JOURNAL OF THE SPANISH INSTITUTE FOR
STRATEGIC STUDIES

Ángel Gómez de Ágreda
Colonel of the Spanish Air Force

E-mail: agomde@ea.mde.es

BOOK REVIEW

THE FIFTH ELEMENT

Author: Alejandro Suárez Sánchez-Ocaña, Publisher: Editorial Deusto, Grupo Planeta, 2015. ISBN: 978-84-234-2178-7, First edition. October 2015, (267 pages). http://www.elquintoelemento.net.

ALEJANDRO SUÁREZ SÁNCHEZ-OCAÑA
Autor del bestseller "Desnudando a Google"
EL QUINTO ELEMENTO
ESPIONAJE, CIBERGUERRA Y TERRORISMO.
UNA AMENAZA REAL E INMINENTE
LA REALIDAD QUE TE ESTÁN OCULTANDO:
EL PRÓXIMO 11-S EMPEZARÁ CON UN CLIC
DEUSTO

"The fifth element", by Alejandro Suárez Sánchez-Ocaña is a tale of espionage, war and terrorism from the perspective of new digital technologies and their consequences. Written in a fast-paced but easy-going style, Suárez presents a succession of cyber-attacks, each one hot on the heels of another, to illustrate the risks and threats posed by cyberspace in 21st century society.

On target in most of his evaluations and supporting data, Alejandro Suárez manages to raise the reader's awareness of the vulnerability of the digital world and sensibly includes a section which also addresses its mitigating factors. Published in 2015, the book chronicles attacks that have already become classics in a world in constant evolution and change. Although its conclusions remain valid, the eighteen months that have gone by since the date of its first edition have meant that numerous and very significant events are not included.

The text leads off with the leaked information by the US Department of Defense published by *Wikileaks* in 2010. A model - although obviously not contained in this book - that has become topical once again due to the use of the same medium for leaking files during the recent US presidential campaign.

The next four chapters focus on economic and industrial espionage, crime, terrorism and war, all within a cyber environment. Finally, Suárez comes up with a number of protection measures against cybercrime and devotes a final chapter to looking into the future.

Setting aside its style, which is sometimes apocalyptic, arrogant and messianic, here we have a book that allows us to comfortably explore the rudiments of what is meant by "the fifth element" or the fifth environment, following earth, sea, airspace and outer space.

Thus, as a fifth arena in the theatre of operations, it has also been defined by the Atlantic Alliance and, in a pioneering way, by Spain. In this sense, it should be remembered that, although not stated in the book, the Spanish Ministry of Defence was among the first to consider cyberspace as a Component Command different from traditional Commands. The creation of the Joint Cyber Defence Force, almost coinciding with the publication of the National Cybersecurity Strategy in 2013, gave credence to this stance and provided a practical application to this doctrinal vision.

Despite the recognition of the importance of the digital environment by Spain and practically all countries and international organisations, we can also agree with the author on the current relative lack of awareness in relation to the real scope of the changes which the internet and the whole of cyberspace have brought about.

As is evident from the events described in the book's 267 pages and even more revealingly from recent events and their almost daily occurrence, cyberspace is more than a differentiated environment with regard to physical spaces; it cross-cuts and interweaves with them, rather enabling than complementing them. It is time to cease to regard digital technologies and communications as a support service for the achievement of the goals of physical actors and to begin to see them as a prerequisite for the exploitation of physical and logical capabilities.

In a post-industrial society evolving towards a "zero marginal cost", real added value is to be found in innovation, ideas and concepts. The protection of intellectual property, of plans and projects, and the preservation of privacy have become fundamental values for both individuals and institutions. Both of these - private and public bodies - see how they are the subject of attention and attacks from the entire spectrum of state, business, criminal and private players. Mainstreaming also translates into a symmetry of capabilities.

In the global era, everyone attacks and is attacked by everyone. The Westphalian order which gave states a monopoly in the use of force is rapidly falling apart. Thus, criminals or isolated individuals turn powerful nations into their targets; the United States reacts against the attack on the company Sony - attributed at the time to North Korea - as if it were a national company; the Islamic State provides administrative services on-line and even groups as unstructured as *Anonymous* openly declare war on Israel or Canada.

The theft of the F-35 aircraft plans, designed by Lockheed Martin, resulted in the manufacture of two fifth-generation aircraft models in China after a huge and sudden qualitative leap in its national defence industry which the Americans, displaying a sense of humour, classified as "the greatest transfer of intellectual property in History." Contrary to what one might think, the transfer of knowledge between state and private players is not limited to countries with command economies, as the author points out in one of his examples. Similar transfers and outsourcing also take place between terrorists and criminals.

In fact, according to Alejandro Suárez, the large multinationals in the sector seem to be not simply protected by the excellence of their products, but also by their usefulness to their countries' respective intelligence services, with which they would share the data required from them. The FBI's lawsuit against Apple, which took place two months after the book's publication, may seem to contradict this connection between states and corporations. It is worth remembering that the bureau asked a Californian judge to order Steve Jobs' company to unblock access to a cell-phone belonging to one of the terrorists of the San Bernardino bombing. Apple's refusal - based on its staunch defence of the privacy of its customers - was sustained with the alleged collaboration of a third party in decrypting the device. Apart from the commercial and propagandistic nature of Apple's advocacy in favour of privacy, the case illustrates the contrast between two security models: that of public office, represented by the FBI, and the private sector, which would leave the responsibility of providing this service to their customers in the hands of multinationals.

As recently as 1982, we witnessed the enforced break-up of the Bell telephone company - which held the monopoly of these communications in the United States and Canada - to allow for free competition and free choice in the marketplace. Only a few years later, not only at national level, but also in a global context, the creation of large digital monopolies was allowed and promoted in a turn of events that was remarkable to say the least. Obviously, economic considerations played a considerable role, but it is more than likely that universal access to data from billions of "subscribers" also played its part in the decision.

The book does not go so far as to analyse how hyperconnectivity is affecting our way of life. Ubiquity and immediacy are essential requirements in the 21st century. *I want it all, and I want it now* I was the chorus sung by Queen 18 years ago now: a refrain that has become a way of understanding the life of the generation born at the time. Universal and instant access to everything has come to be considered as a human right, while the culture of effort, planning, patience and sustained illusion has lagged behind.

That same ubiquity that broadens our daily horizons also makes the value of proximity more relative. The contemporary human being has the apparent ability to individualise his life more than at any other time in history. You can generate as many groups, as many gangs as you want to attend to every aspect of your life, but at the same time, each of these groups is increasingly locked in the reaffirmation of their own beliefs with a form of uncritical thinking that seeks no more than applause and "likes" from as many Internet users as possible.

The last pages of "The Fifth Element" bring us closer to a dystopian future with Orwellian overtones. 2017 seems to be rapidly resembling 1984; the difference being that what in Orwell's novel was imposed by a tyrannical state is now incorporated into our lives at our own expense. The book offers numerous examples of how communications and data are being monitored – through geolocation primarily, but also with systems that rely on facial recognition or consumer behaviour - based on technologies that we acquire, enable and use voluntarily every day.

Not only is our very being affected by digital technologies, cyberspace has also become the preferred setting for social relationships. The way in which these develop differs substantially from traditional relationships. Man continues to be the centre of gravity of social and political relations, but the role he plays in them is fundamentally different. The incorporation into cyberspace of billions of connected objects, which has been called the *internet of things*, will exponentially increase the centralised control of our decisions - or at least influence over them – by whoever controls digital content.

In this scenario, cities become intelligent population nodes. Rural life practically disappears from the image of the future if it does not remain connected. Everything is regulated by algorithms that optimise the available options. Still at an embryonic stage at the time of publication of the book, in recent months autonomous cars have begun to make an impression as a clear alternative in the medium term. Their decisions will also be guided by the best option for passers-by, even if it is a less than satisfactory alternative for the passenger. Will it be necessary to redefine Asimov's laws of robotics?

The central chapters of the book provide the reader with multiple illustrations of criminality, terrorism, and war in the field of cyber-security. The three aspects, however, are intimately linked to one another and, on numerous occasions, one has to resort to interpreting the author's intention to classify an action in one way or another.

In a technological environment such as cyberspace, the ability to perpetrate crime is largely based on technical know-how. Individuals with the ability to hack a system may then personally exploit their skills to gain direct benefits or become qualified service providers for criminals, terrorists, or state agents.

Alejandro Suárez describes in the book some of the possibilities offered by the deep internet, the *Deep web*, in which all forms of virus and other malware codes can be found, including the services of cyber mercenaries who, for a small price, provide access to the pages or emails of rivals, adversaries or enemies.

"The fifth element" is a contemporary tale, dealing with burning issues affecting National Security and the security of each one of us. Without getting overly technical, it conveys the need to take action against the vulnerabilities of our digital world. Perhaps one of the most interesting elements is to see how, only a year and a half after its publication, not only the techniques described in the book have evolved tremendously, but also their degree of penetration and the seriousness of their effects on society.

Submited: January 18, 2017.
Accepted: February 15, 2017.