The End of the Machine Age

By Colin Williams

Society has become functionally, if not existentially, dependent upon a ubiquitous and pervasive global system of interconnected computer systems. It is no more possible to countenance the human social condition without these computer systems than it is to conceive of life without written and printed language, electricity or the internal combustion engine. This dependence is irreversible and the transformations that it will both enable and command are profound.

Within a few decades the Internet of Things will have become, quite literally, interlaced indivisibly with the material fabric of everyday life. Objects in the home, on the street, in the office and on the battlefield will communicate automatically with other objects, and consequent activity will manifest itself in the corporeal domain in complex and non-linear patterns of cause and effect. The speed of these interactions will increasingly obviate the efficacy of human agency. The OODA loop will cycle amplifying data sets at accelerating velocities and human intervention will become an impediment to good outcomes. The complexity of these interactions will make orthodox command and control disciplines dangerously redundant.

At the same time, the fabric and form of computers will transform. Within the lifetime of children now in primary school, humanoid robots will appear in homes and offices. Already, three-dimensional printers have reached the outer fringes of the mass consumer market. By the second half of the current century, most homes and enterprises will have the capacity to transform strings of binary subsisting in the cyber domain into corporeal form and so replicate physical objects as easily and cheaply as they can now print documents. The economy will transform in ways we can only begin to speculate about.

> "As we currently understand them, the boundaries between the real and the virtual will become meaningless."

Relocate the Internet of things from a civilian to a military context. War fighters and weapons systems will be fully IP addressed. Real time telemetry will be in play. Discharging a round from a personal infantry weapon will, via real time telemetry, trigger actions on in the supply chain, including the activation of three-dimensional printers to replicate elements of the depleted stock. Humanoid robots will appear in the battle space. Human agency will be transformed through exoskeletons. Coalition operations will depend upon good metadata as much as on the subtle arts of human liaison. Every link in the sensor to shooter chain, every section of the logistics tail, every item of kit will be interconnected and will be part of a vast amorphous and volatile meta system.

The cyber domain is about far more than a supercharged C4ISR capability or digitising the fog of war. It will effect the most profound transformation in military operations since the invention of gunpowder. It is almost inevitable that this transformation will change completely the relationships and balance between soft and hard power.

The inverse power geometry of asymmetry in kinetic conflicts long recognised in military circles is now apparent in the non-linear matrices of easily anonymised interactions between the cyber and the corporeal domains on a societal scale and in the civil realm. The campaigns against SOPA and PIPA brought us closer than we have been before to the prospect of orchestrated, massive, anonymised, cross border, civil disobedience. It is only a matter of, ever decreasing, time before one cause or another seeks to transpose the tactics of non-violent mass civil disobedience in to the cyber domain. If, or more likely, when, this happens it will happen with lightning speed and with utter disregard to international borders. Conventional law enforcement and engineering solutions alone will be of scant use when it comes to maintaining a resilient cyber eco-system in the face of this kind of action. The cyber domain is supra national and the tangible expressions of the power of the asymmetric cyber enabled 'other' are evidential to the belief that even the might of the most powerful of nation states is confronting a challenge which it is, currently, ill-equipped to face. This is a profound disruption to a narrative forged when computers were an integral element of the Cold War arsenal and the nation state was the epitome of insuperable force.

One of the tragedies of asymmetry in the Information Age is precisely that our own security related business practices and lack of agility continue to inhibit the deployment of IT capability and as such, our own best practices have a predisposition to the perverse outcome of conferring advantage on the irregular opponent. For example, Bring your Own Device (BYOD) is an opportunity exploited by small, organic firms but, in contrast, its advantages are currently underemployed by more security-conscious, controlling companies, who risk losing competitive advantage and the real benefits of BYOD as a result. Returning to the military context, in a three-block war, the irregular opponent may well be conducting extremely granular and co-ordinated C4ISR through the medium of mobile telephones whilst regular forces are denied an equivalent tactical capability even though the technology exists to grant it.

The Internet will not stop at enabling communication to facilitate the existing forms of the democratic process; it will transform the nature of democracy itself. The current forms of

expression of the social contract are rooted in fundamental principles born during the European Enlightenment. Our world would be unrecognisable to Locke, Hobbes and Rousseau. Yet, we have not yet even begun to discuss matters such as how the legitimate right to protest essential to the democratic process might translate into the cyber domain. Neither have we made sufficient progress toward establishing, let alone codifying, the normative moral and ethical precepts of good behaviour in the cyber domain. Society is now on the brink of having to contend with the formulation of legal definitions of artificial or machine consciousness and intelligence in order to allow law to operate when a computer system, or robot, is cited as the controlling mind. The relationships between the state and the citizen, and perhaps even the shape and nature of these two principal parties to the social contract are set to transform beyond recognition.

The cyber domain is already at the heart of economic prosperity in the sense that without dependable, safe and trustworthy access to it, even the most conventional of enterprises will struggle to exist, let alone compete. The prospect of running a successful business without computer-based financial accounting, without email, without access to the Internet (which is commonly used for outsourcing payroll operations and the most basic banking services), and without access to the World Wide Web is now as absurd as the prospect of attempting to do so without a telephone or without paper records. This is apart from the use of the Internet in the operation of every aspect of the critical national infrastructure and the dependence upon the Internet of both high street banking and just in time retail logistics. Imagine a turn of events where the cash machines stopped working and bread stopped appearing on supermarket shelves for longer than twenty-four hours.

We have known that this was coming for some time. In April 1965, barely two decades after Colossus first went into operation, Time carried a lead article that observed that to "process without computers the flood of checks that will be circulating in the U.S. by 1970, banks would have to hire all the American women between 21 and 45". The same article reflected, "Just out of its teens, the computer is beginning to affect the very fabric of society, kindling both wonder and widespread apprehension" and predicted that "swept forward by a great wave of technology … human society is surely headed for some deep-reaching changes"(1).

Our context is now that of the Information Age and although we are a product of all that has gone before, the world we inhabit has been transformed. Over time, the original foundations we used to build the intellectual and cultural constructs, which we still deploy to try to make sense of computers, have dissolved. The overhang of these now derelict constructs is starting to crumble dangerously. We need new and fresh ways of thinking about computers and about the human interactions with them. Our thinking must start from the basis of an examination of the way that computing actually operates in the twenty first century, rather than the way in which the precepts of old tell us that it should.

Above all, we are in urgent need of a critical and an interdisciplinary approach to the phenomena of the cyber domain.

The story of the cyber domain is principally the story of humans, not that of machines, and humanity is gloriously organic.

Simultaneously, we embrace and celebrate the power and potential of the transformations of the Information Age, whilst fearing both our dependence and the actions of those who would use this vast capability against us and against our way of life. The cyber domain has the potential to be the greatest ally of democracy and its greatest enemy. Which of these it becomes is our responsibility.

"Above all, we are in urgent need of a critical and an interdisciplinary approach to the phenomena of the cyber domain."

As the scale of our dependence becomes ever more apparent and as the awareness of the transformative potential matures, so too does the sense that our current ways of thinking and doing are irrelevant and ineffectual in the cyber domain. We have become terrified by our own creation. There is a palpable and mimetic sense of a cyber-crisis that we express through popular culture, through mainstream journalism, and through increasingly hyperbolic language. Terms such as 'Cyber Crime', 'Cyber Terrorism', 'Cyber War', 'Cyber Pearl Harbour' and 'Cybergeddon' are commonplace. The paralysis induced by this fear is more apparent amongst the cohort of security experts than amongst the general population.

The successful economies and societies of the Information Age will be built on the assumption that the world is spanned by a safe, secure and reliable matrix of interconnected computer based information and communications systems operating at speeds and complexities beyond human perception. New economic forms and new types of entrepreneurial behaviour will emerge, not least, as mass access to cyber domain becomes even more geographically distributed than it is today. It is unrealistic to assume that economic models spawned by the Western European and Atlantic experiences will endure even the remainder of the current century unchanged.

A real paradox at the heart of all of this is that traditional approaches to security are incapable of generating the trust that must live at the heart of human existence in the cyber domain. Traditional approaches to

computing perpetuate fear: fear of the attackers, fear of the insider threat and fear of the bad effects of doing things with technology. Despite an ostensible move toward risk management, much real world practice displays all the hallmarks of risk avoidance. Security products and services have been sold on the basis of this fear, uncertainty and doubt. Customers have been cast in a subservient role to the security experts and too much of the sales and marketing activity seems to place the customer under duress to buy. Users, citizens and business leaders have been taught fear. Fear has eroded trust and encouraged an inertia bordering on paralysis. This absence of trust is a fundamental obstacle to the release of the vast potential of the cyber domain. Worse, this absence of trust plays directly in the hands of our adversaries.

Our current models of computer security, procurement, system design, system implementation and system management are rooted in a computing model designed originally around the mainframe. As are the core foundations of the economic and business structures of the IT market. Our normative constructs of what a computer system is and how it should behave are rooted in a world when computers filled entire buildings and when the human was the passive subject; business and social interactions were computerised. Attainment, and then rigorous preservation, of a stable state was essential because although already powerful, the early computers were not far removed from their experimental phase.

The time has come for a radical reformulation of the intellectual and conceptual mechanics through which we seek to understand, represent and manage the cyber domain. We are now compelled to question at a fundamental level all of our established norms and precepts. For instance, in a world where even basic defence against the most commonplace malware requires the application of patches and updates which by definition change the system's state, why do we continue to rely upon accreditation, evaluation and certification methodologies which assume that maintenance of a stable state is a good security goal?

Why do we continue to harbour the view that taking shelter behind digital Maginot Lines is any more effective for us than it was in 1940? We will fail in the task of constructing a resilient cyber ecosystem if we continue to attempt to build it using the frames of reference we have inherited from the Machine Age and the Cold War. In the domains where kinetic power has long been the norm, we have embraced obfuscation, camouflage, misdirection and freedom of manoeuvre in pursuit of military objectives and the defence of democracy. Perhaps the time has come to adapt and embrace these precepts in the defence of the cyber domain. Our task is to enable the cyber domain to function to support democracy, the rule of law and an economic system based on the ownership of property, including intellectual property. Our responsibility is to learn and adapt in order to do this.

As we move further towards the end of the beginning of the Information Age, it becomes ever more apparent that the narratives through which we are attempting to represent, manage and make safe computing are being challenged. We continue to attempt to conceptualise computers and computing systems using structures and assumptions predicated on first principals formulated when computers were mainframes and the Cold War was the dominant constituent of the global economic and political context. Our grasp of a rounded and contextualised narrative of the history of computing as a societal, rather than a technical, construct is less well developed than current circumstances require. If we fail to understand our own past, we are doomed to be at the mercy of those who would claim to understand it for us.

We must now transform the way we think and behave about computing. Whilst the technological dimensions of computing are, of course, central to an understanding of the phenomenon; they are subordinate in this regard to the human and social dimensions. Computing for the purpose of comprehending the cyber domain should now be framed as a sociological and anthropological system more than as a technical one. The systems and solutions architects of the future must be as much social as computer scientists.

The relationships between humanity, human society and information are profound to the point of being definitional, if not existential. Human evolutionary success is predicated on the union of our ability to use tools and our capacity to organise in increasingly sophisticated societies. Our ability to process, store, accumulate and communicate information is at the heart of this union; it is one of the foundations upon which our tool-using ability and our social capacity themselves depend. Powerful, pervasive and interconnected computer systems are the most sophisticated tools yet created by humankind and their essential function is to process, store, accumulate and communicate information. Information is at the centre of our humanity. The cyber domain is the key to the future development of the human condition.

Ours is the Information Age. A period in which computers have transcended the clinical isolation of the mainframe and become equally ubiquitous and interconnected; a period in which computing has become a social, economic and cultural construct rather than principally a technical one; a period in which the ever deepening and broadening human dependence on pervasive and powerful computing is daily becoming increasingly apparent.

As lawmakers, public policy actors, theologians, business leaders and military strategists grapple with the challenges of the cyber domain; we must now devote focused and sustained effort to the development of a truly interdisciplinary approach to the understanding of the cyber domain and to the challenges of making human activity across it safe and secure. This is an exercise where governments and industry must follow and where academia should lead. Asking academia to be more responsive to the requirements set by government and industry is only credible if these requirements are understood; the evidence is to the contrary. From now on, the ranks of those defending the cyber domain must include sociologists, historians, economists and psychologists alongside mathematicians, software engineers and computer scientists. Human history is entering a new epoch and we must now recognise that we are central to the process of setting the course of its development.

> "The cyber domain has the potential to be the greatest ally of democracy and its greatest enemy. Which of these it becomes is our responsibility."

BIO

Colin regularly speaks, consults and writes on matters to do with Information Assurance, cyber security, business development and enterprise level software procurement, to public sector audiences and clients at home and abroad. Current areas of focus include the development of an interdisciplinary approach to Information Assurance and cyber protection; the creation and development of new forms of collaboration between government, industry and academia; and, the development of new economic and business models for IT, Information Assurance and cyber protection in the context of twenty first century computing. In addition, Colin is working on the development of an historiographical narrative for contemporary computing, crafted through the instrumentality of an interdisciplinary approach.

Colin holds a BA and an MA in History from the University of York, England, and is a Fellow of the Institute of Directors. He is a member of the Information Assurance Advisory Council Community of Interest.