



# LIFE IN CYBERSPACE

*Dr Mary Aiken*

BIG IDEAS III



# LIFE IN CYBERSPACE

*Dr Mary Aiken*

**Life in cyberspace**

© European Investment Bank, 2019

All rights reserved.

All questions on rights and licensing should be addressed to [publications@eib.org](mailto:publications@eib.org)

Photos: © Gettyimages, © Shutterstock. All rights reserved.

Authorisation to reproduce or use these photos must be requested directly from the copyright holder.

The findings, interpretations and conclusions are those of the authors and do not necessarily reflect the views of the European Investment Bank.

pdf: QH-03-19-396-EN-N ISBN 978-92-861-4295-6 doi: 10.2867/890925

eBook: QH-03-19-396-EN-E ISBN 978-92-861-4294-9 doi: 10.2867/75897

## BIG IDEAS

Internet is a real place. Every time we switch on our computers, use a program or an application, or log in to a social media site, we enter a virtual space made up of worlds, domains, forums and rooms. But we behave differently when we interact with technology: technology amplifies and accelerates our deeds; it can help us find useful information, benefit from a wide range of services and stay in touch with our friends, but it can also create addictive-type behaviours and subliminally manipulate us online.

Mary Aiken, a cyberpsychologist specialised in the impact of technology on human behaviour, warns us about cybersecurity: “We need a human-centred approach that is mindful of how humans actually use connected things and not how the tech sector presumes or expects them to”.

This is the fifth essay in the *Big Ideas* series created by the European Investment Bank.

The EIB has invited international thought leaders to write about the most important issues of the day. These essays are a reminder that we need new thinking to protect the environment, promote equality and improve people’s lives around the globe.





# LIFE IN CYBERSPACE

## LIFE IN CYBERSPACE

“Cyber” refers to anything involving computers or computer networks, such as the Internet. As a cyberpsychologist, I study human interaction with technology, digital media, artificial intelligence, and mobile and networked devices.

I also research how the Internet and digital activities, such as gaming and virtual reality, affect human behaviour. I focus on Internet psychology and figuring out how technology has the potential to impact or

change human behaviour. The development of information technology has exploded over the past 30 years. We now spend a significant part of our life in a space – cyberspace – that did not exist previously. We all know about the incredible benefits of the “information superhighway” of cyberspace, the Internet: affordability, convenience, connectivity, creativity, altruism, and educational and cultural exchange, along with the growth of entrepreneurship and commercial opportunities. However, the substantial benefits associated with our colonisation of cyberspace have downsides. Cyberactivity can have real-world consequences; claims for the independence of cyberspace are based on a false dichotomy: the physical and virtual are not opposed; rather the virtual complicates the physical, and vice versa. <sup>[1]</sup>

**“ Whenever technology interfaces with a base human tendency, the result is amplification and acceleration.**

In other words, what happens in the cyber ecosystem can affect the “real” world and vice versa. It is essential that we examine this new environment scientifically to maximise its benefits and avoid potential risk and harm.



**CYBERSPACE  
IS A REAL PLACE**



## CYBERSPACE IS A REAL PLACE

Let me ask a question - one that has been fiercely debated: is cyberspace an actual place? My answer is unequivocal: yes. You may be accessing it from a familiar environment, like the comfort of your home or office, but as soon as you go online, you travel to a different location in terms of awareness, emotions, responses and behaviour. Your reactions will vary depending on age, physical and mental development, and personality traits.

People behave differently when they are interacting with technology, compared to interacting face-to-face with the real world: whenever technology interfaces with a base human tendency, the result is amplification and acceleration. We have all experienced technology-mediated adverse psychological effects, from smartphone addiction-type behaviours to being subjected to social technology “weapons of mass distraction”, which hijack attention, and then harvest, profile, micro-target, monetise and subliminally manipulate us online.

The technology of cyberspace was designed to be rewarding, engaging and seductive for the general population. What we failed as a society to foresee was how it would impact deviant, criminal and vulnerable populations, and how this in turn could affect society. Traditionally, members of extreme or marginalised groups found each other with difficulty. Meetings were limited by the laws of probability and proximity. Now, this probability has changed due to a cyber effect that I describe as *online syndication* <sup>[2]</sup> – the mathematics of behaviour in the digital age – not just for sex offenders and proponents of hate speech, racism, and misogyny, but also for cybercriminals, extremists, and young people with self-harm disorders. My prediction is that this form of hyper-connectivity will lead to more incidences of abuse and criminal behaviour in cyberspace and in the real world.

As a cyber behavioural scientist, my job is to provide insight at the intersection between humans and technology or, as some say, where humans and technology collide. Over time, we have developed protective strategies when it comes to physical crime and white-collar crime, but we urgently need to address cyber-facilitated and cyber-enabled crime. Cybersecurity efforts to date have mainly focused on attacks on critical infrastructure. However, the rise of the Internet of Things (IoT), and soon a predicted trillion connected devices, means that in the near future we will be facing attacks not just on critical infrastructure, but on all infrastructure. Hacking and cybercriminal activity are now ubiquitous; perpetrators are engaging in complex global offensives targeting both individuals and businesses. While delivering on connectivity, the Internet of Things increases the threats. We, therefore, need to develop cyber situational awareness, and step up security in cyber contexts.

### So how do we do this?

I contributed to the recent ARM<sup>[3]</sup> *IoT Security Manifesto*<sup>[4]</sup> initiative and my observations were that security is not always built into devices and systems by default; this is compounded by too many assumptions from users regarding their security which generates a false sense of protection – fake safety. Many cyber attacks work because of a lack of digital hygiene, a lack of security by design and importantly a lack of user awareness. Paradoxically, younger generations of users are more digitally savvy, but can be even more complacent about cybersecurity. As academic experts, designers, developers and engineers, we need to care more about the consumer. We need a human-centred approach that is mindful of how humans actually use connected “things”, and not how the tech sector presumes or expects them to.

Cybercrime has also a significant economic impact. The 2018 *No Slowing Down* <sup>[5]</sup> report from McAfee and the Center for Strategic and International Studies estimated that cybercrime now costs businesses close to \$600 billion, or 0.8 percent of global GDP. According to Steve Grobman, Chief Technology Officer for McAfee, “the digital world has transformed almost every aspect of our lives, including risk and crime, so that crime is more efficient, less risky, and more profitable, and has never been easier to execute.” So-called Darknet markets, the unscrupulous bad neighbourhoods of the Internet that are not indexed by standard search engines, are facilitating cybercriminal activity, ranging from ransomware attacks, to identity theft and cyber fraud. However, the cost of what goes wrong in cyberspace is not just financial. We are also paying a high price in human terms, with the evolution of trolling, and online bullying, the rise in sleep interruption and deprivation, the surge in anxiety and depression in young people associated with technology use, the widespread commercialisation of human data, and the gamification of electoral processes, evidenced by the manipulation of constituents’ behaviours online. <sup>[6]</sup>

### **What can we do about this?**

Can experts illuminate this intersection between humans and technology, where humans and technology collide? Can they predict evolutions, identify problems, brainstorm answers, create solutions, and offer advice on cyberspace?



# NEW SCIENTIFIC FRONTIERS

## NEW SCIENTIFIC FRONTIERS

The scientific study of cyberspace began in the early 1990s. Researchers attempted to analyse and predict human behaviour mediated by technology, but these attempts were only partially successful. Very often findings concerning specific types of behaviours could not be described and explained by traditional psychological theory when applied in technology-mediated environments. Now, as we delve even deeper into cyberspace, difficulties with some fundamentals of psychology are becoming increasingly apparent.

Traditional research funding models may not suffice either and arguably the three- to five-year research cycle is becoming increasingly redundant. It is likely, if not probable, that rapid technological developments will overtake the phenomenon under study before it is completed and findings are published. We need accessible funding for “rapid research” initiatives, and we urgently need to broaden scientific investigation. Governments, policymakers and stakeholders along with academics from a wide range of disciplines who embrace cyberpsychology<sup>[7]</sup> will undoubtedly contribute to crystallising new ideas and perhaps to understanding and conquering this new scientific frontier.

**“ We need accessible funding for “rapid research” initiatives, and we urgently need to broaden scientific investigation.**

One of the earliest discoveries in the field of environmental psychology came from Roger Barker’s work in ecological psychology. His field observations in Oskaloosa, Kansas, in the 1940s expanded into the theory that social settings influence behaviour. He developed the concept of the “behaviour setting” to help explain the relationship between the individual and the immediate environment, and how a setting affects its inhabitants.





In 1987, the environmental psychologist Harold Proshansky<sup>[8]</sup> discussed how the field was “value-oriented” due to environmental psychology’s commitment to bettering society through problem identification. This is a valuable observation when it comes to cyber society.

Proshansky, however, only considered environment as a real-world construct. Understandably, his research at the time did not extend into cyberspace. Cyberpsychologists, however, do consider psychological aspects of environments created by computers and online networks. Professor John Suler, the father of cyberpsychology, provided in his groundbreaking work *The Psychology of Cyberspace* an evolving framework for understanding how people react to and behave in cyberspace. The experience created by computers and computer networks should in many ways be understood as a psychological “space”. When users power up their computers, launch a program or app, write an e-mail, or log on to a social technology platform, they feel either consciously or subconsciously that they are entering a “place” or “space.” In terms of considering cyberspace from a classic environmental psychology perspective, many users who have connected to a remote computer and explored the Internet or navigated the murky depths of the deep web describe the experience in terms of travel or “going someplace”. These and other spatial situational metaphors, such as “worlds”, “domains”, “forums” or “rooms”, are commonly used online and support a construct of environment. The literature on human cognition argues that we use place and space-based metaphors for the Internet because our cognitive makeup dictates that we must – in other words, humans are embodied, situated beings, who reason spatially.

The image features three soldiers in silhouette, positioned on the right side of the frame. They are holding rifles and appear to be in a field or on a hillside. The background is a clear, light blue sky. The overall mood is serious and tactical.

# THE THREE LAYERS OF CYBERSPACE

## THE THREE LAYERS OF CYBERSPACE

However, we are not alone – the military also reasons spatially. The most significant official recognition of cyberspace occurred in 2016 when NATO acknowledged it as a new frontier in defence <sup>[9]</sup>, formally recognising that modern battles are waged not only by air, sea and land, but also on computer networks. In fact, a military definition of cyberspace has existed for some time, i.e.: the Armed Forces of the United States joint publication on Cyberspace Operations describes three layers of cyberspace <sup>[11]</sup>: the Physical Network, the layer of cyberspace comprised of the geographic components and physical network components; the Logical Network, the layer which consists of those elements of the network that are related to one another in a way that is abstracted from the physical network and the Cyber-Persona layer – that’s us – humans.

“ [...] the global domain within the information environment consisting of the interdependent networks of information technology infrastructure and resident data including the Internet, telecommunications networks, computer systems and embedded processors and controllers. <sup>[10]</sup>

While the military has a multi-layered and strategic understanding of cyberspace, the European Union sees it merely as a form of “infrastructure” – something like a railroad or motorway. The Internet may be many things, but it is not simply infrastructure; it is an entity that can have an almost overwhelming impact on individuals and society. The technological revolution that delivered connectivity, computers and cyberspace has produced seismic changes for our species – we have had to evolve and adapt to keep up with this rapid change. It has been argued that human culture, which society represents, provides a buffer against facing one’s vulnerability and mortality. Humans need other people for basic survival and over time we have developed some core behaviours when interacting with social situations to help us survive in groups. In other words, humans are highly motivated to get along with others simply because it’s adaptive to do so, i.e. these actions and/or behaviours aid or ensure basic survival.

$$E = mc^2$$






## THE CYBER EFFECT

Humans are now desperately trying to adapt in cyberspace. However, as biological beings we struggle to keep pace with technical advancements – a form of Moore's law of human behaviour. One such example is increasing levels of narcissism and decreasing empathy online, embodied in heightened detachment from the feelings and rights of others online. We see this in extreme harassment and malicious trolling. Anonymity online, the mythical superpower of invisibility, fuels this behaviour, as does a phenomenon known as the *online disinhibition effect*, which can cause individuals to be brasher, judgment-impaired and less inhibited – almost as if they were inebriated. Desensitisation is another effect, a result of access to endless amounts of violent and extreme content in both mainstream and online media. Human behaviour is often amplified and accelerated online, by what I believe to be an almost predictable mathematical multiplier, a "cyber effect", arguably the  $E = mc^2$  of this century.

My recent book regarding this phenomenon, *The Cyber Effect*, was reviewed extensively and well received.<sup>[12]</sup> One particular review by Bob Woodward, the American investigative journalist of Watergate fame, made me stop and think: Woodward wrote, "Just as Rachel Carson launched the modern environmental movement with her *Silent Spring*, Mary Aiken delivers a deeply disturbing, utterly penetrating and urgently timely investigation into the perils of the largest unregulated social experiment of our time."<sup>[13]</sup>

A close-up photograph of a bumblebee on a yellow flower. The bee is the central focus, with its black and yellow body and fuzzy texture clearly visible. It is positioned on a bright yellow, tubular flower. In the background, a large, soft-focus pink flower is visible, creating a vibrant, natural setting. The lighting is bright, highlighting the textures of the bee and the flowers.

**“ These sprays, dusts and aerosols are now applied almost universally to farms, gardens, forests and homes – non-selective chemicals that have the power to kill every insect, the ‘good’ and the ‘bad’, to still the song of the birds and the leaping of fish in the streams, to coat the leaves with a deadly film and to linger on in the soil – all this though the intended target may be only a few weeds or insects. <sup>[14]</sup>**

I am deeply indebted to Woodward for this observation. Rachel Carson was a renowned author and a former aquatic biologist with the US Fish and Wildlife Service, whose 1962 book *Silent Spring* painstakingly documented adverse effects of the indiscriminate use of pesticides on the environment. Her work provided an unequivocal argument that powerful synthetic insecticides such as DDT were poisoning food chains, killing insects and birds.

Carson's *Silent Spring* has been described as "one of the most effective denunciations of industrial malpractice ever written".<sup>[15]</sup> Although her book met with fierce opposition by chemical companies, the outcry that followed its publication forced the banning of DDT and spurred big changes in the laws affecting air, land, and water. Her impassioned plea regarding the future of our planet reverberated worldwide. The most evocative and well-known chapter, "A Fable for Tomorrow", portrayed an American town where all life, "from fish to birds to apple blossoms to human children", had been silenced by the insidious effects of DDT. Carson's work was instrumental in raising popular global ecological awareness and advancing the global environmental movement.

Around the same time, American psychologist and computer scientist Joseph Carl Robnett Licklider published his landmark paper *Man-Computer Symbiosis*. His vision was that man and technology could work together to accomplish great things. Licklider likened it to the symbiotic relationships found in nature, such as an insect pollinating a fig tree.<sup>[16]</sup> While the two are dissimilar organisms, they are nonetheless heavily interdependent, in other words they need each other to survive.



**GDPR**

## ALL INTERNET USERS ARE NOT EQUAL

While Licklider believed that humans and technology could collaborate in a mutually sustaining manner, Carson was less optimistic. Her central proposal was that, at times, “technological progress is so fundamentally at odds with natural processes that it must be curtailed”.<sup>[17]</sup> I believe this assertion resonates today. Is contemporary technological progress now at odds with humankind? My real concern is the impact of technology on developing children, particularly those who are growing up with cyberspace. The Internet was designed as a democratic environment in which all users are treated and regarded equal. However, all Internet users are not equal: some are more vulnerable than others and few special allowances have been made for children online. However, they deserve particular attention. We are living through the largest unregulated social experiment of all time – a generation of young people has been exposed to the best and worst aspects of this new technological environment.

**“ All Internet users are not equal: some are more vulnerable than others and few special allowances have been made for children online. However, they deserve particular attention.**

In May 2018, Europe introduced the General Data Protection Regulation (GDPR), which significantly changed data protection law in Europe, strengthening the rights of individuals and increasing the obligations on organisations in cyber contexts. One of the most important aspects of the GDPR is the protection of children. Article 8 of the GDPR addresses the “Digital Age of Consent” – i.e. the age at which children have the power to let a social media company gather their personal data and profile them. The GDPR sets this age at 16 years by default, but allowed Member States to reduce this to 13. In Ireland, my fellow campaigners and I believed that there were considerable risks associated with enabling children to use social media services that process their personal data for marketing/targeting /commercial gain.





We are convinced that it is critical to protect children from complex algorithmic profiling, which they do not understand and most adults do not understand either. We must be extra careful with young teenagers, who are at a phase of development during which they are vulnerable to influence and manipulation. For this reason, we campaigned to keep parents involved in the lives of young people online, just as they are engaged in the real world. On the legislative front, we were successful. The Digital Age of Consent in Ireland is now 16. This is important in geographical terms, as many social technology companies have headquarters in my hometown of Dublin. <sup>[18]</sup>

The GDPR is a giant step forward in cyberspace regulation, providing protection and control for individuals' personal data. It significantly increases the obligations and responsibilities for organisations and businesses with regard to how they collect, use and protect personal data. The new law requires organisations and companies to be fully transparent about their use and safeguarding of such data. Fundamentally, it represents a culture change for enterprises that operate in this space. They will need to adapt and will be accountable for data-processing activities. However, the GDPR is just one area of protection concerning the data of adults and minors; there are many more problem areas affecting children and young people that must be addressed. These include the ever-increasing scourge of cyberbullying, along with exposure to age-inappropriate content online, such as extreme violence, self-harm material, and adult pornography. As children increasingly navigate and habitate the exciting new world of cyberspace, we need to step up our efforts to address these pressing issues to ensure that – just as Rachel Carson wrote – we protect children from toxic fallout.

It is time to stop, put down our devices, close our laptops, log off, take a deep breath, and do something that humans are uniquely good at.

We need to think. We need to think a lot.





# A HOLISTIC OVERVIEW

## A HOLISTIC OVERVIEW

We need to talk about cyberspace – we urgently need new ideas. We need to find answers and solutions. I am convinced that we can conceptualise technology solutions for technology-facilitated problematic behaviours. Until now, most academics have been looking at the cyber environment through the myopic lens of their individual disciplines. We must take a holistic, gestalt-like overview to improve our understanding. As the network scientists say, it's all about sense-making. We need to make sense of what's happening.

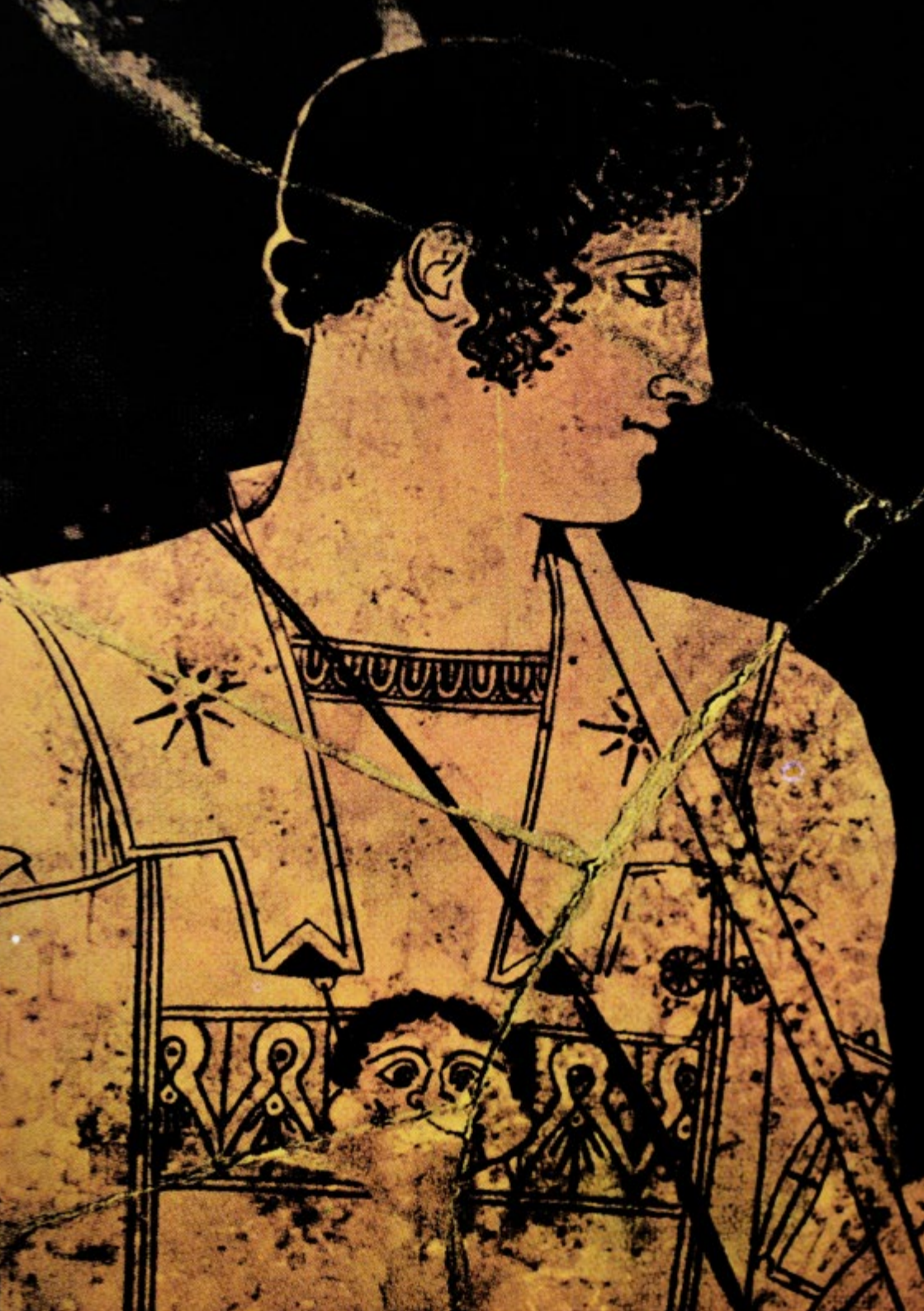
**“ Billions of us now use the technologies of cyberspace unthinkingly, in the same way we breathe air and drink water. It is an integral part of our developmental, social, professional and personal lives.**

The best approach is transdisciplinary. We need expert input from a wide array of disciplines to illuminate the problems and devise the best solutions. We need to stop expecting individuals to manage cyber issues for themselves or their families. Science, industry, governments, communities and families need to come together to create a roadmap for cyber society.

However, some will object.

If we think about cyberspace as a continuum, on one side we have idealists, keyboard warriors, early adopters, and philosophers who feel passionately about the freedom of the Internet and the independence of cyberspace, and don't want that weighed down with regulation and governance. On the other end of the continuum, we have the tech industry with a pragmatic vision of freedom of the Net that is driven by a desire for profit and concerns that governance and restrictions will impact the bottom line. These two very different groups are somehow strategically aligned in cyberspace, and holding firm.





The rest of us and our children – the 99.9 percent – live somewhere along the continuum, in the middle, between these vested interests. Billions of us now use the technologies of cyberspace unthinkingly, in the same way we breathe air and drink water. It is an integral part of our developmental, social, professional and personal lives. We depend on it for our livelihoods and lifestyle, for our utilities, opportunities, networking and even our education. However, at the same time, we have little or no say about this new frontier, where we are all living and spending so much of our lives. Most of our energy and focus has been to simply keep up with a cyber learning curve that gets steeper every year. As we know from environmental psychology, when you move to a new location, it takes time to adapt and settle in. Before we get too settled, let's make sure this is what we want and where we want to be.

Cyber effects can tap into our developmental or psychological Achilles' heel: while making us feel invincible, these effects can diminish us, and distract us from things in life that are much more important, more vital to happiness, and more crucial to our survival. Let's debate more, and demand more.

Our biggest problems with technology usually come down to design. The cyber frontier is a designed universe: if certain aspects of it do not function, those aspects should be redesigned. I can't help but wonder how different the Internet would be if women had participated in greater numbers in its design. Studies show that in business female directors are "less constrained" in their problem-solving skills than male directors. Research findings also support that "Women seem to be predisposed to be more inquisitive and to see more possible solutions,"<sup>[19]</sup> – I find it intriguing that, 100 years after the suffragette struggle and the hard fight for women's rights, we have migrated and are populating a cyber space that is almost exclusively designed and developed by men. We need more women to lean in, make decisions and problem-solve in this sphere.





WhatsApp



Twitter



Telegram



Snapchat



Instagram



Facebook

## THE PRECAUTIONARY PRINCIPLE

In pursuing solutions, we can learn from the legacy of Rachel Carson, who raised awareness regarding humanity's potential to wreak havoc on nature. In an age of technology, we need to focus on our ability to wreak havoc on ourselves, on our potential. We are living in a new environment, cyberspace, but we are not taking care of it and, more importantly, we are not insisting on accountability in this space.

In 2017, a horrific video titled "Easter day slaughter" was posted on Facebook: a man filmed himself killing an apparently random victim. The killer published his crime in real time on Facebook. By the time it was taken down, the graphic footage of a live killing had been viewed over 150,000 times – we don't know how many of the viewers were children. I subsequently wrote an article for *TIME* denouncing the live-streaming of murder.

**“ [...] acts of murder were once reported after the fact, on the news, or were only available in the deepest and darkest parts of the web, so-called ‘snuff’ content. Now it appears killing has become a form of live engagement on social media, generated and distributed by pathological and criminal cyber exhibitionists. <sup>[20]</sup>**

Who is responsible when extreme content disastrously spills online – especially by means of technologies that are used by children and young people? Who is to blame: the individuals who commit the extreme acts, those who share the images and videos, the anti-social technologies that spread them further, or all of these? As a society, we need to decide who is responsible. Does the fault lie with service providers, software companies, or the leadership behind them? Moreover, what is the responsibility of social technology platforms? What is our collective position regarding “content pollution” of cyberspace?



Here's an idea. The environmental movement's "precautionary principle" places the onus on industry to protect the real-world environment. This could also be a principle in cyberspace. Just as oil companies have been forced – by the media, governments and social and environmental activists –to clean up damage, leaks, and pollution related to their products, cyberspace enterprises need to be responsible for spills and effects regarding humanity. We need new standards and new frameworks for our concerns. The clean-up measures are time-sensitive and need to begin soon. Also, let's use machine intelligence solutions to do the dirty work, not young content moderators from developing countries who are employed as human filters to clean up the worst excesses of the Net, and are traumatised while doing so. At an EU policy summit in Brussels in 2018, I argued that the words "content moderator" would in time be considered as a human rights issue, along with human trafficking and forced child labour. Let's not forget that a social technology moderator is also somebody's child.

**“ We need new standards and new frameworks for our concerns. The clean-up measures are time-sensitive and need to begin soon. ”**



VICTORY  
FAITH  
LEAD  
STYLE  
KNOWLEDGE  
CHANGE

EMPOWER  
CAPABILITY  
MOBILIZING  
COACHING  
LEADER

EXAMPLE  
VISION  
EXAMPLE

INSPIRATION  
GROWTH  
HABITS  
TRAITS  
INTELLIGENCE  
MOTIVATION

CHARACTER  
VALUES  
RESPONSIBILITY

# LEADERSHIP

COMPETENCIES  
ACTION  
COMMUNICATION

ACHIEVEMENT  
COMMITMENT

AID  
SOCIAL  
INFLUENCE  
SUCCESS  
POWER  
ENTHUSIASM  
ENERGY

SKILLS  
PASSION

GUIDE  
MOTIVES

BEHAVIOR  
TASKS  
IDOL  
CHARISMA  
SUPPORT  
PRIORITY

On the cyber frontier, we need thought leaders who are prepared to nail their colours to the mast and back their informed instincts. Of course, we need evidence-based studies over time, but how long can we wait? Babies are being born, kids are growing up in the cyberworld, and lives are being changed. Society is being reshaped. We urgently need to reconsider how we handle behavioural problems in this new environment, which are evolving at the speed of technology. I don't believe scientific breakthroughs are achieved by sitting on the fence. We need cyber leadership, and we desperately need "academic first responders".

We are living in a unique period of human history, an intense period of flux, change and disruption that may never be repeated. This moment in time is not unlike the Enlightenment of the 17<sup>th</sup> and 18<sup>th</sup> centuries, when there were significant shifts in awareness, knowledge and technology, accompanied by great societal changes. Some changes have been seductive and incremental, and have caused psychological norms to creep into new places, while others have been sudden and alarming. We need to start thinking and talking about the profound and pervasive impact of the technological environment of cyberspace on the individual and on society.

What is new is not always good. Technology only brings progress when we are able as a society to mitigate its most harmful effects.



## Notes

- [1] Slane, Andrea, "Democracy, Social Space and the Internet", *University of Toronto Law Journal*, 57:81-104, 2007
- [2] Aiken, Mary P., *The Cyber Effect*, New York, Random House, Spiegel&Grau, 2016
- [3] ARM technology is at the heart of a computing and connectivity revolution that is transforming the way people live and businesses operate. ARM advanced, energy-efficient processor designs have enabled the intelligent computing in more than 125 billion chips. Over 70% of the world's population are using ARM technology, which is securely powering products from the sensor to the smartphone and the supercomputer.
- [4] *IoT Security Manifesto*, <https://pages.arm.com/iot-security-manifesto.html>
- [5] <https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/economic-impact-cybercrime.pdf>
- [6] Aiken, Mary P., *Manipulating Fast, and Slow*, 2018  
<https://www.wilsoncenter.org/article/manipulating-fast-and-slow>
- [7] Cyberpsychology is the study of the impact of technology on human behaviour. The field is rapidly evolving from an emerging to an established field within applied psychology. It is expected to enjoy exponential growth in the coming decades due to continued rapid growth of Internet technologies and the unprecedented, ubiquitous influence of the Internet on humans.
- [8] Proshansky, Harold M., "The Field of Environmental Psychology: securing Its Future", *Handbook of Environmental Psychology*, eds. Daniel Stokols and Irwin Altman, New York, John Wiley & Sons, 1987
- [9] <https://www.wsj.com/articles/nato-to-recognize-cyberspace-as-new-frontier-in-defense-1465908566>

- [10] [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf?ver=2018-07-16-134954-150](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150) (JP 3-12: V)
- [11] [http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3\\_12.pdf?ver=2018-07-16-134954-150](http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf?ver=2018-07-16-134954-150) (JP 3-12: I-3)
- [12] *The Cyber Effect* selected as one of the best science picks of the week in 2016 by Nature, and chosen as a UK 2016 Times Book of the Year in the Thought Category
- [13] <http://www.maryaiken.com/cyber-effect/>
- [14] Carson, Rachel, *Silent Spring*, Boston, Houghton Mifflin, 1962
- [15] <https://www.theguardian.com/science/2012/may/27/rachel-carson-silent-spring-anniversary>
- [16] "The fig tree is pollinated only by the insect *Blastophaga grossorum*. The larva of the insect lives in the ovary of the fig tree, and there it gets its food. The tree and the insect are thus heavily interdependent: the tree cannot reproduce without the insect; the insect cannot eat without the tree; together, they constitute not only a viable but a productive and thriving partnership. This cooperative 'living together in intimate association, or even close union, of two dissimilar organisms' is called symbiosis."
- [17] *The Story of Silent Spring*
- [18] Opening Statement by Professor Barry O'Sullivan MRIA and Adj. Assoc. Professor Mary Aiken to the Oireachtas Joint Committee on Children and Youth Affairs
- [19] <http://business.financialpost.com/executive/executive-women/women-on-corporate-boards-better-decision-makers-than-male-directors-study>
- [20] 'Facebook Must Stop Live-Streaming Murder From Becoming the New Normal'  
<http://time.com/4746708/steve-stephens-facebook-killing/>

## BIOGRAPHY

Dr Mary Aiken is an Adjunct Associate Professor at the Geary Institute for Public Policy University College Dublin, Ireland. She is an Academic Advisor (Psychology) to Europol's European Cybercrime Centre (EC3), and a member of the EC3 Academic Advisory Network. Mary is a Global Fellow at the Wilson Center, the leading US institution for in-depth research and dialogue to inform actionable ideas on global issues. She is a lecturer in Criminology and Fellow at the School of Law, Middlesex University, and Fellow of the Society for Chartered IT Professionals.

In 2017, Dr Mary Aiken was inducted into the Infosecurity Europe Hall of Fame, in recognition of her contribution to the information and cybersecurity sector. She is a strategic advisor at European and International levels in policy debates on the impact of technology on human behaviour, and has published and spoken worldwide on this topic. Her research interests include forensic cyberpsychology, AI, human factors in cybersecurity, Internet psychology, organised cybercrime, cyber criminology, behavioural manipulation online and the rights of the child in cyber contexts. Dr Mary Aiken is a member of the Advisory Board of The Hague Justice Portal - a foundation for international peace, justice and security. She is a Strategic Advisor to the European Paladin Capital Group Cyber fund.

Mary's groundbreaking work inspired the CBS prime time television series *CSI: Cyber*. Her recent book *The Cyber Effect* was selected by the Times as 2016 Book of the Year in the "Thought Category", and 2016 Best Science Pick by *Nature*, the international journal of science and technology.





**European  
Investment  
Bank**

*The EIB bank*

A circle of twelve five-pointed stars, arranged in a ring, representing the European Union flag.