



Eidgenössische Technische Hochschule Zürich Swiss Federal Institute of Technology Zurich

Emerging Technologies: Security and Regulatory Concerns

By Nayef Al-Rodhan



Scientific research is no stranger to the battlefield. Technological breakthroughs have often started off in military research labs or prompted by military funding. The trend caught momentum during the Cold War when the superpowers on both sides of the Iron Curtain delegated researchers and huge budgets to the development of technologies of war, space and ocean exploration.

Today, as in the past, security relies on developments from several industries and emerging technologies have a pivotal role in enabling security practices. Take, for instance, border surveillance or illegal immigration

control, which is based on a wide-range of technologies that include: radar systems, optronic sensors (including night vision), nanotechnologies, and biometry (such as face recognition, thermal cartography, or voice-recognition).

The underlying feature of emerging technologies is that they benefit from multidisciplinary approaches. They are prompted by growing convergence among sciences so that technologies and fields previously studied separately are now studied and developed together, such as neuropharmacology or bioengineering, which bring together biologists, engineers, physicists, experts in nanotechnologies and many others. Furthermore, emerging technologies are growing in scope and relevance both for the private and public sectors, or are often developed in joint initiatives.

Nanotechnology, for instance, is explored both by private companies including chemical or pharmaceutical industries as well as the military where the manipulation of matter at the nanoscale is enabling the development of innovative machines or technologies, with varied applications, such as nanoair vehicles (nanospies), or nanoparticles which are tested for body armour and infrared thermal sensors. Similarly, developments with artificial intelligence are now bringing outstanding results for the military. Unmanned vehicles or autonomous weapons, which employ sophisticated pattern-recognition software, are critical to US military operations.

New opportunities are also currently explored with the science of stealth and invisibility, which is already financed by several governments in coordination with research centres and private companies. The principle behind it is simple and fascinating: to develop technologies to render physical presence (including of soldiers, tanks etc) invisible to radars and to the human eye. This is based on the study of light-absorbing meta-materials or nano-sized metal structures which create optical illusions both in visible and infrared environments. The US leads in this field, but other countries like China and Japan are proving a keen and growing interest in stealth research. China`s central government for example, has already reportedly funded at least 40 research teams to develop the "invisibility cloak" for military applications.

Another emerging technology, 3D printing is not only set to change manufacturing but it is now catching up in the military, defence and aerospace which can use additive manufacturing to reduce costs (for instance, by reducing material waste during production). At the same time, this raises security concerns as the possibility to 3D print is virtually unconstrained, thus allowing the printing of weapons by anybody, including non-state actors or private individuals, as well as advanced counterfeiting techniques.

The poorly regulated and fairly liberal environment in which emerging technologies are developing permits both governments and non-state actors to engage with and benefit from them. For that reason, state agencies as well as non-state entities take the potential of emerging technologies seriously, especially given their military applicability.

The rapid pace of developments and spinoffs of emerging technologies renders predictability quite faint. However, a few estimations are possible. Among the range of emerging technologies that are likely to grow in scope and relevance in the near future, I consider *predictive analytics*, now mostly used in financial services, to expand its area of focus and become especially important. Predictive analytics is a field of data-mining which has the main purpose of predicting outcomes and establishing patterns on the basis of computing explanatory variables and predicted variables from the past. This is likely to become increasingly useful for the military, which could input data and employ specialized machine learning algorithms, to develop scenarios and predict security issues.

Brain-computer interfaces are also bound to chart new territories and they will have direct security implications. The possibility to interact with computers through thought alone and on the basis of implanted or external sensors could benefit many patients. However, the same technologies can have deleterious repercussions in the field of cyber security as hackers could use to access sensitive or critical data, hijack systems and manipulate devices.

A few warnings and recommendations are necessary. As the desire to innovate has led to galloping developments with emerging technologies, it is crucial to understand that the absence of clear regulations, laws and ethical guidelines in the relevant industries can cause catastrophic outcomes. This risk is now more urgent than in the past since now private individuals or non-state actors can develop and use emerging technologies more easily.

At the same time, there are other ethical issues to consider. Emerging technologies offer states more instruments and means for control and surveillance, which at the same time, lead to severe infringements of civil liberties. Striking the right balance between the need to collect information and the respect for privacy remains an ongoing and pressing challenge. Furthermore, some of the emerging technologies which were just in initial states a decade ago have now proven outstanding potential to modify the foundations of our existence. I am referring notably to research on cognitive enhancement, biomedicine or synthetic biology, which bring along much more complex risks and dangers for our human future. The possibility of transhumanism, or radical physical and cognitive transformation, is now on the horizon. This could alter the very foundations of human nature, and of instincts that have been fundamental to our evolution so far.

Innovation has clearly and irreversibly changed and benefited our societies and it will continue to break new grounds and change our lives and societies. At this critical juncture, a powerful reminder needs to guide innovation: the concern for human dignity, security and sustainability. Policy-makers and civil society actors need to work with industries and articulate guidelines that respect and incorporate these considerations across the wide spectrum of emerging technologies.

Nayef Al-Rodhan is a Philosopher, Neuroscientist and Geostrategist. He is an Honorary Fellow at St. Antony's College, University of Oxford, and Senior Fellow and Director of the Centre for the Geopolitics of Globalisation and Transnational Security at the Geneva Centre for Security Policy. He is the author of "The Politics of Emerging Strategic Technologies. Implications for Geopolitics, Human Enhancement and Human Destiny" (New York: Palgrave Macmillan, 2011).

This article was originally published on The International Relations and Security Network website on October 10, 2014. <u>http://isnblog.ethz.ch/intelligence/emerging-technologies-security-and-regulatory-concerns</u>