The Ergonomist

No. 537 March 2015

The Chartered Institute of Ergonomics & Human Factors

Cybernomics and the implications of cyber-deception

THE ROLE OF EXPECTATION IN DESIGN

COGNITIVE AND BEHAVIOURAL TRAINING DESIGN IN CONSTRUCTION

SEXUAL HARASSMENT AND PUBLIC SPACES

Editorial

Understanding thought processes

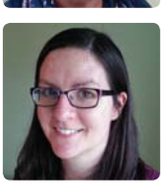
As more young people head to Syria to join IS, the question that keeps coming up is: why?

In our cover article, Peter Hancock and colleagues discuss cybernomics and the way in which cyber-deception is changing warfare. Gone are the days, they argue, where the aim of an enemy is to destroy. In the cyber world, which is built on communication, the aim is to persuade and control, to win the enemy over to a certain mindset. That is certainly what we are seeing with these young people, who are convinced online that Islamic State will provide them with the life they dream of. The article discusses how we might combat this type of warfare and how, just as information can be a tool for destruction, it can also be a force for good.

Ron McLeod explores how the erroneous expectations of various stakeholders can lead to the design of instruments that cause mistakes rather than preventing them. He examines what goes wrong in the design process from the point of view of users, shareholders and managers and discusses how being aware of expectations can reduce human error.

Patricia Meiring and Ann Bicknell describe a study that was carried out with construction workers in the Middle East to determine whether declarative or procedural training is more effective in bringing about change in safety behaviours.

Jane Osmond and Andree Woodcock discuss street harassment and the ways in which transport design can increase safety for women while they are travelling.



If you have any ideas for feature articles on research or practice in ergonomics and human factors, news items, details of relevant events or suggestions for new content for *The Ergonomist*, please email us.

Email Tina: tina@ergonomics.org.uk
Email Frances: frances@ergonomics.org.uk

Chartered Institute of Ergonomics & Human Factors

www.ergonomics.org.uk

Contents

Features

Also in this issue

From the President

Moving with the times

A launch event will be held at the beginning of March at St Pancras International station in London, to celebrate the Institute becoming Chartered. The venue was chosen carefully. Steve Barraclough will say at the reception that St Pancras is "…a place where so many journeys have begun." Gilbert Scott's gothic masterpiece and the adjoining station have a fine history, having changed considerably with the times since the first train arrived into St Pancras in 1868. With expansion, decline, the closure of the Grand Hotel in 1935, bomb damage in 1941, St Pancras has more recently transformed to become the magnificent international transport hub it is today. Important themes during the reception will be the Institute's own proud heritage, the wide ranging and important contributions of EHF to modern life and issues we expect to be tackling in future.

Thinking about the future prompts me to highlight two significant challenges raised by contributors to our journals. Among papers shortlisted for the Institute's Liberty Mutual Award this year is Hancock's article 'Automation: how much is too much?' In his treatise, Hancock highlights a drive to automate because we can, not because we should. He argues for a more intelligent, purposeful approach to automation, giving greater heed to achieving collective, positive human experience. Driverless cars will be mentioned at the reception. My mother, still driving in her mid-80s, depends on this mobility to live an independent life to the full. She is finding driving increasingly difficult however, and for her, fully automated vehicles would be of great benefit. For my son though, in his early 20s, learning to drive and having his own car have been a hedonistic rite of passage. Addressing the consequences of ever more automation presents dilemmas for EHF in achieving artful compromise between widely conflicting user needs.

In 2009, Straker and Mathiassen asked the question "Increased physical workloads in modern work – a necessity for better health and performance?" These authors reasoned that addressing growth in sedentary work and its detrimental effects on health requires a shift from the traditional ergonomics paradigm of reducing risk by reducing physical loads. How then should EHF develop its approaches to function allocation, task, job and system design, in order to achieve good work and good jobs? Ought we to follow Barbieria and colleagues' suggestion in January's edition of *Ergonomics* that office workers should clean their own offices?

There are other major EHF issues on the horizon of course, those arising from population change, climate change, renewable energy generation and the evolution of manufacturing, for example. As we begin our journey as a Chartered Institute, our discipline and its paradigms need to continue to develop with the times. We might reflect on the words of Albert Einstein: "The world as we have created it is a process of our thinking. It cannot be changed without changing our thinking."

Best wishes

Roger

Cybernomics and the implications of cyber-deception

Peter Hancock, Gabriella Hancock & Ben Sawyer

ABOUT THE AUTHORS

Peter Hancock is Provost Distinguished Research Professor in the Department of Psychology and the Institute for Simulation and Training at the University of Central Florida. Gabriella Hancock is a doctoral candidate in the University of Central Florida's Applied Experimental and Human Factors Psychology program studying the psycho-physiological underpinnings of vigilance performance. Ben D Sawyer is an Industrial Engineer and Applied Experimental Psychology Doctoral Candidate at The University of Central Florida. His work on attention and distraction in human-machine systems can be accessed at www.bendsawyer.com.

As digital technologies proliferate and the points of direct and indirect influence between computer-mediated operations and the physical world increase, issues of cyber-security have burgeoned commensurably. Here, we argue that the critical criterion of interest proves to be each individual user's state of mind, as mediated by the technologies with which they now necessarily interact. In consequence, human factors and ergonomics lie at the very heart of all 'cyber' endeavours.

'Cyber' might well be the scientific word of the decade. Everything cyber is now hot and many researchers (including ourselves) want in. Authorities in many nations are now worried, or even downright terrified of what this new and rather amorphous 'threat' might represent.

Labels such as 'cyber-threat', 'cyber-terrorism', and 'cyber-attack', dominate our airwaves and our general social discourse. Each of these terms appear to embody the very darkest interpretation of what actually represents the material expression of our modern, interconnected world. At the end of this article however, we offer a perspective which emphasises that 'cyber' need not necessarily be so threatening, nor possess so doom-laden a connotation as is now attributed to it. Rather, it could be a very hopeful term, especially with respect to the resolution of contemporary forms of asymmetric and akinetic human conflict.

Cyberhealth

The penetration of electronic devices around our planet has now reached staggering levels. The number of mobile phones alone is set to surpass world population in the present year, and thus it is very probable that there are, even now, more personal electronic devices in existence than there are people in the world to use them. The modern generation often carries two or three versions of such technologies on them, but the evolutionary vector here is towards one single, simple and portable portal to all of the electronic realm. Few individuals in the developed world live beyond the reach of the computer and, as the number of devices continues to increase, the percentage of the human race that exist beyond computer influence will become a vanishingly small number. In short, as a species we now live connected.

Like all forms of information exchange such intercourse can be beneficial or damaging, contingent upon your perspective and the respective goals of each contribution to that communication event. In the same way we can view physical contact as a potential source of kinetic and biological threat in the process of all forms of physical intercourse, so we can see the transmission of information in social intercourse also as a matter of individual and public (cyber) 'health'.

In circumstances where trust is low and the level of perceived threat high, we can and should erect semi-permeable, selective barriers to ensure that interaction is accomplished to the safest possible degree. Indeed, we anticipate a new and coming phase of omnipresent encryption, or 'omnicryption', of the all basic electronic data elements, in order to further erect such selective barriers. We have to ensure that these barriers are not so impenetrable that mutual communication cannot occur, or are so prohibitive as to preclude effective communicative behaviour.

In short, cyber security can well be viewed through the lens of public health, and as with many apparently diverse areas of human understanding, as we dig deep enough, we can always find intriguing and intellectually useful commonalties. Barriers to cyber-attack might then well be conceived of as forms of exclusion guarding at interface thresholds, and the notion of a cyber-condom (or any effective form of regulated exclusion zone around your own personal information cache) is both an appropriate and apposite one. In many ways, this is what current forms of security such as passwords, firewalls, etc., seek to achieve. But the mimetic commonality we have identified actually provides insight into many more methods of achieving such ends. However, we must specify the forms of threat to such

boundary layers and how to ensure that only relevant, appropriate, and useful information filters through.

Cyberdeception and cybervigilance

The comparison between cybersafety and public health might well go beyond the concept of a metaphorical equivalence. Now, we can ask whether cyber-related issues are actually rather simple mimetic extensions of biological isolation. So we can link cybersecurity to other 'hot' current issues such as the present, news-dominating Ebola outbreak. Is it reasonable to suggest that cyber-attack and cyber-defence strategies replicate, employ, and adopt certain standard forms of defensive and offensive actions in the same way that biological entities interact?

In the realm of both attack and defence, much of this activity involves deception. The degree to which such deceptive activity is 'intentional', especially at the micro-biological level of analysis, actually becomes very problematic to distinguish. This difficulty in distinction is especially true if only the consequences of the deception are observable. Appearing to be what you are not for accidental or intentional purposes characterises deception, and for online realms we find that the natural (direct) perceptual capacities which humans have developed in order to detect deception can be circumvented in an alarmingly easy manner. Deception here ranges from the unintentional and benign, to the intentional and vastly destructive.

As a general principle, deception detection in artificial realms which characterise the cyber-world follows forms of pattern-based search. Scientists and researchers involved in human factors and ergonomics understand much about these human search capacities but in the cyber-world, the rate of event occurrence is, on a human-scale, prohibitive. Nevertheless, if technological speed forms a major part of the problem, it also provides us with the key to potential solutions.

In cyber-vigilance, for example, the first-pass processing necessarily occurs through the filters of ever-more sophisticated electronic search algorithms. What these forms of search produce are a series of potential candidates which now need human eyes to distil the particular meanings. This latter, human-centred assessment is presently required because, on virtually a necessary basis, these types of attack are currently initiated by human agents in the first place. As in the never-ending interplay between predator and prey, where the ante is always being upped in some fashion, we find humans at both ends of this cyber-predator, cyber-prey channel of intention. When mutual aims and goals are not aligned or indeed are in direct contrast, we see the genesis of conflict.

Cyberconflict

As presciently predicted by Bertrand Russell, the demise of one of the two great stand-off super-powers has left the other in the not necessarily envied position of global domination, but rather one in which history and circumstance have imposed upon them the default function of the world's policeman. Promulgating the cultural and social norms of a single country upon individuals in various diverse nations in differing parts of the globe has brought widespread disapprobation and disapproval to the actions of the United States government. In its turn, America has not essentially grasped and understood this disapproval. Indeed some segments of the US body politic are frustrated by what appears to them to be simply rank ingratitude for essaying an unpleasant but putatively necessary role.

Inevitably, this power imbalance means that the head-to-head conflict of traditional kinetic warfare has been largely obviated by the prevailing superpower's over-dominance. This leads to standard forms of asymmetric or 'guerilla' type response whose tactics are now mediated through improved and improving technologies. Cyber avenues prove very useful conduits for attack for those faced by such overwhelming kinetic force. But in a cyber-world, victory is indexed by states of belief, for example, your own and that of your interlocutor, not necessarily states of destruction. While interference to societal, operational processes, for example, interruptions to power supplies, transportation infrastructures, banking

capacities, communications networks and the like in the physical world are the shibboleth of current thinking. The very notion of physical disintegration of people, materials, and infrastructure is becoming an outmoded aspiration for all conflict in our world. (Although, we readily accept that such vestigial forms of aspiration still predominate, especially in the reporting of the visually hungry news media).

A more modern warfare goal, which looks especially vulnerable to cyber-manipulation is information gathering and veracity. Indeed, it can even be difficult to determine if such cyber 'extract and withdraw' operations have even occurred as, by definition, any such well-executed attack leaves no evidence. To reflect back to our previous 'condom' metaphor, in order to understand the true magnitude of the present exchange of information between governments, corporations and private individuals, we likely have to wait for their offspring, if any, to appear. However even this informational extraction is only an adjunct to the true goals of cyber-conflict.

The real aim of modern conflict is the 'control', which might perhaps be even more polemically expressed as the 'education', of the 'other's' mind. An enemy persuaded to become an ally represents a much more potent victory than one who is merely exterminated. Aspirations for unmitigated destruction merely lend persistence to our traditional conflict narrative, which is often still underwritten by the scourge of religious intolerance. Attached to potent weapons which enable mass civicide, such maladaptive states of understanding must be dissipated if our species is to persist. However, it is at this juncture we believe that the information carrying capacities of cyber penetration can morph from its spectral worst to its opportune best.

The other side of cyber

If the anachronistic and outmoded concept of evil actually lies in human ignorance, then cyber communication could well be the most powerful extant tool for the dissolution of such ignorance today. To a reasonable extent, knowledge is power. Further, the acquisition and sustenance of both acute and chronic expressions of knowledge via cyber sources have now found manifest expression in large-scale social movements, such as Tahrir Square. Oppressive tyrannies and manipulative oligarchies fear knowledge and education since it undercuts the foundation of their power base. Arguably, burgeoning knowledge and inter-communication of that knowledge has fueled most of the recent popular social upheavals. The cyber world is the accessible repository of such knowledge that with convivial interfaces and efficient machines can be accessed by all. Perhaps instead of intelligent munitions, our modern-day military should be dropping iPads?

Some have argued that all technologies are inherently morally neutral, being able to be used for good or ill as their user intends. However, we believe the modern challenge in creating 'cyber' as a weapon against 'the dark side of the force', lies in the intentional design of morally embodied technologies. These could take the form of what we can now begin to conceive of as moral orthotics. We believe that, for the foreseeable future, cyber will be the primary battlefield upon which the war between knowledge and ignorance will be played out. Surely, those in ergonomics and human factors can, should, and do mediate this crucial battlespace?

Our world will soon be spending trillions in its search to secure cybersafety. Rather like the contentious 'theatre' of airport security, this will be imposed upon a confused populous by uncertain politicians and certain capitalists. While the spectre of the potential threat is real, and we cannot pretend that it is not. If we do not recognise, emphasise and exploit the positive elements of cyber-communication then our world will spiral toward a global dysfunctionality. In human factors and ergonomics, we have accepted that communications channels present no inherent 'quality'. The message that is transmitted can be destructive, constructive, or gibberish; the mathematical theory of communication specifies how the message is communicated but neither the value nor the utility of that message.

Now is the time to step beyond such a 'neutralist' stance to focus on those very issues of value and quality that underwrite cyber communication. We must wed process to purpose and it is those who mediate between mind and machine who must lead this next evolutionary step of science in general. Royal imprimaturs and approbation notwithstanding, if we do not embrace this challenge our science fails in this, the fundamental test of its true import. ❖