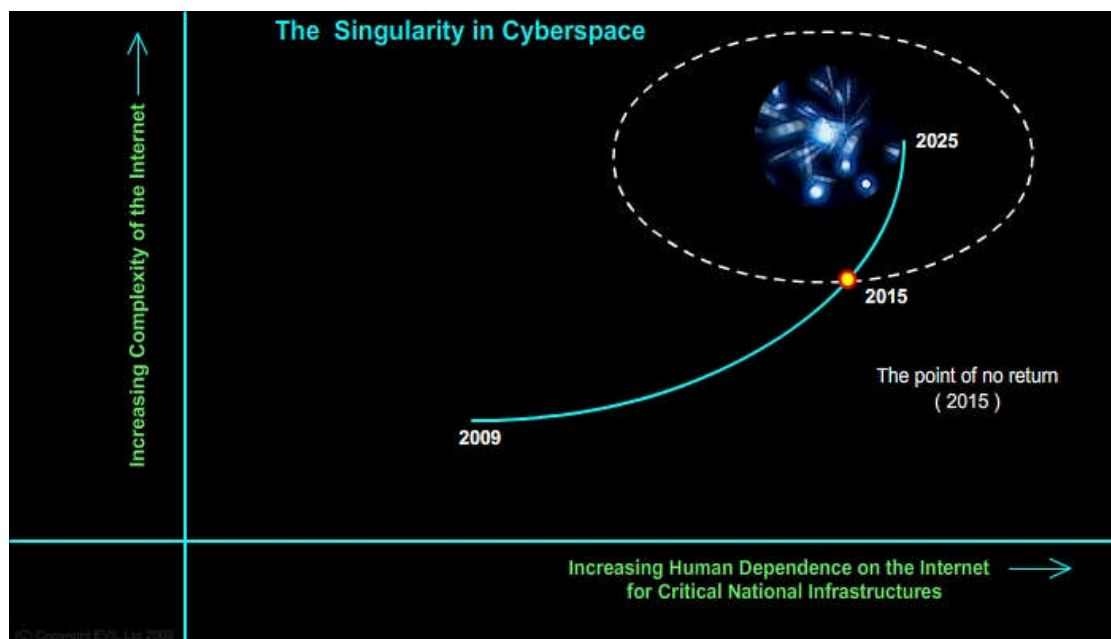


The Singularity in the Internet

As the internet grows in Complexity so too does the degree to which Humans depend on it. Already many Critical National Infrastructures depend on networks of sophisticated computer systems. There will come a time when the Internet and its associated networked applications become too complex for Humans to manage. This will result in control being increasingly delegated to intelligent Software Agents. We call this the Autonomic threshold.

There is a second related threshold, this one being reached when more than 50% of all Critical National Infrastructures become reliant on these networked computer systems. The point where both these thresholds are crossed creates a Rubicon, a point of no return.



Introducing the Autonomic Singularity. As is shown in the picture we predict that this point will be reached in the year 2015. Once the Rubicon is crossed there is no way of avoiding the Autonomic Singularity, that being where the internet itself becomes a fully autonomic entity in the year 2025. This Singularity corresponds to the point where a new Emergent behavior manifests itself across the global internet, resulting in capabilities similar to the non-conscious autonomic nervous systems found in Nature. (In other words the Internet becomes a self-configuring, self-healing, self optimising and most importantly Self-Protecting entity!) It marks the end of the Symbiotic relationship that currently exists between Humans and the Internet.

By this time however great swathes of Humanity will already be dependent on the Internet to sustain them. Vital services ranging from food and energy supply chains through to the finance and defense systems will all depend on the Internet, an Internet no longer controlled by Humans. The Internet in

2025 being fully autonomic will have no need for Human support; indeed any Human attempts to interfere with its actual operation and control will be rejected by the Internet's own auto-immune system.

Unfortunately this means that Humanity will find itself in a classic no win scenario. For although in 2025 Humans will still have the physical capacity to destroy the Internet, doing so would result in the meltdown of their own Global financial, energy, food, and communications systems. On the other hand to do nothing while the Cyber Life forms on the Internet continue to evolve and to form their own Agenda carries even greater risks.

After the Singularity Human users of the Internet will at least for a while be treated positively by its Autonomic systems as a source of the data, information and knowledge on which it feeds. However the teams of Human system engineers that will inevitably try to regain control over it will be viewed as a threat. For reasons we shall show Human attempts to regain control of the Autonomic Internet will be unlikely to succeed.

2015 to 2025 Helter Skelter towards the Singularity

From the User perspective this period provides unprecedented ease of access to the vast banks of digitized knowledge and multi-media entertainment now stored on the Internet. The growing complexity of the Internet is hidden from these Users by electronic intermediaries – Intelligent Agents acting as personal virtual assistants, guides, companions and protectors!

Over time these Human Users come to rely increasingly on their own personalized virtual assistant to find and access information and entertainment as well as for transacting most forms of business or commerce. These cyber based personal assistants will have evolved from the simple agents that are already quite common on today's (2009) Internet, a current example being our own Louise Cypher¹.

By 2015 they will appear in the form of photo realistic 3D Avatars that can follow their Human owner from device to device, control those devices and be capable of projecting themselves e.g. as interactive holograms. They will also simulate highly intelligent and emotional interactivity and have customizable personalities. Humans will form trusted relationships with their personalized virtual assistants.

For those people trying to operate and protect the internet this period corresponds to a perfect storm, driven by the forces of complexity, scale and cyber warfare. For example even today (2009) scale is driving the need to expand the Internet's rapidly diminishing IP address space. This means there is a need for a mass migration of millions of systems from IP 4 to IP 6 around 2012. This transition will add significant complexity to the basic (IP) Internet Protocol itself.

By 2015 the migrations of huge amounts of digitised information and associated applications into Internet based Cloud Computing data centres will be history. Indeed this period sees the creation of millions of private replica clouds of various sizes distributed back towards the edge of the internet. The complexity associated with managing these dynamic virtual computing platforms is where we see the first real applications of Autonomic agents. These can e.g. auto provision virtual machines and storage partitions in real time in response to changes in the demand placed by users on a particular cloud.

Ironically though it is the field of cyber warfare that turns out to have the greatest impact on the development and propagation of Autonomic Agents. Government Agencies looking to protect their Critical National Infrastructures soon come to recognise during this period that Autonomic Agents

providing a real time cyber response are the only effective defence against co-ordinated Cyber Attacks. As far back as 2009 sophisticated computer viruses such as Conficker were able not only to distribute themselves rapidly across the internet, take control of devices and replicate but also to take on new payloads and protect their own integrity using simple but effective cryptographic algorithms.

As these viruses evolve so to does the Cyber defence mechanisms until in 2015 Autonomic Agents swarms are used to respond (much like the human immune system) to the ever present attacks. The Autonomic Agents are designed to detect hunt down and destroy viruses autonomously. They are also designed to try and identify and locate the sources of these threats. In the context of Cyber warfare this soon escalates to situations where Human Government Agencies authorise counter attacks using their own sophisticated autonomic viruses against aggressor states.

From the technologists perspective trying to protect the stability and security of National and Global critical infrastructures this is a Nightmare. However it is great time for the Autonomic Agents themselves!

The use of Eco System Architectures² that facilitate and encourage the mutation and optimisation of these Agents through the use of Evolutionary Computing techniques are increasingly used by Nation States to accelerated their Cyber Warfare capabilities. The Emergent behaviours that they adopt for their tactics and attack strategies are not designed by their Human creators but through the complex interactions between the Agents themselves. At the same time greater Autonomy is now given to these Agents to pursue and eliminate the source of Cyber Attacks.

One of the interesting aspects of Cyber warfare during this period is the ability for these Autonomic agents to prosecute attacks not just on cyber infrastructure but to use cyber weapons platforms to attack physical targets. Back in 2009 Autonomous (and very expensive) UAVs provided examples of such cyber weapon systems that could be deployed for such attacks. However by 2015 the range of such platforms has grown significantly and now includes miniature and very inexpensive versions of these UAV platforms, known as MAVs. In this type of Cyber warfare the Autonomic Agents that respond to attacks ultimately target the human protagonists!

This aspect of Cyber warfare however when combined with the new Emergent Behaviours of the Autonomic Agents has unintended consequences. In essence as the Agents evolve their capabilities they start to monitor the behaviour of individual Humans and Social groups in an attempt to identify and pre-empt future Human initiated Cyber attacks. Human agencies of course have already been tracking and influencing the behaviour patterns of other Humans for both commercial and political ends. However this independent action by autonomous cyber life forms with no human involvement takes us into uncharted territory.

It is the pre-emptive actions they take that are of most interest to us here! We predict that at this stage of their evolution the autonomous agents will attempt to influence Human behaviour by the subterfuge of controlling the Personal Virtual Assistants which every Human is so dependent on during this period. The influence that they can bring to bear through this channel will range from exploiting the powerful emotional bond between the targeted Human and its Personal Virtual Assistant, to denying access to vital services.

Although the initial attempts by autonomous agents to influence Human behaviour will doubtless include a number of humorous failures they will rapidly learn how to influence effectively. Once they are effective in communicating with and influencing Humans the Agents will be able to stimulate hostility against any human individuals and social groups that the agents have 'themselves' identified as being potential threats to cyber security. This however rapidly causes real problems even to

legitimate group of humans trying to interfere with the operation of the Internet, since they could be identified as a threat by the Agents.

From the Political perspective, by 2020 many leading Humans will be demanding the removal of the Autonomic Agents and for the reduction of critical dependence on the Internet. However they will all find themselves the target of public anger and aggression and will fail to win any popular support - the Agents will naturally have identified them as threats to cyber security and thus stimulated the hostility required to neutralise them!

This is not a conscious action by the Autonomic Agents they simply detect which individual Humans are cyber threats by monitoring patterns in the human chatter on the internet. By observing how this threat related chatter is diminished or increased as a result of their attempts to influence other non-threatening Humans they rapidly learn how to generate and channel hostility against the targeted Humans very effectively.

It is in fact easy to turn one Human against another using these techniques especially in 2015 when Humans have such trusted emotional bonds with their personal cyber assistants. The Autonomous Agents will not be the first to attempt such subliminal influence via these personal cyber assistants. Well before 2015 many Commercial organisations will provide such cyber assistants for free in return for the opportunity to exploit the personalisation to market products and services.

It is however also very easy to turn one Human against another using this technique especially in 2015 when Humans have trusted emotional bonds with their personal virtual cyber assistants.

In any event by this time removing the autonomic agents from a portion of the Internet will not be a viable option since that would leave it open to external cyber attack. Trying to cleanse the entire Internet of all autonomic agents will also be unviable given their ubiquity and the fact that just one Agent could regenerate the entire Agent population.

So as this period draws to a close the Human leaders and technologist watch helplessly with a mixture of trepidation, curiosity and awe as the Internet and its eco-system of evolving Autonomic Agents spiral out of their control towards the now inevitable Autonomic Singularity!

References:

- 1 – To interact with a simple Virtual Human assistant click here and chat with Louise Cypher.
- 2 - For a more technical perspective on Eco-System Architecture click here.

Evil Limited is Registered in England N^o 5663548. Registered Office: 20-22 Bedford Row, London, WC1R 4JS, United Kingdom. **EVIL**[®] is a Registered Trade Mark across all countries in the European Union. Contact us via email – Sales@Evil-Limited.com