailored for the security requirements of high-end users like banks and research laboratories. In all cases, the objective and intention of the anti-viral application is to halt malicious damage and preclude future dissemination of the virus to other network users.

A key criticism of the current innovation system that has developed to respond to virus infection is that it is reactive and, as such, ineffective at confronting the causes that lie behind the ongoing proliferation of viruses. These causes have variously been discussed as the inherent vulnerability of the major "closed source" operating systems, the increasing use of peer-to-peer methods for the distribution of infected content and the ubiquity and rapidity of email as a means of spreading the executable viruses.

As such, while the reactive capabilities of the anti-virus industry can be seen as a model of responsiveness, it has failed to address the key issues that allow viruses to spread. We thus see the innovations in anti-viral software as effective only within a limited definition of success. We argue that the use of biological models of viral control will provide a much more successful and comprehensive approach to the development of firstly, an innovative system of anti-viral protection and secondly, a wider metaphor for the development of product and service level innovations.

2. Introduction to the case

In 1983 a series of five controlled viral attack experiments conducted by a promising young doctoral student at the University of Southern California proved the concept of a "computer virus" (Cohen, 1985). Since that early period, it has been observed that

computer viruses have evolved into pieces of software code that exhibit two specific characteristics (Hoffman, 1990, Ludwig, 1996). First, the code has a partial or fully automated capability to reproduce or clone itself. Second, the code can transport itself by attachment to a computing entity (such as a program, disk sector, data file) and ensuing transfers between the various system entities. In the years that followed the seminal research and experimentation, the information systems community has attempted to dissect and develop a greater understanding of computer viruses (Cohen, 1987, Hoffman, 1990, Ferbrache, 1992, Cohen, 1994, Ludwig, 1996, Szor, 2005). In essence, computer scientists and software experts have attempted to understand the pathology of computer viruses, or their basis as an artificial life form (Ferbrache, 1992, Spafford, 1994). Whether the code takes the form of an add-on virus that attaches itself to host programs or software, is an intrusive virus that overwrites the host code, or takes on a polymorphic structure that continues to replicate itself and infect large networks, the quest for greater understanding in this important area of computing security continues.

The parallels drawn with biological hazards, viruses and immune system response has lead to a substantial level of research in the areas of software modelling, biological systems-based design, anti-virus architectures, viral software testing and analysis, and computing heuristics. Some researchers have conducted a matched analysis between human and artificial (computing) immune systems, identifying important similarities (and notable differences) between the immune systems, and describing desirable features that should be mirrored into artificial environments. For example, Skormin *et al.* (2001) identified that both systems were highly complex, distributed and connected with many entry points, were vulnerable to intentional or unintentional introduction of foreign bodies, and must be capable of detecting and neutralising alien matter. Similarly, Harmer *et al.* (2002) asserted that both systems must maintain a massively parallel and distributed architecture for communications and signalling, be capable of self/non-self determination, support autonomic behaviours in attacking new foreign matter and infections, and invoke memory based responses to attacks from past infections. Other research has concentrated on using the biological immune system as an inspirational model for computer anti-virus software (Kephart, 1994, Kephart, 1995, Forrest *et al.*, 1997, King *et al.*, 1999, Goel and Bush, 2004; Goldenberg *et al.*, 2005). The concepts of innate and adaptive biological immune systems are used as direct physical models for developing virus pattern recognition, computer immunological memory, and autonomic virus patch software. Given the evolving business environment where malicious software threats (e.g. worms, viruses, infectious agents) are becoming commonplace, the development of virally immune self-healing or self-defending information systems networks appears to hold some promise.

In exploring this line of inquiry, a review of biological immunity literature suggests that the development of secure networks and software that mimics the human immune system may yield substantial benefits for the protection of critical information and communications technology infrastructure. However, an immune system response to computer viruses and worms would likely involve screening for abnormalities, quarantining the infectious agents, and developing software antibodies to combat the destructive agents. This raises the question: What type of development framework can software organisations use to create security systems and anti-virus software? This

paper presents an innovative development framework that uses biological models for the analysis and creation of artificial systems (Benyus, 1997).

A detailed explanation and summary of the human immune system, including the types of immunity and the biological delivery mechanisms, serves as a theoretical platform for the system development discussion. It is considered important that a comparison and contrast of the biological and information systems immunity problem space be conducted, including the treatment of viruses and virus mutations in both domains. We then emphasize that the development of security systems and software using a biological lens may prove more successful than the current practices and processes. We adopt the biological viewpoint, and describe biomimicry terminology and theory, to discuss some specific examples of how the mimicking of biological systems has supported the solving of human problems (e.g. deep sea sponge structures used as biological models for fibre optic strand development by Lucent Technologies) is developed. The paper then explicates the biomimicry framework and populates the framework with the structure for developing security systems and software, including computer virus immune response. The framework is augmented using examples from current research efforts and developments in the area of information systems network immunity and some commercially available network protection software systems. The paper concludes with some further ICT development opportunities that might be pursued using the biomimicry framework.

3. The human immune systems – a theoretical platform

3.1 Human immune systems

The human immune system is a complex network of specialised cells and organs that protects the body from external biological influences and conditions. Importantly, the immune system provides this protection by responding to antigens (normally large molecular proteins) that gather on the surface of infected cells, viruses, bacterial agents or other pathogens. A large genomic region in our bodies known as the Major Histocompatibility Complex (MHC) contains special genes with critical immune system functions (ie, the Human Leukocyte Antigen (HLA) genes). These HLA genes encode cell surface antigen presenting proteins, as part of the normal cellular structure. This encoding process allows the immune system to use HLA to differentiate between "self" and "non-self" cells. Any cell displaying that individual's HLA type is identified as "self" (no immune response) with cells displaying another HLA type identified as "non-self " (immune response) (Roitt *et al.*, 2001; Paul, 2003; Doherty, 2003).

The human immune system is bifurcated into two major components, Innate immunity and Adaptive (or acquired) immunity. Innate immunity includes the barriers that isolate harmful or foreign bodies as a first line of immune defence (e.g. skin, mucus, stomach acid). The innate system also includes white blood cells, commonly known as phagocytes, that destroy micro-organisms and dead and damaged cells. Innate system phagocytes work by surrounding, engulfing and finally destroying the foreign substances or pathogens. In contrast, the adaptive immune system is based on white blood cells (termed leukocytes) that are produced by stem cells in the bone marrow, and ultimately mature in the thymus gland and/or lymph nodes of the body (Roitt *et al.*, 2001; Paul, 2003; Doherty, 2003).

The adaptive immune system can be partitioned into two further protective sub-systems (Roitt *et al.*, 2001; Paul, 2003; Doherty, 2003). The first sub-system is the

Humoral immune system. Under this immune system, a special type of leukocyte termed B Lymphocytes (or B cells) are formed in bone marrow and produce antibodies (termed immunoglobulins) that bind to the specific bacteria or virus, thereby making it easier for the phagocytes to target and kill the antigens. The second sub-system is the Cellular immune system that destroys virus infected cells with T Lymphocytes (also known as thymus cells or T cells). Cytotoxic or Killer T cells ($CD8^+$T cells) identify infected cells by using receptors to scan the cell surface. $CD8^+$T cells release granzymes that trigger apoptotic ("suicidal") behaviour, thereby killing that cell and any viruses it may be creating. Helper T cells ($CD4^+$T cells) activate a specific form of phagocyte termed Macrophages that ingests the dangerous material, while also producing proteins known as cytokines (interleukins) that induce the proliferation of B and development of T cells (Doherty, 2003).

3.2 Biological and artificial computer viruses

Biological viruses are microscopic parasites that infect the cells of biological species and organisms. Viruses are obligate intracellular parasites that reproduce and replicate by invading and controlling other cells. Importantly, these types of parasites do not have self-reproduction machinery and tend to infect single and multi-celled organisms. Viruses typically carry a small amount of nucleic acid surrounded by a protective coating of proteins, lipids, glycoproteins or a combination of these substances known as a *capsid* (Roitt *et al.*, 2001; Paul, 2003).

Comparatively, a computer virus is an executable program that can replicate itself by invading a host (much like a biological virus), and spreading to other devices as the host is shared or exchanged amongst the device population (Ferbrache, 1992, Spafford, 1994). The growing portability of computing and wireless communication devices is providing expanding opportunities for the transfer of viruses and infected agents. Additionally, viruses may spread through multiple devices accessing network file systems. The most common type of virus is the file virus that infects files or program libraries on an operating system. Macro viruses can be hidden in embedded macros within documents and can self execute when the file is opened, while boot viruses infect the boot sector of diskettes or the master boot record of a hard disk.

Computer worms and Trojan horses are other forms of malicious software that have evolved from the early viruses (Szor, 2005). A computer worm is a self-replicating form of program that is similar to a virus. However, a worm is self-contained code and does not need to be part of another program to propagate across the network. Worms are configured to utilise the file transmission capabilities of computers and network devices, and issue copies of the worm program to other system components. Also, worms often consume large segments of network bandwidth and materially damage the performance of the network and business environment.

Trojan horses take the form of legitimate software programs and perform undesirable technical functions. The functions generally have a malicious intent including spying and backdoor access, which may allow the computer to be remotely controlled (also known as a "zombie" terminal). Advances in the construction of Trojan horse programs have allowed these types of software to replicate through the invasion of a host program or system. This type of evolution has meant that current Trojan horses act much more like viruses, and are generally more infectious than in the previous forms.

3.3 Using biology to develop security systems and software

Experts in the field of computer viruses and malicious software have noted that:

> Natural immune systems protect animals from dangerous foreign pathogens, including bacteria, viruses, parasites, and toxins. Their role in the body is analogous to that of computer security systems in computing. Although there are many differences between living organisms and computers, the similarities are compelling and could point the way to improved computer security. (Cohen, 1987, Forrest *et al.*, 1997)

This analogy suggests that biological and computer viruses share many of the same technical characteristics (e.g. spread through host agents and systems, take mutated forms, highly infectious) and conventions (e.g. strain identification and nomenclature). A good example of common biological and computer virus convention is viral identification schemas. The identification of the various hepatitis viruses by strain and alphanumeric nomenclature shares similar features with the identification tags placed on malicious "Nimda" and "Sasser" computer worms as shown in Table I.

Given the similarities between the biological and computer viruses, the development of security software and systems and computer immune responses might follow parallel pathways. For example, antivirus systems might be designed to act like innate phagocytes where the malicious code, on entry into the environment, is "surrounded and neutralised". In a similar manner, a new design might include a B Lymphocyte type behaviour where remedial code is "attached to the computer virus" making the virus easier to identify and neutralise.

These types of design concepts suggest that the issue of virus outbreak lead times would present fewer problems for security analysts. Rather than designing an antivirus patch (following identification of a vulnerability and publication of the exploit code by programmers and hackers) in anticipation of a viral outbreak, a self-healing or immune network would allow the infection to be identified and neutralised upon entry (Bekker, 2003). The outbreak of computer viruses during

Biological Virus ID	Computer Worm 1 ID	Computer Worm 2 ID
Hepatitis A Virus	W32.Nimda.A@mm; W32.Nimda.A@mm(dll)	W32.Sasser.B.Worm
Hepatitis B Virus	W32.Nimda.A@mm(dr); W32.Nimda.A@mm(html)	W32.Sasser.C.Worm
Hepatitis C Virus	W32.Nimda.B@mm(dll); W32.Nimda.B@mm(dr)	W32.Sasser.D
Hepatitis D Virus	W32.Nimda.C@mm	W32.Sasser.E.Worm
Hepatitis E Virus	W32.Nimda.corrupt	W32.Sasser.F.Worm
	W32.Nimda.E@mm; W32.Nimda.E@mm(dr)	W32.Sasser.G
	W32.Nimda.enc; W32.Nimda.enc(1); W32.Nimda.enc(dr)	W32.Sasser.gen.Worm
	W32.Nimda.I@mm	
	W32.Nimda.J@mm	
	W32.Nimda.K@mm	
	W32.Nimda.M@mm	
	W32.Nimda.N@mm	
	W32.Nimda.P@mm	
	W32.Nimda.Q@mm	
	W32.Nimda.R	

Table I.
Summary of hepatitis biological virus and Nimda and Sasser computer worm identifications (Symantec AntiVirus 9.0.3.1000, 15 January 2006, Revision 8)

2001-2004, and the short patch deployment lead times as shown in Table II, demonstrates that a self-defending network security paradigm may have been more effective than current design practices (Cisco Systems, 2005).

4. Biomimicry – terminology and theory

4.1 Biomimicry – using biological models to solve complex human problems

Biomimicry is the scientific discipline that studies the best concepts in nature and biology and imitates these types of designs and processes in order to solve complex human problems (Benyus, 1997). The Biomimicry term has latin roots with "bios" meaning "life", and "mimesis" meaning "to imitate". The discipline is based on the premise that nature and biological species have efficiently solved a multiplicity of problems that humans are still looking to resolve. Some examples of biomimicry being used to solve complex human problems are outlined as follows:

- The Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense, and the National Aeronautics and Space Administration (NASA) are conducting a joint study of the navigational systems and locomotive strategies of insects and entomological species in order to design the next generation of autonomous robots and space exploration vehicles.
- University of Leeds researchers are studying the jet-based defence mechanism of the bombardier beetle to determine whether the insect can assist them in designing a re-ignition system for a gas-turbine aircraft engine in mid-flight. The beetle is capable of spraying potential predators with a high-pressure stream of boiling liquid excreted at 100 degrees Celsius.
- Nanotechnology researchers at the Massachusetts Institute of Technology (MIT) are attempting to understand the soft-bodied structures of sea snails and other like creatures in order to develop lightweight armour systems for soldiers, police and other law enforcement officers. The MIT scientists are studying the structure and mechanics of the tough inner layer of mollusk shells called "nacre" or "mother-of-pearl" at extremely small nanometer-length scales (one billionth of a metre).

4.2 The biomimicry development framework

The biomimicry development framework is composed from a series of actions and questions that guide the design of new systems, devices and mechanisms (Biomimicry Guild, 2005b) and is depicted in Figure 1.

The first part of the framework asks the designer to identify the problem space and outline the important "why" questions (e.g. Why do the current systems fail? Why do some computer viruses appear impervious to firewalls?). The second part of the

Computer virus ID	Patch ID	Patch availability date	Virus outbreak date	Total lead time
Nimda worm	MS00–078	17 October 2000	18 September 2001	336 days
Slammer worm	MS02–039	24 July 2002	25 January 2003	185 days
MSBlaster.A worm	MS03–026	16 July 2003	11 August 2003	26 days
Sasser.A worm	MS04–011	13 April 2004	30 April 2004	17 days

Source: Merkl (2004)

Table II.
Examples of computer virus and worm outbreaks 2001-2004

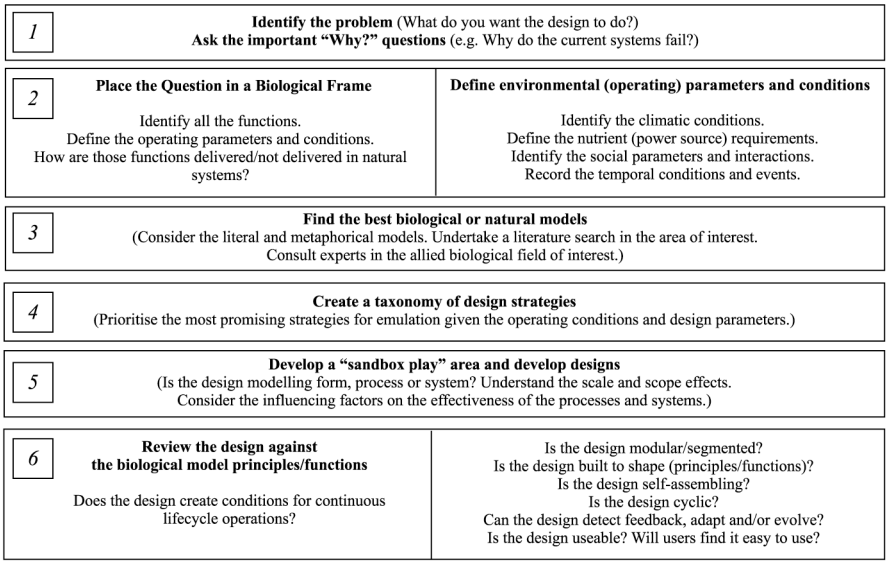

Figure 1.
Biomimicry development framework

Source: Biomimicry Guild (2005b)

framework requests that the designers place the problem in a biological frame (or lens) and define the operating parameters and conditions, including the prevailing climate, social interactions, and temporal conditions and events. The third part of the framework asks that designers examine and select the best biological and natural models for their functional designs. This may include detailed discussions with experts in the allied biological field of interest (e.g. immunology, virology, parasitology). The fourth part of the framework allows the designers to make value judgements and trade-off decisions in developing a prioritised taxonomy of designs. The fifth part of the framework facilitates further development of the designs through testing and "sandboxing". Sandboxing may be defined as the testing of viable alternatives with any problematic impacts quarantined from the main system. The benefits of this part may be seen to include the development of an understanding of the effects of scale/scope and influential design factors. The final part of the framework is a design review that compares the solution with the biological model's shape, characteristics and functions.

4.3 Using biological immune system models to develop security software and systems – a populated framework

The following sections provide summaries of the biomimicry framework segments (parts 1-6) as applied to the development of security software and systems using biological immune system models. The development steps are augmented with examples from the current base of literature and commercial system development activity.

4.3.1 Part 1 – Defining the problem. The problem is best defined as:

> The development of a self-healing (or defending) network that is capable of an active immune response to any introduced computer virus, worm, or other evolving forms of infection.

The reasons behind developing these forms of virus immune networks include the increase in network security threats (through hacking and intrusion), the present inefficient system development paradigm that depends on building antivirus scripts in anticipation of a security event or incident (noting the decreasing lead times), irregular updates of antivirus software by users and clients, high rates of re-infection from un-patched terminals and devices over extended periods of time, and the limited availability of dedicated vendor and user resources for real-time security patch development and proactive deployment (Somayaji *et al.*, 1997; Chen and Robert, 2004; Dasgupta, 2004).

4.3.2 Part 2 – Identify functions and define environmental parameters and conditions. The functions of the security systems and software should include the capability to "detect" abnormalities in the network's operations and systems, "isolate" the computer virus and/or infections, and "develop" software antibodies that "neutralise" the viral effects through "destruction" of the malicious code or rendering the code ineffectual through mediation induced behaviours (Kephart and Arnold, 1994; Kephart *et al.*, 1997; Chen and Robert, 2004).

These types of functions are delivered in biological settings in the form of human and animal immune systems and include the functions for engulfing and destroying infected cells and foreign substances, the generation of antibodies that facilitate and assist virus eradication, and cellular mediation that modifies the infected cell's behaviours (e.g. cellular self destruction or apoptosis) (Roitt *et al.*, 2001; Paul, 2003).

The operating environment in which computer viruses and infections can be encountered includes dynamic local and wide area computing and communications networks, with complex arrays of operating systems, software applications, and databases, coupled with a broad range of system hardware and devices (Bradley and Tyrrell, 2001). These types of computing environments tend to have temperature and air quality controls with multiple users in various locations. Administrative procedures and normal daily network operations suggest that users are continuously added and removed from the networks, while users concurrently access various applications and datasets.

4.3.3 Part 3 – Biological or natural models. In this biomimicry framework exercise, the human immune system has been selected as the "default" best biological model on which to base the proposed security systems and software solution (Biomimicry Guild, 2005a). Other biological or natural system models may provide an equivalent level of utility for this form of system development (e.g. the use of anti-venom treatments for neutralisation of poisonous snake and spider bites which in turn mirror treatments that naturally exist in the environment).

4.3.4 Part 4 – A taxonomy of designs. The taxonomy of designs for this biomimicry exercise may include "identify-surround-neutralise" (phagocyte), "identify-attach-neutralise" (antibody) and "self destructive" (apoptotic) virus immunity systems and software. Typical priorities (based on the likelihood of successful product development) that could be applied to the designs might be phagocytic, antibody, and apoptotic, where phagocytic designs may prove the most successful of all the systems developed, while apoptotic designs may provide greater social and technical challenges in the immediate term. These ratings serve only as examples, and would typically be based on expert opinions provided by antivirus

software developers and vendors. Figure 2 depicts the design schemas for the proposed systems.

4.3.5 Part 5 – Sandbox and design development. In this biomimicry framework exercise, no sandbox area has been designated for system prototype design and testing. However, in current international research and development activities, computer virus test bed environments are available. Good examples of the test environments are the Internet Technology Laboratory test bed at the University of Arizona (Hariri *et al.*, 2003), the sand-boxed test environment at Columbia University (Sidiroglou and Keromytis, 2005), and IBM's High Integrity Computing Laboratory (Kephart *et al.*, 1997). These test environments would allow the system and software designers to evaluate the detection range of introduced viruses and infections, speed of delivery and dissemination of anti-virus prescriptions, and scalability factors such as reduced data rates and vulnerable system components. Importantly, these laboratory environments would support the critical fifth part of the biomimicry based system development.

4.3.6 Part 6 – Design review. In this biomimicry framework exercise, no formal design has been developed and accordingly no design review conducted. However, a number of commercial computer immune systems products, such as Microsoft's Network Access Protection (NAP) and Cisco Systems' Network Admission Control (NAC), provide examples for a simulated review (Cisco Systems, 2005; Microsoft Corporation, 2005). The NAP and NAC products form part of the network quarantine group of technologies. These products monitor, assess and isolate system components (e.g. personal computer terminals, servers, and personal digital assistants) that increase network vulnerability through their possession of non-compliant antivirus programs, out-of-date virus signatures, or un-patched applications and operating systems. The products take a "reverse approach" to traditional antivirus technologies (e.g. Symantec Antivirus) by quarantining vulnerable or infected systems and components rather than attacking the computer virus itself. In this example, the products possess some detection functions, but clearly do not display the more direct virus and infection isolation, neutralisation or destruction functions established under part 2 of the development framework. Consequently, the part 6 review may usefully identify a number of functional variations or deficiencies when compared with the biological or natural system models.

5. Biomimicry – current activities in computer immune systems

Some specific high profile activities demonstrate that the commercial and research communities of interest are presently investing in the research and development of security systems and software that mimic biological immune systems. First, the United

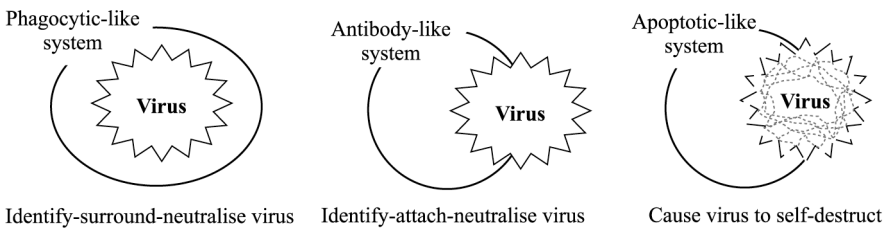

Figure 2.
Design taxonomy – schemas for phagocytic, antibody and apoptotic mimicked immunity programs

States Army Research Office has provided the Electrical and Computer Engineering Department at the University of Arizona with a US$1 million grant to develop bio-mimicked security software. The software is scoped to screen information technology networks for abnormalities, isolate infectious viruses and worms, while developing coded antibodies to fight infections. The first part of the research program will establish the rudimentary modelling techniques and tools, while the second part of the research will be focused on implementing the antiviral techniques (Stiles, 2005). In the second example, the Electronics Department at the University of York has established a funded artificial immune systems research network, comprising of over 125 computer related academics and professionals, under its Bio-inspired Architectures Laboratory. The network supports researchers in establishing the collaborative infrastructure to drive forward research in the areas of computer system immunity, fault tolerant hardware systems, and active machine learning (Network for Artificial Immune Systems, 2005). These activities serve as important examples of the innovative use of biological models for researching and developing computer system immunity.

6. Conclusions

6.1 Biomimicking innovation

Innovation drives product research and commercialization down many paths that may not have been necessarily explored given the often conventional approaches adopted by system designers and engineers. The use of biological and natural system models in the development of artificial and man-made systems and products could certainly be characterized as technically and managerially innovative. Examples presented earlier in this paper demonstrate the value and utility of the approach in solving complex human problems.

In this paper we have presented the theoretical platform relating to biological immune systems and drawn parallels with computer network immunity and antiviral approaches. Our introduction and explication of the biomimicry framework as a system development tool provides a different and innovative dimension to the development of artificial immune systems. The biomimicry framework comprises six parts or steps that allows system designers and developers to define the problem, analyse and identify the desired functions, select the premium biological model, develop and sandbox test the taxonomy of designs, and review the outturn systems or products. The framework enables a different set of thought processes when compared to the predominantly technical and mathematical literature related to computer network immunity.

In this paper we have also demonstrated the viability of the framework through our augmentation approach. This includes our use of expert opinion in extant literature, identified system functions and desired characteristics, and commercial computer immunity products, in populating parts of the framework. Finally, while some current research programs are exploring the use of biomimicry for computer system immunity, other opportunities for developing bio-inspired information technology exist. As an example, the development of "self-healing" optical fibre remains one of the biggest unsolved problems within the telecommunications industry. Damage to the fibre due to earthworks and unauthorized site excavation presents a common maintenance

problem for telecommunications providers. A biomimetic fibre material or technology might be developed to solve this problem.

6.2 Applying biological innovation systems to practice

The natural world provides researchers in every field of endeavour with myriad examples of success and failure in systems development. The worked example above has shown that the natural processes of systems immunity present in the human organism are far more complex and comprehensive than what is evident in the artificial systems of computer anti-viral applications.

In assessing the applicability of mimicking of biological systems to the wider question of product and process innovation, a number of generalisations can be made. The processes of evolutionary variation that are present in nature provide an exemplar of search and testing. The development of cross-fertilised plant species (both facilitated and naturally occurring) with inherent positive traits, provide examples of attribute recombination. The cyclical processes of seasonal variation evident in various landscapes provides an exemplar of systemic regeneration that is generally absent from most business enterprise planning.

When innovation is primarily viewed as a linear process, rather than a complex and adaptive one, choices and issues beyond the examined path are generally ignored. The use of biological systems metaphors to examine innovation processes tends to challenge the limiting assumptions of the technical focus that belies the parsimonious attributes of simplified models exemplified in the primary case of anti-viral software discussed above.

References

Balthrop, J., Forrest, S., Newman, M. and Williamson, M. (2004), "Technological networks and the spread of computer viruses", *Science*, Vol. 304 No. 5670, pp. 527-9.

Bekker, S. (2003), "Appearance of Exploit Code means time is running out to apply critical windows patch", *Enterprise Magazine*, available at: www.entmag.com/news/article.asp?EditorialsID = 5953 (accessed 19 December 2005).

Benyus, J.M. (1997), *Biomimicry: Innovation Inspired by Nature*, William Morrow and Co., New York, NY.

Biomimicry Guild (2005a), "Biomimicry: an introduction", available at: www.biomimicry.net/biom_project.html (accessed 2 November 2005).

Biomimicry Guild (2005b), "Evolving biomimicry methodology", available at: www.biomimicry.net/essent_resourc.html (accessed 17 January 2006).

Bradley, D.W. and Tyrrell, A.M. (2001), "The architecture for a hardware immune system", paper presented at the 3rd NASA/DoD Workshop on Evolvable Hardware, Long Beach, CA, 12-14 July.

Chen, T.M. and Robert, J.M. (2004), "Worm epidemics in high speed networks", *IEEE Computer*, Vol. 37 No. 6, pp. 48-53.

Cisco Systems (2005), "Network admission control", available at: www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html (accessed 1 October 2005).

Cohen, F.B. (1985), "Computer viruses", unpublished thesis, University of Southern California, Los Angeles, CA.

Cohen, F.B. (1987), "Computer viruses: theory and practice", *Computers & Security*, Vol. 6, February, pp. 22-35.

Cohen, F.B. (1994), *A Short Course on Computer Viruses*, 2nd ed., Wiley, New York, NY.

Dasgupta, D. (2004), "Immuno-inspired autonomic system for cyber defense", *Computer Science Technical Report*, May.

Doherty, P. (2003), "Sir John Eccles Centenary Lecture", University of Melbourne, Melbourne, 18 March.

Ferbrache, D. (1992), *A Pathology of Computer Viruses*, Springer-Verlag, Berlin.

Forrest, S., Hofmeyer, S.A. and Somayaji, A. (1997), "Computer immunology", *Communications of the ACM*, Vol. 40 No. 10, pp. 88-96.

Goel, S. and Bush, S.F. (2004), "Biological models of security for virus propagation in computer networks", *Login*, Vol. 29 No. 6, pp. 49-56.

Goldenberg, J., Shavitt, Y., Shir, E. and Solomon, S. (2005), "Distributive immunization of networks against viruses using the 'honey-pot' architecture", *Nature Physics*, Vol. 1 No. 3, pp. 184-8.

Hariri, S., Guangzhi, Q., Dharmagadda, T., Ramkishore, M. and Raghavendra, C.S. (2003), "Impact analysis of faults and attacks in large-scale networks", *IEEE Security and Privacy*, Vol. 1 No. 5, pp. 49-54.

Harmer, P.K., Williams, P.D., Gunsch, G.H. and Lamont, G.B. (2002), "An artificial immune system architecture for computer security applications", *IEEE Transactions on Evolutionary Computation*, Vol. 6 No. 3, pp. 252-80.

Hoffman, L.J. (1990), *Rogue Programs: Viruses, Worms, and Trojan Horses*, Van Nostrand Reinhold, New York, NY.

Kephart, J.O. (1994), "A biologically inspired immune system for computers", *Proceedings of the 4th International Workshop on Synthesis and Simulation of Living Systems, Cambridge, MA, July*, pp. 30-9.

Kephart, J.O. (1995), "Biologically inspired defenses against computer viruses", *Proceedings of International Joint Conference on Artificial Intelligence*, pp. 985-96.

Kephart, J.O. and Arnold, W.C. (1994), "Automatic extraction of computer virus signatures", in Ford, R. (Ed.), *Proceedings of the 4th Virus Bulletin International Conference, Virus Bulletin, Abingdon*, pp. 179-94.

Kephart, J.O., Sorkin, G.B., Swimmer, M. and White, S.R. (1997), "Blueprint for a computer immune system", *Proceedings of the Virus Bulletin International Conference, Virus Bulletin, Abingdon*.

King, R.L., Lambert, A.B., Russ, S.H. and Reese, D.S. (1999), "The biological basis of the immune system as a model for intelligent agents", *Proceedings of the 11th IPPS/SPDP'99 Workshops Held in Conjunction with the 13th International Parallel Processing Symposium and 10th Symposium on Parallel and Distributed Processing*, pp. 156-64.

Laursen, K. and Salter, A. (2006), "Open for innovation: the role of openness in explaining innovation performance among UK manufacturing firms", *Strategic Management Journal*, Vol. 27 No. 2, pp. 131-50.

Leydesdorff, L. and Etzkowitz, H. (1998), "The triple helix as a model for innovation studies", *Science & Public Policy*, Vol. 25 No. 3, pp. 195-203.

Ludwig, M.A. (1996), *The Little Black Book of Computer Viruses*, American Eagle, Show Low, AZ.

McAdam, R. (2005), "A multi-level theory of innovation implementation: normative evaluation, legitimisation and conflict", *European Journal of Innovation Management*, Vol. 8 No. 3, pp. 373-88.

Merkl, W. (2004), "Self defending networks", Cisco Systems, available at: www.cisco.at/partner/pdf/wmerkl-7423.pdf (accessed 15 June 2005).

Microsoft Corporation (2005), "Network access protection", available at: www.microsoft.com/technet/itsolutions/network/nap/default.mspx (accessed 1 December 2005).

Network for Artificial Immune Systems (2005), University of York, York, available at: www.artificial-immune-systems.org/artist.htm (accessed 7 February 2006).

Paul, W.E. (2003), *The Immune System: An Introduction, Fundamental Immunology*, 5th ed., Raven Press, New York, NY.

Pavitt, K. (2004), "The process of innovation", in Fagerberg, J., Mowery, D. and Nelson, R. (Eds), *The Oxford Handbook of Innovation*, Oxford University Press, New York, NY.

Roitt, I., Brostoff, J. and Male, D. (2001), *Immunology*, 6th ed., Gower Medical Publishing, London.

Rothwell, R. (1992), "Successful industrial innovation: critical factors for the 1990s", *R&D Management*, Vol. 22 No. 3, pp. 221-39.

Sidiroglou, S. and Keromytis, A.D. (2005), "Countering network worms through automatic patch generation", *IEEE Security and Privacy*, Vol. 3 No. 6, pp. 41-9.

Skormin, V.A., Delgado-Frias, J.G., McGee, D.L., Giordano, J.V., Popyack, L.J., Gorodetski, V.I. and Tarakanov, A.O. (2001), "BASIS: a biological approach to system information security", *Proceedings from Mathematical Methods, Models, and Architectures for Network Security Systems (MMM-ACNS) Conference 2001*, pp. 127-42.

Somayaji, A., Hofmeyer, S. and Forrest, S. (1997), "Principles of a computer immune system", *Proceedings of New Security Paradigms Conference, Great Langdale, 23-26 September*, pp. 75-82.

Spafford, E.H. (1994), "Computer viruses as artificial life", *Journal of Artificial Life*, Vol. 1 No. 3, pp. 249-65.

Stiles, E. (2005), "UA ECE fets $1 million to fight cyberspies with bio-mimicking software", University of Arizona News Release, 28 October, available at: http://news.mongabay.com/2005/1206-ua.html (accessed 15 December 2005).

Szor, P. (2005), *The Art of Computer Virus Research and Defense*, Addison-Wesley Professional, Boston, MA.

Corresponding author
John Rice can be contacted at: john.rice@adelaide.edu.au