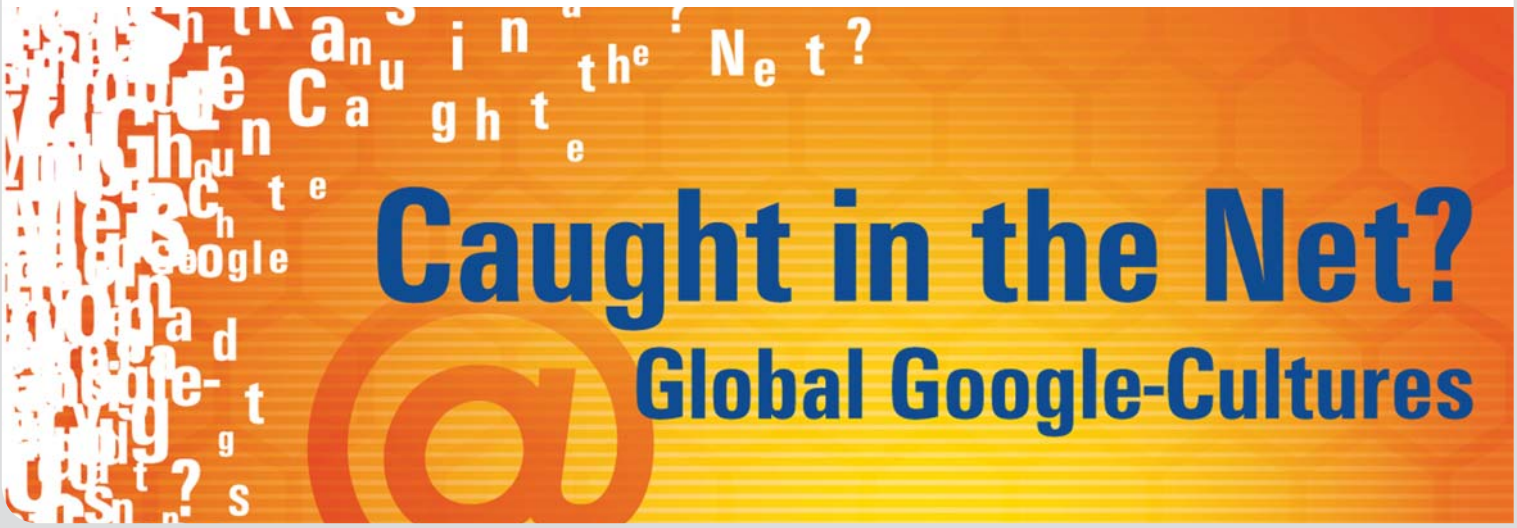
Karlsruhe Institute of Technology

ZAK

Thinking About How to Think About Cybersecurity

Richard J. Harknett



KIT – University of the State of Baden-Wuerttemberg
and National Research Center of the Helmholtz Association

ZAK | Zentrum für Angewandte Kulturwissenschaft
und Studium Generale
Centre for Cultural and General Studies

The lead title of the 2011 Karlsruhe Dialogues, 'Caught in the Net', is quite instructive in that it suggests a context of surprise and struggle. In the case of the Internet, we can at least accept a beginning default premise that much of what has evolved was not anticipated. Significantly, our inability to anticipate the dynamics associated with the rise of the Internet has contributed to an environment in which the security of that environment is under increasing strain and risk. Cybersecurity is tenuous, which is a highly problematic condition since cyberspace is a ubiquitous context of life in the 21st century.

This essay asks us to dwell on fundamentals as we reflect on the future of the Internet. Specifically, I posit that thinking about the relationship between individuals, technology and the state provides a distinct foundation on which to assess where we are heading in this early stage of the Internet age; whether the net we are caught in will strangle us, or carry us to new opportunities, will depend on getting those fundamentals correct.

And we are at an early stage. In his book, *Out of Our Minds*, Sir Ken Robinson offers a compelling visualisation to put the current technological developments in context. He suggests that we start with the recognition that humans have been communicating in some form of writing for some 3000 years. If we imagine that history as one hour on a clock, each minute represents 50 years. Looking at time in this fashion, we should note that for most of human history we communicated through pictures and etchings and then writing in a very limited fashion. But 550 years ago, about 11 minutes ago on our clock, Gutenberg created the printing press which unleashed the ability to communicate broadly on an exponentially wider scale and with higher speed. The social, political and economic impact of the printing press took many years to unfold and understand. The emergence of networked computers, and thus of what we refer to as cyberspace, seems to be of a similar dramatic and revolutionary character. In terms of our human history clock, and this is the critical point to recognise, we only have been dealing with the Internet for about 12 seconds – a very short period of time.[1]

[1] *Robinson, Ken*: Out of Our Minds. Learning to Be Creative, Oxford 2001, chapter 1.

It is always difficult to recognise challenges to fundamentals when you are living during periods of revolutionary potential, in part, because we all tend to think that the time in which we are living is significant. The term 'revolutionary' does indeed tend to be overused, but it does seem reasonable in the case of the Internet to explore the premise that the digital networked computer environment is unleashing significant discontinuities from previous eras.

The point of the clock metaphor is to emphasise that if this is a revolutionary period on the scale of the printing press, we are, in fact, very early into this revolution and, thus, it is critical for effective analysis that we spend time thinking about how to think about cyberspace. We need to strengthen our ability to understand the fundamentals of what is going on.

The following reflection offers one base formulation to guide such thinking about how to think about cyberspace and it is predicated on the assumption that all of the sociological, economic, and political implications of 'the Net' ultimately are shaped by the dynamics of cybersecurity. If we cannot feel secure in our financial transactions, in sustaining our critical infrastructures, and in maintaining our personal identities, this wonderfully exciting new world will be susceptible to collapse. Since we are early into the evolution of the Internet, all we can empirically consider are trends, and the trends are not positive in this regard. Financial losses from fraud, disruption of system functions, growing compromises via identity theft and the introduction of precise cyberweapons, such as Stuxnet, are cumulatively suggestive of an environment of increasing vulnerability. Struggling with that unanticipated security fundamental – in large part because we did not concentrate on it at all in the initial development of the technology and when we did think about it, we understood it incorrectly – will be an on-going issue early in the 21st century.

1. Cybersecurity

The term 'cybersecurity' is used both narrowly and broadly to capture the technical aspects of computer coding within a digital system to national policy statements and strategies, which governments around the globe are now issuing. For the purposes of this reflection, it is best to begin with a broad framing and thus understand cybersecurity to be inclusive of actions taken to protect against cyberaggression. For definitional purposes, cyberaggression can be viewed as a continuum of activity taking place across digital platforms that can be, for analytical purposes, categorised into three areas: crime, espionage, and war. Each of those top tier categories include a sub-set range of activities each of which vary in intensity and potential ill-effect. For example, cybercrime can range from individual cyberbullying, minimal disruption of service, stealing of identities or proprietary information, to financial theft in the tens of millions, to name just a few.[2] Those engaged in cybersecurity parallel in range, of course, from the individual using anti-virus software and good passwords to corporate intranets to national governments protecting both directly and in partnership the critical infrastructures of their countries that rely on digital components (which of course is now ubiquitous, including financial, transportation, water, electric and power networks).

From a technical standpoint, the Internet was not developed with security necessarily in mind. The original purpose of the ARPANET was to create a communication platform that could survive a surprise nuclear attack. The infrastructural solution of a network of nodes in which there was no central hub and the process solution of open portals to facilitate access produced a technological advancement in which security principals were set aside (notions of restricted access, hierarchy, and central control).[3] It has left us with a technological foundation in which massive economic activity is compromised with alarming levels of financial

[2] For full development of the definitional framework of cyberaggression, see *Harknett, Richard/Callaghan, John/Kaufmann, Rudi:* Leaving Deterrence Behind. Warfighting and National Cybersecurity, in: Journal of Homeland Security and Emergency Management, No. 1, Vol. 7, March 2010, pp. 1-24; Onlinedokument http://www.bepress.com/jhsem/vol7/iss1/22/ [09.02.2012].

[3] Of course we should not lose sight of the irony that a major advancement meant to solve a particular national security threat has evolved into major and new national security vulnerabilities.

loss; where individual social networking is compromised with individual loss of identity; and where advances in precision guidance are increasing military lethality, while asymmetrically the most powerful military is under assault from hundreds of thousands of computer intrusions a day.

While much of the insecurity found in cyberspace does follow from its original design that did not anticipate its future application on the commercial and social side, it is reinforced potently from the fact that we have tended to think about cybersecurity from the incorrect frame.

2. The Fundamental Relationship

The level of security in cyberspace flows from the fundamental interaction between the individual, technology, and the state. How technology intervenes in that core relationship between the individual in society and the role of the state, in particular, is critical.

In the context of on-going discussions of an 'information age', one conceptualisation of the relationship between the individual, technology and the state has dominated all others – Big Brother. This literary metaphor suggests a future in which the state would be able to leverage technology to the point of subsuming society under a system of total control. In terms of the fundamental relationship, technology would empower the state over the individual.

In a remarkable coincidence of timing, George Orwell's setting of his totalitarian nightmare in the year 1984 corresponded with a societal awakening to the prospect that computing, once the province of large institutions only (companies and governments), could be harnessed at the individual level. Curiously, as the reality of personal computing evolved to the point at which it became clear that individuals were actually becoming empowered, the perceptive frame remained anchored on the ominous threat of the empowered state. While the threat remained focused on the Orwellian outcome of the totalitarian state, the reality on the ground reflected Orwell in reverse – the empowered individual.

Consider the most recent and stark manifestation of this trend. When we look at Middle Eastern authoritarian states in 2011, when they were faced with managing public dissent, they literally turned the technology off. While there is no doubt that more savvy states such as Iran and China can use cyberspace for surveillance and societal shaping, ultimately the pattern is one of an inverse relationship between digital technology ubiquity and state control around the world. China is dancing around cyber technology in the most sophisticated manner, but in the end they fear it more than they exploit it. It is not the relationship of which Orwell forewarned.

The implications of framing the relationship incorrectly has been profound, because in overemphasising the threat of state empowerment, cyberspace has evolved with a default of keeping the state as minimally involved as possible. This actually undermines the sustainability of two other variants of the relationship between the individual, technology and the state.

Two alternative frames to Big Brother have been part of the cyber discourse of the past several decades – the Demos and Customiser visions. Both see benefit in constraining the state, so that individual empowerment can flourish. The Demos vision has tended to see the role of the state as a minimal economic regulator containing the excesses of monopolies on technology development and is highly sensitive to any state involvement on content regulation. The vision is a cyberspace of free-flowing access, grass-root forms of organisation, new individual-based knowledge creation and new forms of media. It is a vision of free and fluid association.

The Customiser frame approaches cyberspace from a business model perspective and seeks to minimise the role of the state to avoid impediments to leveraging technology to provide consumers with greater customisation and convenience in all of their social and economic activity. In this frame, the state provides minimal regulation for management of content use so as to produce some expectation of a protection of privacy in order to get people to use the technology. In many instances, the lure of customisable individual-based convenience leads users knowingly to accept less privacy (or control over their ability to keep things private).

Both of these perspectives recognise the great potential for individual empowerment found in cyberspace, but have incorrectly defined its source. Both have sought to support it via direct minimisation of the role of the state; that is, if the state was kept out, individuals would thrive. In this regard, in essence, they are no different than the Big Brother perspective in assuming that if the state could attain total control, it would (they differ from Orwell only in the presumption that they can prevent the state from becoming totalitarian).

What all three perspectives miss is that it is the essence of the technology itself that has empowered individuals, not the active carving out of social, economic, and political space apart from the state. Big Brother is not the real threat when it comes to security; the unconstrained empowered individual is. Our security (personal and national) is at risk not from the state, but from our own practices and the infrastructure that we allow to persist. This is because we have combined the Customiser and Demos perspectives to produce an environment in which convenience and individuality crowd out all other organising principles that have traditionally been associated with civil society. There is a difference between an individual and an individual citizen: the individuality of the latter is defined in the context of participating in a larger civil construct (be it global, national or local).[4] The state has an essential role to play in positioning individuals to be productive citizens. In cyberspace, privacy, for example, is not under assault from the state, but rather it is being lost to and through the marketplace and other individuals. In the United States, when consensus emerged that health records needed explicit protection, it was the state, through a reasonable regulatory environment, that needed to enter in and protect individual rights – neither the marketplace nor free association could accomplish that protection – confidently.

[4] For a more developed argument on the role of the cybersecurity citizen, see *Harknett, Richard/Stever, James*: The Cybersecurity Triad. Government, Private Sector Partners, and the Engaged Cybersecurity Citizen, in: Journal of Homeland Security and Emergency Management, Vol. 6, Art. 79, Winter 2009, pp. 1-14; Onlinedokument http://www.bepress.com/jhsem/vol6/iss1/79/ [09.02.2012].

3. Avoiding Insecurity

The increasing lack of security in cyberspace is flowing from the absence of norm- and regulatory-based support of the state and an actively engaged cybercitizen who partners with, rather than avoids, the state. To borrow from another English literary classic, cyberspace is trending more toward the island of children whose unconstrained individuality and loss of societal framing created a threat to all. It is not the emergence of Big Brother we need to prevent, but the collapse into the chaos of *Lord of the Flies*.

This can only be achieved if we go back to the fundamental relationship that defines security and recognise that there is a balanced role for the state to play in a world of technologically empowered citizens, so that those individual citizens thrive. In allowing for the state to play a constructive role in cyberspace's development, a more sustainable, prosperous, enriching, and secure environment may emerge. When thinking about the fundamental relationship between the individual, technology, and the state, we have to allow for the state to be an active part of the solution set that will advance cybersecurity, and in doing so sustain a cyberspace that can flourish.

References

Harknett, Richard/Callaghan, John/Kaufmann, Rudi: Leaving Deterrence Behind. Warfighting and National Cybersecurity, in: Journal of Homeland Security and Emergency Management, No. 1, Vol. 7, March 2010, pp. 1-24 ; http://www.bepress.com/jhsem/vol7/iss1/22/ [09.02.2012]

Harknett, Richard/Stever, James: The Cybersecurity Triad. Government, Private Sector Partners, and the Engaged Cybersecurity Citizen, in: Journal of Homeland Security and Emergency Management, Vol. 6, Art. 79, Winter 2009, pp. 1-14; http://www.bepress.com/jhsem/vol6/iss1/79/ [09.02.2012]

Robinson, Ken: Out of Our Minds. Learning to Be Creative, Oxford 2001

15th KARLSRUHE DIALOGUES

11th–13th February 2011

15th Karlsruhe Dialogues
„Caught in the Net? Global Google-Cultures“
11th-13th February 2011

Presented by:
ZAK | Centre for Cultural and General Studies
Karlsruhe Institute of Technology (KIT)

Convenorship: Prof. Dr Caroline Y. Robertson-von Trotha
Organisation: Swenja Zaremba M.A.

Editorial Team:
Silke Flörchinger M.A.
Janina Hecht M.A.
Sonja Seidel

www.zak.kit.edu