

SOCIAL CYBER INSIGHTS

SHAPING FUTURES IN AN UNCERTAIN WORLD

Understand how a social cybersecurity approach can contribute to a responsible digital future

KEY POINTS

The digital era is best understood not as a technological revolution per se but one where technologies must be understood in their societal impact.

Leaders and legislators need to take a multidisciplinary approach to understanding and mitigating the broad threats that digital technologies are unleashing on individuals, businesses, societies and democratic systems.

The emerging field of social cybersecurity provides insights and frameworks from the social sciences to develop competency in, and mitigation strategies for, the new digital age.

Like the technological revolutions of the past, the disruptive digital revolution of the 21st century, has brought unwelcome advances in the conduct of warfare and terrorism. Cyberthreats such as malware, viruses, hacking and ransomware have been met with vigilance and measured counterattacks on adversaries. Warfare takes many shapes, however, and a new digital threat to democratic systems now claims our attention. Social media have made individuals, businesses, cultures and nations vulnerable to misinformation and hostile manipulation. The emerging field of social cybersecurity takes a multidisciplinary approach to safety and security in the digitally-mediated world.

HISTORY



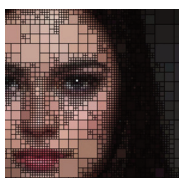
History shows us that disruptive change is not new. We can learn from the past that technological revolutions inflict a seismic impact on the prevailing social order and its cohesion, with gains for a few people and losses for many others.

ECONOMICS



While the US military kickstarted the digital revolution in the 1950s and 60s, private corporations were there from the start and over the next 30 years the internet became dominated by the huge and powerful commercial entities known to us all: Facebook (now Meta), Google, Amazon, Microsoft and others. Amongst the most capitalised companies in the world, their other currency is data. The computational methodology of academic economics can help us to understand the new businesses of data collection and social media.

ANTHROPOLOGY



Industrial anthropology, along with the more focussed digital anthropology, investigates the cultural impact of rapid technological change. For many decades, with admirable foresight, anthropologists have been examining the implications of Artificial Intelligence (AI) and other questions raised by human-technology interaction.

POLITICAL SCIENCE



Political science focuses on the shaping and sharing of power. Many idealistic leaders have been blind to the dangers of the digital revolution, but this is changing. Political science can lay out options for regulative public policy and digital governance. Section 230 Section c (1) in Title V of the US 1996 Telecommunications Act, was the regulation that set the stage for the Internet. It was an effort to block and screen offensive material, however, it defined internet providers as platforms not publishers. Massive unintended consequences flowed from this regulation, which may well be reviewed in response to Facebook’s egregious excesses.

PSYCHOLOGY



Psychologists in the 1960s already knew that negative news travels fastest and furthest (known as ‘negativity bias’) – and that human beings don’t search out information they disagree with (‘confirmation bias’). Policy makers of the 1990s, ironically focussing on the utopian possibilities for social media rather than any negative implications, failed to latch onto these understandings early enough to regulate against and prevent the influential information silos of today’s networked social media or the limitless moneymaking potential of negative news. Psychology can also explain the neurological and behavioural drivers behind the success of the algorithms that reward a user’s connection and interaction with social media.

SOCIOLOGY



The mindset of sociology defines change as something that happens within networks and shows up in everyday life. This is almost the definition of social media. The conceptual tools of sociology equip us to decipher the implications of technological disruption, particularly ‘cultural lag’, when different sectors of culture respond to technological upheaval at different speeds, leaving some sectors behind as others surge forward. The losers become anxious, the winners complacent. In this environment, the Internet, for all its benefits, through ‘hyperconnectivity’ is able to distort, mislead, shatter trust, and manufacture hatred and instability on a scale and at a speed unprecedented in human history.

INTERNATIONAL RELATIONS



Both strategic and commercial interests are observable in the digital era’s geopolitical and corporate competition. International relations studies the risks and threats of the digital world from the perspective of ‘protean’ power, which is uncertain, fluid and unpredictable. Internationally, despite obvious potential to improve democracy using digital technology, the Chinese and Russian central governments, aided by the West’s digital titans, have turned the Internet into a tool that sustains autocracy and manipulation.

Acting together to focus on social cybersecurity, these seven social sciences can deploy their methodologies, tools and intellectual frameworks not only to improve democratic resilience and develop mass competency in the new digital age, but also to help leaders and legislators comprehend, rein in and control runaway technology.

Summary adapted from *Shaping Futures in an Uncertain World: Navigating the human-technology interface through trust and digital governance in the age of information warfare* (2021) written by Don DeBats, Maryanne Kelton and Emily Bienvenue.

This training resource was funded through a partnership with the William and Flora Hewlett Foundation.