SOCIAL CYBER INSTITUTE

Research Paper #1

CREATING SOCIAL CYBER VALUE

Greg Austin and Glenn Withers

OCTOBER 2019

SOCIAL CYBER INSTITUTE

Research Paper #1

CREATING SOCIAL CYBER VALUE

Greg Austin and Glenn Withers

October 2019

ABSTRACT

All security outcomes in cyberspace are determined by individual people, whose behaviour is shaped by their social setting, either organisational or cultural. Yet there has been little evidence globally of the necessary adjustment of policy or practice that gives due weight to the social science dimensions. There is a sharp imbalance between investments in technology for security in cyber space as against social science at almost every level: national government, business enterprise or academia.

This shortcoming is compounded by three others of equal or greater importance. First, the further socio-technical threat of unintended system failures, which may be dubbed "cyber incompetence", is also largely unstudied outside the technical realm. Yet it may be even more costly and far more common than the more prominent concern for addressing cyber-attacks. Second, decisions for digital transformation in all organisations can undermine or enhance security, and are in turn impacted by the competence levels of the decision-makers. Third, the susceptibility of leaders, managers and users to be swayed by disinformation generated by the media or even vendors in fast-moving situations is an equally important threat to business and security.

We see these four problem sets as inextricably linked, and argue that we can only analyse any one of them by reference to the idea of the "social cyber ecosystem" in which they all exist. It is their interaction in the shared ecosystem that determines all security and welfare outcomes dependent on cyber space.

We argue for the centrality of social science in cyber space management at all levels of national policy, enterprise development and human welfare. We introduce a novel concept to help achieve this reorientation: "creating social cyber value". This refers to optimised information ecosystem performance: maximizing benefit while minimising insecurity and incompetence. Moreover, it argues that this can only be attained when the human use and misuse of relevant technology is recognised as central.

The new spirit might be based on the conviction that a social retooling at a system level is not only feasible but a social imperative and moral duty. The benefit of addressing social cyber system value in this proposed comprehensive fashion (insecurity, incompetence, digital transformation, disinformation threats) is that it creates the conditions for the appropriate reflection on important new ethical questions (especially privacy but also worker values) that are raised afresh in the information age. The paper imagines how a process of radical adjustment to the social and systemic influences of security in cyber space might be undertaken to deliver more viable social cyber ecosystems that can match the escalating novel threats, while exploiting more effectively untapped potential of the technology-driven information revolution, still in its early stages.

Table of Contents

Introduction

It is suggested in this paper that that social science should be a central foundation for managing the key driver technologies of cyberspace. It is also argued that this gives rise to a massive research agenda, in both scope and scale, and that the associated emergence of social cyber science is both necessary and desirable.

The need for new social science approaches to modern cyberspace problems has been confirmed in a recent report of the U.S. National Academies on social science and national intelligence (National Academies 2019). The report includes a key chapter on "social cyber security" and distinguishes it from engineering and computer science approaches that consider social science at the margins only and not as an equal centrepiece of analysis.

To ground this argument, consider the following examples of "Five I" problems in cyber that a social science perspective can help mitigate:

- Cyber **insecurity**: as documented by Greenberg (2017), one random cyber-attack caused one company to lose US$340 million. Known losses across all companies from the same attack, NotPetya, reached a total of US$10 billion.
- Cyber **incompetence**: an Australian government agency, AUSTRAC, imposed a fine of US$500 million[1] on the Commonwealth Bank of Australia for its failure to monitor possible money laundering through its Intelligent Deposit Machines (Austrac 2018).
- Cyber **intransigence**: the estimated loss from slow digital transformation and slow uptake of related technologies is estimated for the case of Australia to be $37 bn[2] over a decade (PWC 2014: 2).
- Cyber **ignorance**: S&P stocks fell on Wall Street by US$136.5 billion in six minutes in response to a mistaken claim on twitter that there had been an attack on President Obama in the White House (CNBC 2013).
- Cyber **insensitivity**: Facebook saw its share value drop by 44 per cent in 2018 and 2019 as it struggled to meet reshaped global expectations for privacy and security. By July 2019, Facebook was forced to pay a fine of $5 billion for its errors and omissions in cyber space (Brody and McLaughlin 2019).

From these case illustrations we can see, anecdotally, the need for new approaches for each of the following five problem sets made prominent by the cyber era: maximizing security in cyber space, minimising incompetence in digital choices, avoiding technological lock-in, defending against information uncertainty, and creating solid ethical foundations for navigating the information revolution.

It is the contention of this paper that there may be substantial benefit in an overarching approach that treats the five problem sets as unified, in the sense of their all deriving from inadequate understanding of the human factors in cyberspace. If this is correct, an approach that adds the social to the technical could optimise financial outcomes in big business, and community outcomes in non-profits, as well as policy outcomes for government. The proposed approach is to manage them all through the concept of the social cyber ecosystem.

The key foundation feature of the ecosystem that cuts across the five problem sets is perceiving the human component operating through the lens of human capital and its capacity to generate social cyber value.

Currently, the world faces a severe and worsening shortage in many aspects of workforce development for information technology, to the extent that the US President has declared an arms race in cyberspace human capital dimensions (Austin 2019: 34). In China's case alone, by 2020, this shortage—just in the field of cyber security—is estimated to reach 1.4 million cyber security posts for which suitably trained applicants are not available (Austin 2018: 34). In a situation of shortage of appropriately trained people, an increased percentage of people will be promoted to sensitive jobs that are beyond individual competence levels unless specific steps are taken in anticipation to compensate for gaps in individual knowledge and skills through building an appropriate human ecosystem of talent. To that can be added an appreciation of also building trust and ethical behaviour within organisational cyber communities to maximise the positive human benefit.

[1] Exchange rate as of the date of the announcement.

[2] Exchange rate as of 30 June 2014.

A mature and comprehensive information ecosystem approach

The concept of information ecosystem was usefully defined in a paper for the Institute of Electrical and Electronic Engineers (2013) as follows:

A digital ecosystem is defined as an open, loosely coupled, demand-driven, domain clustered, agent-based, self-organised environment where species/agents form short and long-term coalitions for specific purposes or goals, and everyone is proactive and responsive for its own benefit or profit. Interactions among peers in Digital Ecosystems may involve, besides unbridled competition, new modalities of pre-competitive and collaborative partnerships. Digital ecosystems are characterised by complexity – demanding radically new solutions (Guetl, Ismail and Lexar 2013).

What is notable in this definition coming from an engineering professional association is how much the fourteen separate descriptor terms of a digital ecosystem so specified (such as loosely coupled, unbridled competition, collaborative partnerships to name just three) already represent highly complex social phenomena, and not just technical ones.

The recent further evolution of this holistic information ecosystem approach can be tracked through key contributions. See Wang et al (2017) for a literature survey:

- Yurcik and Doss (2002) provide an early recognition of the value of an ecosystem approach (entirely technical rather than socio-technical) for the value of security. Their approach is predominantly technical rather than socio-technical, but they recognise that "over-reliance on protection solutions for system components at a singular layer" contributes the fragility of information systems when viewed as a whole. For example, the use of authentication and encryption "may actually add more vulnerabilities to the system as a whole than they eliminate".
- Schwartz (1999, 2002) at the same time proposes the idea of digital Darwinism for evolution of such systems with adaptable businesses being the vehicle for advance along with new technology, a conception furthered by Walton (2015). Walton concludes however that the "realities of information exchange" are being transformed more quickly than the "conventions of exchange" are able to adapt
- Floridi (2002) extends the introduction of such social phenomenon into these ecosytems by also investigating the moral philosophy of these developments in the digital age.
- Arina (2009), building on Iansiti and Levin (2004), identified several species of information actors in contestation, with some exploiting the new environment and others enhancing their society with the balance determining advance or detriment.
- Masys (2014) observed correctly that resilience is as important as security and that "this does not reside purely in cyber security patches and technical solutions but requires a more comprehensive and collaborative approach that embraces the social, organizational, economic, political and technical domains."
- Kovacs et al (2017:5) suggested that there is a need for "new approaches for exploring technology and society relationships" and that the "pervasive ICT ecosystem shapes interactions and relationships between humans and technology on different levels"
- Richards et al (2008) developed similar ideas for technical architecture of space systems, where risk aversion is high because of cost penalties, They propose five design principles as listed in Table 1 to correct five major flaws in contemporary approaches, notably including recognising that "architecting for survivability is a poorly understood, socio-technical issue".

Scholars, therefore, have a clear focus on how complex systems evolve under the influence of technological development and stakeholder actions, but there is equally a clear consensus that these influences should be further defined, refined and elaborated.

The socio-technical aspects: how visible is social science?

The socio-technical character of cyber security and the importance of associated analysis is now clear. There has been growing recognition of how vast, complex and deceptively (un)manageable the social dimensions have become. What is less clear is what this involves and how it should proceed.

Table 1: Design Principles for Space System Survivability

Corrective Design Principles	To Fix Contemporary Design Flaws
Incorporate survivability as an active trade in the design process	Treatment of survivability as a constraint
Capture the dynamics of operational environments over the entire lifecycle of systems	Static threat reports (selected operational scenarios are not likely to truly represent future conflicts," "unanticipated technological developments will affect combat operations," and "adversaries in real conflicts will adapt to our capabilities in unanticipated ways" (citing Anderson and Williamsen 2007)
Capture path dependencies of system susceptibility and vulnerability to disturbances	Assumption of independent disturbance encounters: "Perrow (1999) finds that failures may also arise from unanticipated, dysfunctional interactions among components and then subsequently be exacerbated by the rapid propagation of local failures due to tight coupling in complex systems."
Extend the scope of architecture-level survivability assessments	Narrow scope of survivability design and analysis ("tremendous amount of progress has been made to improve the survivability of individual elements in aerospace system architecture (Nordin and Kong 1999; Paterson 1999). Less progress has been made at the architecture-level where systems tend to evolve in an ad-hoc manner—accommodating constraints from legacy systems and forming temporary coalitions to support emergent missions. More generally, architecting for survivability is a poorly understood, socio-technical issue"
Take a value-centric perspective to allow alternative value-delivery mechanisms	Lack of a value-centric perspective. "Success of a system is dependent on how much value it is perceived to deliver to its stakeholders" but stakeholders have to document the value proposition.

Conceptually, rational knowledge is created through logic and evidence, as opposed to intuition and experience. Such rational knowledge is what formal research pursues and formal education conveys–in both cases in open, transparent, accessible, systemic documented form. The documentation is the foundation of sharing the knowledge. The social mechanisms of disseminating knowledge have become profoundly disturbed by the information age.

Where the knowledge is focused on the natural and physical world it is seen as science, technology, engineering and mathematics (STEM) knowledge. Where the knowledge relates to human behaviour and interaction, whether individually or through community and cultural, business, economic or political and governmental collectivity, it is seen as humanities, arts, and social science (HASS) knowledge.

For the cyber world, understanding the imminent social complexities identified above as crucial is made more difficult by the persistent dominance of technical practitioners of cyber security within the policy and research domains. This is understandable as the issues first required physical world insight to be developed and, while social implications still follow inexorably, codified social science knowledge of that has yet to catch up to and inform the technology imperatives.

At the most simple level, in spite of thousands of scholarly research articles over more than two decades, we arrived at the point in 2018 where three UK specialists concluded that "industry, policymakers, law enforcement, public and private sector organizations are yet to realise the impact individual cyber behaviour has on security" (Benson, McAlaney and Baranowski 2018:1). They called for recognition that "cybersecurity is inherently a complex socio-technical system". With a focus on behavioural psychology, they advocated especially for new work practices that reflect research on workplace behaviour of individuals (p.5). This is perhaps the best recognised social consideration. The individual human is however, as indicated above, only part of the picture.

There are institutional factors as well. Given the business imperative to capitalise on the new technology, it has been natural to look to the structure and practices of organisations as a starting point for moving beyond individual behaviour, abstracted from social context. As three American scholars found a little earlier in 2017: "Contrary to our theorizing, the use of more IT security is not directly responsible for reducing breaches, but instead, institutional factors create the conditions under which IT security investments can be more effective". They went on to say that the implications of their results "are significant for policy and practice", particularly the "discovery that firms need to consider how adoption is influenced by institutional factors and how this should be balanced with technological solutions" (Angst, Block, D'Arcy and Kelley 2017: 893). Other researchers have travelled the same terrain (Kraemer, Carayon and Clem 2009, Tang and Zhang 2016). On the other hand, ecosystem factors such as legal regulation can have negative impacts on cyber security (Clark-Ginsberg and Slayton 2018).

A series of studies take this further and look at the linkages between IT governance, risk management and information security (De Smet and Mayer 2016). They concluded that more research would be needed to "define how to well integrate security and risk management in the IT governance framework" and they suggested sector-based approaches in research on IT governance to take better account of the unique context of different organisations.

Beyond organisational factors, there is less research. But an emergent literature is to be found on questions of cyber security as a complex social system (Salasin 1976, Courtney et al 2009, Rebovich 2010, Baskerville 1996). There is also work on the impact of complex social systems in turn on broader resilience questions for other relevant domains, such as Bellavita (2006) for general homeland defence missions; Lafond and DuCharme (2011) and Dmitrova (2017) for general security policy; Clarke et al (2016) on environmental security.

The research is embracing further issues of path dependence and complex dependencies and recognizing these as new even more complex problems (Kovács et al 2017). Here social science moves beyond the individualism or organisation analysis common in behavioural social science and management, through to the aggregations often used in social science areas such as sociology, economics and political science and to the evaluative questions posed by ethics.

Researchers at Carnegie Mellon University saw "social cyber security" at present as self-limiting to political or cultural manipulation of victims (Carley et al 2018:389). They, therefore, proposed moving beyond this by seeing the field as multi-disciplinary, carving out a new field that mirrors the term "socio-technical". They see social cyber-security as a "computational social science" which they say is "noticeably distinct from a pure computer science approach or a pure social science approach". The methods and theories being developed: (a) take the socio-political context into account methodologically and empirically; (b) are predicated on issues of influence, persuasion, manipulation, and theories that link human behavior to behavior in the cyber-mediated environment; and (c) are focused on operational utility rather than just improving scores for machine learning algorithms or theory testing" (390).

The focus of this approach is to address negative impacts on security through malign influence or manipulation, and it does not appear to extend to the concept of second or third order effects of cyber security practices back inside the broader information ecosystems of organisations, communities or countries from the perspective of IT governance outside security or digital transformation in the broad. Even so, within the narrower remit they observe that "new research is needed in many areas", and they single out "bias estimation and reduction in data; movement of actors and ideas within and between media; semi-automated identification, assessment of impact of, and effectiveness of counter-messaging" (Carley et al: 393). In the longer run, the concept can also turn to emphasise methods of analysis for focus on enhanced use of cyber, not only in relation to security but in positive use of the technology in general for organisational and social advance.

Such new interest in the social dimensions of cyber security can be discerned in the emergence of the term “social cyber physical”. But there is a long way to go before this displays mainstream acceptance. The Scopus database records the first entry for that term in 2003, and five for 2018 at the date of search.[3] Of these only two distinct articles mention the term “cyber ecosystem”. For the search term “cyber social” as keyword in the Abstract, Scopus records 67 articles, with the first in 2003, and eight for 2018 at the date of search. Of these only three mention the word ecosystem. The SSRN database returns zero articles showing “social cyber” as in “abstract, title and keywords”, and only two that reflect the term “cyber ecosystem”.[4] Some sixteen articles reflect the search terms “cyber” AND “ecosystem”. Of the items identified by the above searches, there were three that touch on aspects relevant to this paper.

Zeng et al (2016) observed correctly therefore that studies of cyber physical social systems “are still at their infancy, most recent studies are application-specific and lack systematic design methodology”.

Trautman’s quite short paper (2017) goes to a foundational problem (a departure point) in developing research on social cyber security. Having observed the complexity of the cyber security problem for many of the social and organisational factors mentioned already, he notes the lack of a common discourse among key stakeholders (business, government and individuals). He suggests that over time, group dynamics have produced disincentives for more rational approaches and even working against candor in discussion of problems between various groups. He suggests (1) that “navigating the cyber ecosystem and structuring effective solutions to the cyber problem will require recognizing and overcoming difficult truths about organizational and human behavior”.

It will also need to recognise and overcome difficult truths about research methodology. Scholars are rooted in disciplinary specialisation. This has indeed been a productive engine for insight. It allows deep insight through understood shared and well-defined specialist concepts and methods. But problems of interest to decision-makers and stakeholders beyond the Academy are often searching for integrated or holistic insight.

The current state of play was foreshadowed in a 2013 analysis of the state of cyber security research. In a long list of under-researched areas, the last mentioned was the social aspect. Referring to a paper on “Reducing Systemic Cybersecurity Risk” by Sommer and Brown (2011) prepared for the OECD project on global economic shock, the authors (Craygen, Walsh and White 2013:14) suggest that “research responses should adopt a cross-disciplinary approach that combines “hard computer science” with the need to understand social science dimensions because “information system security are achieved only by a fusion of technology and the ways in which people and organizations actually try to deploy them”.

One of the best guides to this nascent but emerging field of social cyber research is a report from the U.S. National Academies (2019) on strengthening the role of social and behavioral sciences in intelligence analysis. Using the term, “social cybersecurity science”, and using a somewhat forced and limiting definition of the emerging field, it says that it emerged to serve two primary objectives (cited verbatim):

- “characterize, understand, and forecast cyber-mediated changes in human behavior and in social, cultural, and political outcomes; and
- build a social cyber infrastructure that will allow the essential character of a society to persist in a cyber-mediated information environment that is characterized by changing conditions, actual or imminent social cyberthreats, and cyber-mediated threats”.

The report distinguishes between cybersecurity dominated by engineering perspectives that can take account of social science considerations and social cybersecurity, where the researchers are linked by their commitment to:

- “take the sociopolitical context of cyber activity into account both methodologically and empirically;
- integrate theory and research on influence, persuasion, and manipulation with study of human behavior in the cyber-mediated environment; and
- focus on identifying operationally useful applications of their research.”

There is a useful summary assessment of the interactions between social cybersecurity and other disciplines. Box 1 lists the main findings and

[3] As of 2 December 2018.

[4] As of 2 December 2018.

proposed research directions for this field as defined by the report. The report is valuable for its scoping analysis but is limited by its narrow focus on national security intelligence analysis and its bias toward understanding the impacts of potential human machine interaction in that field. Wider social science in law, ethics, economics, management, politics and community awaits like examination.

Thus, while social considerations are certainly increasingly evident in modern approaches to cyber security, they have rarely been analysed as part of a complex socio-technical system. The preference has been either to see the people problem as distinguishable and separated from the technical challenges; or in the cases of some research, to see the human as an extension of the machine. Prevailing approaches include security vetting of personnel or subsequent monitoring of them, and courses in basic cyber hygiene (especially phishing and password control). There has been little exploration of incentive-based approaches to cyber security and cyber competence, or the construction of new cyber ecosystems. The idea of linking IT governance and digital transformation to the security challenge has not been researched widely, and nor has the impact of cyber incompetence as a broader social phenomenon independently of the specific cases referenced in the first pages of this paper.

What is needed is a more conscious and systematic cyber eco-system approach just as outlined conceptually in Figure 1 for optimizing social cyber value, but drawing on the full range of social science disciplines seen as basic to achieving a full system integration approach;

- individualist theory foundations: behavioral psychology, organisational analysis
- quantitative data interpretation: statistical and computational analysis including for big data
- institutional aggregation: political, economic, social and cultural modes of analysis
- ethical and value interrogation: philosophy

These are applied to the activities being generated by science, technology, engineering, and mathematics disciplines as they too come together to generate the new cyber universe. Appendices A and B show how these component areas can contribute currently to the wider social cyber system concept, for the contributing disciplines of economics and ethics, respectively.

Inter-disciplinarity and integrating social science influence

There is as yet no accepted meta-discipline of interdisciplinarity. The intellectual challenge of defining the standards and methods of excellence for such work is evolving.

In 2015, Australia's Council of Learned Academies (ACOLA) sought to pursue a multi-disciplinary analysis of the closely related issues around innovation. This took a wide definition of relevant disciplines across each of the natural and physical sciences, engineering and technology, social sciences and humanities, and sought to use that approach to analyse the impact of technological lock-in on that country's innovation (Williams et al 2015).

This "lock-in" phenomenon might offer some explanation for lack of progress globally toward more comprehensive and up to date policies for cyber security. One need cite only the persistence of the highly insecure Microsoft Windows as an acceptable operating platform. But the challenge is not confined to the technologies. As Gaycken and Austin (2014) observed, that software system represents an inherently insecure technology (tens of millions of lines of code that require regular patching to prevent major security breaches) yet the market dominance of such systems effectively prevents or delays the advent of "highly secure computing".

The bigger challenge still arises from the social foundations of the inertia. Referencing Leo Marx (1999), the Australian study calls these foundations a "socio-technical complex", a system that "consists of manufacturers, developers, businesses, industry and users, and includes cultures of manufacture, regulation, and the networked and interlinked technologies and infrastructure" (Williams et al 2015). Referring to "sunk costs and vested interests", the report (24) sees these as barriers to change "even when there would be clear benefits" from it.

The summary of how "lock-in" occurs that is offered in the report is highly relevant to understanding of the current dominance of the "technological" approach to cyber security. It says:

> "Once a market is established, institutions such as technical and professional associations often emerge as gatekeepers

Box 1: Main Findings on Social Cybersecurity in U.S. National Academies Report

Conclusions 6.1 and 6.2 call for:

- A comprehensive multi-disciplinary research strategy for the study of social cyber attacks
- Scientific methods for assessing bias in online data
- New computational social science methods for monitoring social networks and narratives
- Operational computational social science theories of influence and manipulation in cyber-mediated environment.

The chapter has seven specific proposed lines of future research:

1. Continue work on developing better theories and methods for identifying perpetrators of cyberattacks.
2. Conduct interdisciplinary research to develop computational models and theories about information manoeuvres in cyberspace and the respective strategies of influence and manipulation.
3. Conduct research to develop techniques and tools with the capabilities to determine automatically and rapidly the intent of those conducting social cybersecurity information manoeuvres.
4. Conduct research to develop multimedia diffusion theories and a better understanding of the co-movement of people and ideas through cyberspace.
5. Develop methods for measuring the impact of an information campaign, in both the short and long terms.
6. Better characterize those groups at risk of social cyberattacks, and identify ways to increase awareness of malicious information manoeuvres and strengthen the resistance of at-risk topic-groups to such attacks.
7. Support the design of countermessaging strategies in cyberspace.

> between end-users and individual professionals. Voluntary associations such as social automobile clubs, unions, industry associations or media channels such as magazines or electronic social media sites can act as non-market (i.e. social, cultural or governance) forces of "lock-in". Emergent technologies can also create brand new academic disciplines which are then absorbed into research and teaching institutions. Social norms play a part in 'lock-in' when people can become locked into new social practices associated with the uses of technologies." (25)

The report mentions an important set of break-out measures to overcome technological "lock-in" (25):

> "Lock-in created by technological inertia and vested interests means that a substantial technical performance improvement is often needed in order to induce a transition from a widely adopted technology to a new technology. Such substantial improvements often come from niche and entrepreneurial entrants to the market. To achieve structural change, policy must support the growth of new technologies and industries. Legislation can help to create niche markets, and if there is variety in the niche markets created then technical advances are more to likely occur".

The report later addressed the specific case of Australia, calling out a list of 11 factors that were likely to shape Australia's response to advanced technology (31-32). See Box 2. At least five of these have sharp resonance for the discussion in this paper. They will be revisited later in this paper.

The proposition that the cyber security scene globally is dominated by some sort of technological lock-in would seem to be confounded by the vast creativity and invention we see in the sector. But it is possible to see even the creativity as bounded by a preference for technological solutions to security in cyber space. There is little evidence globally of the necessary adjustment of policy at national, enterprise or community level that gives due weight to the reality that cyber security is a socio-technical phenomenon. This is evidenced by the sharp imbalance between investments in technology as against social science at almost every level where prosperity and security are affected by cyber space.

The potential scope of social cyber research was flagged quite comprehensively if indirectly in the report by the Australian Council of Learned Academies just mentioned (William et al 2015: 31-32), and as reproduced in Box 2. That is a fairly traditional set of social science topics. An agenda laid out in the National Academies (2019) report, and referred to above in Box 1, is more ambitious because it takes account both of the revolutionary changes in social cyber ecosystems under the influence of technology and, at the same time, of the new and unrealised potential of the same technologies to better study (and document) the novel social interactions catalysed by them.

Box 2: One Set of Agenda Items for Social Cyber Research

Attitudes to changing technology and practices
• Model best practice in organisational and workforce change, taking into consideration how new technology will require new roles, work patterns, modes of communication, reward systems, leadership models and workplace training. • Mitigate against negative attitudes to new technology in general by ensuring that there are effective retraining schemes and social safety nets for affected workers.

Approach to risk and failure
• Through education, vocational training and lifelong learning, develop a business/industry/national culture that accepts the uncertainty and failure inherent in innovation. Train people to experiment, and how to learn from (and benefit from) failure. • Recognise there is also risk in maintaining status quo, and not adopting new technologies. • Experiment with multiple technological options for a given problem, recognising that it is unlikely there is only one solution

Skills
• Recognise advanced skills are needed to make use of a new technology effectively, as well as for its invention and creation. • Influence training and education schemes to encourage flexibility, creativity and the ability to try new things. • Minimise constraints on worker mobility e.g. stringent visa rules. • Ensure training content is sufficiently generic to enable workers to adapt to the evolving job requirements imposed by new technologies, rather than highly specific content that is focused on existing technologies employed in past and present jobs

Open data
• Ensure data that is owned by the government, or that the government is a custodian of, is made freely available and shared by default.

Privacy and security
• Impediments to adopting wireless and cloud technologies in many businesses include security and privacy concerns. This is particularly important in industries such as healthcare where high security standards need to be achieved to ensure patient confidentiality”.

Social Cyber Value: A new concept

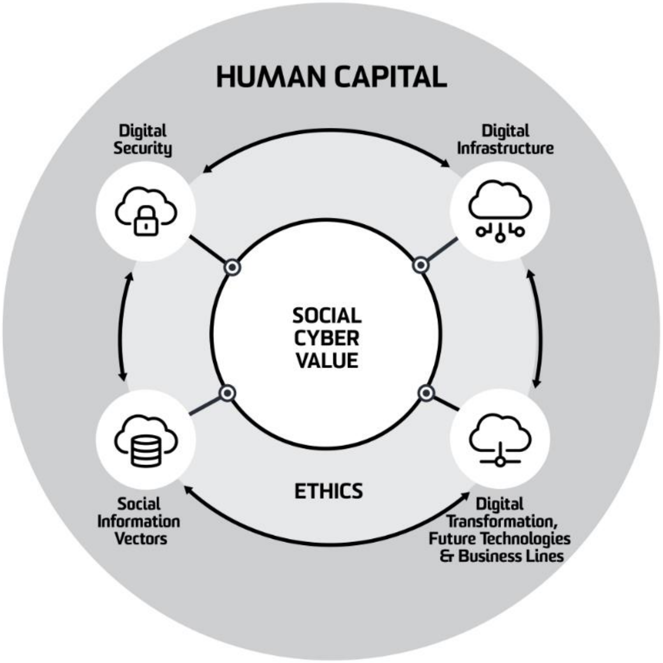
This paper proposes that such social science inputs can be achieved by focusing on optimised information ecosystem value derived from a more comprehensive accounting of the interaction between technical, social, political and ethical realities inside and outside the corporate entities (in business, government or community). We call this "social cyber value".

The departure point for this concept was cyber security. But the stream of research in recent times just outlined leads us to see the problem as lying well beyond the traditional positioning of cyber security as a separate domain of largely defensive activity led by a class of technically qualified "cyber guardians".

Rather, we conclude, as some in business and government already have, that a preferred approach is a broader one. In the same way that national security depends on deeper social and economic realities of a country, so too security in cyber space, either for a large corporatised entity or a country, depends on harmonisation of the social, ethical and economic aspects of cyber space with the technical. The arrival point therefore is one of optimizing full social cyber system value.

The concept of social cyber value that results is represented graphically in Figure 1. It proposes an integration of management of four pillars of business activity: cyber security, digital infrastructure management, strategies for digital transformation (business processes), and human resources (a function which has to become human resources for digital life as well as digital competency). Underpinning the proposed new interaction between all of these four pillars is the consideration of ethics underpinning the social and political values of the enterprise.

Figure 1: Information Ecosystem Optimised for Social Cyber Value


HUMAN CAPITAL
Digital Security
Digital Infrastructure
SOCIAL CYBER VALUE
Social Information Vectors
ETHICS
Digital Transformation, Future Technologies & Business Lines

Enterprise-level adoption of cyber social value

An eco-system approach to cyber instinctively connotes big picture complexity. It is important though to recognise that the social cyber issues can be canvassed at each of micro, meso and macro levels; and that the units of analysis, as indicated, can stretch across a spectrum from individual focus across to individual nations and the globe. Components of the ecosystem can be examined through "deep dive" research as well as in wider context. But the core unit for intermediating all the forces at play is the organisation. It is therefore affirmed that rich analysis of organisations is necessarily central, if not sufficient, for the success of the eco-system perspective.

The premier information age utilities companies, such as Google, Facebook, and Microsoft, are the principal organisations currently under scrutiny. They have all now set themselves high aspirational benchmarks through integrated, ethics-based approaches to their entire enterprise and its information ecosystem. None have quite cracked the challenge, as evidenced by repeat stumbles of one kind or another, especially on the ethics front. Nevertheless, the aspiration of these corporations to set new standards also saw them create novel forms of management to address the challenges. What we can take from the leadership example of these corporations, if only at an anecdotal level, is this. If your corporate structure operates more or less as it did a decade ago, and if the lines of authority between the pillars of your information ecosystem represented in Figure 1 (information security, digital transformation, resilience of legacy systems, and human capital) remain largely in silos, then it may be reasonable to assume that your enterprise is at a higher risk of digital disaster than ones that have made fairly fundamental and integrative changes. That said, change by itself, without continuing validation of the success of the change, can often be more destructive than no change at all.

If the basic proposition in this paper is valid, and it certainly remains under-researched and untested, one might imagine that large corporations and government agencies might realign their organizational structures around an ecosystem approach that would see the creation of new posts, perhaps with the title such as Vice President for social cyber ecosystems. Perhaps governments will even create new Ministerial appointments for Social Cyber Systems, instead of drawing ad hoc on separate portfolios for cyber security, digital transformation, education, industry and employment.

As just one illustration of the potential for change, Figure 2 shows how a new post, Senior VP for Cyber Ecosystems might be genetically inserted into the current cyber DNA of an organisation. The concept reorganises the reporting lines and diffuses the functionality of four existing separated functions: the VP for Human Resources (digital human capital),[5] the CIO (functionality of current IT), the CISO (security of current IT), and the VP Strategy (seizing profit gains from future IT transformation). They would all report to a Senior VP for information ecosystem management. The concept, like the diagram, is indicative only.

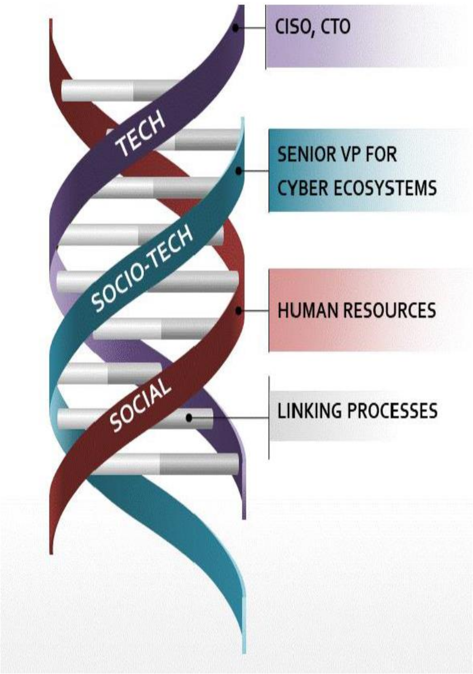
Figure 2 illustrates this concept using the image of a triple helix where three broad strands (technical, socio-technical, and social) constitute the DNA of any information ecosystem. A central assumption of this idea of optimised social cyber value is that solutions will be unique to each organisation and that each organisation needs to invest in longitudinal social science research by in-house teams to devise optimal outcomes. The field of activity is simply too complex to leave to the imagined leadership judgement of senior executives uninformed of detailed consequences, for the reasons discussed in this paper.

While the preceding paragraph illustrates the concept with an intra-firm approach, the concept is as relevant to large communities, countries and even transborder relationships. We can and should imagine single political entities as a cyber ecosystem, comprising many component cyber ecosystems. Cyber sovereignty does exist. But the national authority of the sovereign is now seriously diluted, whatever the intent, by disruptive

[5] There is a basic assumption that the digital aspect of human resources management and development is today and into the future, one that over-rides all others. The central idea is an ecosystem approach. Social influences and interactions involved in managing an information ecosystem are "path dependent"; the basic assumption is that the boundaries, character and destiny of a cyber ecosystem, however fluid, are defined by the people in it.

influences of trans-national cyber ecosystems or business ecosystems that cut across politically bounded ones. These disruptive influences can be structured or chaotic. But they are all too real, so calling for a new wider vison of the international (cross-border) character of cyberspace through cyber eco-system analysis.

Figure 2: Managing an Enterprise Level Information Ecosystem



Conclusion

Few businesses and few governments around the world have well developed policies to respond to the fundamental social behaviour and ethical transformations under way as result of the information revolution. Policy and management have been oriented largely toward both the technologies and the business preferences of the technologists. Where broader interests have come into play, these have been confined largely to workplace regimes (efficiency from automation) or to exploiting consumer responses to technology products. We have not seen social and ethical questions arise much in new types of "information training" for government and business. Leading moral philosophers of the information age, such as Floridi, signal ways in which we should expect society to respond to the new moral qualities of the information age, but we don't see it.

In this paper, we suggest an ecosystem approach that sees leaders and executives construct a vision of the specific cyber ecosystem in which their enterprise activity takes place and in which they can create new forms of social cyber value. The paper takes as its departure point and end point the dualistic Floridi proposition that diffusion of power (democratisation) is a central organising principle of the information age, and that what will matter most is how that power is re-aggregated. Business and government have to adapt, profoundly, in ways that respond to the new sentiments of direct democracy and millennial "rights sensitivity". The main direction of that change needs to be in the high-level ranks of organisations who need to yield authority both to lower levels and to social scientists. In the same way that the technology of the information revolution transformed workplaces several decades ago with new work roles, including Vice President for Information Technology and large-scale lay-offs because of efficiencies from automation, then the emergent sociology of the information revolution—including the human rights aspects—will bring forth new work roles and work structures. In addition to specialised roles that emerged more recently, such as the Chief Information Security Officer, will we now look to appoint Chief Information Sociology Officers? They will have not only a narrowly commercial function but will be the main champions of human rights promotion inside business ecosystems—because in the information age, there will be higher costs to those corporations and government agencies which ignore human rights.

Drawing on Floridi (2002, 2012), the paper assumes that the norm of freedom of information objectively shapes concrete outcomes in the business world, both within a single enterprise and between the enterprise and the outside world. The paper ties that proposition to an evolving concept of "social cyber" management which identifies important gains and penalties for corporations or large government agencies which fail to take into account the centrality of non-technical aspects in the outcomes produced by their technology-based information objects. The non-technical aspects include the ethics of the work force, the corporation, and international society writ large. But the non-technical aspects also include considerations of how to manage business outcomes for digital transformation at the same time as managing for cyber security and for cyber competence.

The paper argues that by addressing these limitations and bringing social science to bear on the cyber ecosystems, all actors could simultaneously unleash untapped positive potential for digital transformation that has hitherto been constrained by the focus on the technical domain (tools and inventions such as autonomous vehicles and robots). The new spirit might be based on the conviction that a social retooling at a system level is not only feasible but is also a moral duty.

An additional important outcome of social science study of specific cyber ecosystems will be enhanced protection from information threats, such as malicious campaigns to destroy national confidence, undermine shareholder value, or direct attack on key actors in the work force. An overarching benefit of addressing social ecosystem development and issues in this comprehensive fashion (insecurity, incompetence, digital transformation and information threats) is that it creates the conditions for the appropriate reflection on important ethical questions (especially privacy but also worker values) that are unique to the information age.

This paper imagines how a process of radical adjustment to the social and systemic influences of security in cyber space might be undertaken to begin to deliver more viable social ecosystems that can match the escalating threats while exploiting more effectively the untapped potential of the information revolution, still in its early stages. The keys are to adopt a wide perspective, make it socially aware and embrace all levels of insight while being ecosystem focused, multi-disciplinary and with firm micro-foundations. This is a big agenda for analysts but with huge potential pay-off, intellectually and in the cyber worlds of government, business and individual people.

References

Angst C.M. Block E.S. D'Arcy J. and Kelley K. 2017. When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly* 41(3)

Arina T. 2009. Digital Ecosystems. Speech at Finnish Digibusiness seminar. 13 January 2009. Presentation slide set available at https://www.slideshare.net/infe/digital-ecosystems-presentation-913157

Austin G. 2019. Digital China: Has Australia been spooked. Asia Society. https://asiasociety.org/australia/digital-china-has-australia-been-spooked

Austrac. 2018. AUSTRAC and CBA agree $700m penalty. 7 June 2018. http://www.austrac.gov.au/media/media-releases/austrac-and-cba-agree-700m-penalty

Bellavita C. 2006. *Changing Homeland Security: Shape, Patterns, Not Programs*. Naval Postgraduate School Monterey CA. Center for Homeland Defense and Security

Benson V. McAlaney J. and Frumkin LA. 2019. Emerging Threats for the Human Element and Countermeasures in Current Cyber Security Landscape. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1264-1269). IGI Global

Boeing. 2019a. Boeing CEO Dennis Muilenburg addresses the Ethiopian Airlines Flight 302 preliminary report. 19 April 2019. https://www.boeing.com/commercial/737max/737-max-update.page?gclid=CjwKCAjwwZrmBRA7EiwA4iMzBB9paUYfNpArSz2YcURbtvY7YbnShfkFH7fgDwmBmdlxdPJ8XQlzMRoCsRYQAvD_BwE

Boeing 2019b. About the Boeing 737 Max. https://www.boeing.com/commercial/737max/index.page. Accessed 29 April 2019

Brody B and D Mclaughlin. Facebook Agrees to Pay Record $5 B, 24 July. *Time*. https://time.com/5633513/facebook-ftc-settlement/

Carley K. 2018 October. The Science of Social Cyber-Security. In *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. 459-459. ACM

Carley K.M. Cervone G. Agarwal N. and Liu H. 2018. July. Social cyber-security. In *International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation.* 389-394. Springer

Clarke J. Chen H. Du D. and Hu Y. 2018. Fake News, Investor Attention, and Market Reaction. Georgia Tech Scheller College of Business Research Paper No. 18-29. Available at SSRN: https://ssrn.com/abstract=3213024 or http://dx.doi.org/10.2139/ssrn.3213024

Clarke, J. Coaffee J. Rowlands R. Finger J. Hasenstein S. & Siebold U. 2015. Resilience Evaluation and SOTA Summary Report. European Union. Horizon 2020 Program. http://resilens.eu/wp-content/uploads/2016/08/D1.1-Resilience-Evaluation-and-SOTA-Summary-Report.pdf

Clark-Ginsberg, A. and Slayton R. 2018. Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*. https://academic.oup.com/spp/advance-article-abstract/doi/10.1093/scipol/scy061/5184558?redirectedFrom=fulltext

CNBC. 2013. False Rumor of Explosion at White House Causes Stocks to Briefly Plunge; AP Confirms Its Twitter Feed Was Hacked. 23 April 2013. https://www.cnbc.com/id/100646197

Cornish. 2017. Personal communication with the author

Courtney T. Gaonkar S. Keefe K. Rozier E.W. and Sanders W.H. 2009 June. Möbius 2.3: An extensible tool for dependability, security, and performance evaluation of large and complex system models. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. 353-358. IEEE

Craigen D. Walsh D.A. and Whyte D. 2013. Securing Canada's Information-Technology Infrastructure: Context, Principles, and Focus Areas of Cybersecurity Research. *Technology Innovation Management Review 3*(7) 12-18

De Smet D. and Mayer N. 2016 October. Integration of IT governance and security risk management: A systematic literature review. In *2016 International Conference on Information Society (i-Society)* (pp. 143-148). IEEE

Dimitrova S. 2017. Challenges of the Security Environment Before the Correlation "Resources-Capabilities-Effects". In *International conference KNOWLEDGE-BASED ORGANIZATION* 23 (1) 89-93. De Gruyter Open

Floridi L. 2002. Information ethics: an environmental approach to the digital divide. *Philosophy in the Contemporary World 9*(1) 39-45

Floridi L. 2012. Hyperhistory and the Philosophy of Information Policies. *Philosophy & Technology*. 25(2) 129-131

Floridi L. 2013. *The Ethics of Information*. Oxford University Press. Oxford

Gaycken S. and Austin G. 2014. Resetting the System: Why Highly Secure Computing Should Be the Priority of Cybersecurity Policies. *EastWest Institute*, *New York/Brussels/Moscow*, January

Govender S.G. Loock M. and Kritzinger E. 2018 October. Enhancing Information Security Culture to Reduce Information Security Cost: A Proposed Framework. In *International Symposium on Cyberspace Safety and Security* (pp. 281-290). Springer Cham

Greenberg A. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History" Wired 22 August 2018 https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Guetl C. Ismail L. and Lexar C. 2013. Track A: foundations of digital ecosystems and complex environment engineering. In *2013 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST)* (pp. 1-1). IEEE

Heidt M. Gerlach J. and Buxmann P. 2019 January. A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*

Iansiti M. and Levien R. 2004. The keystone advantage: What the new dynamics of business ecosystems mean for strategy, innovation and sustainability. Boston Massachusetts: Harvard Business School Press

Isaac M and Kang C. 2019. Facebook Expects to Be Fined Up to $5 Billion by F.T.C. Over Privacy Issues. *New York Times*. 24 April 2019. https://www.nytimes.com/2019/04/24/technology/facebook-ftc-fine-privacy.html

Kovács L. Nemeslaki A. Orbók, Á. and Szabó A. 2017. Structuration Theory and Strategic Alignment in Information Security Management: Introduction of a Comprehensive Research Approach and Program1. *AARMS* 16 (1) 5-16

Kraemer S. Carayon P. and Clem J. 2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & security 28* (7) 509-520

Lafond D. and DuCharme M.B. 2011 April. Complex decision making experimental platform (CODEM): A counter-insurgency scenario. In *2011 IEEE Symposium on Computational Intelligence for Security and Defense Applications (CISDA)* 72-79

Masys A.J. 2015. The Cyber-Ecosystem Enabling Resilience Through the Comprehensive Approach. In *Disaster Management: Enabling Resilience.* 143-154. Springer

National Academies. 2019. *A Decadal Survey of the Social and Behavioral Sciences: A Research Agenda for Advancing Intelligence Analysis*. https://www.nap.edu/download/25335

PWC. 2014. Expanding Australia’s Economy: How digital can drive the change. https://www.pwc.com.au/consulting/assets/publications/expanding-australias-economy-apr14.pdf

Rebovich G. 2010. Systems thinking for the enterprise: a thought piece. In *Unifying Themes in Complex Systems*. 556-563. Springer. Berlin, Heidelberg

Richards M. Hastings M.G.R.D.E. Rhodes D.H. and Weigel A.L. Systems Architecting for Survivability: Limitations of Existing Methods for Aerospace Systems. http://seari.mit.edu/documents/preprints/RICHARDS_CSER08.pdf

Salasin J. 1976. A control systems model of privacy. In *Proceedings of the June 7-10 1976 national computer conference and exposition*. 45-51

Schwartz E. 1999. *Digital Darwinism: 7 Breakthrough Business Strategies for Surviving in the Cutthroat Web Economy*. New York: Broadway Books

Schwartz E. 2002. *Digital Darwinism: 7 breakthrough business strategies for surviving in the cutthroat Web economy*. Crown Business

Sommer P. and Brown I., 2011. Reducing systemic cybersecurity risk. *Organisation for Economic Cooperation and Development Working Paper No. IFP/WKP/FGS (2011) 3*

Tang M. and Zhang T. 2016. The impacts of organizational culture on information security culture: a case study. *Information Technology and Management 17*(2) 179-186

Torok S. and Holper P. 2017. *Securing Australia's Future: Harnessing Interdisciplinary Research for Innovation and Prosperity*. CSIRO Publishing

Trautman L.J. 2017. Governing Risk and the Information Silo Problem: Engineering a Systemic Cultural and Communications Solution for Cyber

Walton P. 2015. Digital information and value. *Information 6*(4) pp.733-749

Wang X. Guo Y. Yang M. Chen Y. and Zhang W. 2017. Information ecology research: past, present, and future. *Information Technology and Management 18*(1) pp.27-39

Wheeler C Shipman T and Hookham M. 2018. UK war-games cyber attack on Moscow. The Times. 7 October 2018. https://www.thetimes.co.uk/edition/news/uk-war-games-cyber-attack-on-moscow-dgxz8ppv0?_ga=2.58052266.1684028993.1538922478-959467586.1538672718&wgu=270525_54264_15599569933948_26b89a5eb2&wgexpiry=1567732993&utm_source=planit&utm_medium=affiliate&utm_content=22278

Williams C. 1997. Intel’s Pentium chip crisis: An ethical analysis. *IEEE Transactions on Professional Communication. 40*(1) 13-19

Williams RC, Raghnaill M., Douglas K, Sanchez D. 2015. *Technology and Australia’s Future. New technologies and their role in Australia’s security, cultural, democratic, social and economic systems*. Australian Council of Learned Academies. Securing Australia’s Future. Final Report 05. https://acola.org.au/wp/PDF/SAF05/SAF05_Report_web_17Sept.pdf

Yurcik W. and Doss D. 2002 June. A Survivability-Over-Security (SOS) Approach to Holistic Cyber-Ecosystem Assurance. In *IEEE Workshop on Information Assurance*

Zeng J. Yang L.T. Lin M. Ning H. and Ma J. 2016. A survey: Cyber-physical-social systems and their system-level design methodology. *Future Generation Computer Systems.*

ABOUT THE SOCIAL CYBER INSTITUTE

Social science research on our emerging cyber world is not keeping pace with the “gifted technologists” and "talented tinkerers". Knowledge transfer from world-class social science researchers to leaders of business and government is slow, haphazard, and undisciplined. The Social Cyber Institute (SCI) creates new modes of thinking specific to individual corporations, government agencies and their operating ecosystem. We help you understand the social DNA of your InfoTech and rewire it for the future. SCI is the public research and public analytic arm of the Social Cyber Group consultancy.

ABOUT THE AUTHORS

Greg Austin leads the Cyber, Space and Future Conflict program of the International Institute of Strategic Studies. He is also a Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra. His academic career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included eight books on international security, as author or editor, and leadership of several international research projects. His service as a research leader for prominent global NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London with leading governments at Ministerial level (Russia, China, UK, India, United States, Turkey, Australia), major international organisations at leadership level (United Nations, International Atomic Energy Agency, R20 for Climate Action), and leading corporations (AT&T, BT, Perot Systems). He has consulted for the UK Cabinet Office, the UK Ministry of Defence, the Foreign and Commonwealth Office, the European Commission, and the Australian Department of Foreign Affairs and Trade. He began his career in Australian public service roles, including posts in Canberra and Hong Kong in defence intelligence, parliamentary committees, and ministerial staff. Austin has a Ph D in International Relations and a Master of International Law, both from the Australian National University.

Glenn Withers AO is a Distinguished Honorary Professor at the Australian National University and Visiting Professor at the University of New South Wales Canberra. His Harvard PHD was on the topic of human resources for defence. He has held appointments at Harvard University and Cambridge University, and has consulted widely for governments and companies from the OECD and the North-West Shelf Consortium to the US Defense Department and the Prime Minister of Malaysia. In Australia. He has been Chair of the National Population Council and the Commissioner of the Economic Planning Advisory Commission and helped to establish the Bureau of Labour Market Research, the Bureau of Immigration research, the Productivity Commission, Crawford School of Government and Universities Australia. He was awarded honours by the Australian government for developing the Australian Immigration Points System. He is immediate past President of the Academy of the Social Sciences in Australia and the Australian Council of Learned Academies. Currently, he is Chair of the Global Board of the Global Development Learning Network, a World Bank affiliate that operates in 60 countries. He has a wide range of publications in books, academic journals, government reports and consultancy reports, particularly focusing on education, skills, workforce and population issues

ABOUT THE SOCIAL CYBER INSTITUTE

Social science research on our emerging cyber world is not keeping pace with the “gifted technologists” and "talented tinkerers". Knowledge transfer from world-class social science researchers to leaders of business and government is slow, haphazard, and undisciplined. The Social Cyber Institute (SCI) creates new modes of thinking specific to individual corporations, government agencies and their operating ecosystem. We help you understand the social DNA of your InfoTech and rewire it for the future. SCI is the public research and public analytic arm of the Social Cyber Group consultancy.

ABOUT THE AUTHORS

Greg Austin leads the Cyber, Space and Future Conflict program of the International Institute of Strategic Studies. He is also a Professor of Cyber Security, Strategy and Diplomacy with the University of New South Wales Canberra. His academic career, including a Senior Visiting Fellowship in the Department of War Studies at Kings College London, has included eight books on international security, as author or editor, and leadership of several international research projects. His service as a research leader for prominent global NGOs, such as the International Crisis Group and the EastWest Institute, has seen him work from Brussels and London with leading governments at Ministerial level (Russia, China, UK, India, United States, Turkey, Australia), major international organisations at leadership level (United Nations, International Atomic Energy Agency, R20 for Climate Action), and leading corporations (AT&T, BT, Perot Systems). He has consulted for the UK Cabinet Office, the UK Ministry of Defence, the Foreign and Commonwealth Office, the European Commission, and the Australian Department of Foreign Affairs and Trade. He began his career in Australian public service roles, including posts in Canberra and Hong Kong in defence intelligence, parliamentary committees, and ministerial staff. Austin has a Ph D in International Relations and a Master of International Law, both from the Australian National University.

Glenn Withers AO is a Distinguished Honorary Professor at the Australian National University and Visiting Professor at the University of New South Wales Canberra. His Harvard PHD was on the topic of human resources for defence. He has held appointments at Harvard University and Cambridge University, and has consulted widely for governments and companies from the OECD and the North-West Shelf Consortium to the US Defense Department and the Prime Minister of Malaysia. In Australia. He has been Chair of the National Population Council and the Commissioner of the Economic Planning Advisory Commission and helped to establish the Bureau of Labour Market Research, the Bureau of Immigration research, the Productivity Commission, Crawford School of Government and Universities Australia. He was awarded honours by the Australian government for developing the Australian Immigration Points System. He is immediate past President of the Academy of the Social Sciences in Australia and the Australian Council of Learned Academies. Currently, he is Chair of the Global Board of the Global Development Learning Network, a World Bank affiliate that operates in 60 countries. He has a wide range of publications in books, academic journals, government reports and consultancy reports, particularly focusing on education, skills, workforce and population issues

CONTACT

info@socialcyber.co

www.socialcyber.co