Of Quickers, Bytes and Cakes

Colin Williams, SBL

Our world seems to us unfathomable, uncertain and dangerous. Looking back it was less so during the Cold War;notwithstanding the long shadow of nuclear conflagration. We are unsettled; afraid. For every generation thereis a Golden Age; yesterday. Arcadia is a place of imagination and memory, and distance dulls the memories ofpain. It offers the apparent comfort of predictability rather than the disruptive uncertainties of the future. Paradiseis, eternally, lost. Arcadia is discovered by each generation in its turn; an inevitability of age as much a product of objective contextual change; nonetheless, ours are interesting times.

We are Generation X. The controlling minds of the institutions of the state, of society and the economy; and those who offer them sage counsel. The technocratic elite of computing, and of cyber security. We are the experts. Our grasp of the levers of power and influence is temporary, and we have been served our notice by Generation Y. These Millennials are impatient for control. We have a finite and diminishing period of time in which to contribute to the solution of the problems of our time, and therefore of our creation, and so control our legacy. Incessant repetitions of the descriptions of these problems, and ever more hyperbolic celebrations of their complexity and ostensible intractability, are insufficient.

Our social, economic and political context was forged by and during the Cold War. Similarly our intellectual and cultural frames of reference. The world we made, the time and space we lived in, and the ways in which we sought to make sense of it all were given their shape and form within a context. A context within which we were simultaneously subjects and objects; we made it as much as it made us. More so than any other species, humanity is the instrumental agent of its own defining and formative context.

This context was one of conflict with a clear, predictable and symmetrical adversary. Nation state faced nation sate, directly and through proxies. Two diametrically opposed ideologies competed, to the death. But both were the products of the grand unifying thought systems of the nineteenth century. The conflict was, literally, existential, and the adversary the definitional other. We crafted the narrative of our own identity through differentiation from the narrative of the Soviet other that we ourselves also created. The differences between them and us were clear, certain and deeply rooted in the consensual and communal sense of our righteousness. The identities we forged unified us within and across national boundaries. We had a mission; a way of life to defend, an existence to preserve, powerful allies at our side and a clearly defined enemy to confront. It was simple.

Our war may have been, largely, cold. It was nonetheless total. Clothes, architecture and popular culture were as much a dimension of the front line as overseas aid, support for proxy states and combat in Vietnam.

The Cold War was, deep in its core, an economic contest. The ultimate victory a product of financial, as much as ideological, bankruptcy. Unfeasibly complex and far-fetched weapons systems plucked from the realm of science fiction did not have to be able to work in reality; they simply had to cause the adversary to expend time and treasure in preparing against the possibility, however remote, that they might. The bureaucracy and torturous logistics of the Warsaw Pact were doubtless as frustrating, even to their own apparatchiks, as were there those of NATO; and as costly. In reality, neither NATO nor the Warsaw Pact actually had to worry overmuch about an Article 5 deployment of conventional forces because by that stage the missiles would already have been airborne. The vast war games enacted across Europe served both as regular reminder of the futility of conventional forces in the face of the nuclear threat and as a means of sustaining the tempo and magnitude of the defence budgets of the protagonists. Blowing stuff up is a great way of driving an inventory refresh.

OUR WAR MAY HAVE BEEN, LARGELY, COLD.
IT WAS NONETHELESS
TOTAL.

We are beginning to apprehend, belatedly, the enormity of the transformations of the Information Age. Now, belatedly, we catch our first true glimpse of the gaping chasm separating us from the Millennials. We are easy prey to the collective paralysis of future shock. Some of us are beating a retreat to Arcadia. The symmetry, clarity, predictability and certainties of the Cold War appear comforting. A world of clear and certain binary choices; of absolutes of right and wrong. Of survival or total destruction. A world in which the instruments of our potential destruction were artefacts of the Industrial Age. To us, atomic weapons were machines delivered by machines. Artefacts of engineering, apparently deterministic systems, which we could comprehend, command and control. Bunkers of the mind are as real as those of steel and concrete. The one the tomb of the intellect as the other was the tomb of hope.

The computers of the Information Age were born in the crucible of total war; at Bletchley Park. From the outset the modern electronic computer was a device of war, deployed by the nation state in the prosecution of the mission of survival and victory. The computers of the Cold War were likewise an intrinsic and indispensable part of the existential struggle that defined the twentieth century.

The Cold War dictated the pre-eminence of strict confidentiality. The mere fact of the existence of a system, let alone its function, mode of operation or data stores, could be subject of the most extreme secrecy conditions. Soviet infiltration of the Manhattan project taught us some hard lessons. The nature of early computers dictated that the requirements of integrity and availability were elevated alongside those of confidentiality in the canonical triumvirate of CIA.

Early computers were complicated, unstable and temperamental; little removed from the realms of highly experimental research. Each time was the first time. There was no prior art, no set of standards, no experience to be learnt from. Occupying vast spaces, housed in protected environments, consuming prodigious amounts of power; they were nurtured and coaxed in to operation by a special and new type of expert human.

was no prior art, no set of standards, no experience to be learnt from. Occupying vast spaces, housed in protected environments, consuming prodigious amounts of power; they were nurtured and coaxed in to operation by a special and new type of expert human.

Computers obeyed the precepts of logic; inexorable and unquestioning. Natural human language lacks the precision and linear logical structure required to tempt them to render their services. These new experts had to transliterate and mediate between their charges and the users. Humans had to learn to speak Boolean rather than computers having to learn to speak human. The human operator became the weakest link in the chain; tiny errors in punched card inputs could amplify throughout a complex system of onward calculations with a speed never experienced by humans before. Already, the complexity of these early systems meant that the recursive tracking of the source of an error that had spread exponentially prior to detection at the end of the computational process was a task of gargantuan proportions. The costs and risks of such errors rapidly assumed similar dimensions. Garbage in, garbage out became the stern injunction.

Early computer systems seemed knowable by humans in a way that the cyber systems of the Information Age do not. The appropriation and evolution of the concept of ontology by computer science from philosophy illustrates this. For a philosopher, the exploration of ontology of a thing is about the essential 'itness' of the thing; the nature, limits, types and quantities of all of those properties required for an it to be an it rather another, different, it. For a computer scientist, the ontology of a system is a map of the domain. The all-encompassing cartographic record of the systemic totality. Arranged in logical, ordered, categories; precisely defend and clearly delineated.

The presence of such an ontology is a normative predicate for commencing system operation. This ontology is the essential narrative construct of the deterministic computer system. It is the obliteration of the illogical and imprecise vagaries of natural language and the chart through which cause and effect can be modelled and so predicted. The human dimensions of the system were problematic precisely because they were indeterminate; autonomous sources of feedback, deviant signals that altered the system state in violation of the prescriptive ontologies. Disruptions to the formal patterns of linear logic.

A certain kind of mathematical intellect, a predisposition towards obsessive precision, mastery of linear forms of logic, a desire for certainty, a craving for predictability and an absolute reliance on routine were the desired attributes for the new breed of computer expert; for the humans who could build the requisite ontologies and mould the systems in to compliance with them. Typically, those possessed of such qualities tended to find their fellow humans less comfortable companions than the new computers. Previously, those swelling the ranks of the emerging computing professions had struggled to attain social status or prestige.

The attainment and maintenance of a known and stable state was an essential and necessary principle of Cold War computing. Survival against the Soviet threat was impossible without computers. Their failure meant failure of the military capability upon which deterrence depended. Friend and foe had to believe that when the button was pushed the missiles would launch.

Through the combination of the heroic endeavours at Bletchley Park, the subsequent work of Turing at Manchester and elsewhere, the brilliance of Wilkes and others at Cambridge, and the astonishing achievements of the Lyons catering company in building the world's first commercial business computer in the form of LEO, the UK established an early lead in the nascent field of computers and computing.

However, by the end of the 1950s the early advantage had been squandered and by the early 1960s the US supply base was already several years ahead. Amidst the complex multitude of subordinate reasons for this, the principle cause was the difference between US and UK government behaviour. During the 1950s the US government directed around $400 million to IBM alone, principally in the form of research and development contracts. So, by 1964, the pre-war manufacturer of nineteenth century punched card Hollerith mechanical tabulators launched the new System 360; the product of some $5 billion of research and a construct that was to exercise definitional dominance over the remainder of the mainframe period.

By around 1966, IBM was able to devote more on research and development than the turnover of all of the UK computer companies combined. In the early 1960s the UK government was able to muster a mere £2 million to support the development of the Atlas scientific computer by Ferranti . IBM built 56 Semi-Automatic Ground Environment (SAGE) computers for the US missile air defence system from 1958 onwards; each at a cost of $18 million. Throughout the 1950s the SAGE project accounted for around 10% of IBM's gross revenue.

Despite the ever widening and deepening gulf of vision and funding capabilities between them, the UK and US governments constituted the dominant protagonists in the NATO alliance, the anchor points of the economically and culturally dominant Atlantic axis, and the powerhouses of the post war development of computers and computing. Across the span of the Cold War, US and UK government spending in general, and defence and intelligence spending in particular, dominated and shaped computers and computing. These governments spent according to their established patterns, within the dominant macro-economic structures of the age, and according to the imperatives of the Cold War.

In the macro-economic conditions of the middle decades of the twentieth century, assurance about the provenance and security of the supply chain were, by comparison with the challenges of the Information Age, relatively easy to obtain. This was a period in which the great companies of the age were characterised by a tight and deep vertical integration that has long since ceased to exist. Perhaps the most apposite example is that of the Lyons catering company.

The core business of Lyons was food and drink. They operated a chain of retail bakeries, restaurants and coffee shops alongside a broad portfolio of retail food brands. In accordance with the practices of the age, they secured their supply chain by owning it. Lyons tea was grown on their own plantation, processed in their own factories and then distributed to their own tea shops in their own fleet of trucks.
Facing rising costs and changing patterns of social and economic behaviour in the post war period, Lyons despatched two senior managers on a study trip to the US. Lyons had long been noted for its progressive and innovative management methods. Accordingly, the Lyons delegation found little of novelty or interest with respect to commercial practice. However, almost by accident and at the end of their trip, they encountered the early US work on computers. Returning home, their report convinced the Lyons' directors of the desirability of a computer as an integral element in the management of complex and time sensitive business processes. Accordingly, they built their own; almost entirely in house. In accordance with their own ethos and conformant to the business orthodoxies of the day, they assured and secured the supply chain by being it.

The Lyons Electronic Office (LEO) was the first commercial computer designed for business use in the world. Lyons outsourced computer services to, amongst others, Ford UK, Shell, Heinz, Dunlop and various UK defence and government agencies. It sold significant units of LEO computers to the UK postal service. Senior staff trained by Lyons were absorbed by many of their customers. Through a long process of mergers and acquisitions, the company created by Lyons to run their computer business was acquired by Fujitsu and continues to exist, in a form, as Fujitsu Services Limited. The methods and models developed by Lyons as they grew their own computer manufacturing and services business continue to find expression in the international standards systems and in the core practices of the IT systems integrators and service providers. Latter variants of LEO remained in service until the 1980s.

The business of computing followed the pattern of the age. The supply chain for computers was vertically integrated. Narrow, short and almost entirely knowable. Little of the work went beyond the commercial boundaries of the principal players and even when it did, it did not stray far. This sense of knowability extended even to the intellectual capital. The ideas driving the early developments in computing came from minds in academic and commercial research centres located almost without exception in the UK and the US. . The entire supply chain, should, and could, be mapped. Represented ontologically. From research and development, through to specification, implementation, testing, integration, operation and disposal; the system life cycle was predictable. The supply chain a part of the deterministic system as a whole. The idea of a complex matrix of volatile, recursive and nested sub contracts and outsourced obligations, if it occurred at all, would have been a nightmare of apocalyptic proportions
Across the supply chain, the mission of Cold War survival proved invaluable in invoking loyalty, preserving secrecy and driving creative endeavour. Business was done. Money changed hands and commerce occurred; so work and loyalty obtained financial reward. And, at the same time, there were the unifying imperatives of moral rectitude, the defence of freedom and existence. The supply chain became a cohesive community with badges of identification, signs of belonging and membership organisations through which those who belonged could confer and commune. Select individuals within companies and universities worked closely with government agencies and enjoyed considerable prestige, enhanced by more than a little mystique, as a consequence. The requirements placed on the supply chain were considerable, even onerous; the rewards generous.

Government drove technological innovation and entire technologies were created at their behest and for their exclusive use. Government paid the piper and called the tunes. By the last decades of the twentieth century, this situation had inverted. The major technology companies were setting commercial standards and pursuing commercial developments that governments were increasingly being compelled to accept. Costly aftermarket attempts to modify commercial off the shelf technologies through the agency of systems integrators and service providers did not meet with universal success. Accordingly, the situation is now such that even the largest and most critical of government requirements will deploy commercial technology. The GPS system is perhaps the least ever example of a major cyber technology developed initially for exclusive government use under government funded research and development. Governments no longer have either the monopoly or the control of technologies with the power to attain strategic military or societal effect.

The vertical integration of the sort practiced by Lyons, and across the military industrial complex of the Cold War has gone. Outsourcing, globalisation, just in time disciplines, the emergence of what were once developing economies as principal actors in shifting patterns of geo-political power, have all converged to produce a supply context of bewildering complexity. The supply cartography of our context is essentially unknowable, partly because of its intrinsic and accumulated complexity, and partly because of its volatility. Whereas the commercial relationships of the vertically integrated constructs of the Cold War prized stability and longevity, those of the Information Age thrive on velocity. In the Machine Age we etched company names in stone, inscribed job titles in brass plates and kiln fired enamel adverts with retail prices emblazoned in ceramic permanence. Now, our advertising hoardings are computer monitors; facets of the cyber phenomenon. Our Millennial staff enmeshed in patterns of loyalty utterly different to ours.

Computing as we think that we understand it is an agent and a function of the Cold War context, in all of its manifestations and across all of its facets. Both context and computing have vanished through transformation. Neither now exists. Our thinking and doing have yet to adapt.

Computing, as distinct to computers, is a socio-technical phenomenon. It is intrinsically located at the functional centre of the axis of the relationship between humans and information. This relationship is itself at the heart of our humanity and it is precisely this relationship that is being changed by cyber.

We are as, and what, we are because of our bipedal posture, our opposable thumbs and our capacity to store, accumulate, retrieve, process and communicate information. Our existence and development as a species is conditioned by, if not dependent upon, our capacity to meet the necessity of organising ourselves in to social groups wherein we simultaneously compete and co-operate. The very existence of our societies depends upon our faculties with information.

Computing is a tool born of our relationship with information and whereas it was once an artefact of war, it has now attained a societal significance. It has broken free of the control and ownership of the, largely, self-anointed experts. The entirety of the human condition as it now obtains depends utterly and completely on the operation of the vast ubiquitous and interconnected systems of computers upon which and within which the cyber phenomenon exists. Cyber is about far more than computers and computer networks, however vast, far reaching and powerful they are. It is about far more that the Internet; whether of information or of things. It is about far more even than the laggardly realisation that the great interconnectedness of everything encompasses ICS and SCADA systems and, therefore, the totality of the critical infrastructure of every nation on earth.

Humanity is existentially reliant upon cyber. Cyber is an utterly transformative phenomenon. In cyber the human and the machine are interlocked and interoperate each to recreate the other in a constant, amplifying and self-reciprocating matrix of incessant feedback. It is non-linear and non-deterministic. Cause and effect obtain, but are dislocated and disassociated in time and space. Neither are in any way susceptible to governance through the command and control discourse of the Machine Age and the Cold War. Cyber is a chaotic construct. Management through observation of apparent, and contingent, effect is the key to the safety of the human condition.

Cyber is about the ubiquity of the means of human communication. It is about three dimensional scanners and printers; means by which a corporeal object can be represented as binary, transmitted around the world at Internet speeds, and recreated at will. Such means are already producing replacement human body parts. The capacity to print electronic circuits has already moved to the brink of consumer availability, the capability to do likewise with lithium-ion batteries is next in line. Food replication is a realistic expectation. Three dimensional printing or micro fabrication will, within decades, destroy, disrupt and recreate entire swathes of economic activity; whilst creating entirely new ones. Our lack of understanding of the cyber supply chain is already scaring us and yet we only have a few years to wait until computers will be manufactured in homes around the globe as easily as we now print off airline boarding pass. We have only begun to experience the first tingling of what will become abject terror at the prospect of the impact on structures of warranty, indemnity and liability of a supply chain where spare and replacement parts for critical systems are locally fabricated using binaries downloaded from the Internet and so utterly devoid of provenance or attestations of fitness for purpose.

Our precepts of intellectual property assume that the intellect in question belongs to a human. The ability to address the problematic of the property rights of machines might seem to be somewhat beyond the capabilities of a legal system still unsure about how to deal with the impact of the Internet on the ancient system of trial by jury. Likewise, the question of the extension of the democratic franchise to non-human citizens appears intractable to a polity yet to enable Internet voting.

These new forms of manufacture represent one of the vectors through which cyber is transforming the primary economy; the economy of real things. And, simultaneously, cyber is morphing every other dimension of capitalism, including the nature of the means of exchange and the foundational dynamics of the access to capital itself. Bitcoin offers us the credible glimpse of a world in which the cyber domain has its own means of exchange; obviating the role of the nation state in the creation and management of the money supply. Crowdfunding is a now, more than nascent, alternative model of capitalism in which control of at least some of the means of production transfers from a minority elite to a cyber-enabled consensus through gestalt.

In the Machine Age we organised the entire economy, including clerical and ancillary functions, as well as the secondary and tertiary sectors, according to the logic and dynamic of the industrial model of mass production. Offices were fashioned as factories for knowledge workers. The human experience of information was industrialised. This experience was given structure, strata and hierarchies. New elites arose to manage, control and mediate access within the industrialisation of information. Factory style time disciplines were developed across the economy. The principles and practices of scientific management and of time and motion spread from the factory to the office to the shopping mall. Unities of time and place were imposed. Structures were formed with which humans conformed.

The cyber phenomenon is precisely the destruction of the artefacts of mind, matter and culture of the Machine Age. Cyber is indeterminate. It does not simply blur the lines between what we once thought of as real and virtual; it redefines that nature of these constructs entirely. The distinctions between the public self and the private self, between state and non-state actors, between human and machine are all subject to its creative destruction. Established elites are being deposed just as surely and inevitability as the hegemony of the Catholic priesthood fell under the onslaught of the Bible in the vernacular communicated via the mechanical printing press. New ones are forming and with them new patterns of social, political and economic power. The fabric of the social contract is being re-woven using cloth of a new sort.

We are anxious about the cyber supply chain. There are three established streams of our concern. The first, and most acute, is that we see the supply chain itself as a source of vulnerability and risk to the operation of the critical computer systems themselves. The whispered fear is that of malware lodged deep in silicon by a powerful nation state adversary. A legion of cyber sleepers invisibly infiltrated in to every one of the computing devices upon which we know we depend. The hidden menace. Living undetectably amongst us, silently

awaiting remote activation. Alien invaders capable of bringing about our total destruction. The second is that we see the supply chain as a vector for the execution of the intention of hostile actors such as criminals and intelligence agencies. Here the recent thefts from the Port of Antwerp stand as the exemplar. The third, and to us less significant fear, is the damage sustained if the supply chain itself ceased to operate and the supply of computing technology was threatened.

This last concern is the substantive fear to minds more attuned to the critical societal significance of informal computing than ours. We might usefully reflect on the absolute reliance of computing technology on scarce mineral deposits known collectively as rare earths. We might further usefully observe the equally rare deposits of these minerals and on the geographical location of such deposits.

In addition, there is now an emerging stream of concern about the vulnerability of the supply chain to infiltration by counterfeits and forgeries of the products of established and trusted brands. This will mature rapidly to reciprocate and magnify the first and foremost of our concerns.

Our anxiety is amplifying on a daily basis, edging us ever closer to the brink of a 'something must be done' response to a sense of impending crisis. We must now pause and ask ourselves this; to what extent and in what ways is this sense of crisis borne out by empirical evidence and cogent analysis? Or, from a different direction; to what extent is our sense of crisis the result of a panic reaction to a new context that we neither understand nor control? To what extent are we victims of future shock? Are we holding ourselves prisoner in Cold War bunkers of the mind?

There is no doubting either the complexity of our supply chains or the fact of the existence of manifest vulnerabilities. The physical fabric of computing, the very computers themselves, are artefacts of profound and increasing supply chain complexity. Supply chains are atomised, fragmented, volatile, unpredictable and unknowable. Key components are, and will continue to be, designed and manufactured across the globe. And so in areas where those with hostile intentions towards the continued existence of liberal democracies can operate with greater tolerance and latitude then would be possible in the established heartlands of these democracies. The location of the episode of the assembly of the components in to a finished market ready device, is in terms of the assurance of the supply chain, irrelevant. Assurance models predicated on the susceptibility of devices, let alone systems, to code or component level recursive analysis are, at best, redundant.

However, the existence of vulnerability does not in and of itself constitute a risk. For risk to obtain there must be commensurate threat and for a threat to obtain there must be a combination of both intent and capability. Moreover, even if risk were to obtain, the impact of its realisation is relative and contingent. Therefore the application of counter measures and mitigations must be similarly so.

Assertions of the abstract fact of the existence of vulnerability devoid of context, data, or substantive rational argument, are as useless in generating meaningful utility as they are attractive to those with something to sell. Even in the most benign of circumstances they are an insufficient basis for action. In times of limited resources they can easily become the cause of costly and unproductive failures. When the subject of concern is itself a societally critical phenomenon then the raising of defences that will inevitably reduce the beneficial effects of the thing being protected should only occur after thorough analysis. To destroy a thing in order to protect a thing is an unacceptable price to pay when we depend upon that which we defend for our very existence.

As I write this, the UK Prime Minister has just returned from leading a large delegation of senior business leaders on a trade mission to China. He returned for the debate in Parliament on his coalition government's Autumn Statement; the mid-year finance bill. Whilst in China, the Prime Minister faced down criticisms that he was sacrificing a commitment to human rights with the counter that he was "unapologetic" about his emphasis on the economy. Britain, he observed, is a "trading nation ", and as such whilst "some in Europe and elsewhere see the world changing and want to shut China off behind a bamboo curtain of trade barriers. Britain wants to tear those trade barriers down ". During his trip, the Prime Minister pressed the Chinese authorities openly for a "proper cyber dialogue" whilst at the same time choosing to highlight that "we need … to up our investment in cyber security and cyber defence" because "there is an enormous amount of work to be done ". The "Global Times", a nationalist leaning tabloid owned by the Communist party ran an editorial arguing that "the Cameron administration should acknowledge that the UK is not a big power in the eyes of the Chinese. It is just an old European country apt for travels and study ".

The same newspapers that carried the stories of the UK delegation to China also carried reports of Amazon's plans to use aerial drones to deliver packages directly to customer's homes. The cries of 'impossible' and 'unsafe' fading out of earshot as the whir of driverless electric cars whispers in across the horizon and the march of fully autonomous weapons systems shakes the ground deep beneath our feet. Where Amazon sees parcels, others see Semtex.

These stories encapsulate much of the difficult realities of our age. David Cameron travels to China to bid for business. China needs access to the economies of Europe and America if it is to continue to grow just as it holds the old world in aloof contempt. David Cameron returns to the UK for a debate on a bill that legislates for further austerity in order to counter the effects of a financial crisis precipitated by a failure of the US and UK banking systems. The financial crisis itself revealing that a longer term strategic shift in the axis of geo-political and macro-economic power had been underway for many decades; masked latterly by a credit fuelled boom in consumer spending. Chinese concerns continue to invest heavily in overseas infrastructure of every sort; including the next generation of the UK's nuclear power stations and the new high speed train system. The Internet would simply not exist without equipment of Chinese manufacture.

China and the world of which it is a part are locked together in indivisible interdependency. The rise of a middle class has been both predicate and a consequence of the Chinese economic miracle. The Chinese middle class enjoy less direct political and societal power and influence than their equivalents in the liberal democratic heartlands. The key to the continued, relative, quiescence of the Chinese middle class is sustained and substantial economic growth. Affluence a necessary palliative to the frustrations of political impotence and essential to the deflection of the middle class from the leadership of populist protests. History teaches that an alienated and disenfranchised middle class make formidable leaders of those similarly alienated and disenfranchised elsewhere across society and that the exercise of such leadership is far more likely during periods of extended economic contraction. The political leadership of China has no rational interest in crippling or even seriously degrading the economies of the world upon which it depends for its very survival.

There is however, no singularity called China any more than there is a singularity called the United Kingdom or the United States of America. Nation states are shifting amalgams of conflicting and competing interests, with complex and contested histories, and uncertain and indeterminate futures. If there is a certainty here it is that China will increasingly seek to exert overt geo-political power commensurate with its economic might, with an inevitability echoing the behaviours of the UK and the USA in the eighteenth and nineteenth centuries. We can no more prevent this than could the beneficiaries of Pax Britannica or Pax Americana. We can only compete and defend against the inevitable with all the means at our disposal.

There is no doubt that bad things are happening. There is no doubt that they will continue to happen. Individuals, companies, social constructs and nations compete; using any and all means at their disposal. We need to gather more evidence than we currently possess about the nature of these bad things as they are manifest in the cyber domain. We must quantify and analyse data exfiltration rather than simply assert its, undoubted, existence. We must contextualise our analysis and root it in the reality of the world as it is, rather than the world we once knew. We must learn a far more nuanced way of thinking and a far more agile and responsive way of acting. We must relinquish the use of two dimensional categories such as 'User', and 'State', and 'Non State'. They conceal more than they reveal; expose more than they protect.

In a tiny number of cases it will be appropriate and necessary to entirely internalise the cyber supply chain. To design and manufacture the very silicon wafers themselves and assemble the finished computing devices under the tightest controls possible. To render every aspect of the process the subject of full disclosure and trusted hands. The costs of this, in every sense, will be astronomical; unsustainable beyond the tiny portion of the overall requirement for which they will be essential. System capability will be degraded, agility will be compromised, and any notion of a financially prudent return on investment will be laughable. Such efforts, necessary though they will be, must be confined to the absolute minimum. Any attempt to generalise such extreme remedial counter measures as a response to the great supply chain fear would represent an attempt at economic autarky. History repeatedly teaches that attempts to pursue such a strategy as anything other than a narrow and exceptional response to extreme conditions is doomed to fail, often precipitating crisis worse than that which it sought to avoid. Lessons that Kim Jong-un would do well to re-visit as he continues the practice of the Juche ideas he inherited from his father.

We must relinquish the legacy of the deterministic systems thinking that won us the Cold War and embrace instead the more subtle and less certain arts of the management of complex systems through the observation of effects and the generation of perpetual feedback cycles. We must actively enable the core structures of our systems to depend upon continuous modification of their own states. At the root of our fears about the vulnerabilities of the supply chain specifically, and of cyber more generally, is the apprehension that our adversaries have proven better able to exploit the true form of cyber than we have, and even less comfortably, the darker fear that the deep cause of our failure to counter the success of our adversaries is us.

We ensure our capacity to mount military operations regardless of climate and terrain through enabling our systems, including their human components, to adapt and improvise. We assume the existence of environmental hazards and hostile actors. We fashion protective mechanisms that absorb and deflect blast energy. We combat armour piercing ordinance by exploiting and manipulating its own sophistication. We forecast the weather; we do not seek to render it subject to linear command and control disciplines. Soldiers carry waterproof clothing, they do not give orders to clouds. The judgement of history is harsh against generals who command their armies to invade Russia in the summer and forbid them winter clothing because rapid victory is assured and carrying an overcoat is tantamount to defeatism. We use the indeterminacy and nuances of the human condition to practice the complex craft of intelligence. We disrupt, and conceal, and deceive, as much as we shoot. As a matter of course, we assume that our adversaries will extract optimum advantage from every opportunity and we prepare and equip accordingly. We anticipate that enemy combatants will prosecute their aims with every means at their disposal.

The systems of the cyber domain are unimaginably complex and inextricably interconnected. Every nation, every society, every institution of the state, every individual, our entire global civilization, depends upon this new phenomenon. Thus arise a paradox deep at the heart of our primal fears about the security of the cyber supply chain. Given precisely this complexity, and interconnectedness, and existential dependence; then, if the core silicon is infected, the execution of the attack will destroy those who perpetrated the atrocity just as surely as it destroys those against whom it was aimed. Because of the atomised, fragmented and volatile nature of the modern supply chain, it is in principle possible to plant a latent attack capability at such a low level within systems that detection is indeed impossible. However, the execution of such an attack is, literally, a zero sum game. Or perhaps more accurately; an extinction level event.

The chaos of our cyber systems is a function of their complexity. Both complexity and chaos are at the heart of the transformative and empowering qualities of the cyber phenomenon. We must emerge from our deep state of shock

very power we have come to fear. Cyber is a transformation in human affairs of at least equal significance to that of the Neolithic Revolution, the Reformation, the Enlightenment and the Industrial Revolution; combined. To the extent that the computer systems upon and within which cyber exists were once ours; they are no longer so. Cyber belongs to society. Cyber is society. Our job is now to enable and empower the evolution of society through the development of a safer human experience of cyber. Victory in the Cold War was a beginning; not an end.