

**ESADE**

Ramon Llull University

ESADEgeo-CENTER  
FOR GLOBAL ECONOMY  
AND GEOPOLITICS

**E**

**34**

**Book reviews  
on global economy  
and geopolitical  
readings**

*ESADEgeo, under the supervision of Professor Javier Solana  
and Professor Javier Santiso.*



Fundación  
**REPSOL**

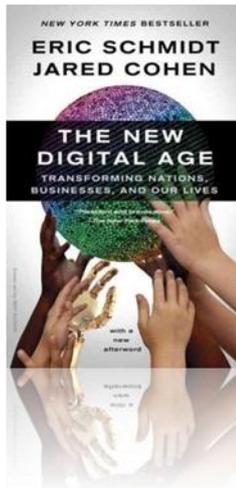


Obra Social "la Caixa"



# The New Digital Age: Reshaping the Future of People, Nations and Business

**Eric Schmidt & Jared Cohen (2013), Alfred A. Knopf, Borzoi Books, New York.**



*“There is a canyon dividing people who understand technology and people charged with addressing the world’s toughest geopolitical issues, and no one has built a bridge.”*

*“By 2025, the majority of the world’s population will, in one generation, have gone from having no access to unfiltered information to accessing all of the world’s information through a device that fits in the palm of the hand.”*

*“The consequence of having more citizens informed and connected is that they’ll be as critical and discerning about rebels as they are about the government.”*

*“The vast majority of the world will be net beneficiary of connectivity, experiencing greater efficiency and opportunities, and an improved quality of life.”*

## Summary

What will the world be like when technology reaches every corner of the planet, as expected within a decade? This is the question that Eric Schmidt and Jared Cohen tackle in *The New Digital Age*, a book about the opportunities and dangers posed by this new era. How will the connection of five billion people to the internet affect nation-states, our personal lives, and concepts such as privacy, information, revolution, and terrorism? Global connectivity will arrive much sooner than expected, and by 2025 computers will be 64 times faster than today. However, these changes will not affect everyone equally, and it will be people living in the least developed nations who benefit the most.

Meanwhile, nation-states must be prepared for the enormous influence that technology will have on diplomacy. At the individual level, there are two realms of daily life and relationships – the physical world and the online world – and government policies will have to adapt to operating on two levels in the same way. In addition, cyber-terrorism will find new tools and channels, increasing the need for new mechanisms to control terrorism.

Almost the entire world will have access to a huge amount of information, and this will provide citizens with a wide variety of arguments both for and against their

governments – as well as non-state insurgent groups. The centres of power will diversify into a new digital age: something that can already be seen in applications for voice identification and medical diagnosis. The true magnitude of these changes will become apparent as people with mobile phones increasingly gain access to the largest databases ever assembled.

## The authors

**Eric Schmidt** (Washington DC, 1955) was CEO of Google from 2001 to 2011 and was on the board of Apple from 2006 to 2009. Schmidt is a science and technology adviser to the American and British governments. He also chairs the board of the New America Foundation, and is a trustee of the Institute for Advanced Study at Princeton University.

**Jared Cohen** (Weston, Connecticut, 1981) is the director of Google Ideas and adjunct senior fellow at the Council on Foreign Relations. He graduated in history and politics at the University of Stanford, and studied a master's in international relations at Oxford as a Rhodes scholar. Cohen advised American secretaries of state Condoleezza Rice and Hillary Clinton on counterterrorism, and is now advisor to the National Counterterrorism Center. He is the author of several books, including *One Hundred Days of Silence* and *Children of Jihad*, and was named by TIME magazine as one of the 100 most influential people in the world.

## Key ideas and opinion

The authors represent two generations of influential personalities in the field of new technologies, and this depth of experience lends added credibility to their predictions about what the world will be like when almost everyone is online. **They point to 2025 as the date when five billion people will be interconnected using the fastest computers ever** and this forecast should set some alarm bells ringing. **Both the rulers and the ruled must consider new ways of relating to each other**, as well as considering new ways of guiding international relations, and handling controversial problems linked to **privacy** and **database management**, which will multiply over the coming decades.

**Schmidt and Cohen paint the broadest possible picture of the future**, and even predict how we will spend our early morning hours in the new technological dawn: gently waking without an alarm clock; savouring the smell of freshly brewed coffee; enjoying a pleasant massage provided by a high-tech bed; using health applications to scan our skeleton to see if any bone is broken; checking holograms that project our diary for the day; and listening to sensors inside our shoes that warn us not to be late for an appointment. However, it is their **predictions for the future of government**,

**terrorism, and social revolutions** that merit closer attention and justify the (sometimes too categorical) tone of their predictions.

For the authors, the image of the future is crystal clear and they are even certain about how technology will affect everyday lives in places currently without electricity. **There are moments in the book when we might appreciate the authors expressing a little uncertainty** as they confidently explain how the new virtual world must coexist alongside the physical world – sometimes for the better and sometimes for the worse. **Many of their conclusions are already obvious in events such as the Arab Spring or the revolution in the Ukraine:** the impact of technology on communication will bring a shift in power away from governments and institutions, and towards individuals. This is the challenge for the future: it is essential that there is a human hand guiding the way, so that the future depends on how we handle technology, and not the other way around.

### The future of identity, citizenship and media coverage

The virtual global population over the next decade (in terms of users with profiles in multiple networks) will exceed the physical population. The result will be vast internet communities and huge amounts of data. The authors believe that **this increased volume of information is generally good news for everyone**. However, dangers arise in the management and use of this data – especially by governments – and the degree of respect given to privacy. **Identity theft and theft of personal information** may increase with this flood of information, a matter the authors discuss with **Julian Assange – the founder of WikiLeaks**. Assange hopes for a world based on complete openness and transparency – yet this will be difficult to achieve because states will enhance their ability to control and censor information.

On the controversial issue of **privacy**, the authors remind us that **the ‘delete’ button has been removed**. Everything is recorded and people should be as careful about what they do online as they are in the physical world. We must fight for privacy or it will be lost forever. The **traditional media** will have to contend with the presence of increasing numbers of spontaneous reporters using mobile phones to tell us in real time what is happening around the world. **The importance of the traditional media could decline and its future will lie mainly in its legitimacy as a source of verification and interpretation of news events.**

For Schmidt and Cohen, it is clear that **democracies** will be further influenced by citizens closely watching the activities of politicians. **Poor autocracies**, meanwhile, will make considerable efforts to acquire the tools to dominate the virtual world – while **richer dictatorships** will eventually build modern police states to tighten control over their citizens. All states will have to **restructure their national and international policies, designing two versions: one for the physical world and another for the virtual world.**

## The future of states

In this chapter, the authors discuss the **balkanisation of the internet**. This refers to **each state implementing its own models of control and legislation on the world wide web**, basing these measures on the regulation of the physical world. Internet as a global concept is being fragmented into national networks, and the authors describe the **three main models**, starting with **China**, where the state applies highly restrictive information filters. The authors also emphasize the ‘sheepish’ model implemented in **Turkey** and elsewhere, where rulers attempt to manage the pressures between separate religions and tendencies within their populations by discreetly controlling or censoring certain websites or domains. The third – and most common – model openly controls, or restricts, the internet with the support of national legislation. This is the case of **North Korea**, but also **Germany**, where pages that provoke racial hatred, or deny the Holocaust, are eliminated.

The authors discuss several interesting concepts, such as *virtual asylum* or even *virtual citizenship* for dissidents who are not allowed to use the internet in their own countries and so ask to express themselves through the internet of other nations. Another future trend is *virtual multilateralism* based on actions of political or ideological solidarity that, for example, protect industries vulnerable to foreign threats.

As for the **dreaded cyber-attacks**, which are dangerous and difficult to persecute, the authors point out that although today only a few countries can currently launch such attacks, there will be many more in the future. **As a protective measure against attack, spaces of cyber-influence will be created**. These spaces will generate new groupings with rules of engagement **that will partially resemble the Cold War** in aspects such as espionage, war by proxies, and a limited civil presence (given the specific and complex skills required). As in the Cold War, the margin for error is immense and there is a **great likelihood of error in the risk assessment, which will cause some cyber conflicts to escalate into true wars**.

## The future of the revolution

Global connectivity will create a greater number of revolutionary outbreaks but, as shown by the Arab Spring, they will not all result in full revolutions and real, effective policy changes. The cause of these failed revolutions is a lack of strong leaders to occupy the space that arises after an uprising. Information technology creates space for expressing opinions, while proclamations can be rapidly broadcast worldwide. New technologies have erased the limits of age, gender, or socio-economic status that previously prevented some sectors of society taking part in a revolution (as demonstrated by the active presence of women in the Arab Spring). Thanks to the internet, people can participate while taking only a minimal physical risk. The consequence of these changes will be the birth of the most active and global civil society in history.

Revolutions will be easier to start, but more difficult to finish. Technology cannot create individuals with the attributes necessary to be good political leaders and, indeed, the armies of young people who ignite revolutions by tweeting do not usually include thinkers who can lead the way to a coherent political transition.

## The future of terrorism

Just as revolutions will expand their reach through technology, the same will happen with messages broadcast by **terrorist groups**, and their actions will become even more visible through social networks. Moreover, **recruitment, training, and the implementation of attacks will increasingly go through virtual channels**. However, the authors claim that the **virtual world will also make life harder for terrorists, mainly because of the increasing risk of being located** through the electronic devices they use. **Osama Bin Laden** understood from the very beginning that absolute disconnection was the only way to avoid being captured and remained in technological isolation for five years – something which, in turn, reduced his influence within Al Qaeda. Terrorists also have less room for error in the virtual world, where a single photo taken with a mobile phone can provide geolocation data.

Recruits to **cyber-terrorism** (a term which, the authors point out, cannot be applied to Anonymous or WikiLeaks) tend to be young, and therefore less careful when protecting information – and such youthful behaviour is liable to jeopardise the entire organisation. **The West will continue identifying hackers and persuading them to work for the government** to enhance cybersecurity, meaning terrorists will have to take precautions against these risks. However, governments also tend to use the excuse of ‘national security’ to monitor their own citizens, and a **continuous struggle between privacy and security** will feature prominently over the coming decades.

## The future of conflict, combat and intervention

According to the authors, increased connectivity will change the patterns found in the various phases of an armed conflict (discrimination, persecution, combat, and intervention). **Although technology will reduce risks, it will also complicate conflicts**. Technology will facilitate, for example, **repression**, and give government greater access to data and more effective, ‘clean’ options for the **harassment of minorities** (by blocking their websites or deleting any information about the groups).

**The number of electronically isolated groups will increase** and virtual exclusion will be combined with the dominant tactic so far – legal exclusion. Conflict will also feature multidimensional and **powerful ‘marketing’ wars in which, through social networks, dangerously distorted pictures of conflicts will be presented to the public**. But not everything is bad news for the quality of information on conflicts in the digital age: advances will enable **digital verification** to ensure the accuracy of images and protect against tampering.

It seems clear that in the coming years **we will witness the first smart rebel movement**. Using technology as a new weapon, groups in a conflict can prepare the ground, attract followers, and even create false trails to confuse the enemy – before firing a single bullet. The actual clash, however, will still play out in the physical world.

## The future of reconstruction

**In the phase of reconstruction**, when a conflict has come to an end, **technology is likely to have its most positive effects**. While technology alone cannot rebuild broken societies, it can accelerate the political and economic efforts. The first step after a conflict is the reconstruction and repair of the communications network. Establishing mobile telephone system is essential and was in fact the first priority in Haiti following the 2010 earthquake and after the Egyptian uprising against Mubarak. **In the failed state of Somalia, telecommunications provide the only organised structure** and mobile phones are one of the few systems that has been successfully implemented despite the anarchy that reigns throughout the nation. These devices offer the Somalis jobs, security, and information. Access to digital tools empowers individuals, informs them, and helps create stronger societies.

## The two civilisations of the future

To Schmidt and Cohen, the future is clear. Within a few decades, we will see the coexistence of two civilizations: a physical world that has been developed over thousands of years, and virtual world that is still being formed. Both must coexist as best they can, each helping to resolve the shortcomings of the other. **While the digital world will provide an escape from repressive states, the physical world will apply rules and laws to contain virtual anarchy** and protect people from cyber-attacks. Both civilizations will affect each other in every area of life, and the authors suppose that the result will **be a world that is generally more transparent, egalitarian, and interesting** – providing that people and governments grasp the opportunity in a constructive manner.