Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
armasuisse
Science and Technology S+T

HIGH LIGHTS

THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

- Megacity
- Energy
- Mobility
- Information
- Communication
- Force-Effect

Publication n° 001 of the decade
January - 2020

Contributors

Maison d'Ailleurs
Swissnex San Francisco
Centredoc
IABG

Details of the publication

Contact
Dr. Quentin Ladetto
Research Director - Technology Foresight
Tel. +41 58 468 28 09
quentin.ladetto@armasuisse.ch

https://deftech.ch
http://sicherheitsforschung.ch

Publisher	armasuisse, Science and Technology, Feuerwerkerstrasse 39, CH-3602 Thoune
Editorial	Research Management and Operations Research, tel. +41 58 468 29 11, www.armasuisse.ch/wt See contributors below
Production	Maison d'Ailleurs, Museum of science fiction, utopia and extraordinary journeys
Translation	Versions Originales Sàrl, Neuchâtel
Reprinting	Reprinting: exclusively by permission from the editorial department © armasuisse
ISBN	978-3-9525175-0-5

Contributors

Maison d'Ailleurs (House of Elsewhere), which was founded in 1976 in Yverdon-les-Bains (Switzerland), is the only museum of its kind in Europe. The museum has more than 130'000 objects related to Science Fiction, Utopia and Pop Culture in its collections. The museum is therefore one of the most important research centres in the field. Every year Maison d'Ailleurs holds several exhibitions, presenting important artists and exploring the main sci-fi themes such as flying cars, futuristic urbanism, video games or superheroes...

Marc Atallah - Frederic Jaccaud - Danilo Pierotti

swissnex San Francisco is part of the swissnex global network connecting the dots in education, research, and innovation. Its mission is to support the outreach and active engagement of partners in the international exchange of knowledge, ideas and talent. The swissnex global network consists of five locations and outposts established in the world's most innovative hubs. Together with around twenty Science and Technology Offices (STO) and Counselors (STC) based in Swiss Embassies, they contribute to strengthen Switzerland's profile as a world-leading innovation hotspot.

Laura Erickson - Birgit Coleman - Perrine Huber - Eryk Salvaggio

On the strength of a multidisciplinary team of engineers, CENTREDOC provides a comprehensive range of services in the fields of technology, commercially sensitive and strategic monitoring, as well as patent, technical and economic information searches. CENTREDOC also provides consultation services for setting up monitoring systems.

David Borel - Rebeca Valledor - Pascal Jauslin - Jean-Baptiste Porier - Princia Yaï - Andreana Daniil - Sébastien Grandpré

Industrieanlagen-Betriebsgesellschaft mbH (IABG) was founded in 1961 at the initiative of the German government as a centralised analysis and testing facility for the aviation and defence ministries. IABG was privatised in 1993 and is today an owner-led European technology company with core expertise in analyses, simulation & testing and plant operation. "Safety" is the common motto for the portfolio: functional safety of technical innovations and the safety of the country, economy and society are at the core of testing activities. In this context, IABG offers technical services for private as well as public-sector customers.

Philipp Klüfers - Pascal van Overloop - Felix Gläser - Antonia Schlude - Sebastian Bech

Table of content

Introduction

Dear Reader,

Our world is changing fast these days. Never before in human history has technology brought about such significant social and economic transformations in such a short time. The democratisation of access to certain technologies that used to be more or less exclusively reserved for government agencies has made forms of conflict possible that were previously unknown or even inconceivable. The institutions responsible for national security therefore have a strategic interest in tracking technological trends and disruptions with a view to anticipating opportunities and threats for civilians and the military alike. armasuisse Science and Technology (S+T) coordinates the necessary research to develop the scientific and technological expertise that we need to confront future threats.

While the digital revolution is already in full swing on the civilian side, it is still in its infancy as far as the armed forces are concerned. The complexity of these changes can only be understood through an interdisciplinary and transdisciplinary approach in which experts at various levels and in various fields address a subject and seek to shed light on it from different angles.

Gaining better understanding of what is happening in the civilian and industrial world is therefore paramount to anticipate, adapt, and ultimately innovate to tailor those new technologies, products and processes to our Swiss specificities.

Let this publication represent a step forward in this direction.

We hope you enjoy reading what follows.

Dr. Thomas Rothacher
Director
armasuisse Science and Technology

Dr. Hansruedi Bircher
Director of research
armasuisse Science and Technology

Introduction

Dear Reader,

This publication (which we hope is original in its structure and content) has its origin in the growing trend of using civilian technologies in a military context. These technologies are commonly called dual-use technologies. Even if military research is still leading in a few specific areas, we have to acknowledge that wherever there is a civilian incentive to innovate - logistics, mobility, materials, telecommunication etc, - the advancement and adoption of change is usually quicker and on a larger scale than within the armed forces. Of course, the requirements are not always similar, but adaptation and ruggedization of innovations from the civilian domain might still offer a quicker way to adoption than a complete re-development.

If something should happen in Switzerland, given the structure of the country, it will take place and have major consequences for urban and peri-urban areas. It is therefore of importance to anticipate how these areas might look like and understand which technologies might drive the changes in order to ensure the non-obsolescence of our systems as well as the military doctrine.

Based on this belief, which can of course be challenged, we have considered the main military capabilities as chapters, dividing each of them into sub-chapters with the aim of answering the following questions:

1. What could be the future of that capability from a science-fiction perspective?
2. How does the innovation landscape look with respect to that argument?
3. What is happening in Switzerland in this regard?
4. How is this matter relevant for the armed forces?

These four steps introduce logically a fifth question being "What does this subject mean for the Swiss Armed Forces?". This last element is not developed in this publication. It will however be discussed and considered with the appropriate entities based on this publication. The main purpose here is to set the scene so that debate can take place; this is one of the tasks of the Technology Foresight research program of armasuisse Science and Technology.

We would, as always, welcome any input, comment and suggestion in how to improve knowledge transfer, anticipation and propagation of such concepts that might (or not) impact and change, in a near or distant future, the security landscape of our country.

In the meanwhile, we wish you good inspiring reading!

Yours faithfully,

Dr. Quentin Ladetto
Research Director - Technology Foresight
armasuisse Science and Technology

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

Megacity

Urban environment

An urban environment poses a lot of challenges if viewed as a potential battlefield. Wide or narrow streets, immediate proximity of civilians, massive presence of IoT (Internet of Things i.e. sensors, cameras, etc), verticality in constructions from underground tunnels to high-rise buildings; the opportunities or difficulties to hide and the complexity to defend are obvious. The vulnerability of infrastructures – transportation, electricity and communication – makes them sure and simple targets for new unconventional digital and physical threats. Are current military systems and doctrines adequate and optimized to operate in such environment?

The megacities of science fiction

Introduction

With its tentative beginnings at the end of a 19th century that had undergone profound transformations in the course of the second industrial revolution and the massive scale of urbanisation in the West, science fiction literature is a narrative technique – in other words, a specific way of telling stories – which relates the issues encountered by individuals contending with a world generally located some time in the future, that invariably bears some resemblance to our own, although different, in that it is constructed around motifs based on conjecture, in other words extrapolated from the current status of science and technology (climate change may give rise to a narrative constructed around an imaginary, fictional conjecture, a world destroyed by natural disaster). For this reason a structural feature of science fiction is the setting of gigantic, mega-cities, or 'planet cities', new forms of energy, or worlds that are terribly impoverished, fascinating flying cars or spacecraft with hyper-drives, psychotic supercomputers, or highly evolved surveillance technologies, melancholic robots, or bellicose extra-terrestrials... All these motifs, and their list could be considerably extended, as the genre's narratives evidence such creativity in this respect, must not however, be read – as has previously been too often the case – at the first level, in other words what they literally evoke (a robot is not primarily a machine), but, on the contrary, as metaphors, more or less original in their conception, in other words, as images that permit a different perspective of human beings and the world.

In order precisely to ascertain what the notion of "metaphor» encompasses, we should remember that we always think of man and the world in terms of concepts, whereas these concepts themselves have been profoundly altered by the second industrial revolution, which began over one hundred and fifty years ago, and whose rhizomatic ramifications continue to affect us. In consequence, and because our concepts have been altered in minute detail, it is no longer possible to conceive of ourselves – or of the world – as though science and technology were merely superficial dimensions of our reality: the human condition is, on the contrary, affected, in its very essence, by these recent upheavals. Today, mankind must also conceptualise itself differently in order to understand the world in which we live; and this different concept entails the use of a different kind of language, a language which, in the signifying elements that constitute it, is capable of addressing what we have now become. Without revisiting here the entire theory of metaphor, I will focus on the original thinking of Melina Marchetti, which she is developing in a thesis being written at the University of Lausanne: metaphor, by definition, consists of semantic dissonance, in other words, the placing in correlation of a subject and predicate which, a priori, do not go together. The metaphor is thus, according to Marchetti, a phenomenon – particularly a textual one – which shakes up our concepts in order to create new ones – semantic dissonance is a semantic innovation – and, because these concepts are those we use in order to think and to derive our conception of the world, to create reality, and thus to reveal the nature of being in a different light. This is exactly what (ambitious) science fiction does, so long as we are capable of decoding its metaphors: it is this different conception, it is this language of our time, which, through the creation of images, seeks another way of perceiving what is becoming of us and of the world. A language therefore, which fleshes out reality, by giving it a name, describing its flavours, discussing its smell; the language of our time, of our world, and overall, of our existence. Let us therefore seek to understand, using some examples and famous instances of conjecture, how science fiction confers a metaphorical aspect upon our world, and what it tells us about our world – and our humanity, because we are indeed the ones living in this world – once this metaphor has been deciphered.

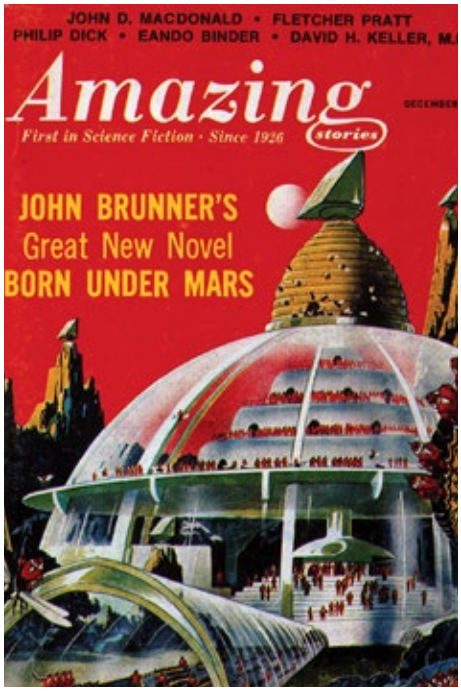
Giant cities

As a worthy successor to the utopic tradition, science fiction, from its earliest beginnings, has always created cities – sometimes with the proportions of an entire planet: consider the planet city Coruscant in the world of Star Wars (George Lucas, 1977-2005) or Trantor, the ecumenopolis of forty thousand million inhabitants, at the heart of the Foundation cycle (Isaac Asimov, 1951-1953) – which, in order to provide a better symbolism of the gargantuan process of industrialisation currently underway, saw their size in hyperbolic expansion. Put differently, cities became gigantic, as in the film Metropolis (Fritz Lang, 1927) or in the cyberpunk novel Neuromancer (William Gibson, 1984), not so much to indicate, explicitly, that our future will see the appearance of this kind of metropolis, although, strangely, our societies have indeed tended towards this kind of territorial organisation, but in order to convey, implicitly, that spatial gigantism metaphorically represents the exploitation of this same space: the city world of the film Dark City (Alex

Proyas, 1998) is a closed world whose topography is constantly being reinvented, in other words, endlessly drawing upon its own resources. In the giant cities of science fiction we find the ontological intuitions of the German philosopher Heidegger, who, in Die Frage nach der Technik [The Question Concerning Technology] (1954), demonstrates that the essence of technology, in the industrial era, expresses a new relationship between man and nature that he calls "enframing" (Gestell): nature is now in fact, "on notice to deliver an energy that can, as such, be extracted and accumulated", in other words man forces nature to be considered as a reservoir of energy that man will relentlessly focus on exploiting. The tentacle-like cities of science fiction are in this sense the metaphors of "enframing": there is no more nature, there are no more reserves to exploit, no more energy to be extracted, or, rather, the science fiction city represents the asymptotic direction of this enframing process, or the disappearance of nature, giving way to a pure technical device. The giant city is energy; the giant city is the metaphor of enframing, the image that expresses, through semantic innovation, the essence of modern technology. But Heidegger goes further than this, and specifies that, in order to enframe nature, it is necessary that mankind, as the vector whereby this enframing of nature is possible, must itself be already enframed. The metaphor of the mega-city is doubled therefore by a second metaphor: the mega-city represents a nature whose entire energy has been extracted (nature has therefore disappeared), but also the human being considered as a "natural resource", whose entire energy as been extracted (man disappears in the shadow of the city's gigantism) – which the film Matrix, by the Wachowski brothers (1999), demonstrates superbly, also by superimposing both the motif of the planet-scale mechanical city and that of man who has become a pure energy resource nourishing this same mechanical city.

Conclusion

Science fiction, as practised by the founding aesthetic of a new language, in order to envision the new world order, could not fail to construct giant cities, constituting a metaphor of the process of enframing, that has been so well described conceptually by Martin Heidegger. Man, just like nature, has become a resource whose energy is to be extracted, thus resources that ultimately can only disappear, once all their energy has been extracted. The mega-city, is therefore a metaphor for lines of force that inform our relationship with the world and with ourselves; representing them in fictional narratives is not so much a value of futurological perspectives, but a determination – that some may find bitter – of a new order for the world, where it is essential to measure its ineluctability, and for whose description a new language is required. This language, which is that of science fiction, and this motif, which is that of the giant city, enable a reflection on our day-to-day existence – our relationships with the world and ourselves must be conceived through the prism of enframing – but also a reflection on many other themes, such as energy, mobility, information, communication, and "protection/safety". I propose to elaborate on this reflection over a period of months, and I sincerely hope that this will convince you of the imperative of giving due consideration to science fiction, in order to consider, with the assistance of appropriate language, the transformations that our human condition and the world in which we are evolving has undergone from the second half of the 19th century, and thus to seek to anticipate the contours of our potential future.



Megacities

INTRODUCTION

Megacities will be the centre of attention of future wars. The bombings of Hiroshima and Nagasaki belong to the most significant events of World War II, they killed over 100,000 people immediately and many more in the aftermath. Considering that the two cities had a combined population of approximately 500,000, the ratio of lethally injured inhabitants is striking. The point is clear: Megacities are a state's weak spot, they do not get more vulnerable than that. Compared to the size of today's urban areas, Hiroshima and Nagasaki are small villages. Currently there are 33 megacities, with another six on the way by 2030[1]. Any city with a population over ten million falls within that category. While the actual threat of a nuclear attack is negligible, megacities are and will be the focus of terrorist groups, organized crime and any potential enemy with the political objective to weaken a state.

Megacity: Urban environments with more than 10 million inhabitants challenge conventional energy supply
Source: IABG

Urban warfare develops into a new form of military task requiring special capabilities. For regular armies, fighting in megacities is not only manpower intensive – their technological advantages over asymmetric actors are less effective. As we know, urban warfare bears a large destructive potential for critical infrastructures and high civilian casualty counts.

CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Megacities as future theatre of war

Due to emergent urbanization processes, cities and megacities will re-enter the focus for military operations. Recent publications of the US Army and other NATO countries show the need to prepare for urban warfare[2]. In these future theatres of war, potential hostile actors can use several tools of asymmetric warfare more efficiently. Especially the distinction between combatants and non-combatants becomes more challenging and likewise does the handling of the civil urban population.

With a rising urbanization rate, state actors must deal with an increasing domestic conflict potential because social and economic differences are unleashed due to an urban-rural or centre-periphery divide. At the same time, ethnic divisions bear conflict potential causing social unrest. Organized crime groups or actors with political dependencies towards hostile states support "parallel" structures causing insecurity and no-go areas. Subsequently, this causes "failing cities" and "mega slums" without domestic control.

The combination of internal and external threats poses a complex challenge to the military in special and the state as a whole. Sharing of intelligence, cooperation of state institutions and a comprehensive approach to urban warfare will be key to answer the versatile challenges originating from the emergence of megacities.

Fragility and vulnerability of megacities

Cities and megacities can be understood as complex living organisms. Like an organism having a biological metabolism that transforms an input (e. g., sunlight, food, water, and air) into energy and by-products (e. g., waste), many scientific studies brought up the idea of an "urban metabolism", as those spaces require daily inputs of clean air, water, food and resources to sustain people, infrastructure, and terrain. If one understands megacities and cities as an organism, they are primarily characterized by their population, their size and their social organization as vital components. Urban spaces die, when their vital components are permanently damaged or destroyed. If the essential inputs that keep the vital components supplied and the city functioning are radically changed or removed, the population slowly disappears while the city dies. Therefore, urban spaces and especially megacities are extremely dependent on critical infrastructure and external supply, what makes them valuable targets for hostile actors. Already by damaging a city's physical structures while the population survives, it can be severely wounded. In terms of urban warfare, a megacity need not be annihilated to tilt the advantage on the battlefield. Capitalizing on one of the cities weaknesses

can be enough to achieve success[3].

As history shows, natural catastrophes have devastating consequences for the life of a city followed by massive humanitarian consequences. In this sense, Pompeii remains the most iconic example in history – and today, especially Asian megacities are considered as likewise endangered.

Asymmetric actors prioritize densely populated cities due to potentially high casualty figures and collateral damage. Different hostile actors know various inhibition thresholds to aim for cities or urban spaces, thus defining the ethical dimension of urban warfare. Media hypes concerning "urban catastrophes" raise public and political pressure to intervene with armed forces.

Urban population and civil situation

Focusing on the challenges of the future security environment in cities and megacities, the civil situation is of special significance. The diversity of the population becomes a challenging factor when it comes to maintain social peace. Existing division and social distinction can be exploited by various hostile actors to endanger a stable and peaceful coexistence. Riots and social unrest occur to have a much bigger impact in a dense urban terrain than in a rather rural area. A rioting crowd in a closely populated area can cause continuous social unrest with a certain snowball effect. As the 2019 protests in Hong Kong show, authorities were not able to calm the situation for months and clashes between police and activists have become increasingly violent, with police firing live bullets and protesters attacking officers throwing petrol bombs. The possibility of a military intervention cannot be neglected.

IMPLICATIONS FOR THE MILITARY

Concept of urban operations

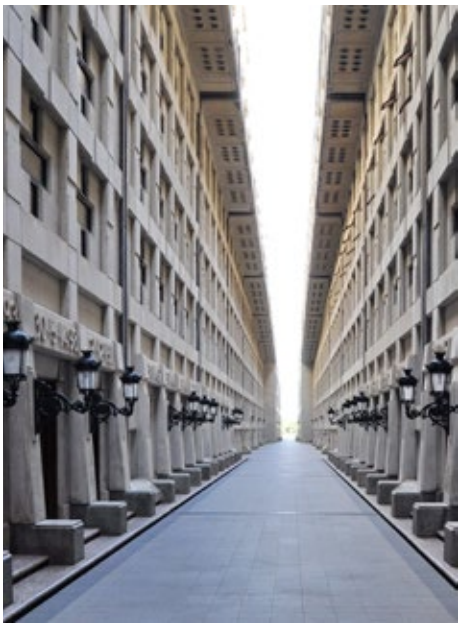
Not only within NATO and most Western countries, several concepts on urban operations have been revisited in the past decade. These advancements in operational and tactical thinking are mainly due to new technologies which have been emerged in the civil sector – and thus have been used as off-the-shelf products by military non-state actors. A state's military answer to these threats within the urban sector focuses on customized high-tech solutions and the broad integration of state-of-the-art technologies. Modern concepts for urban operations are therefore multi-faceted and highly complex, but nevertheless refer to a common denominator:

- Formation of capabilities to fight in multi-dimensional urban battlefields
- Command posts designed for urban warfare
- Common concept of tactics, techniques and procedures in urban operations
- Integration of technological inventions (Robotics, AI) within urban spaces
- Coordination und cooperation with NGOs, GOs and urban key players
- Combination of lethal and non-lethal weapons

Analysis competence and target discrimination

The success of a military mission does not solely depend on winning on the battlefield, as the perception of an operation is crucial. A mission's narrative and the kinetic effects of military actions must be aligned. The tolerance of western societies for civilian casualties is vanishing and mistakes of soldiers are broadcast to a large audience via social media. Because of the high probability of civilian contact in densely populated areas, special precautions must be taken to avoid unintentional damage. Target discrimination is the cue when it comes to preventing civilian casualties. Especially because terrorist organizations use civilians as human shields, the on-site analysis competence of regular armies is an indispensable ability for future urban operations.

It is important for the soldier of the future to understand that every action on the battlefield has direct influence within the information domain. That is why urban operations must be planned on the strategic, operational and tactical level with special focus on the civil situation of a city. To do so, military leadership needs processed information not only on the military and infrastructure situation but also on the political, economic and social environment. Existing analysis frameworks must be revised for civil considerations and implemented on all levels. Those analysis frameworks are of special significance to understand a city itself not only as an entity but also as a complex system with all its implications for urban warfare[4]. Moreover, just as every battlefield is



Urban living: Frictions can lead to social unrest with unintended consequences
Source: IABG

different, no city is the same. Therefore, operations in urban terrain will make it absolutely necessary to perform adequate reconnaissance in support of mission planning and execution according to the analytical frameworks to prioritize operation objectives. Besides common exercises of urban operations on a tactical level, this analysis process needs to be exercised from operational level onwards. Furthermore, the precision of lethal and non-lethal weapons needs to be increased to make it possible for the military to operate in urban terrain. The development of future weapon capabilities to discriminate targets will be of special significance.

The city as a battlefield

Unlike a conventional battlefield in open terrain, urban battlefields are multi-dimensional. Fights can occur from the super-surface areas (roofs of buildings, towers), to the ground level (streets, highways, surface waterways) and the sub-surface areas (subways, tunnels, sewers, cellars). Local hostile actors are therefore in advantage since they have inside knowledge conventional troops lack. A further disadvantage for conventional troops is the (slow) speed with which they move and fight in a city, while the urban battlefield offers many possibilities for asymmetric forces to hit and run or use close-quarters battle tactics. In conclusion, military forces either need high numbers of force to take or retake control of a city or very specialized troops trained for urban warfare. Both solutions involve high costs.

CONCLUSION

As the urbanization process continues, cities and megacities will become the future theatre of war. Their fragility and vulnerability in combination with the implications within the information domain makes them valuable targets for potential hostile actors. Their objective is to "kill the city" by aiming for the physical structure or the urban population. To counter future threats, a consistent concept for urban warfare is inevitable. Narrative and military action must be closely coordinated in order to develop a holistic effect. Kinetic effects must always be understood against the background of narrative implications. Especially when it comes to analyse competence and discriminate targets, the development of future capabilities is of special significance. Ultimately, as the world urban population continues to grow, the future of global security will be determined by what happens in the cities.

SWOT-ANALYSIS for swiss military planners

Strengths • Advanced civil and local infrastructure • Existing contingency plans and operational routines • Existing special forces teams	**Weaknesses** • Fragility and vulnerability (infrastructure, population, ...) • Potential of high casualty figures • Target discrimination
Opportunities • Work with NGOs and local key players • Professional training of regular forces in urban warfare • Bigger impact of information activities in densely populated areas	**Threats** • Cyber attacks • Asymmetric hostile actors • Mass demonstrations • Terrorist and criminal groups • Natural catastrophes

List of links included in the article

1. United Nations (2018): The World's Cities in 2018. P. 5.
2. Margarita KONAEV, The Future of Urban Warfare in the Age of Megacities Focus stratégique, No. 88, March 2019.
3. John Spencer, The destructive age of urban warfare; or, how to kill a city and how to protect it, March 28, 2019, online: https://mwi.usma.edu/destructive-age-urban-warfare-kill-city-protect/ , (accessed on 16.10.19)
4. John Spencer, The destructive age of urban warfare; or, how to kill a city and how to protect it, March 28, 2019, online: https://mwi.usma.edu/destructive-age-urban-warfare-kill-city-protect/ , (accessed on 16.10.19)

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

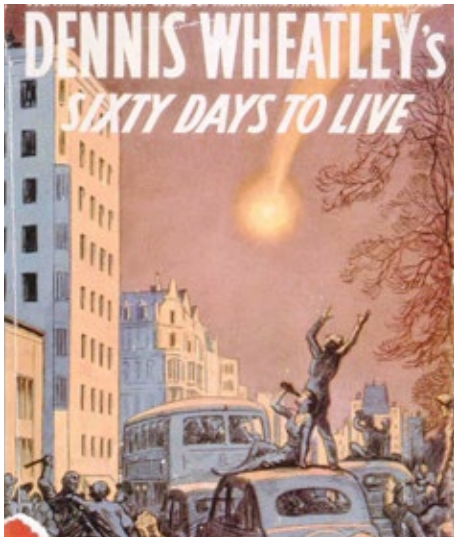
URBANITY

Energy

In science-fiction, energy is often available in abundance without mentioning really how it is created! Digitization assumes that processing, computing, analysing data as well as the availability of sensors, processors and machines (or systems) in general is guaranteed. Everything relies, in one form or the other, on permanent access to different forms of energy, and this on the move or while stationary. Solving the supply and demand equation could mean less power-hungry electronics components and products, and changes in habits and lifestyle in conjunction with optimized energy production. The race is on for such a politically, societally and environmentally sensitive topic.

Consuming and depleting!

Ecofictions and the post-apocalyptical



While science fiction is a new language with which to describe a new world order, it is also an aesthetic practice which questions – through the use of narrative and creation of original metaphors – our utopias, in other words the ideological substructures that give meaning to our behaviours and our institutions. This is why, despite the numerous criticisms of it, the consumer society wins our support: the consumer act is not first and foremost a Western pathology, but the action that is deemed to give us access to existential fulfilment. This choice made by society, and learned discourse evidences this deliberate awareness since the end of the 19th century, has the consequences of depleting natural resources and disrupting ecosystems due to a growing need for energy: consumerist utopia thus seems to be leading unwaveringly towards catastrophe. Precisely this identity {consumerist utopia (consumerist) = catastrophe} was to be at the heart of certain science fiction narratives from the 1970s, where their authors borrow the ecologists' discourse and place it on a canvas that paints the backdrop to their novels, in order to mark out, metaphorically, the utopian dreams that are destroying us: the world is laid waste, energy disappears, and humans – the survivors – seek, more or less happily, to recreate a viable society and, most often in balance with the natural environment. In other words, science fiction narratives – referred to as "ecofictions" or, when taken to the extreme, "post-apocalyptic" narratives – will extrapolate the catastrophe in order to evoke our ecological concerns, but the catastrophe responsible for all future catastrophes: our utopias – in particular, but not uniquely, consumerism. Here were see the metaphorical act emerging in all its splendour: ecological catastrophes or energy crises are the images of this already active catastrophe, namely consumerist utopia. This is what can be seen in the novel Ecotopia (Ernest Callenbach, 1975), the comic book by the Marvel publisher Guardians of the Galaxy (Steve Gerber, Sal Buscema and Al Milgrom, 1969-1977) or the feature film Soylent Green (Richard Fleischer, 1973) all three of which reflect – as in a distorting mirror, and to varying degrees – the issues of pollution, aerosols or the mode of consumption of a putative Western world "adrift". However, one must remember, the dénouement of Soylent Green leaves no doubt on this point, that the industrial proceeds from an economic form whose axiomatic-axiological basis necessarily leads to the world and human beings being considered as resources to be consumed in order to be happy. Unlike the fictions that flooded the publishing world in the 1950s-1970s that tell of the consequences of nuclear energy for civil society – the novels The Day of the Triffids (John Wyndham, 1951), I am Legend (Richard Matheson, 1954) or the excellent Dark Universe (Daniel F. Galouye, 1961) come to mind –, the storylines of ecofictions lead to a perception of the democratic world as an alienating operator, and, by extension, ecological disasters as an inevitable consequence of the utopias of this same world. Here, there is no intent to frighten the readers or audiences (we are far from the "heuristic of fear" of Hans Jonas), but much more a narrative configuration, which aims metaphorically to mark out the ontological deviances of a modernity whose dreams lead to depletion.

Offering an image-rich description of the utopian unthinkable element that is irrigating our contemporary and techno-scientific societies also helps us to give meaning to our consumerist aberrations, even though we do not generally conceive them as such. The novels Le Goût de l'immortalité [A Taste for Immortality] (Catherine Dufour, 2005) and Treis, altitude zéro (Norbert Merjagnan, 2011), or the films WALL-E (Andrew Stanton, 2008) and The Book of Eli (The Hughes Brothers, 2010) illustrate, by means of the catastrophe metaphor, how consumption is destroying our individualities and our world: our every day actions do not mean that we inhabit our world, but are (unconscious) ways of depleting and destroying it. While Treis, altitude zéro supposes for example, that the aberrations of science led to ravaging climatic wars, WALL-E portrays a humanity that has deserted an earth that is covered in waste – a metaphoric signifier whose graphical treatment leaves nothing to doubt: the Western world, is, ontologically, a construction of waste originating from waste.

It must be determined, on the one hand, that the two waves of ecofictions (the 1950s-1980s and 1990-2019) represent, in an indexed way, the pregnancy of catastrophist discourses in the social fabric: the novel The Road (Cormac McCarthy, 2006) illustrates this pregnancy marvellously well, since it dispenses it from explaining the cause of the destructive catastrophe – the reader is immersed in so many "apocalyptic scoops" that it instantaneously renders the fictional world intelligible. Otherwise, these two waves of publications, albeit each in their own way, require that the ecofictions are above all considered as metaphorical constructions that extrapolate a catastrophe in order, in fact, to mark out the catastrophe that lies at its origin: if the world of Mad Max (George Miller, 1979) is energy poor, this is not

in order to tell us that, in the future, this will be the case, but to evoke in an indirect way, that our every day actions – wallowing in a utopia of consumption – are, in themselves, catastrophic acts. Unfortunately, and certainly due to the media imperialism saturating us with ecological discourses, the "first level" interpretation of narratives that are nonetheless ironic (in the sense of "distanced") may give the impression that ecofictions are warnings, or representations of what is about to happen. Whereas the works of Jean-Marie Schaeffer (in Pourquoi la fiction? [Why fiction?], 1999) or Jean-Pierre Esquenazi (La Vérité de la fiction [The Truth of Fiction], 2009) demonstrate that we should not approach (science) fiction narratives as "accounts" of reality – the fiction is always separated from the real –, but rather as scenarios, in other words as representations intended to elucidate our human condition and the meaning we give it. Put differently, ecofictions do not portray a (quasi-)certain future; they seek, on the other hand, to diversify the narrative models – the "paraphrases" with which to respond to the notion forged by Esquenazi – whereby we can tell the stories of our lives in a society impregnated by discourses that are a priori disembodied. In fact human beings cannot comprehend themselves – or the place they should occupy in the world surrounding them – without being able to articulate their existence in coherent narrative: consumption is firstly a narrative that we recount and which is based, even tacitly, on a concept of happiness. At a time of climatic warming and a range of climate problems, it seems therefore imperative to restore the view of, and to understand our utopias which, even though they are intended to contribute to our fulfilment, are actually the real catastrophes; that it is our conceptions of happiness that are responsible for the depletion of the world. And it is because they seek to set out how our utopias are destroying the world that ecofictions are endowed with an exemplary virtue: they constitute symbolic resources invented by our imagination to tell the story of our existences, to show how they are informed by dreams which, even though laudable in themselves, are not as such without harmful consequences. In summary, the representations of the future proposed by ecofictions only contribute the capability of narrating a present made opaque by our incapacity to take possession of it, or, using the biological term, to "metabolise" it.

Conclusion

We have demonstrated – albeit very briefly – that science fiction diffuses within the social fabric numerous scenarios of intelligibility which, amongst other functions, serve to enable us, as readers and film audiences, to give meaning to our existence in a society saturated with discourses that are either alarmist (ecology) or utopic (infinite growth); however, even though there are narratives that are implicitly based on a world of inexhaustible energy resources (the Foundation cycle of Isaac Asimov being the best known example) it is in order to evoke the fragility of our way of life that authors most commonly incorporate issues relating to energy. This latter situation in fact enables us to be reminded, by means of fiction and its metaphors, that our consumerist mode of behaviour on the one hand presupposes an infinite resource of energy (consumption has no limit) and, on the other hand, that this behaviour is at the same time the condition for the possibility of the end of all scope for action. A logical paradox in which we are ensnared and which is also at the heart of our incapacity to behave otherwise, despite our awareness of the damage that we contribute to inflicting upon our world and, by extension, upon our own existence. Ecofictions, therefore, these narratives where the catastrophe has destroyed our world and where energy has become so rare that it only allows for a handful of survivors to wander in a sad world, are artistic reactions that challenge us: are we ready to sacrifice our existence (= catastrophe) for a dream (= utopia) which, as has been proved to us, can only be... deleterious?

The Energy Paradox: Powering a Growing World

Europe seen at night, captured by a passing satellite. [PHOTO NASA/ESA]

The aspirations of a growing planet have a cost: at current rates of growth, global energy consumption will increase by 28% by 2040[1] , with a 60% increase in demand from China and India alone. How might energy suppliers, producers, and consumers respond to the paradox of powering a growing planet while reducing energy emissions?

The price paid globally for the dream of energy-on-demand is the existential crisis of climate change: environmental threats posed by carbon emissions. Today, a third of the world's[2] energy is provided by coal, oil, and gas; nuclear fuels are a distant fourth. To meet the criteria set by the environmental pledges of the 2016 Paris accords, this mix of energy will need to be drastically reconsidered.

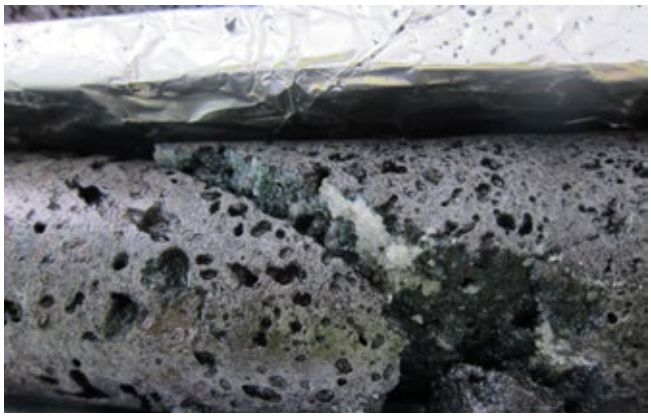
Current models project global temperatures could rise 3-5°C[3] by the end of this century, which has been linked to rising sea levels, longer droughts, and increased tropical storms . Even nuclear energy, once considered green, has been re-imagined amongst the public. Disasters in Japan, questions on the storage of radioactive waste, and criticisms that the plants are costly to build and operate, have transformed the nuclear reactor into a symbol of catastrophic, not utopic, possibilities.

Fear of environmental threats is driving global demand for cleaner sources of power for global ambitions, and for technology that can efficiently integrate and distribute this energy into the grid. The energy mix of 2040[5] could be the

most diverse that the world has ever seen — with a 40% surge in use of renewable energy, particularly in the area of wind, hydro, and solar. How will those technologies transform our use of energy? What new technologies could contribute to this new energy mix?

New Technologies: From Producing to Capturing Emissions

Fear of climate change is boosting interest in green energy, but new technology could reduce the harm of today's most-used sources of fuel. So-called "Negative Emission Technologies" (NETs) can pull carbon dioxide (CO2) from the environment and/or reduce how much is released into the atmosphere — reducing emissions and increasing fuel efficiency.



CO2, captured from the air and mineralized by a Climeworks facility in Iceland. Top photo by Sandra O Snaebjornsdottir, bottom Zev Starr-Tambor, via Climeworks.

A geothermal site in Iceland is today able to capture the emissions equal to one household, creating an energy source that contributes to climate cleanliness. The Icelandic plant[6] is the first test of a Carbon-Capture Device which can stand apart from power plants or just adjacent to them; its effect could capture 900 tons of CO2 per year, transforming pollutants into fertilizer for vegetables. At that pace, capturing 1% of current CO2 emissions would require 250,000 plants.

The device produces fertilizer, but other NETs are focused on turning captured carbon into a reusable fuel supply, such as carbon bricks[7] or jet fuel[8]. Others have made progress toward "artificial photosynthesis[9]", which can transform CO2 into organic matter that can be re-used as a fuel supply, creating additional energy while reducing emissions by 57%.

While promising, NETs alone cannot be the sole cure for averting a climate catastrophe. Without policies to increase adoption and research, an unlikely growth rate of 26% per year for thirty years[10] would be required to reach UN climate goals by 2050. Cleaner energy sources will remain an essential part of the mix.

Nuclear: From Fission to Fusion

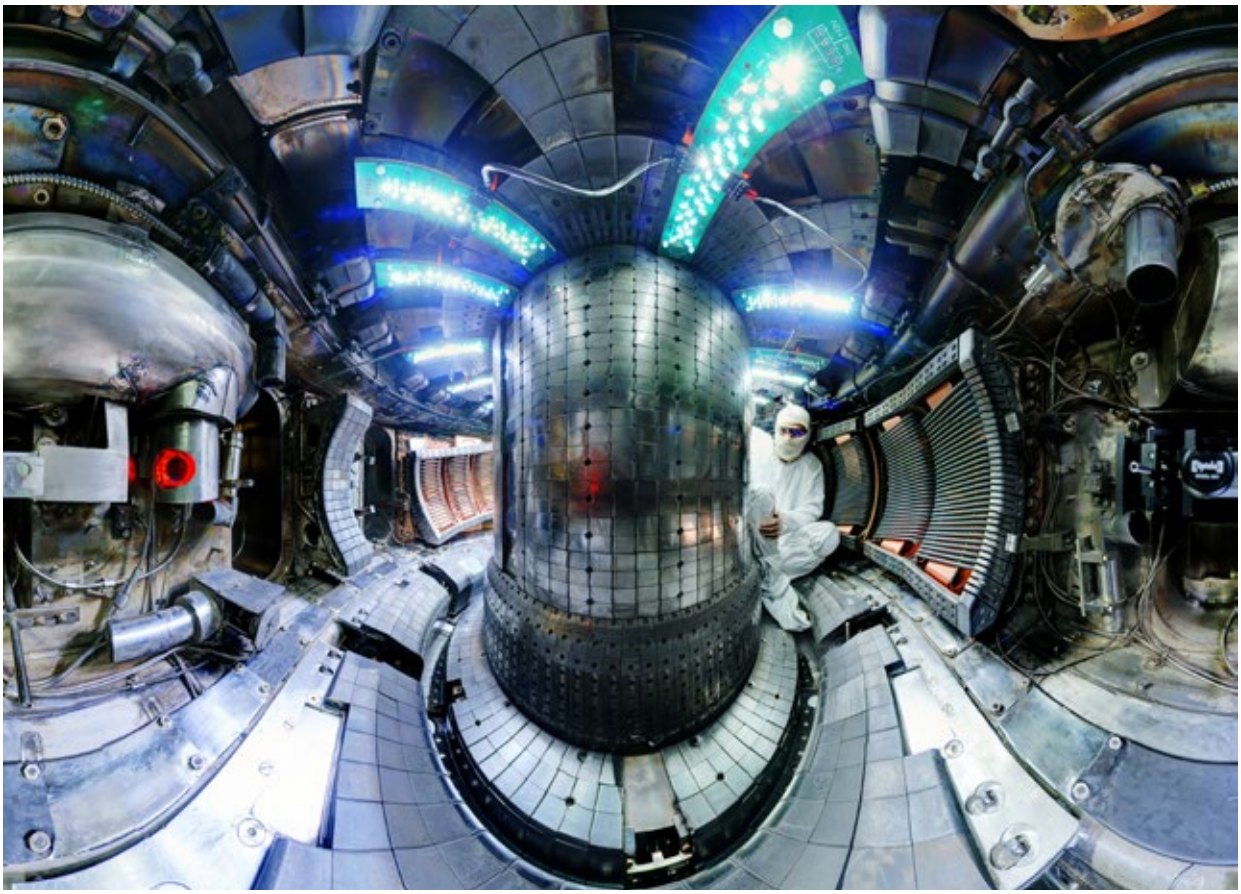
"Nuclear" is not often associated with clean energy, owing to the possibility of meltdowns, the production of radioactive waste, and it's linkage to human catastrophes. Investments into nuclear plants had declined by 45% in 2017[11], though some analysts[12] see a surge in nuclear by 2040, mostly as China brings more plants online. As nuclear plants are phased out around the rest of the globe, researchers (and investors) are eyeing a radical new source of nuclear power: capturing the energy "fusing" two hydrogen particles, rather than splitting atoms (fission).

Fusion energy would be remarkably clean. In theory, just 11 pounds of hydrogen in a fusion reactor could create the same energy output as 56,000 barrels of oil, but without the corresponding carbon emissions. Fusion reactors[13] rely on helium or nitrogen, rather than uranium, so they don't produce radioactive waste. They also don't have meltdowns, improving their safety over nuclear fission plants.

New superconductive materials are behind the SPARC[14] plant, an experimental fusion reactor. It uses electromagnets made from yttrium barium copper oxide (YBCO) — a compound that withstands higher temperatures than past fusion reactors, and can be cooled with liquid nitrogen, which is cheaper than liquid helium used in previous theoretical reactors. MIT is betting that these high-temperature reactors will result in pulling more power from smaller, cheaper reactors that are easier to build. SPARC would produce 50-100mw (enough for roughly 3,600 homes) in short bursts, and is on track to launch in 2026.

MIT researchers themselves suggest that fusion power may contribute to the energy grid until 2035, but investors such as Bill Gates and Jeff Bezos are betting on fusion's commercial future, earmarking almost $1 billion[15] for these investments since the Paris Climate Accords were signed in 2016. In Canada, efforts are already underway to commercialize fusion technology[16] on an accelerated timeline, bringing its fusion power to the grid by 2025. This project is drawing on research from McGill (CAN) and Princeton (US) universities, backed by investments from Microsoft.

Photo: Inside the MIT-based SPARC reactor. Bob Mumgaard/Plasma Science and Fusion Center, MIT.



One speculative technology that seems to be limited to science fiction stories is Cold Fusion, the idea that energy could be created through fusion without excessive heat. In a surprise announcement, Google announced that it had spent four years revisiting research reported in 1989 that turned out to be irreproducible by any other lab. In May 2019 it published its research[17], confirming that its own experiments had also failed.

Energy Distribution: The Rise of the Smart Grid

New forms of energy are being coupled with a new capacity for distributing energy in more efficient ways. The challenge of collecting, distributing, and regulating energy transmission is being shaped by smart grids, a combination of artificial intelligence (AI) for grid planning and energy-use prediction; and the internet of things (IoT) for communicating needs between devices, homes, and/or vehicles.

Chinese electronics giant Huawei predicts that 75 billion electrical devices[18] will be connected and sharing data worldwide by 2025. If these devices can communicate with one another and with the grid where they get their power, it unlocks a vast potential for conservation and convenience. Energy could be redirected from places where demand is low to the locations it is needed most. These pieces would come together with an AI, its algorithms playing a managerial role, creating a "smart grid" system for energy distribution.

Huawei is exploring the digital transformation of China's energy grid, predicting that: "Smart metering, alongside electric vehicles, fuel cells, and smart appliances and devices where users can flexibly configure power use, will generate more energy than is consumed, [and] will allow users to potentially sell excess electricity to power companies. Increasingly managed by software, grids will start to manage themselves, for example, by self-adjusting to reduce losses, respond to voltage variations, and self-optimize to avoid electricity disturbances."

Research has shown that smart grids would adapt quickly[19] to changing energy needs within a network, preventing blackouts, increasing transmission capacity, and improving system transmissions — reducing operating costs in the United States while delivering additional services to ratepayers.

Smart grids and the digitalization of energy would open up a market for decentralized peer-to-peer (p2p) trading between smaller, self-organized networks, such as rural farmers with a mix of solar, wind, and biogas, advancing the so-called "prosumer" market. A pilot program to study the economics and infrastructural needs of this kind of energy sharing has started in the United Kingdom, in which a city block in London will trade energy on a distributed ledger[20],

while research focused on measuring energy use[21] is beginning to create a better understanding of how such grids can more effectively cooperate.

Distributed ledgers, in the form of blockchain, are being eyed for a similar pilot in Australia, as the Australian Renewable Energy Agency (ARENA) introduced a small blockchain pilot[22] — along with energy company AGL and IBM — to test this prosumer model. In another pilot, ARENA created an energy exchange marketplace[23] that pays rewards into a digital wallet. Others have pursued an "eBay for energy"[24] model, with early backing from UK and Japanese energy providers.

Decentralization would also increase energy efficiency. 15% of the energy we produce is lost in the transmission process, diminishing as it travels. Moving energy from smaller sources to closer users reduces that loss. This is driving some novel approaches to small-scale, highly localized capture and storage, such as concrete towers and weights[25] to store kinetic energy. Towers with wind-capturing mechanisms can be installed anywhere; as the wind blows, it elevates a platform of bricks; when more energy is needed, the bricks collapse onto a lower platform, which "collects" the energy of the impact.

Energy Distribution: From Stations to Storage

Steady supplies of green energy may seem like a utopian vision. But today, a challenge for the clean energy ecosystem is how to capture and preserve an irregular supply: the wind doesn't always blow on turbines, the sun isn't always up for solar. Climate change is starting to affect hydropower flows[26], such the extreme glacial melts in Switzerland. These are creating short-term boosts in energy supply that go to waste if they aren't immediately used. This raises the problem of managing temporary energy surplus: this is why the future for clean energy requires batteries and storage.

The Hornsdale Power Reserve in South Australia is the largest lithium-battery storage site on Earth in 2019, and was constructed in less than 100 days.

Australia, China, Germany, Italy, Japan, South Korea, the UK, and the US are today embracing centralized storage. These sites can collect and store up to 10 GW of power — enough energy to power 3 million homes for a day. The Hornsdale Power Reserve in South Australia was completed by Tesla in 2017 in under three months, and is the largest lithium-battery site in the world.

Another strategy is decentralized storage: installing smaller, "behind-the-meter" batteries at a point of use, such as a consumer's home. Rather than large, centralized power storage, these batteries allow individual consumers to store smaller amounts of energy on site. Germany, Italy, UK, Australia, Japan, the Netherlands, and China are using some blend of these models. Germany leads the way with 100,000 batteries installed in homes.

About 90% of the batteries used today are lithium-ion, a material that can store, dispel, and refresh its energy supply, creating "rechargeable" batteries. Lithium-ion batteries have their limits — one of which is the growing global demand for the cobalt, which is used to build them. As battery demand has risen, so has the cost of cobalt, tripling in price since 2016. Two-thirds of the global supply of cobalt today are from the Democratic Republic of the Congo, while the majority of batteries — 65% by 2021[27] — are, and will be, manufactured in China, which is investing heavily to diversify the mix of battery materials.

Today's lithium-ion batteries use wet electrolytes in the process of storing energy. Liquid batteries are risky: if a battery component breaks, leaks, or short-circuits, that liquid is extremely flammable. This makes them dangerous in the use of mobile vehicles, where they could be damaged by accidents. They also have a diminishing capacity for storage, losing their charge in the short term and losing maximum storage capacity over time.

One alternative to the current lithium-ion battery is the solid-state battery, which still relies on lithium-ion, but makes use of dry energy storage rather than wet electrolytes. Solid-state batteries would be lighter, cheaper, and less flammable than "wet" counterparts. They would also hold their charge longer and withstand higher temperatures (150°C/302°F), making them more useful in a variety of settings, including electric vehicles.

The Swiss Fraunhofer Institute for Silicate Research has announced a three-year partnership[28] with the Swiss Federal Laboratories for Materials Testing and Research (Empa) in 2019, a strategic move to create a European battery technology to rival the dominance of Asia in the market . The research focusses on identifying the best materials for energy storage density and is explicitly focused on bringing these batteries to market.

There is already heavy investment from the private sector. Caterpillar, the world's largest construction and mining company with product lines including diesel and natural gas engines, industrial gas turbines, and diesel-electric loco-

motives, recently launched a strategic investment into solid-state batteries[29]. Auto companies such as Ford Motors[30] have invested in solid-state battery technology, while its Japanese rival, Toyota, announced it was ahead of schedule[31] and would bring a fleet of solid-state EVs to market by 2020.

Research also points to the sea, building batteries from sodium and chloride, both of which are found in the world's oceans. The oceans are also a key to the future of molten salt batteries, developed in 1985 but not widely used today. Built of nickel and salt, these batteries can hold charges longer than lithium ion, and operate in a wider variety of temperatures. Empa[32] has moved to create versions of these batteries with longer lifespans, creating a cobalt-free competitor to lithium ion batteries for stationary uses.

Another tantalizing future scenario revolves around engineering viruses that can organize energy, essentially creating biological batteries. Angie Belcher's work at MIT has shown that a living organism — the M13 bacteriophage[33], which is harmless to humans — can be mutated to bind with metals such as gold, cobalt oxide or iron phosphate. Belcher's lab has created a library of these materials, each capable of using these materials to collect, store, and dispel energy, and purposefully encloses them within existing battery casings to make them directly usable. This approach is crucial the next goal of the lab, which is to build larger power-storage equipment that can be built into elements of a car — for example, creating a steering wheel that is also its battery. Outside of batteries, the lab has also used the M13 bacteriophage to transform natural gas into gasoline[34].

On a science-fiction horizon, research is starting to examine the viability of quantum batteries[35]. These batteries rely on changes in the way particles behave on very small "nanoscales." One such behaviour is entanglement: strange linkages between particles that are isolated from one another. This means charging a single particle could charge all of the particles linked to it — charging an entire battery, and even multiple devices, much more quickly. As the number of batteries being charged increases, the faster they charge. Physicists at the **Italian Institute of Technology (IIT)** aim to move this research from theory to physical applications within three years.

What's Next?

The rise of populations and temperatures around the globe creates an energy paradox, in which the need to curtail fossil fuel use is mixed with a rapidly expanding demand for energy. The crisis demands a united effort among stakeholders — in this case, the entire planet — to find solutions. Opportunities exist for expanding cooperation between scientists in academia and the private sector, between social enterprise, industry, NGOs, and government agencies. This article has examined just some of the promising potentials for addressing climate through innovation in technology, but left alone broader developments in policy and social mobilization that could amplify — or constrain — progress toward this collective goal.

List of links included in the article

1. https://www.eia.gov/todayinenergy/detail.php?id=32912
2. https://cdn.exxonmobil.com/~/media/global/files/outlook-for-energy/2017/2017-outlook-for-energy.pdf
3. https://www.reuters.com/article/us-climate-change-un/global-temperatures-on-track-for-3-5-degree-rise-by-2100-u-n-idUSKCN1NY186
4. https://climate.nasa.gov/effects/
5. https://www.bp.com/content/dam/bp-country/de_ch/PDF/Energy-Outlook-2018-edition-Booklet.pdf
6. https://www.sciencemag.org/news/2017/06/switzerland-giant-new-machine-sucking-carbon-directly-air
7. https://globalthermostat.com/
8. https://www.opus-12.com/technology
9. https://www.sciencedaily.com/releases/2018/11/181130111637.htm
10. https://iopscience.iop.org/article/10.1088/1748-9326/aabff4
11. http://www.world-nuclear-news.org/NP-Investment-in-new-nuclear-declines-to-five-year-low-1707185.html
12. https://cdn.exxonmobil.com/~/media/global/files/outlook-for-energy/2017/2017-outlook-for-energy.pdf
13. https://www.iaea.org/topics/energy/fusion/faqs
14. http://www.psfc.mit.edu/sparc
15. http://www.b-t.energy/ventures/board-investors/
16. https://generalfusion.com/
17. https://www.nature.com/articles/s41586-019-1256-6
18. https://www.huawei.com/minisite/giv/en/download/whitebook.pdf
19. http://energy.mit.edu/wp-content/uploads/2011/12/MITEI-The-Future-of-the-Electric-Grid.pdf
20. https://www.sciencedaily.com/releases/2019/04/190430103440.htm

21. http://www.apep.uci.edu/research/partnership_ISGD.aspx
22. https://www.agl.com.au/about-agl/media-centre/asx-and-media-releases/2017/may/agl-tests-solar-energy-trading-technology
23. https://greensync.com/solutions/dex/
24. http://www.electron.org.uk/index.html#our_products
25. https://energyvault.ch/
26. https://www.nytimes.com/interactive/2019/04/17/climate/switzerland-glaciers-climate-change.html
27. https://about.bnef.com/blog/china-is-about-to-bury-elon-musk-in-batteries/
28. https://www.isc.fraunhofer.de/en/press-and-media/press-releases/solid-state-batteries-for-tomorrows-electric-cars.html
29. https://www.caterpillar.com/en/company/innovation/caterpillar-ventures/news/fisker.html
30. https://www.businesswire.com/news/home/20190411005017/en/Solid-Power-Receives-Investment-Ford-Motor-Company
31. https://www.motorauthority.com/news/1111715_toyota-accelerates-target-for-ev-with-solid-state-battery-to-2020
32. https://www.tagesanzeiger.ch/wissen/technik/die-batterierevolution/story/31038511
33. http://belcherlab.mit.edu/
34. https://www.siluria.com/
35. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.117702

The future of energy in Switzerland

From 1950 until today, energy consumption has risen by a factor of 5 in Switzerland. This increase is related to the evolution of the population and the economy: volume and size of apartments and vehicles, industrial activity or distances travelled have all increased. Even though energy efficiency has largely improved, Switzerland will also face the challenges of powering a growing country while reducing emissions.

S Start: no real activities | T Trend: Early activities | A Advanced | R Ready | S T A R

Swiss energy system and vision

S T A R

Apart from hydraulic energy and wood (combustion), Switzerland has limited resources in terms of conventional energy sources. Around 75% of internal consumption is imported, which mainly includes oil, gas, coal and nuclear fuel. During winter, Switzerland must also to import electricity[1].

Within the country, electricity is mainly generated from hydroelectric plants (60%), followed by 32% in the 5 currently functioning nuclear power plants. The rest (about 8%) comes from biogas, photovoltaic plants, wind, wood and waste incineration[1]. Of the total energy consumed in the country in 2017, around 12% came from hydroelectric plants. Renewable energies represent about 22% which is clearly above global trends[1]. Electricity produced by photovoltaic systems, from wind or biomass started to grow ten years ago and has since sharply increased[2].

Efficiency is key when resources are limited: in Switzerland in 2018, even after an increase in population (0.7%), GDP (2.5%), vehicles (1%) and housing, energy consumption decreased by 2.2% compared with 2017. Apart from more favourable climatic conditions in 2018, the efforts put into energy efficiency contribute towards offsetting the demands of a growing country[3].

In 2007 the Federal Government focused its main energy strategy in four pillars: energy efficiency, renewable energies, replacement and new construction of large power stations (including nuclear) for power generation, and foreign energy policy. After the Fukushima disaster in 2011, a progressive withdrawal from nuclear power has been accepted. This decision, together with changes in international energy environment, has led to the Energy Strategy 2050 which deals with a necessary upgrade to the Swiss energy system. In this context the parliament has already approved laws regarding the development of renewable energies and the power grid[4]. The aim is to greatly increase power generation from renewable sources, double the energy efficiency per capita, and reduce electricity consumption by 10-20%. Additionally, Switzerland is committed at the international level to reduce greenhouse emissions by 20% by 2020 with respect to 1990[5].

Flanking the federal Energy Strategy 2050, two long-term visions have been developed by the Federal Institutes of Technology in the same direction: firstly, the "2000-watt society" initiative, which is based on the idea that by 2100 per capita energy demand throughout the world should decrease to about 2000 watts (contrasting e.g. with 6500 watts in Switzerland in 2012)[6]. Secondly, the "1-tonne CO2 society" (per capita and year), which would permit an increase of energy use provided it comes from renewable sources[5]. Several projects can be found throughout Switzerland[7]. In the same direction, Canton of Fribourg has recently accepted a new law aiming at a "4000-watt society" in 2030[8].

Innovation

S T A R

Following the energy strategy of the Federal Government, more than 400 MCHF have been invested in public research, development and pilot projects in Switzerland in 2017. More than 140 MCHF have been granted to projects related to renewable energies, and more than 175 MCHF to energy efficiency. In the last 10 years, public fonds dedicated to renewable energies have more than tripled; the highest amount (54 MCHF) has been granted to solar power related projects[9].

The Swiss Federal Office of Energy also developed the Cleantech Coordination instrument, with the purpose of securing suitable framework conditions for the innovation in the areas of efficient use of resources and the use of renewable energy[10].

Eight Swiss competence centres for energy research (SCCERs) promote cooperation between research centres, universities and industry, and support the technology transfer[11]. Established in 2014, they will receive financial support until 2020.

ETHZ has founded the Energy Science Centre (ESC) in 2005 as an interdepartmental competence centre to facilitate energy research and teaching activities across research fields and departments[12].

Smart Grid

S T A R

Power distribution in Switzerland is highly complex since there are around 650 companies; however, the transmission system is solely regulated by the national power transmission company Swissgrid. Additionally, the development of renewable energy sources leads to a more decentralised and fluctuating system, challenging the existing power grid. The Swiss Federal Office of Energy identified smart grids as a possible solution as early as in 2009, as well as carried out an impact assessment on the introduction of smart grids and elaborated a smart grid roadmap in 2015[13]. The roadmap identifies the necessary functionalities and technologies in order to develop the smart grid in Switzerland and encourages research projects in this area[14].

A collaboration agreement concerning research on smart grids was signed in 2009 between Switzerland, Germany and Austria[15,16].

One of the eight Swiss competence centres for energy research, FURIES ("FUtuRe SwIss Electrical InfraStructure"), is dedicated to grids and their components. They provide Swissgrid with information about socio-economic and ecological factors upon which planning can be based, and they are aligned with the smart grid roadmap.

EPFL is very active in this domain and has created the Smart Grid Project by joining the efforts of two laboratories[17]. One of their projects consists on developing sensors and phase meters for monitoring load in real time in a test power grid on the EPFL site[18]. This tested technology is now being used by Services Industriels Lausanne (SIL); and is being tested under real conditions in Rolle (Vaud) and Onnens (Vaud) with the participation of Romande Energie[19]. EPFL has also developed Commelec, a real-time control method of the electrical grid allowing the large-scale integration of renewables[20], which has been demonstrated in the EPFL Microgrid and at the NEST building of EMPA[21].

Private companies are also joining efforts in this domain: the Smart Grid Swiss Association was created in 2011 by 12 electrical companies to promote introduction of smart grids at a national level[22]. They have promoted the introduction of the "SmartGridReady" label[23]. For instance, the headquarters building of Elektroplan Buchs & Grossen AG in Frutigen is considered SmartGrid ready and has demonstrated an 80% reduction of electricity consumption by using a building automation system based on KNX technology[24].

Several start-ups are involved in developing this kind of technology: Swiss company DEPsys has developed GridEye[25], a digital grid optimizer allowing to integrate renewables and to design, manage and automate any power distribution network. Companies like Romande Energie AG have integrated this innovative tool[26]. Imperix, a company in the field of power electronics, develops high-end control equipment and prototyping hardware for smart grids[27]. Misurio AG proposes integrated solutions for optimizing operational planning in the energy sector[28]. Another example is Adaptricity AG, who optimizes and simulates software for adapting electricity grids to renewable energies[29].

Energy storage

S T A R

Switzerland has tested several decentralized energy storage systems, from individual houses to industrial sites. As a successful example, the Walter Schmid AG autonomous building in Brütten, operational since 2016, which is completely independent and disconnected from the power grid[30]. This kind of decentralised systems are promoted by the Holistic Urban Energy Simulation (HUES) platform[31], a project fostered by the "Future Energy Efficient Buildings & Districts" competence centre (one of the eight SCCERs)[32].

Almost 90 MCHF of public fonds have been invested in Switzerland in energy storage technologies in 2017[9]. Another one of the eight Swiss competence centres for energy research, the "Heat & Electricity Storage" centre, is dedicated to storage solutions. Their projects cover five areas: heat storage, battery storage, synthetic fuels and storage technology integration[33]. Thermal energy storage is expected to play an important role in Switzerland's future energy system since heat generation is responsible for about 50% of primary energy consumption. ETHZ, EPFL and SUPSI in collaboration with an industrial partner, Alacaes SA, have developed what could be the world's first adiabatic compressed air energy storage system, a possible alternative to pumped hydro storage to store energy during periods of excess power generation[34]. In a project between PSI and ETHZ, a full cell sodium-ion battery has been developed as a more economical alternative to Li-ion batteries[34]. Another proposition to "store" the excess of energy from renewable intermittent energy sources, is to use it to reduce the CO2 footprint by converting it into fuels. A collaboration between PSI, ETHZ and University of Bern has managed to demonstrate the feasibility of the conversion, and the development of a prototype is planned[33]. The centre is also investigating in new materials for energy storage with hydrogen[35]. An industrial prototype consisting of a formic acid-based power supply unit, using a PEM (proton exchange membrane) fuel cell for electricity production was presented in 2018, a project resulted from the collaboration between EPFL and GRT Group SA[36].

Solid-state batteries are also an alternative to Li-ion batteries currently in use, which no longer contain flammable electrolyte materials. In 2016, researchers of ETHZ presented an entirely solid-state battery, assembled using methods of the industrial production[37]. University of Geneva is also involved in developing solid-state electrolyte materials[38]. In 2019 the Swiss Federal Laboratories for Material Testing and Research (EMPA) and the Fraunhofer Institute

for Silicate Research have launched a 3-year research project aiming at removing the most important technological barriers to the industrial production of solid-state batteries. The project would also reduce dependency on Asian companies, who mainly control the Li-ion battery market today[39].

Swiss start-ups also play a role in the development of new solutions for energy storage: Battrion AG proposes innovative technology that modifies the microstructure of the Li-ion batteries to achieve faster charging and more efficient use[40]; Enairys Powertech manufactures solutions for the management and storage of clean energy based on compressed air[41].

S T A R

Nuclear fusion

In 2017 the Swiss voted and accepted to phase out nuclear (fission) power by 2050 at the latest. Construction of new plants or modification of existing plants is banned. Nuclear fusion is a clean alternative, which does not seem to be a key energy technology in Switzerland. From more than 400 MCHF invested in R&D related to the Energy Strategy 2050 by the Federal Government, only 25 MCHF have been assigned to projects related to nuclear fusion[9]. No mention of this technology is found in the research reports from the eight Swiss Competence Centres for Energy Research[42].

However, Switzerland participates in international research projects in nuclear fusion in a European context[43], and in particular ITER, one of the largest international collaboration projects designed to prove the feasibility of fusion as a large-scale and carbon free source of energy[44]. The Swiss Plasma Centre (SPC) at EPFL[45] is one of the world's leading fusion research laboratories and they actively participate to the construction and development of ITER. The TCV ("Tokamak à configuration variable") experiment of the SPC is, together with two experiments in Germany and United Kingdom, considered in the European Roadmap for fusion energy.

S T A R

Negative Emission Technologies (NETs)

Capturing carbon dioxide is another solution to reduce environmental emissions and to increase fuel efficiency. This exactly what Negative Emission Technologies do. Swiss start-up Climeworks has developed the world's first commercial carbon removal technology that captures CO2 directly from ambient air through engineered chemical reactions[46]. They have several CO2 removal plants in different countries; the one in Iceland, for instance, stores the CO2 in the subsoil, where it reacts to form solid minerals[47]. Climeworks proposes also other uses for captured CO2 (elaboration of fertilizers, production of carbonated drinks, etc.). However, their technology is still expensive and energy intensive, so for the moment their plants make only sense if combined with renewable energy sources.

Swiss Academy of Sciences emphasizes that NETs should be complementary measures that cannot replace efforts focused on reducing emissions[48]. In this sense, the Swiss parliament has recently accepted that NETs must be tackled and considered in the future swiss political energy strategy[49].

S T A R

Companies involved

Several companies have been mentioned and are involved in developing energy solutions mentioned in this report, such as Alacaes SA[50], GRT Group SA[51], Flumroc AG[52], Leclanché SA[53], Arbon Energie[54,55], DEPsys[56], Romande Energie SA, Swissgrid AG[57], Imperix[27], Misurio AG[28], Adaptricity AG[29], Battrion AG[40], Enairys Powertech[41] and Climeworks[58].

The Smart Grid Suisse Association, founded in 2011 by 11 swiss enterprises, now counts 12 members[59]: AET – Azienda Elettrica Ticinese, AEW Energie AG, BKW, CKW – Centralschweizerische Kraftwerke AG, EWZ – Elektriztätswerke der Stadt Zürich, EKZ – Elektriztätswerke des Kanton Zürich, EWB – Energie Wasser Bern, Groupe E, IWB – Industrielle Werke Basel, Repower AG, Romande Energie SA, SIG.

Among the top 100 Swiss start-ups 2018[60], six are related to clean technologies. Several examples are: Insolight SA (developing solar panel with record efficiency)[61], H55 AG (electric propulsion solutions)[62], GRZ Technologies AG (renewable energy storage solutions)[63] or Skypull SA (renewable wind energy with tethered hybrid drone)[64].

Over the last 10 years, 207 clean technology start-ups have been created in Switzerland and are still active, 63 of them are directly related to the development of clean energy solutions[65].

Social impacts

One of the eight SCCERs is focusing not on technology but on people and their behaviour (the Swiss Competence Center for Research in Energy, Society and Transition, CREST)[66]. Interdisciplinary research teams (economists, psychologists, political scientists and legal scholars) propose recommendations for policy and business measures that support energy transition. Their research looks at incentive schemes, social acceptance and company behaviour. They investigate how to encourage the proliferation of efficient technologies and behavioural changes in private households.

More than 5000 swiss households have participated to surveys made by CREST focusing on socio-economic, psychological and sociological aspects to optimally support authorities and companies through the energy transition process.

>>

Conclusions

Switzerland's strengths	Switzerland's weaknesses
• R&D • Political awareness (strategic plans in place) • Hydroelectrical capacities	• Limited classical resources • Limited territory
Opportunities	**Threats**
• Reduce dependency on imports	• Private households' behaviour • Fusion nuclear energy is not considered in the political strategy

List of links included in the article

1. https://www.swisscom.ch/en/about/medien/press-releases/2015/05/20150512-MM-selbstfahrendes-Auto.html
2. https://www.postauto.ch/fr/projet-smartshuttle
3. https://www.mobility.ch/en/news/self-driving-vehicles/
4. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-70243.html
5. https://www.lenouvelliste.ch/articles/suisse/transports-publics-les-navettes-autonomes-se-multiplient-en-suisse-mais-pour-quel-bilan-845877
6. https://staedteverband.ch/cmsfiles/180911_baslerfonds_afz_phase_a+b_summary_f.pdf
7. https://www.cnbc.com/2018/09/14/hyperloop-the-revolutionary-tech-that-could-change-transport-forever.html
8. https://www.rts.ch/info/regions/valais/10068875-le-valais-accueillera-le-premier-site-de-test-en-suisse-de-l-hyperloop-.html
9. https://www.rts.ch/decouverte/sciences-et-environnement/environnement/la-mobilite/10292791-retour-sur-efploop-le-projet-suisse-qui-a-atteint-la-finale-de-l-edition-2018-du-concours-de-l-hyperloop.html
10. https://www.post.ch/fr/notre-profil/entreprise/medias/communiques-de-presse/2016/la-poste-teste-des-robots-de-livraison-autonomes
11. https://eu-smartcities.eu/initiatives/840/description
12. https://www.ge.ch/document/pionnier-canton-geneve-annonce-sa-participation-etude-europeenne-faisabilite-drones-taxis
13. https://www.bloomberg.com/news/articles/2019-01-13/swiss-rail-service-planning-electric-air-taxis-sonntagszeitung
14. https://www.thelocal.ch/20190114/switzerlands-sbb-sets-sights-on-hi-tech-flying-electric-taxi-service
15. https://www.post.ch/en/about-us/company/innovation/swiss-post-s-innovations-for-you/drones
16. https://www.post.ch/en/about-us/company/media/press-releases/2019/swiss-post-to-resume-drone-flights-for-medical-services
17. https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/aktivitaeten-des-bundes-.html
18. https://www.nsl.ethz.ch/impact-of-autonomous-vehicles-on-the-accessibility-in-switzerland/
19. https://www.ethz.ch/en/news-and-events/eth-news/news/2019/06/driverless-congestion.html
20. https://www.swissinfo.ch/eng/mobility_-driverless-vehicles-may-lead-to-more-congestion-in-cities/45016308
21. https://developpement-durable.epfl.ch/fr/mobilite/tp/navette/
22. https://bestmile.com/
23. https://www.letemps.ch/economie/demain-deja-voitures-autonomes
24. https://www.ethz.ch/en/news-and-events/eth-news/news/2018/06/home-of-drones.html
25. https://asl.ethz.ch/research.html
26. https://www.atlantiksolar.ethz.ch/
27. http://rpg.ifi.uzh.ch/research_mav.html
28. https://www.astra.admin.ch/dam/astra/fr/dokumente/abteilung_strassennetzeallgemein/automatisiertes-fahren.pdf.download.pdf/Conduite%20automatis%C3%A9e%20%E2%80%93%20Cons%C3%A9quences%20et%20effets%20sur%20la%20politique%20des%20transports.pdf

29. https://news.sbb.ch/fr/article/52794/entretien-avec-le-chef-du-projet-cff-dedie-aux-vehicules-autonomes
30. https://www.amotech.ch/en/company/category/about-us
31. https://www.tpf.ch/en/-/une-navette-automatisee-pour-desservir-le-marly-innovation-center;jsessionid=C0B4BB5A44C-90F543D7039CA3D94D5F7
32. https://www.nzz.ch/zuerich/autonomer-verkehr-fahrerloser-linienbus-zum-rheinfall-ld.1304382
33. https://www.trapezegroup.eu/news/self-driving-bus-in-the-streets-starting-this-march
34. https://www.swissinfo.ch/eng/swiss-innovation_welcome-to-the-drone-valley/44375836
35. https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171094
36. https://www.post.ch/fr/notre-profil/entreprise/medias/communiques-de-presse/2018/robots-de-livraison-la-poste-tire-un-bilan-positif-des-tests-a-duebendorf
37. https://www.letemps.ch/suisse/robots-autonomes-poste-nont-droit-se-deplacer-seuls
38. https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/rechtliche-situation.html
39. https://www.astra.admin.ch/dam/astra/en/dokumente/abteilung_strassennetzeallgemein/merkblatt-fuer-pilotversuche.pdf.download.pdf/Fact%20sheet%20for%20conducting%20pilot%20tests%20in%20Switzerland.pdf
40. https://www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/u-space.html
41. https://www.skyguide.ch/fr/evenements-medias/actualite/#p95092-95111-95112
42. https://staedteverband.ch/fr/detail/conduite-automatisee

Energy

INTRODUCTION

The world is steering towards a seemingly unresolvable paradox. Saving the planet from global warming and pursuing a connected, globalized and prosperous world are, at first glance, incompatible goals. Growing populations and economies, especially in emerging nations, are pushing up global demand for energy. Even though research on and usage of renewable (green) energies keeps expanding, the world will be dependent on fossil fuels, coal and gas in the medium term. Energy demand of megacities and urban areas will increase as a consequence of globalization, population growth and urbanization. New standards of living, usage of computers, cell phones and Internet-of-Things devices, digitization of all aspects of life and industrialization of the world are irreversible and will keep growing. The question of effectively storing and using renewable energy remains necessary[1].

Power Mix: Energy supply will become more complex
Source: IABG

Energy supply remains one of the most pressing questions of today and the future[2]. It concerns all areas of society, the economy as well as the military. The development of military technology has become increasingly dependent on electricity and energy. The militarization of the cyber and information domain is one of the most striking examples.

CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Dependencies of producing states

Imagine it is wintertime, you turn on the heat but your house does not get any warmer. As Russia demonstrated in 2006, energy policy can be an influential bargaining chip. In future, resource scarcity (e.g. rare earths) will increase drastically. Some states have to rely on importing energy[3] or the resources to produce it. Importing states will become highly dependent on exporting states who have access to resources. This can lead to a challenge if cooperation is disrupted - for instance, when political tensions emerge. Since dependencies pose threats to the security of energy supply, the vulnerability of importing countries such as Switzerland increases. It can limit the range of political and military options of a country if some opponents are "off-limits" because of their importance as a supplier of energy.

Conflicts over sources of energy

The potential for conflicts over energy sources increases the more dependent a country is on imported energy. Especially the distribution of rare resources (e.g. cobalt) will be a difficult subject of discussion in the future[4]. With asymmetric and irregular forces like terrorist organizations and revolutionary forces becoming aware of the importance of energy supply, power plants and oilfields in conflict regions become more vulnerable[5].

Infrastructure in Megacities

Europeans are not prepared for blackouts[6]. People living on the European continent are so used to a perfectly functioning electricity network that they do not see the necessity to prepare for a blackout. While Argentina and Uruguay remained comparatively calm about the recent massive incidents[7], a city (and banking centre) like London or Zurich would not be able to handle power failure as well.

Globalization, economic development from agriculture to manufacturing and, finally, to service-related industry has led to the emergence of megacities. It is expected that over two-thirds of the world's population will live in urban areas by 2050[8]. Cities are highly dependent on a steady supply of technology. With mobility and communications relying increasingly on electricity, the blackout of a (mega) city would have severe consequences. It would trigger chaos and panic among large sections of the public. Hospitals and other important infrastructure could only rely on their emergency backups, public transport would be dysfunctional, refuelling would not be possible and the general water and food supply would be disrupted. The banking system would crash. Chain reactions would damage the economy and could lead to enduring economic consequences as well as large-scale riots. The peace of a city relies on its power supply; this makes the energy grid the most critical infrastructure of all.

The importance of uninterrupted energy supply to urban areas and megacities is an open secret. This makes the vulnerability of critical infrastructures a main target for opponents. Especially asymmetric or irregular actors can explore comparatively cheap and effective forms of attacks on power grids, distributors and control systems. Because of digitization and connectedness of infrastructure, it is possible – but not necessary – to use kinetic force to disrupt the power supply of a city. Cyber-attacks as a part of hybrid warfare could be a way for non-state actors such as terrorist organizations to orchestrate the disruption of a city's energy supply. The utilization of dual-use technologies (e.g. drones) poses another new threat, especially from asymmetric actors relying on cheap and publicly accessible (dual use) technologies.

Transformer station: High energy demand makes megacities dependent and vulnerable
Source: IABG

Technology in operations

During World War II, the German Army used 2.75 million horses[9]. They were the backbone of the German troop deployment. Instead of expensive fuel, the horses consumed just hay and water. The German propaganda machine did not mention this because it did not fit into their picture of modern warfare. Since then, most armies have become dependent on fossil fuels to move their troops and systems. In all domains of war-fare (land, sea, air, space, information), energy is important to conduct successful operations. Energy is – besides several other factors (e.g. water, food, secured bases) – one of the most important factors for soldiers to survive in operations. Power must be generated for a functioning operation base (e.g. communication with the home country, internet connection), for devices like navigation systems to function as well as for medical care. Especially in the information domain (including cyber-defence), energy is highly relevant. Without a functioning energy supply, computers or laptops will be inoperative and are therefore useless. Without these devices, soldiers will not be able conduct cyber operations successfully. On the other hand, one could argue that a lack of electricity would result in a return to more traditional ways of communication and therefore safety from cyber-attacks.

While all domains are dependent on energy, its loss has different consequences. Systems on land, sea and in air depend on different kinds of fuel, making different chains of supply interdependent. The supply of high-grade fuel might not be guaranteed in every area of operation. Digitalized communication systems need a constant, uninterrupted flow of electricity to work properly. Interoperability with partners needs certified standards to share energy resources. While aerial systems are more dependent on (jet) fuels, the base of operations and communications has a higher need for electric energy and storage capacities. Land troops are dependent on aerial reconnaissance and fuel-driven land systems such as tanks. Because of the interdependence of all domains, it is hard to say which would be most affected by lack of energy. The military system's overall connectedness makes it more dependent on constant energy supply and more vulnerable as a whole. While western state-actors rely on highly developed and energy-intensive technologies to protect their soldiers, tactics of potential opponents may be less dependent on energy.

Weapons systems

Directed Energy Weapons (DEW) have been an important scheme in the Sci-Fi-Literature since the 1898. In the 1960s, the development of those weapon systems expedited. In the future, those systems will become real threats with high destructive power[10]. Several types have been developed over the years – for example, Directed Energy Weapons (DEWs), High Power Microwave weapons (HPM) or High-Energy Laser weapons (HEL). These weapons use highly focused energy, including lasers and microwaves and can be applied to target personnel, missiles and optical devices. They can reach almost six times the speed of sound and are highly effective. Nevertheless, DEWs, HPMs, HELs are all reliant on energy. Especially for the use of DEWs and HELs a steady and high-energy supply and large-scale energy storage capacities are required so development of these capacities is important to integrate these systems in military airplanes, vehicles or ships. The next decade will reveal the emergence of high-energy weapons as a high speed and highly effective operational capability.

IMPLICATIONS FOR THE MILITARY

Protection of critical infrastructures in Megacities

Protecting critical infrastructure within urban spaces needs a nationwide effort. The military must work together with other state institutions and private actors. Competences and responsibilities need to be assigned by the responsible authorities, depending on the threat and the capabilities of a potential opponent. Resilience of digitized systems and smart grids need to be guaranteed and repeatedly tested. Chain effects of a blackout have to be assessed and minimalized – for example, using back-up generators and energy storage. Especially in urban areas, it is the responsibility of government agencies to protect power supply from kinetic and cyber-attacks.

In case of a successful attack on a city's energy supply, emergency and control plans need to be developed, imple-

mented and practiced. Continuing urbanization poses a huge challenge to current security concepts. Further formations of large urban areas need to be included in current planning and concept development.

Energy supply in the military

Besides the security of energy systems in the home country, the military must diversify its energy during operations. Bases cannot solely rely on fossil fuel, but also have to use solar energy, wind backups and generators. To be independent from external factors, bases have to be energy-efficient and energy-diverse. One example is a mobile hybrid solar-plus-battery system, which could reduce the dependency on diesel-powered generators and reduces the demand of diesel convoys. Moreover, energy storage systems on base can guarantee their independence.

These energy storage capacities are relevant outside as well as inside bases. New battery systems allow enduring, time-consuming operations outside of base and increases resilience. However, those systems are heavy and cumbersome. The development of compact solutions is therefore essential – and collaboration with scientists indispensable. Energy storage also enables decentralized production chains and additive manufacturing. With the help of 3D printers, soldiers can produce materials and replacements. Also, high-energy weapon systems are reliant on energy supply and the development of energy storage capacities.

CONCLUSION[11]

To counter future threats, it is vital that states search for new resources, efficient methods to produce energy and form stable alliances. Moreover, states have to invest in research in order to find new ways to produce and store energy. The supply of energy will be of greatest importance. Military cooperation with the private sector is important to secure critical energy infrastructure. Moreover, diversification of energy sources is necessary, especially on operation bases. The development of new energy storage capabilities helps soldiers enduring in operations while increasing operational bases' autonomy. New high-energy-weapons develop fast and gain more importance in war.

SWOT-ANALYSIS for swiss military planners

Strengths • Stable relations to exporting partners • Energy Strategy 2050[12] • National Strategy for the Protection of Critical Infrastructures[13] [13a]	**Weaknesses** • Dependency on energy imports[14] • Political pressure on nuclear energy
Opportunities • Nuclear phase-out as start for renewable energy • Cooperation with technological advanced civil corporations (adaption of energy innovations)	**Threats** • Hybrid attacks from state-actors • Vulnerable urban areas as targets of terrorist organizations • Cyber-attacks on energy grid[15]

List of links included in the article

1. World Economic Forum (2019): These are the 4 most likely scenarios for the future of energy. Online: https://www.weforum.org/agenda/2019/05/chart-of-the-day-here-are-4-future-energy-scenarios-and-only-2-look-remotely-sustainable/. (last download 18.06.2019)
2. See articles in "Science-Fiction" and "Future trends" in "Energy" chapter of this publication
3. https://www.spiegel.de/wirtschaft/energiestreit-russland-dreht-georgien-das-gas-ab-a-456254.html
4. See «Future trends» in «Energy» chapter of this publication: Two-thirds of the global supply of cobalt today are from the Democratic Republic of the Congo, while the majority of batteries — 65% by 2021 — are, and will be, manufactured in China, which is investing heavily to diversify the mix of battery materials.
5. https://www.theguardian.com/world/2014/nov/19/-sp-islamic-state-oil-empire-iraq-isis
6. https://bnn.de/nachrichten/blick-in-die-welt/blackout-experte-warnt-vor-stromausfall
7. https://www.zeit.de/gesellschaft/zeitgeschehen/2019-06/blackout-argentinien-uruguay-stromausfall-mauricio-macri
8. «Future trends» in «Mobility» chapter of this publication
9. https://www.welt.de/geschichte/zweiter-weltkrieg/article159718383/Sie-waren-die-wichtigsten-Helfer-der-Wehrmacht.html
10. Air Power Australia (2014): High Energy Laser Directed Energy Weapons. Online under: http://www.ausairpower.net/APA-DEW-HEL-Analysis.html (last downloaded 27.06.2019)

11. https://www.cilip.de/2003/08/29/militaerische-assistenzdienste-die-schweizer-armee-hilft-im-inland-aus/
https://www.vtg.admin.ch/de/aktuell/einsaetze-und-operationen.htmlhttps://www.vtg.admin.ch/de/aktuell/einsaetze-und-operationen.html
https://www.gsoa.ch/armee-einsatze-im-inland/
https://www.aargauerzeitung.ch/schweiz/wann-genau-kommt-die-schweizer-armee-zum-einsatz-129733962
https://www.20min.ch/schweiz/news/story/In-diesen-Notfaellen-rueckt-die-Schweizer-Armee-aus-16770695?httpredirect
12. https://www.bfe.admin.ch/bfe/de/home/politik/energiestrategie-2050.html
13. https://www.babs.admin.ch/de/aufgabenbabs/ski.html
https://www.sta-network.ch/wp-content/uploads/2016/07/Referat_Oberst_F_Huber_Schutz_kritischer_Infrastrukturen.pdf
14. https://www.tagesanzeiger.ch/schweiz/standard/Die-Schweiz-importiert-jedes-Jahr-nobrfuer-13-Milliardennobr-Franken-Energie-/story/25368868
15. https://www.vtg.admin.ch/de/aktuell/themen/cyberdefence.html#bedrohung

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

Mobility

Drivers vs autonomous vehicles; fossil fuel vs electricity; ground vs air; these are only a few alternatives that might come to mind when thinking about mobility. Mobility is, however, not only about goods and people, but also about information moving at unprecedented speed, the digital allowing the stealthy crossing of physical boarders. How will all these new possibilities combine and challenge our more classical (and reliable?) logistic models? The answers will appear by asking ourselves the right questions and stepping out of our present comfort zone. Immobility and cumbersomeness are long dead; welcome to a world of speed and agility where dimensions interact and separate domains now connect!

A DOUBLE-ACTION MAGAZINE

A disturbing (im)mobility

From flying cars to autonomous cars

Has anyone not dreamt of a flying car? Strange cars illustrate the covers of the American pulp magazines of the 1950s like the DeLorean DMC-2 in the film Back to the Future, Part II (Robert Zemeckis, 1989), the flying car has fuelled the fantasies of many generations, to the extent that this motif seems actually to have become, perhaps despite itself, the icon of a resplendent future. On this subject, we should note that this same future cannot be perceived other than with disappointment, because to date, no flying car – other than a few experimental prototypes – has crossed our skies, which is on the other hand heavily populated by planes. However, rather than gazing towards the skies in the hope of spotting a flying car, we should remember that science fiction is destined to create worlds with a futuristic appearance: science fiction stories are destined to suggest that the future represented was feasible. This procedure is an illusion, a mirage: it serves to add credibility to the narrative world – a future world must have its share of novel technologies – rather than in anticipation of our future. More substantively, at least two reasons can be cited to capture one's interest and populate a fictional world with flying cars: the first, by far the least interesting is specifically this need to "futurise", to create a décor that gives the reader the impression of moving around in a world in a future state. In this sense, flying cars – in the same way as laser guns, cosmic space ships, or the multiple, eccentric, strangely named gadgets – are semiotic gearings used to shift the science fictional world to at least one remove from the empirical world. The second reason will be of more interest to us: the flying car – and futuristic modes of transport – can also be a metaphor evoking something other than a means of transport, the sign of an altered reality that is condensed, full of imagery, in a motif that is readily intelligible. In other words, the metaphor of the flying car could indicate, in an analogous mode, something in our world for which it is the offset emblem. And there, an entire interpretative horizon opens up for us – as has been seen in the previous texts on sprawling cities, or energy poverty.

The flying car symbolises, in the first instance, human ambition to conquer all the dimensions of the universe, and not to allow limitations to stop it – limitations that the human spirit treats as obstacles to be overcome. Is this not also one of the central values that has driven technological innovation since the beginning of the 19th century? Crossing the boundaries? Pushing back the limits of knowledge? Not allowing oneself to be confined by external contingences? According to this perspective, the flying car might be the sign – textual, or recorded on film – of our incessant desire to go beyond the realms of our condition, always higher, faster, further. However, science fiction, when it 'metaphorises' our techno-scientific utopias, does not do so by way of an apologia, but in order to indicate, in an evocative way, one the consequences: utopia goes hand in hand with the extravagant – what the Greeks referred to as hubris, which, in a number of narratives, is linked to the figure of the mad scientist, who refuses to remain within the confines assigned to him. Flying cars, just like, more recently, autonomous cars, generate problems: traffic jams are even more disastrous, with people not only overpopulating the ground, but also the skies. This is what we see for example in Le Cinquième élément [The Fifth Element] (Luc Besson, 1997) where human excess has saturated reality by denaturing it, and by inviting the viewer to experience a feel of nauseous malaise: there are cars everywhere, the world has become a giant traffic artery, there is no more free open space, or space for contemplation – there is simply mankind, and nothing but mankind. This unpleasant sensation resonates closely with the words of the physician Werner Heisenberg, who saw in technological development the sign of an unconscious desire on the part of man to be surrounded by his own creations, in other words, by himself. It is also this omnipresence of man in all the interstices of reality that led Heisenberg to state that science – techno-sciences, we might say now – was like a rudderless boat, a boat that was advancing and contaminating everything without knowing why...

But this is not all. The flying car – and its contemporary avatars – can also 'metaphorise' the paradoxes of mobility in a particularly acerbic way: it operates like a symbol of society that goes at "a hundred miles an hour" and which is facing its own incoherences. In fact, as we know, the free market world, but also the digital world, are worlds constructed on the notion of speed, the pursuit of impulsive instantaneity: one must travel fast, be mobile, have the capacity to be everywhere at once, one must not allow for time the – sometimes tragic – depth that it was able to occupy in past cen-

turies. And given that ubiquity is not yet included amongst our competences, there is only the development of means of transport that enable the shortening of space and time, not wasting a minute or a centimetre – while at the same time retaining the comfort of the personal vehicle. However, and the ecological issues have rendered this paradox even more evident: how can one be mobile without, in the same movement, also being a polluter; and how can one not be a polluter if individual comfort takes precedence over collective initiatives (car sharing, public transport, etc.), causing traffic saturation and the hypertrophy of the urban networks? According to this perspective – exploited to the full by science-fiction authors, notably in the film Minority Report (Steven Spielberg, 2002) –, the futuristic modes of transport of science fiction seek to create an awareness both of travelling fast, and the consequences of such a necessity: disaster movies, for example cannot do without the sequence – which has now become commonplace – where individuals, trapped in the metal shells at rush hour, look on, powerless, and fascinated as a tsunami breaks over them (for example in the film The Day after Tomorrow by Roland Emmerich, released in 2004); a tsunami of water or ice whose origin is to be found in the actions of individuals with little care for the fate of their ecosystem. Concerning post-apocalyptic narratives, where space has resumed its immensity and where time has suddenly extended, it is scarcely surprising to see cars left on the roadside, abandoned, relegated to their coffin symbolism – a symbol applied to mankind, but also to nature. This situation is set out particularly well in the novel The Road (Cormac McCarthy, 2006): the world has been completely destroyed, cars are wrecks stranded in the ruins of civilisation, and human beings, haggard, seek through dialogue, and thus through the articulation of a discourse, to recreate their identity in a world where everything has become dangerous and where space – to be crossed, but also the space of language – can no longer be ignored and reduced to a breeding ground where information is exchanged. The two protagonists in The Road rediscover, painfully, that space is first of all a space where existence is deployed and not a location to be "consumed" or "optimised".

Conclusion

Questions relating to mobility are at the heart of numerous social debates, because they affect as much the form our daily actions take, as they do individualism or ecology. Must we continue to give priority to global mobility, thus a free market, or should we come together and co-operate – but at what price? –, mobility in proximity? She we continue, for our own personal comfort to favour solipsistic personal transport, or use public transport together? Should we mourn the loss of our week's holiday on a paradise island or learn to view with pleasure the environment that is all around us? These questions, and many more, are matters of choices for civilisation; science fiction, albeit more modestly, seeks not to respond to these interrogations, but to set out what it is that disturbs us in these same interrogations. In fact, the narratives surely confront us with our own paradoxes? We seek comfort, while recommending a way of life, which can ultimately only annihilate the very thing that we seek; we want a future for our children, while we are incapable of doing without this drug represented by the flying car, the autonomous, private vehicle... Does the car exert such a power of dependency that we would be unable to do without it? Science-fiction askes the question in a different way: are we addicted to individual means of transport or to what they represent, in other words, freedom, comfort, independence at last attained? It is perhaps at this point that the car transforms into a coffin: it encloses us in our impossibility of encountering the world and others...

Reimagining mobility in our cities: smart, connected megacities of our future

Image: A residential compound in Yanjiao, about an hour from downtown Beijing. Photography credit: Sim Chi Yin, New York Times

Today, there are 33 megacities[1] worldwide, each with populations of 10 million or more. They present a wealth of investment, education and employment opportunities, but also face rising issues such as overcrowding, traffic congestion, air pollution and income inequality.

Currently, half of the world's population lives in urban areas, but by 2050, this will increase to two-thirds[2] with 70% of that growth happening in 10 emerging-world centres: Delhi, Dhaka, Kinshasa, Shanghai, Lagos, Cairo, Chongqing, Karachi, Beijing and Mumbai.

So how will our cities improve transportation systems to cope with this rapid growth in population? What are the technological innovations that will help make mobility in cities more functional and sustainable, and ultimately make cities more liveable?

This article focuses on key mobility trends and technologies being implemented and regulated by companies and cities across Asia, North America, and the Middle East, and gives insight into a future driven by design — one that reimagines urban space and uses technology such as 3D digital mapping, high-tech cameras & sensors, data transparency, artificial intelligence and robotics to make mobility through our cities simpler, faster, and more efficient.

Autonomous and connected mobility: From Drivers to Passengers

It is expected that by 2030, one in four cars on the road will be autonomous. But which cities are leading the global race to replace the current automotive industry with a safer and more efficient solution for getting from A to B?

In the United Arab Emirates, the local transport authority in **Dubai** recently launched the world's first tests of autonomous, modular and electric pods[3] as part of their wider strategy to make 25% of all journeys in Dubai autonomous in the next 12 years, with units designed to travel short distances through metropolitan areas in dedicated lanes. The pods can also be joined together or detached in less than 15 seconds, marking the next phase of the future of ride share services in our cities. After travelling on pre-programmed routes for the inaugural years, the pods will eventually be available for pick-up from home using an app.

Image courtesy RTA, Dubai

Truck Drivers: Moving from Humans to AI

Turning to the movement of food and goods, autonomous long-haul trucking is likely to fill gaps in ever-increasing demand, with urban density contributing to rising costs of storing goods in urban warehouses. Instead, the future will rely on comparatively fast delivery over greater distances. Autonomous trucking was approved in the United States[4] in 2018, with early commercialization predicted within the next two years and full automation anticipated within the next 7-20 years[5].

Reducing the cost of delivery by up to 40%, AI-guided long-haul delivery has shown it could reduce fuel use by 15%, thanks to increasing efficiencies in routes and "platooning" — chaining large numbers of vehicles together to unify movements, reducing drag over long distances. Since 2016, Volvo has deployed a self-driving concept truck[6] in a diamond mine in Sweden, the same year that an autonomous convoy completed a route through Europe[7].

Innovation and Regulation: Autonomous Vehicles in the US

In the **US**, technology companies and governments are working together to create regulations that support innovation and safety concurrently with autonomous vehicle testing without a safety driver[8] being carried out in Arizona, Nevada, and California.

In **Arizona**, a 'braintrust' of companies, government, and universities, the Institute for Automated Mobility (IAM), has recently been set up to collaborate on autonomous vehicle testing in the state. With an industry expected to grow up to $400 billion by 2026[9] due to the expanding food delivery and ride-hailing industries, there is an increased need for the private and public sectors to collaborate to meet the market demands of the next 10 years in the US.

Meanwhile, forecasts suggest automated freight in the US could make redundant any number between 294,000 to 2.1 million jobs[10], with long-distance drivers affected first.

Innovation and Regulation: Autonomous Vehicles in China

In **China**, the pace of urbanization is happening at an unprecedented rate with the urban population expected to hit one billion by 2030. By then, China's cities will add more people than the entire population of the US, and the government is preparing for the pressures on infrastructure and the environment by restricting private car use, building metro systems[11] and high-speed rails.

It has also singled out the autonomous vehicle sector in the Made in China 2025[12] program to transform the country. They suggest that driverless technology will reduce transport costs by 20 cents per mile, car ownership, and reduce carbon emissions in cities already suffering from toxic air quality. This move, alongside a strong technological ecosystem underpinned by global giants Tencent, Alibaba, and Baidu, shows that China is well placed to win the race on creating a driverless future.

The Sky Becomes a Roadway

As urban spaces become more crowded, technology companies are looking to the skies to solve mobility problems of the future.

Image courtesy Volocopter

In **Singapore**, the future of air taxis is being tested , with pilot trials commencing in late 2019. The Volocopter[13] is an 18-rotored human-sized drone that can fly for 30 minutes, adding a new transport option for future urban commuters. However, although the technology is ready for testing, the company still needs to navigate regulatory institutions, and bring governments up to speed with the technology before it's ready for the market, in approximately 5 years.

Fuelling Autonomy: The Future of Maps

Autonomous vehicles require large amounts of data—1gb per second[14] —to stay on the road safely. For maximum efficiency, autonomous vehicles will require a consistent communication system for sharing their location and destination that can be understood by all of the other drivers—robots and humans—on the road.

Such real-time map creation, where human movement is tracked in real-time within dense environments, raises the spectre of surveillance by one's own state and for espionage. This year, the New York Times was able to track the position of the city's mayor[15] , and several employees of nuclear power plants, using data gathered from a weather app which they willingly installed on their phone. The journalists were also able to pull "compromising" data based on other location-based activities.

The future of mobility for smart cities is inherently tied to the need for positioning data; cities will need to balance privacy and security concerns with the need for positioning data in our GPS systems. It is also predictable that maps themselves could become less often used by humans, as we see today an increase in "input and output" models of navigation: asking a phone how to get somewhere, and following its instructions.

Electricity in Motion: Batteries and the Future of Mobility

Today, the transportation sector uses more petroleum, gasoline, and oil than any other source. As the global energy mix moves toward cleaner, locally-produced alternatives, the transportation sector will be radically transformed. Paris, London, Mexico City, Los Angeles and 13 other cities have committed to clean fleets for public transportation by 2025, and 1 to 3 million public charging points for electric vehicles (EVs) could be needed in Western Europe by 2030.

According to a Bloomberg analysis[16] , EVs will match the cost of gasoline vehicles by 2025 and could make up 33% of vehicles by 2040. If 1 billion EVs were on the road by 2050, as predicted by the International Renewable Energy Agency (IRENA), their energy consumption would be equivalent to more than 10% of today's global electricity demand. While this could be cleaner energy, it also needs to be abundant and accessible.

China is emerging as a leader for the adoption of electric vehicles, chiefly through adopting electric buses, which transport more people more efficiently through personal vehicles. As of 2019, China has announced it will not grant permission to new automotive companies that build cars relying on fossil fuels; it also restricts the private ownership of such vehicles.

New technology is also bringing new ideas and approaches. In **Japan**, electric vehicles (EVs) are being evaluated as portable batteries, allowing them to become part of the emergency response grid. In the case of an earthquake or other natural disaster, communities could draw power from their vehicles as if they were electrical generators.

South Korean vehicle manufacturer Hyundai[17] is planning to commercialize an "autonomous valley" service by 2025 to solve the problem of overcrowding at charging stations. Like parking spaces, charging stations are limited, and owners tend to park, charge, and go about their day, using the space for much longer than intended. Hyundai's EV solution is to create self-driving cars that can detect when they reach a full charge, disengage, and move themselves to free the station for another vehicle.

Siemens/Eviation aircraft.

Some batteries might grow wings. Siemens and **Israeli** startup Eviation plan to launch an electric airliner, Alice, for nine passengers in the United States by 2021. A secondary effect of electric aircraft could be a boom in short-distance air travel: today's engines burn most fuel at liftoff, making longer distances more cost-effective. By shifting to electric engines, these fleets could make traveling by air affordable even for local travel.

Rolls Royce, Boeing and Airbus all have hybrid aircraft engines in development. **British** airline EasyJet is looking for 100% electric craft for all flights fewer than 300 miles by 2030, and Norway has called for domestic air travel to be 100% electric[18] by 2040 .

The constraint today is on battery weight: advances in miniaturizing batteries, expanding capacity, or reducing weight could hasten more widespread adoption of electric aircraft. Uber Technologies has been betting that the pace of weight reduction will be fast enough to promote an electric-motor aerial taxi service for launch by 2023. The company has already signed on as an advisor to NASA[19] 's efforts to regulate US air traffic for the coming era of electrified vehicles in the sky.

Courtesy of Uber

Rebuilding our transit systems: A Return to Railways

As metro transit systems around the United States face the reality of aging infrastructure and increased needs to meet the challenges of a growing population, some cities are developing incubation programs to help find solutions for the future. In **New York**, an aging subway and bus system has led the Metropolitan Transportation Authority (MTA) to turn to tech companies for solutions by setting up the nation's first transit tech lab[20] , an incubation accelerator program for start-ups solving public transportation challenges.

They are seeking to answer two main challenges faced by the country's largest public transport system suffering from increasing congestion and breakdowns: how can we better predict subway incident impacts and how can we ensure buses run faster and more efficiently? The MTA believes this challenge will incubate transit-improving tech possibilities such as ultra-wideband wireless technology, onboard sensors and cameras, and robotic installation systems to control subway tunnels. Another goal is to invent new A.I. solutions that utilize big data to analyze historical subway data to find patterns that can be used to predict future disruptions.

In China, a main challenge facing urban planners is how to meet the demands of a growing population in the tight confines of existing cities. So they're going underground, and building high-speed metro networks marking a revolution with almost as many kilometres of rail tracks being built in the next decade as in the past 150 years. Although this technology isn't 'new', it marks a trend in what mobility will look like in some of our megacities in the near future: underground and electrified.

In California, entrepreneur Elon Musk's "Boring Company" has pinned investments and energy into the Hyperloop, an encapsulated train using air pressure and gliding mechanisms to reach theoretical speeds of 760 mph (1,223 km/h), though the current record holds at 260mph (418 km/h). Currently, there are proposed routes for Hyperloop connections between Los Angeles and San Francisco in the United States, Chennai and Bengaluru in India, and Helsinki and Stockholm, a journey which take just 30 minutes by tunnelling beneath the Baltic Sea. The first European test track will open in Valais in 2019[21].

Back to the Streets

In urban communities in the **U.S**, streets make up 30% of all space. The traditional notions of how streets are used is being challenged from merely supporting the movement and storage of vehicles to one which is more aligned with societal values. Greenfield Labs[22] —a Ford Smart Mobility research and innovation team—is questioning what streets might become in the future with a vision of serving a variety of functions and needs: from walking, biking, running a business, relaxing, exercising, and connecting with peers. Streets will be seen as economic & social generators: an area for social activity and a conduit for everything that moves.

Over the next 15 years, governments and technology companies will play an interconnected role in redesigning mobility in our cities to meet the needs of rising populations and infrastructure constraints. China's ability to fast-track government regulation on the latest innovations means they will lead the way in rolling out new technologies that reimagine mobility in megacities, with autonomous transport expected to hit the consumer market within the next five years. In other major cities around the world, human-centric design and data-driven technologies, such as smart network systems and autonomous vehicles, will transform urban environments, but the timing of this will depend on the ability of governments to keep up to speed with innovation.

List of links included in the article

1. https://en.wikipedia.org/wiki/Megacity
2. https://www.theguardian.com/world/2018/may/17/two-thirds-of-world-population-will-live-in-cities-by-2050-says-un
3. https://www.reuters.com/article/us-emirates-transportation-autonomous/dubai-tests-autonomous-pods-in-drive-for-smart-city-idUSKCN1GD5G6
4. https://www.usnews.com/news/national-news/articles/2018-10-15/the-race-is-on-after-feds-pave-way-for-driverless-trucks
5. https://www.theicct.org/publications/automation-long-haul-challenges-and-opportunities-autonomous-heavy-duty-trucking-united
6. https://www.youtube.com/watch?v=uOlsTeNqtQ8
7. https://www.theguardian.com/technology/2016/apr/07/convoy-self-driving-trucks-completes-first-european-cross-border-trip
8. https://www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/
9. https://venturebeat.com/2018/10/11/arizonas-institute-for-automated-mobility-will-research-and-develop-autonomous-vehicle-technologies/
10. http://laborcenter.berkeley.edu/driverless/
11. https://medium.com/@UrbanResilience/8-ways-china-is-winning-on-transportation-1032687006a9

12. http://english.gov.cn/2016special/madeinchina2025/
13. https://www.volocopter.com/en/
14. http://www.kurzweilai.net/googles-self-driving-car-gathers-nearly-1-gbsec
15. https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html
16. https://about.bnef.com/electric-vehicle-outlook/
17. https://www.engadget.com/2019/01/04/hyundai-kia-self-charging-ev/
18. https://www.theguardian.com/world/2018/jan/18/norway-aims-for-all-short-haul-flights-to-be-100-electric-by-2040
19. https://www.nasa.gov/partnerships/about.html
20. https://transitinnovation.org/lab
21. https://www.swissinfo.ch/eng/sci-tech/future-transport_canton-valais-to-test--hyperloop--train-technologies/44616820
22. http://greenfieldlabs.com/

Future mobility in Switzerland

Today, the biggest city in Switzerland is Zürich with ~1'354'000 persons. With 84.8% of the population living in urban areas and a very small territory, Switzerland will cope with the same problem as megacities in terms of transportation. Autonomous vehicles will play a major role in the solution.

S Start: no real activities | T Trend: Early activities | A Advanced | R Ready | S T A R

Tests of terrestrial autonomous vehicles

S T A R

First test in Switzerland takes place in 2015 with the Swisscom's "New future" project in Zürich, where a driverless car was tested[1].

A few more tests on individual public transportation have been conducted since then, like the "Smart Shuttle" project being performed by PostAuto Schweiz AG in Sion[2], or the collaboration between Mobility, SBB, ZVB and the Technology Cluster Zug in Zug[3]. Nine authorisations are currently granted, concerning mainly public transport companies[4,5]. Several other test applications are being treated by the Federal Roads Office4.

Autonomous trains are being already operational for several years in well-defined and isolated routes (Lausanne metro, airport train shuttle in Zurich). However, no solution has been implemented or tested for long distance and regional lines[6].

Goods and persons transportations may be disrupted by Hyperloop technology, a fully autonomous and enclosed system that would produce no direct carbon emissions first envisioned by Elon Musk[7]. A first test of Hyperloop in Switzerland (Eurotube[8]) should take place in a 3 kilometers test track located in Vallis during the second half of 2019. The CFF are involved in the project. It is not yet defined if it will be dedicated to persons or goods transportation. EPFL is also involved in this technology with the EPFLoop[9] project that reached the final stage of 2018 Hyperloop contest in Los Angeles.

Swiss Post has tested autonomous delivery robots in Bern and other swiss cities[10] for goods transportation.

Tests of aerial autonomous vehicles

S T A R

Canton of Geneva has been a pioneer in joining the European initiative "Urban Air Mobility" (UAM)[11] to evaluate the feasibility of drone taxis for transportation of passengers[12].

SBB is also interested in aerial transportation, and they have signed a letter of intent in the beginning of 2019 with German company Lilium to develop flying taxi services to transport passengers from train stations to their destinations[13,14]. For the moment a pilot would be present in the aircraft.

Swiss Post has tested autonomous delivery drones to transport laboratory samples in Zurich and Lugano[15]. After successfully completing over 3000 flights, all drones have been grounded on April 2019 following an emergency landing[16].

Innovation

S T A R

The Federal Roads Office has launched an "automated driving" research package to enable research institutions to examine the future of mobility[17].

For instance, ETH Zurich is involved in the research in future mobility by simulating different scenarios in Switzerland[18]. They have been mandated by the federal government to analyse the impacts of self-driving vehicles on the capacities of Switzerland's transport system. One of their last publications[19] show that autonomous taxis would not displace personal transport as long as private autonomous vehicles are also available[20].

EPFL has been also traditionally interested in mobility, already since the 90s when they failed to launch the "Serpentine" project in Lausanne due to legal reasons[21]. More recently EPFL created a research department on this topic from which Bestmile[22], a start-up, was created for the software operation of autonomous fleets[23].

Drones and in particular fully autonomous drones and their potential are the subject of much R&D in Switzerland, and

the country plays a leading role in drone technology nowadays[24]. To mention only a few, the ETH Zurich's "Autonomous Systems Lab"[25], that has developed AtlantikSolar[26], the first unmanned, autonomous and solar powered aircraft; or the "Robots and Perception Group", affiliated with both the University of Zurich and ETH, which is developing aerial robots that don't need GPS or remote controllers[27].

The Federal Institute of Metrology (METAS) has implemented a project to acquire know-how on "autonomous vehicles and data security"[28].

The federal government also encourages platforms to exchange know-how, like www.auto-mat.ch, launched in collaboration with the Touring Club of Switzerland (TCS).

Companies involved

S T A R

The main companies involved in autonomous terrestrial vehicles in Switzerland are Swisscom[1], PostAuto Schweiz[2], SBB[29], Swiss Post[15], AMoTech[30] and Mobility[3], as well as regional public transportation entities like TPF (Transports publics friburgeois)[31], Schaffhauser Verkehrsbetriebe[32], ZVB (Zugerland Verkehrsbetriebe)[3] or VBZ (Verkehrsbetriebe Zürich)[33].

Concerning aerial transportation, SBB[14] and Swiss Post[10] are involved in developing new solutions. Additionally, Switzerland is very well known for its competencies and innovation in drone technologies, with more than 80 start ups in what is called the "Drone Valley"[34].

Transportation of people

S T A R

The Federal Roads Office report[28] on the consequences and impact of automated driving considers that despite Switzerland has a high-quality transport system, the infrastructure is reaching its spatial, ecological, social and systemic limits. This fact leads to an urgent need for a greater efficiency. Autonomous vehicles open up new opportunities to better use the available capacities, with the condition that people are prepared to change their mobility behaviour and are willing to share the use of their vehicles. Otherwise, the focus on individual private transport only, together with the increase in demands coming from new user groups such as the elderly, people with disabilities or children, could give rise to an even greater traffic volume. An ETH's study on the Zurich area corroborates this possible negative effect[19].

The use of autonomous vehicles and the further development of car sharing and car pooling services could make the boundary between public and private transport become fuzzy. The federal government, the cantons and municipalities, as co-proprietors of transport companies will have to position themselves on this rapidly changing market.

Residential areas could become more attractive due to the improved accessibility which could favour rural sprawl. To avoid this trend the government has already introduced precautionary measures within the scope of the Spatial Planning Act[28].

Concerning aerial transportation of people, the "Drone taxi" project of the canton of Geneva will be evaluated during 2019 and if positive, a first demonstrator is expected to be launched in 2020-2021[12].

Transportation of goods

S T A R

In 2018, the federal government estimated that Truck Platooning and autonomous long-haul trucking for transportation of goods wouldn't add significant value to the transport system due to the small Swiss territory. Such technology is not adapted to "last mile delivery" and the swiss road system is hardly compliant with its requirements. Nonetheless, Switzerland is open to a test phase[35].

Autonomous robots open up new possibilities for the distribution of goods in the last kilometer. Swiss Post has considered and tested this option for a flexible and fast transportation of parcels in a local environment (same day delivery, same hour delivery, delivery of food or medicine). First test results are encouraging even though swiss legislation doesn't allow yet the use of completely autonomous robots and an accompanying person had to supervise the robot's movements during the tests[36,37].

The arrival of autonomous vehicles is expected to encourage providers of freight services to shift to the transport of goods by road, and consequently rail freight transport and the swiss federal government's policy of shifting the carriage of goods from road to rail would come under increased pressure[28].

Aerial vehicles propose several advantages in logistics, especially in sectors like healthcare where the delivery speed might be crucial, in the last mile to transport high priority consignments, or to deliver supplies to places cut off from the outside. Swiss Post is aware of the importance of drones in this area and has been a pioneer in the deployment of drones in Switzerland for transportation of goods[15].

Regulation

S T A R

The Vienna Convention on Road Traffic represents the central regulatory framework, which has been adapted in 2016 to allow the introduction of driver assistance systems. Nevertheless, the current legal situation imposes the presence

of a driver that can override the system anytime, and therefore forbids the use of completely autonomous vehicles in Switzerland[38]. It won't be possible until the necessary level of vehicle safety has been demonstrated and the international legal framework has been adapted.

In order to be ready to adapt to the international changes, swiss road traffic legislation will have to consider traffic regulations (under which conditions drivers could be released from their obligations), homologation of vehicles, licensing of drivers, criminal liability issues and insurances.

A fact sheet for conducting pilot tests in Switzerland is available in the website of the Federal Roads Office[39]. During the different implantation phases of autonomous vehicles, the coexistence of vehicles equipped with different technologies (and different levels of autonomy) will be a major challenge for the legislator as well as for the operators and users of the roads.

Concerning aerial transport, the European Commission has launched the concept of U-Space to integrate and regulate drones in the airspace. The Swiss Federal Office of Civil Aviation has already facilitated the creation of the Swiss U-Space Implementation (SUSI) platform[40], and the Swiss U-Space was recently presented (June 2019) at a summit hosted by Skyguide in Geneva[41].

Social impacts

Several studies coincide on the positive effects that autonomous vehicles would have for the society: increased service flexibility, increased comfort, increased safety and more accessibility. People would be willing to travel longer distances. New user groups would become more easily mobile, like the elderly, children and people with disabilities. The infrastructure will be more efficiently utilized and the capacity augmented, since distances and time between vehicles could be reduced.

On the other hand, private autonomous vehicles will probably represent higher costs (implementation of sensors and radars, communication requirements). Infrastructures will have to be adapted too (sensors, roads signaling, traffic management, etc.). Different ethical questions will have to be addressed, especially those concerning the responsibility in case of accidents, and the data protection and sharing in a highly connected environment.

New user groups represent nowadays a third of Switzerland's population. Additionally, it is expected that the use of driverless vehicles will imply a considerable number of empty rides, which might increase travelled distances up to 15% in the roads.

The balance between the increase of infrastructure capacity and efficiency and the increase of the demand and empty rides is not clear, and an augmentation of traffic congestion is even possible after full autonomous vehicles are largely adopted. This negative effect will also depend on people's behavior towards the new possibilities offered by autonomous vehicles: are people willing to share their vehicles and to share their journeys with unknown citizens, or would they prefer the comfort of using their own private autonomous vehicle ("Share it" versus "Own it")? Four different scenarios considering also the government's role and other society values are analysed in the report prepared by the UVS (Union des villes suisses) together with BaslerFonds and other partners on the use and effects of autonomous vehicles in Switzerland[42]: the impact might vary from an very individual concept of mobility to a more conscious organization where different options like car sharing, car pooling and public transports coexist leading to a more sustainable mobility.

Conclusions

Switzerland's strengths	Switzerland's weaknesses
• R&D • Well positioned in cellular communications • Pioneering tests performed in Swiss territory • Expertise in drone technologies	• Dependence on international legal regulations • "Follower" role concerning private autonomous vehicles • Dense and saturated terrestrial infrastructure nowadays
Opportunities	**Threats**
• Precursor role in public transportation • Increase of infrastructure's capacity and efficiency • More safety	• Focus on private use of autonomous vehicleslead to an increase of traffic volume and congestion • Cybersecurity and hacking • Public acceptance

You'll find on the next page the list of the links included in the article >

List of links included in the article

1. https://www.swisscom.ch/en/about/medien/press-releases/2015/05/20150512-MM-selbstfahrendes-Auto.html
2. https://www.postauto.ch/fr/projet-smartshuttle
3. https://www.mobility.ch/en/news/self-driving-vehicles/
4. https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-70243.html
5. https://www.lenouvelliste.ch/articles/suisse/transports-publics-les-navettes-autonomes-se-multiplient-en-suisse-mais-pour-quel-bilan-845877
6. https://staedteverband.ch/cmsfiles/180911_baslerfonds_afz_phase_a+b_summary_f.pdf
7. https://www.cnbc.com/2018/09/14/hyperloop-the-revolutionary-tech-that-could-change-transport-forever.html
8. https://www.rts.ch/info/regions/valais/10068875-le-valais-accueillera-le-premier-site-de-test-en-suisse-de-l-hyperloop-.html
9. https://www.rts.ch/decouverte/sciences-et-environnement/environnement/la-mobilite/10292791-retour-sur-efploop-le-projet-suisse-qui-a-atteint-la-finale-de-l-edition-2018-du-concours-de-l-hyperloop.html
10. https://www.post.ch/fr/notre-profil/entreprise/medias/communiques-de-presse/2016/la-poste-teste-des-robots-de-livraison-autonomes
11. https://eu-smartcities.eu/initiatives/840/description
12. https://www.ge.ch/document/pionnier-canton-geneve-annonce-sa-participation-etude-europeenne-faisabilite-drones-taxis
13. https://www.bloomberg.com/news/articles/2019-01-13/swiss-rail-service-planning-electric-air-taxis-sonntagszeitung
14. https://www.thelocal.ch/20190114/switzerlands-sbb-sets-sights-on-hi-tech-flying-electric-taxi-service
15. https://www.post.ch/en/about-us/company/innovation/swiss-post-s-innovations-for-you/drones
16. https://www.post.ch/en/about-us/company/media/press-releases/2019/swiss-post-to-resume-drone-flights-for-medical-services
17. https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/aktivitaeten-des-bundes-.html
18. https://www.nsl.ethz.ch/impact-of-autonomous-vehicles-on-the-accessibility-in-switzerland/
19. https://www.ethz.ch/en/news-and-events/eth-news/news/2019/06/driverless-congestion.html
20. https://www.swissinfo.ch/eng/mobility_-driverless-vehicles-may-lead-to-more-congestion-in-cities/45016308
21. https://developpement-durable.epfl.ch/fr/mobilite/tp/navette/
22. https://bestmile.com/
23. https://www.letemps.ch/economie/demain-deja-voitures-autonomes
24. https://www.ethz.ch/en/news-and-events/eth-news/news/2018/06/home-of-drones.html
25. https://asl.ethz.ch/research.html
26. https://www.atlantiksolar.ethz.ch/
27. http://rpg.ifi.uzh.ch/research_mav.html
28. https://www.astra.admin.ch/dam/astra/fr/dokumente/abteilung_strassennetzeallgemein/automatisiertes-fahren.pdf.download.pdf/Conduite%20automatis%C3%A9e%20%E2%80%93%20Cons%C3%A9quences%20et%20effets%20sur%20la%20politique%20des%20transports.pdf
29. https://news.sbb.ch/fr/article/52794/entretien-avec-le-chef-du-projet-cff-dedie-aux-vehicules-autonomes
30. https://www.amotech.ch/en/company/category/about-us
31. https://www.tpf.ch/en/-/une-navette-automatisee-pour-desservir-le-marly-innovation-center;jsessionid=C0B4BB5A44C-90F543D7039CA3D94D5F7
32. https://www.nzz.ch/zuerich/autonomer-verkehr-fahrerloser-linienbus-zum-rheinfall-ld.1304382
33. https://www.trapezegroup.eu/news/self-driving-bus-in-the-streets-starting-this-march
34. https://www.swissinfo.ch/eng/swiss-innovation_welcome-to-the-drone-valley/44375836
35. https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171094
36. https://www.post.ch/fr/notre-profil/entreprise/medias/communiques-de-presse/2018/robots-de-livraison-la-poste-tire-un-bilan-positif-des-tests-a-duebendorf
37. https://www.letemps.ch/suisse/robots-autonomes-poste-nont-droit-se-deplacer-seuls
38. https://www.astra.admin.ch/astra/fr/home/themes/intelligente-mobilitaet/rechtliche-situation.html
39. https://www.astra.admin.ch/dam/astra/en/dokumente/abteilung_strassennetzeallgemein/merkblatt-fuer-pilotversuche.pdf.download.pdf/Fact%20sheet%20for%20conducting%20pilot%20tests%20in%20Switzerland.pdf
40. https://www.bazl.admin.ch/bazl/en/home/good-to-know/drones-and-aircraft-models/u-space.html
41. https://www.skyguide.ch/fr/evenements-medias/actualite/#p95092-95111-95112
42. https://staedteverband.ch/fr/detail/conduite-automatisee

Mobility

INTRODUCTION

While Swiss Post is developing drones to deliver packages[1], international terrorist organizations use the exact same technology – to deliver bombs onto the battlefield[2]. The technological progress has made the world more connected; it brings everything closer together. Mobility is as high as it has ever been. But what does the term "mobility" mean? And why is mobility and its broad variety of meanings relevant to the future of urban warfare? Mobility describes the ability of people to move from one place to another, in order to be closer to their workplace, or simply to experience a different environment. Hence, a city's concept of mobility concerns public transport, regulation of traffic and planning of infrastructure. Unlimited and immediate mobility of data and information is the consequence of digitization of all aspects of our life. "Social mobility" refers to the movement between social classes – the "American Dream" being one of the most famous examples.

Urban Mobility 2.0: Increasing urbanization calls for new mobility concepts
Source: IABG

Mobility in a military context usually describes the ability to redeploy troops, weapon systems, equipment etc. from one area of operation to another, or from home country to the region of conflict. Mobility can also be a tactical term for the ability of quick movement on the battlefield. When it comes to urban warfare all the addressed meanings of the term "mobility" play a role for future military planning.

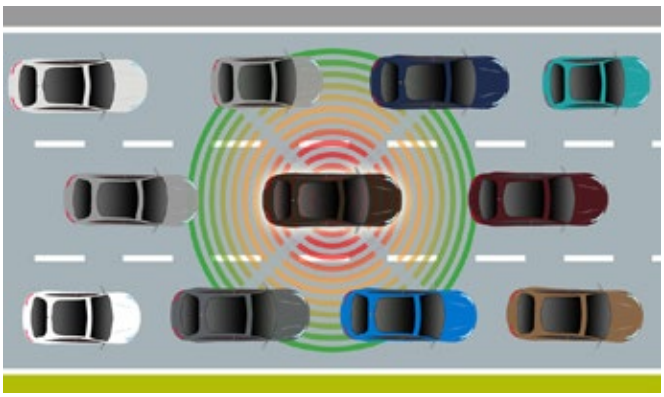
CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Mobility and urbanization

Mobility is one of the factors contributing to urbanization. People are willing and able to leave their current location in order to accept a new job or to pursue other opportunities. Often times, these opportunities occur in or around urban areas where big companies are concentrated. Increasing housing prices, gentrification, social disintegration and an elevated risk of protest against inequity are possible consequences. Up until 2050, two-thirds of the world's population will live in urban areas, leading to the evolvement of Mega Cities around the globe. Already, 84.4% of the Swiss population lives in urban areas, with Zurich (1,354,000 residents) being the biggest one[3].

Mobility concepts in urban spaces

Expanding urban areas demand a constant adaptation of mobility concepts and mobility management. Technological developments like Artificial Intelligence or autonomous driving via drone taxis are complemented with new concepts of public transportation or car sharing concepts[4]. While relieving traffic within urban areas, these concepts bear many new vulnerabilities. They make the area of operations for military missions in urban areas increasingly crowded and digitized. During operations, differentiation of friendly and hostile actors will become more difficult. Civil areal traffic will complicate reconnaissance and operations in the air. In addition, connected and digitized infrastructure of autonomous driving and smart cities present risk of cyber-attacks, creating a new vulnerability.



Autonomy: New technologies bear chances as well as risks
Source: IABG

Mobility of data and information

Widespread internet connection, digitization, the distribution of smartphones and Internet-of-Things devices – all these factors lead to a more connected world where information and data can be disseminated quicker than ever and the pace of communication increases steadily. A connected world had also "yielded" the Arab Spring dynamics, a wellmeant peaceful protest which turned into one of the biggest crises in recent history. Hence, mobility of data and information bears many chances and risks at the same time.

In the eye of urban warfare, many new threats emerge. Opponents might use the internet to spread manipulated information, deceiving the population. This could lead to dangerous situations, for example if during a conflict news of a ceasefire are falsely spread, civilians are put at risk. The ability to access private data can be used to pressure service members by threatening their family. Chain reactions following disinformation campaigns are especially harmful in urban areas, where many people live together in confined space.

Mobility in the military - relocation of troops

Conflicts are becoming more complex and confusing, new types of actors emerge and alliances change. New types of conflict require agile and flexible responses. The ability to relocate troops, weapon systems and equipment quickly and over long distances becomes increasingly relevant to a successful mission. The Very High Readiness Joint Task Force (VJTF) of the NATO is only one example of military institutions elevating the mobility of their troops to a new level.

Missions in densely populated urban areas require particularly fast deployment, as many civilians can be affected within a short time. It's essential to be able to generate quick and thorough overviews of the situation, reconnaissance from the air and within the cyber and information domain. The ability to redeploy quick response forces is gaining importance and requires cooperation of all domains. Because of their vulnerability, urban areas and mega cities will be a prime target of asymmetric opponents. Since irregular actors might have different moral inhibitions, strikes against large civil populations promise to be an effective way of urban warfare for them.

Mobility in the military - organizational structures and urban warfare

Future wars will not be won by gaining land and territory. By contrast, whoever controls the cities, controls the fate of a nation. The fall of Mosul is one of the most recent examples for the loss of a city held by a conventional army to an asymmetric opponent. Islamic State fighters were able to take Mosul within few days, using new tactics of urban warfare. Because of their flexible organization and structure, they were able to surprise their opponents and activate sleeper cells within the city.

The structures of non-state actors enable them to quick decision-making. Thereby, they have advantages over the stiff and hierarchical organization of conventional militaries. The organizational structure of asymmetric non-state actors facilitates fast deployment of fighters and the rapid change of battlefields. Conventional armies have to cope with the disadvantage of long chains of commands and the timely relocation from military personnel. As the battlefield gets more and more elucidated by reconnaissance, fast movements of troops are important to operate undiscovered.

IMPLICATIONS FOR THE MILITARY

Development of urban warfare concepts

In order to deal with the consequences of mobility and urbanization, defensive urban warfare concepts need to be developed. It is of importance to view this as a statewide task, which can only be resolved by cooperation of various government departments. As urban areas with large infrastructure are potential targets to asymmetric-attacks, they need special security precautions that do not impede the flow of people and vehicles. Traffic and mobility management needs to be considered, and so do evacuation plans and security of supply. It is a political task of the Swiss government to clarify the responsibilities in the case of a terror attack on a Swiss city[5].

Besides the protection of own cities, operations within foreign urban areas also need to be viewed on from a new perspective. To operate effectively within urban areas, the military needs to have multi-dimensional offensive and defensive abilities. It is necessary to develop skills in order to analyse and assess chain-reactions and cascade effects. Urban warfare concepts (offensive and defensive) need to include:

- new operational command structure
- adaption and integration of new technologies
- cooperation with IOs, NGOs and local institutions
- trainings and exercies
- protection and safety concepts for critical infrastructure

Rethinking of organization and structure

When it comes to the organizational structure of military, form does not follow function anymore. Future conflicts have changed and will keep developing – and so has and will the army's range of tasks. Organizational mobility has

become an integral factor for success. An organic structure that can adapt driven by incidents and tasks rather than by tradition and hierarchies could be a possible solution. The desired outcome should be decisive for the development of the future organizational structure. In order to combat asymmetric actors, military command chains have to gain speed and have to be adjusted to the high mobility of the opponent.

Integration of new technologies

As mentioned earlier, the military should integrate as much new technologies as possible but not more than necessary. Whenever new technologies are implemented, they come with certain costs and training needs, which also bear the possibility of errors. Artificial Intelligence and Big Data Analysis will facilitate the analysis and assessment of situations in order to find the best response possible. This increases an army's agility and mobility within urban areas.

Human Enhancement will drastically increase the sustainability of soldiers. Long distance works can be expanded, even if the soldier is tired. Moreover, the development of robots will support mobility. For example, they could help by crossing wet and dry gaps, to counter mines and other obstacles, develop routes, improve routes or they could guarantee route clearance[6]. Another connected point is the autonomy of future mobility systems. The army could profit from those developments by using already existing non-military-technologies for their own purpose – being closely connected with rapid changes of command post. Armies require for technical equipment and vehicles to change as rapid as the opponent does. Smaller and untraceable vehicles, small airplanes or drones are therefore essential.

CONCLUSION

Mobility is an ambiguous term. Whoever is tasked to define it, will come up with various interpretations. In the eyes of a military planner, mobility has implications for almost all military tasks and domains. Especially for urban warfare, it plays a versatile role. Mobility is both root and solution for urban warfare. It is one of the causes of urbanization and the emergence of mega cities – and so of potential protests and political instability. The mobility of data and information bears the risk of mass protest and chain reactions but is also fundamental for military communication. The mobility of asymmetric actors requires the military to adapt its organizational structure and to develop new concepts for urban warfare. New technologies can contribute to a military's own mobility – but also increase its opponents' strength.

To conclude, mobility is and will be the key for modern armies. All domains and every operation are dependent on mobile soldiers. As asymmetric opponents and proliferation will become faster and more mobile, the army has to adapt to these new circumstances. Especially Human Enhancement and robotics can be helpful in order to guarantee more and safer mobile soldiers.

SWOT-ANALYSIS for swiss military planners[7]

Strengths • planning and concepts for future challenges of mobility • cooperation of civil and military institutions • political understanding for the need of moderni-za-tion to adjust to "era of mobility"	**Weaknesses** • partly outdated or non-mobile equipment • late start to modernization process • more static-classical elements in military plan-ning and thinking
Opportunities • end of many product life cycles make room for im-provement and innovations • strong cooperation with technological advanced civil corporations (potential adaption of "mobile" innovations)	**Threats** • hybrid attacks from state-actors • urban areas as target of terrorist organizations • urban areas as center of social conflict

List of links included in the article

1. https://www.post.ch/en/about-us/innovation/innovations-in-development/drones?shortcut=opp-en-about-us-company-innovation-swiss-post-s-innovations-for-you-drones
2. https://mwi.usma.edu/guide-islamic-states-way-urban-warfare/
3. See "What does it mean for Switzerland" in "Mobility" chapter of this publication.
4. See "Future trends" in "Mobility" chapter of this publication.
5. https://www.aargauerzeitung.ch/schweiz/wann-genau-kommt-die-schweizer-armee-zum-einsatz-129733962
6. https://www.obranaastrategie.cz/en/archive/volume-2017/1-2017/articles/the-requirements-for-future-military-robots-supporting-mobility.html (last download 18.06.2019)
7. Based mostly on: https://www.vbs.admin.ch/de/verteidigung/bodentruppen.html

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

Information

Digital data is now ubiquitous. Produced by humans, by applications or by sensors, the volume is growing every day. Transforming the content (images, sounds, text, etc.) in structured and unstructured formats into meaningful and actionable information requires new capabilities. With the proliferation of sources and the possibilities offered in the cyber world, reliability as well has become a real issue. If bringing continuous information permanently everywhere has never been so easy, getting the right information to the right place at the right might have never be so hard!

A society of disembodied information

The brain, a computer?

We live in an information society. Even more than that: we are, its seems, beings who only exchange information and adapt ourselves to these exchanges. This new ontology also resonates closely with a society whose intimate architecture is increasingly using the Internet of things, big data, artificial intelligence, etc. – in short, only technologies that involve... information. Have we finally found the Holy Grail, the key to existence, the mystery of the universe? Let us not go too fast. Information theory, recent avatar of cybernetic theory forged by the American mathematician Norbert Wiener from the end of the 1940s (see: Cybernetics, or Control and Communication in the Animal and the Machine, 1948), has become the central paradigm for our time, the model in terms of which we think – literally – all the manifestations of the real: DNA? Genetic information. The brain? A machine for processing information. I.T. and the digital world? A language and a simulation based upon information. The list could clearly be extended, and would only be a reminder that today, few dimensions of our reality escape this epistemological monism: reality is constructed, if the learned discourses are to be believed, around a fundamental entity – information – and upon its multiple modes of expression – biological, I.T., etc. It is, for example, due to this reality shared by all beings that certain contemporary philosophico-scientist movements, such as transhumanism, hope one day, to be able to upload human consciousness to the digital networks: our identity would in fact be a specific form of organisation of our neuronal pattern, and given that the brain is considered to process information like a computer, it would be a short step to "grafting" this consciousness – this pattern – onto servers. The advantage of this procedure? Silicon is less fragile than flesh, illnesses only affect that which is biological – we would be almost immortal, and like software packages, we would be able to duplicate, or update ourselves, become... humans vers. 2.0, in other words, "post-humans". One might call this complete science-fiction – but one only has to read the essays of Marvin Minsky (for example The Society of Mind, 1987), Hans Moravec (Robot: Mere Machine to Transcendent Mind, 1998) or Kim Eric Drexler (Radical Abundance: How a Revolution in Nanotechnology Will Change Civilization, 2013) to realise that, strangely enough, science fiction seems to have emancipated itself from the pages of novels and cinema films to populate the dreams of those that the philosopher of science Dominique Lecourt calls, in Humain, posthumain (2003), the "technoprophets".

It is not for me to consider the relevance of these theories or fantasies, others have done this already and continue to do so better than me. On the other hand, it seems to me interesting to see how science fiction – this aesthetic "sounding board" for our techno-scientific utopias – has been impacted by these theories, how it has processed these and in order to say what. At least three metaphors punctuate the history of the relationships between science fiction and information theories: the first, that of the "brain in a vat", that appeared in the 1940s (as chance would have it...), echoes the theoretical postulate whereby the humanity of mankind – as well as its identity – resides in the brain, and this being so, that it would be sufficient to conserve an individual's brain to have all the relevant information concerning that individual. One can better understand why, on 18 April 1955, Albert Einstein's brain was removed so that it could be placed in formaldehyde... This metaphor, exploited endlessly on the covers of the pulp magazines – popular magazines in which science fiction authors cut their teeth and published novels in serials –, is relatively easy to decipher: the human brain being merely a machine for processing information (a computer therefore), the biological body can be reduced to an interface with reality, a set of sensors enabling the collection of this same information. In other words, the body, so long as it can find more efficient mechanisms for collecting data, is not necessary: it can disappear. The metaphor of the "brain in a vat" comes to symbolise the reduction of humanity to a cybernetic machine (in this respect similar to the thesis of Céline Lafontaine in her 2004 essay, L'Empire cybernétique) – and it is in order to criticise this state of affairs, or at least to exaggerate the anthropological consequences, that science fiction has amused itself in reducing the human being to the convolutions of their brain. One can also understand that this image of the brain in isolation enables the interrogation of the reader by obliterating that which is the spice of their existence: can flesh, sensuality and pleasure really be reduced to mere sensors? Can they so easily vanish without our being amputated from our humanity? What is interesting above all, in science fiction, is that the brain-computer is a metaphor, an image; in the real world, it is a little more frightening, this image is no longer considered an image...

This first metaphor was to transform, from the 1960s, into two new metaphors, which, in themselves merited in-depth analysis, but whose contours I can merely resume in a few lines: the cyborg (since the 1960s) and artificial intelligence (from the 1980s). As all complex systems are "machines" for processing information, there is no relevance in distinguishing men from computer systems: the difference is not in nature, but in degree. It is hardly surprising therefore, to see flourishing in society discourses that imagine a concrete hybridisation of man with a machine (a cyborg) or a fear of developments in artificial intelligence (these software packages could be more efficient than our own cerebral "software"). However, and even if science fiction incorporates these discourses in its narratives, it uses the cyborg not in order to speak to us of the beings of the future, but of their dependence – a metaphorical interpretation of hybridisation – increasingly present in technologies: the cyborg in science fiction is a "junky", a man who has become dependent, in their being, upon technological devices – as seen in the novel Neuromancer (William Gibson, 1984) or the film Matrix (Lana and Lilly Wachowski, 1999). The science fiction cyborg is, in consequence, the image of our dependences and, sometimes it goes as far as 'metaphorising' the fantasies of omnipotence that drive us all to thinking about changing our body: David Le Breton analysed this state of affairs perfectly (L'Adieu au corps [Farewell to the body], 1999) and coincidentally resonates with the fictional story of Duane Fitzgerald in the sublime Der Letzte seiner Art [The last of its kind] (Andreas Eschbach, 2003). In this sense, and because we are all slaves to technology, we are all cyborgs (in the science fiction sense)! An analogous reasoning presides over the formation of the third metaphor: artificial intelligence (AI) is frightening – even Stephen Hawking allowed himself to be taken in to some extent! –, because it gives the impression of scientists toiling in their laboratories to create the "creature" of the future, or rather, the sophisticated machine that will annihilate us. As for science fiction, in particular since the birth of the "cyberpunk" genre in the 1980s, it does not use AI to reflect on our possible successors, but rather, and more in the manner of the observer in the film Her (Spike Jonze, 2013) or Transcendence (Wally Pfister, 2014), in order to signify our solitude, which had become terrifying in the age of social networks and digitisation of our interaction platforms. It is certainly of little importance to science fiction authors to adopt a position on the (metaphysical) questions, of whether man is software, or whether he has a soul or if the body is superfluous; on the other hand, the image of AI is particularly suitable for the consideration of solitude. In fact, the body has not (yet) actually disappeared, but, as we increasingly place value on virtual communications, human beings find themselves mutually isolated, incapable of constructing human relationships: the only relationship they can construct, is with their communication interface (the interlocutor perceives a sense of self behind an avatar or lines of text) – which can only lead them back to their own solitude, because 'the other', in their corporeality, has disappeared from the exchange.

Conclusion

"Brain in a vat", cyborg, artificial intelligence: these motifs, also present in the real world, but 'metaphorised' in science fiction, mark out the recent transformations of the human condition. And this transformation is particularly sad: man is reduced to software, dreams of omnipotence, sees his body lose all significant form if not optimised in order to process information even more effectively, and has almost no relationship with anyone else other than via the digital web. The 'post-human', a superior, enhanced being? One might wonder... Rather: an individual confined to an interminable solitude – is this not what the clones experience in La Possibilité d'une île [The possibility of an island] (Michel Houellebecq, 2005)? –, an individual assailed on all sides in their dignity and who encounters only pixels when seeking comfort.

Induced Complexity: The Future of Information

Anxieties (and hopes) for the future have been explored in science fiction through three views of intelligence — the Matrix offers us the "brain in the vat," in which human consciousness is isolated from the body, making decisions in a virtual landscape. The cyborg, which comes by way of the Terminator or Data from Star Trek, places the human and machine on a spectrum, rather than a binary. AI, from the coldly terrifying HAL of 2001: A Space Odyssey to the more quite-literally-loveable office assistant of Samantha in Her, presents us with the conundrum of a machine that knows our world even better than we do.

It's sensible to ask ourselves how close these fictions are to reality today. Each approach to new technologies relies on new ways of processing, and interacting with, information in our physical world. Each offers a vision to reduce the gap between the mounting streams of data[1] and the limits of the human mind to comprehend and mould that data into actionable knowledge.

The Brain in the Vat supposes that a digital replica of our minds can be used to better anticipate human response, increasing the speed of decision-making — from cities to biology. Today, we have digital twins (computerized replicas of real-world spaces), bionic brains, and complex simulations that some believe will pave the way toward a science fiction future of uploaded memories, thought-reading devices, maybe even eternal digital life. The cyborg supposes new, seamless interfaces for the body: contact lenses with digital displays, a device-free future in which our body is the mouse, the screen, and the camera. All the while, Artificial Intelligence imagines a machine that is smarter than its human creators, capable of conversing and anticipating our every need, including our rising desire for a machine that can explain the machines.

Beyond these frames is also the question of whether humans can adapt to a torrent of data about their world; how we can adapt ourselves to avoid manipulation and exhaustion that makes this data useless. How can technologies aid us in discerning facts from falsehood? As the level of complexity in our daily lives expands beyond our ability to focus, it is inevitable that machines will help us to "simplify" this world for daily life. What will we surrender for this illusion of simplicity and oneness with the world of information?

Brain in a Vat: From the Mind to the Cloud

One of the transformative ideas we face in the future is the notion of the mind as a collection of data. Today we aim to create "digital twins[2]" of our environments, objects, and even the human mind, complex electronic copies of our real world conditions that adapt to reflect what's happening in their real-world counterpart. Google has launched Sidewalk Labs on the Eastern Waterfront of Toronto, a model of a smart-city that relies on an overlay of digital infrastructure to inform more sustainable, community-friendly decisions. But Sidewalk Labs has faced a legal and cultural backlash[3] that suggests that the human community is perhaps unwilling to trade personal data security for artificially intelligent stop lights and other accoutrements of a data-driven neighbourhood.

But the digital twin may go deeper than cities, and neuroscientists are applying the concept to the understanding of the human mind. The Blue Brain Project[4] aims to create a simulation of complex brains, starting with the goal of mapping mice by 2020. The project is a complement to the EU's Human Brain Project[5], which (among other aims) seeks to increase the reliability of computer models for testing theories, treatments, and models "in silico[6]" with greater accuracy. These models are simulations — proper digital twins reflect real-time conditions of their counterparts, which is a long time off for biology.

But advances in biological engineering, such as the discovery of CRISPR Cas-9, which illuminated a method for editing segments of DNA to remove genetic diseases, could be combined with digital models to create a kind of 3D printing for synthetic human organs. This is one ambition of Genome Project-Write[7], described as "the difference between editing a book and writing one[8]". Taking the understanding of data from the electronic logic of 0s and 1s to the logic of nucleotides (GTCA), scientists are approaching the future of the human genome in ways much akin to a complex programming problem. In 2017, scientists at the University of Washington were even able to create a virus within human DNA — a computer virus[9] that would infect and corrupt computer systems designed to analyse DNA for evidence of diseases. The University had previously worked with Microsoft to inscribe a music video[10] into human DNA.

The relationship between the computer and machine is likely to extend even further, expanding the capacity to inscribe computer data into human and animal DNA at reduced cost[11] — it currently stands at roughly $3,500 per megabyte.

Could memory ever be extracted from the human mind and updated to the cloud, bringing the dream of "the mind in a vat" to its extreme? The controversial neuroscience startup Nectome[12] faced widespread condemnation for suggesting it as an area of research in 2018, with a possibly ill-advised PR campaign promising "100% fatal" digital backups of the human mind. Shortly thereafter, the Massachusetts Institute of Technology (MIT) publicly distanced itself from the startup[13], which it had initially offered a small business grant, going so far as to publish a blog post criticizing the science and the approach, which is worth quoting:

> "It's possible that someday we will be able to simulate, in a computer, neural circuits with great accuracy, based on detailed enough biomolecular maps. But currently we do not know how to determine what such a simulation, even if scaled up to the size of the human brain, would «feel» like. To understand this will require new science that represents a nonlinear jump from the neuroscience occurring today, and some people regard this as an unsolvable problem (aka the "hard problem" of consciousness)."

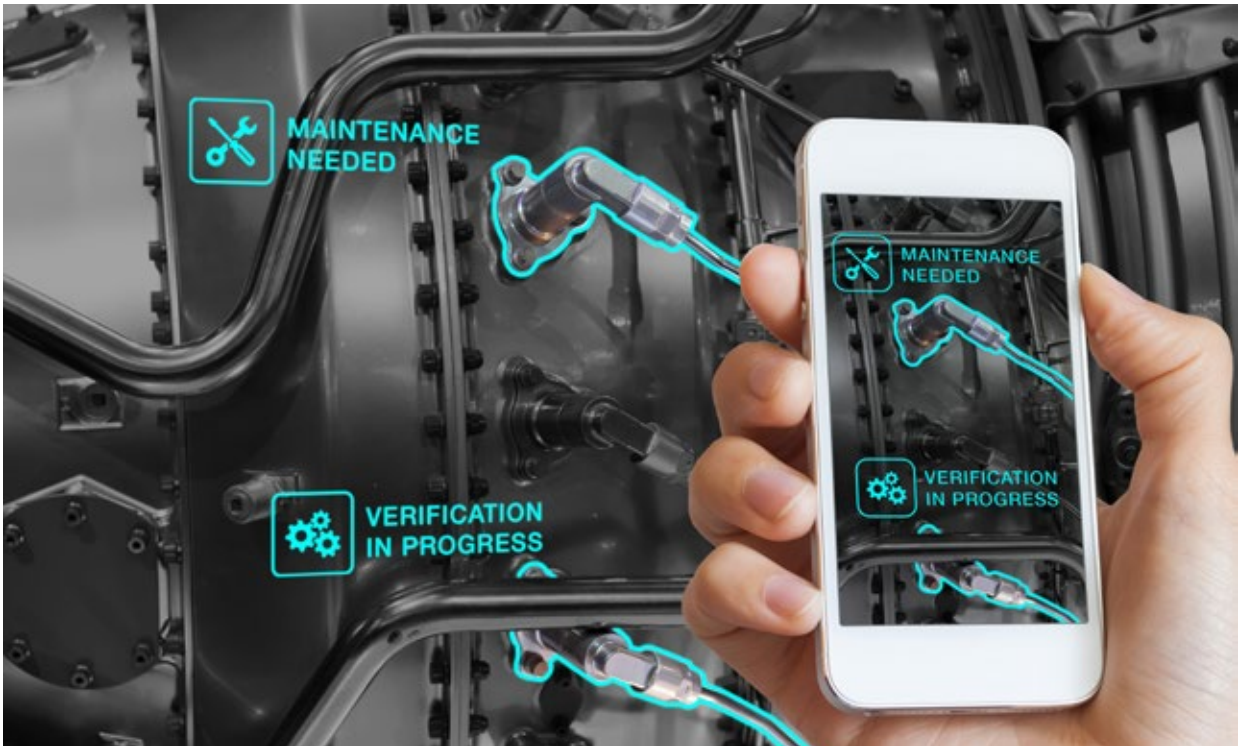
The company has pivoted[14] to the study of human memory preservation and extraction.

Is a simulation of a human brain within reach? An international group of scientists has published research suggesting the algorithms governing the functions of neurons and synapses that control the human mind, but there is no computer on earth powerful enough to test it. Running the simulation would require computers 100 times more powerful[15] than the most complex hardware available today , and while success would deliver a new tool for analysing brain functions relevant to the treatment of seizures and abnormalities, it does nothing to replicate the function of memory or personality. For now, the dream of a mind uploaded to live on in the cloud as information remains entirely speculative.

The Cyborg: The Body Becomes Machine

As researchers cultivate deeper models of the human mind, and expand their capacity to exchange biological and "in silico" data, then the prospect of the cyborg — a cyber-organic human — begins to come into sharper focus. Far from the science-fiction scenarios, a line of thought today proposes that the cyborg is any human with a digital enhancement — including those with cochlear implants[16] to help improve their hearing.

Now done through smartphones, seamless points of entry for information have been a driving force behind projects from Google's Glass[17] or Snapchat's Spectacles[18]. Both are pieces of eyewear that add a digital capacity — whereas Spectacles can record what you see, Glass can add a data layer to your sight of the world.

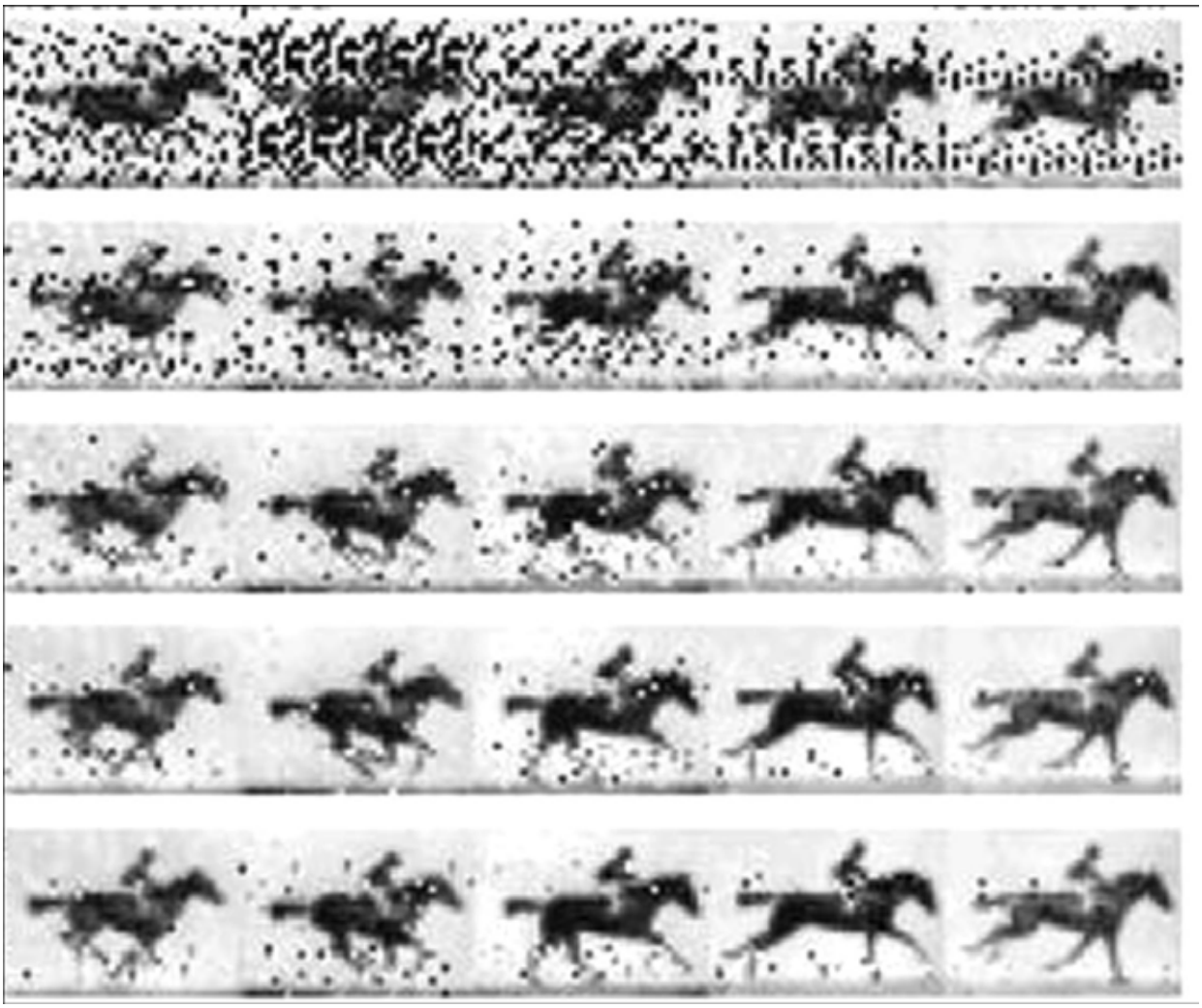


A mock-up prototype for an augmented reality interface applied to engineering, in which information about the real world is analysed and data presented as a digital layer through a device.

Not content with eyeglasses, research is underway into the development of smart contact lenses, which can be placed over the human eye to create a seamless interaction with the physical and data worlds simultaneously. Some prototypes have been developed to track the glucose level in tears[19], which could be used to alert diabetics to health risks. But more complex data analysis and displays are difficult to produce. Samsung has filed a patent[20] for a smart contact lens that can record video, though whether this is a speculative design or a working prototype has yet to be seen.

One of the challenges for so-called smart lenses is power: most contacts are made of hydrogel, a soft, flexible material that is safe to place on top of the human eye. But hydrogel is 90% water, which makes it difficult for interfacing with electrical power systems. Other avenues of development include a flexible microbattery[21] that could power a contact-lens display for several hours, though it has been recommended as an interface rather than a screen, as it is better suited for transmitting commands to an external device by tracking eye movement and blinks.

Meanwhile, biohackers are already exploring the body as a site for data storage. A team of biohackers has created an implant that runs a chatroom and streaming movie service[22] from inside of their bodies, "installing" wireless-charging devices into their bodies. The devices do nothing more than a cleverly arrange hard drive but raise security concerns. Data can be stored secretly, and files transmitted to anyone in close range, without the use of a visible device. The devices can also be networked in close range, creating the potential for an "internet of things" that operates between "hacked" human beings, transmitting data on an alternative network, raising the possibility of a new, "human dark web" where illegal data can be surreptitiously transmitted.



Frames of video of a man riding a horse, which had been encoded as visual data into DNA samples and retrieved. Shipman et al., doi 10.1038/nature23017.

Today that technology is hardware implanted into a body. But researchers have made progress in developing computers that use genetics-editing technology (CRISPR) to create a dual-processor core[23] that can exist within human tissue, and respond to chemical signals in the body — for example, releasing a specific kind of medicine in response to the presence of a disease. Meanwhile, encoding data into human DNA has been possible since 2017, when researchers encoded 2GB of data[24] — including an entire 1895 silent film — into human DNA, which, once inscribed, can hold that data for more than 1 million years[25]. If the combination of these technologies opens the door to biological computing done within our bodies, using entirely organic systems, then we are even closer to the era of a science-fiction cyborg.

Artificial Intelligence: From Assistants to Managers?

The merging of human and machine is one inflection point for the future, but another is the rise of a wholly independent intelligence. Such an intelligence would be capable of doing mental tasks independently of humans, or work alongside humans to solve challenging problems at scales beyond the comprehension of a human mind, such as quickly finding patterns and making predictions from vast datasets. If the vision of the cyborg is an interface through the eyes and ears, the imagination of the artificial intelligence is often through the voice.

We have long focused on artificial intelligence as a way of thinking that achieves an understanding of language. But soon, machines will be able to convincingly imitate that type of intelligence. Speaking out loud to today's virtual assistants, such as Siri or Alexa, requires devices with a sophisticated understanding of human language. This is encouraging recent investment and development into Natural Language Processing (NLP), a kind of AI that can recognize complex spoken or typed language and respond appropriately. In 2019, OpenAI[26] (a non-profit research institution based in San Francisco) released the GPT2 language model for an NLP called Transformer, which was originally developed by Google to predict text as it is being entered into a smartphone. When OpenAI trained an artificial intelligence program on 8 million web pages, the researchers found that the same software could create everything from fake news reports to short stories based on just a few sample sentences. OpenAI refused to distribute the model[27] in its full form, fearing the unanticipated consequences of public use.

Such natural language processing technology would go beyond opening up new interfaces for humans and machines. NLP can generate text, but can also be used to intelligently analyse text, and one goal is to create a machine that can read complex materials and create reliable, human-readable summaries[28]. For example, Google and Stanford University have been testing software that listens in on doctor's meetings with patients, and produces a simple-language summary[29] of the diagnosis for electronic health records. Another is to create chatbots and other kinds of virtual assistants. Commercial products, such as Replika[30], X2AI[31], and Woebot[32], aspire to transcend the task-setting applications of Siri or Alexa to become emotional assistants capable of having a late-night chat about human feelings.

But if NLP will create a sense of human intimacy with a machine, it may equally be applied to the use of machines to inspire further divisions between human users — further empowering computational propaganda, and the use of social media bots to amplify divisive political messages. In 2018, social media site Twitter suspended 70 million accounts[33] that were run by bots — that same year, Facebook announced that 3 billion[34] of its users were fake — created for various reasons, including to bolster the popularity index of other accounts, or to spread specific messages online. Such "bot armies" are chiefly used to distribute a false narrative — retweeting a message written by a human, to bolster its search rank, or social capital and perceived popularity. But combined with even rudimentary NLP software, such accounts could take a single sentence from a human master user, scan it, create near-infinite variations, and even respond to comments on the topic in untraceable ways, further blurring the ability to discern between "bot" from "human" behaviour on websites such as Facebook and Twitter.

There is ample evidence of human-controlled misinformation and persuasion campaigns[35] using bot networks to influence elections in Brazil, Turkey, Sweden, the UK, the US, and many others; expanding on these technologies to include Natural Language Processing could create more convincing, autonomous accounts that could be deployed to create the illusion of grassroot support for a political party or initiative; generating thousands of fake complaints or comments to a journalist, politician, or petition; or coordinating harassment campaigns against individuals or institutions through social media.

If it is impossible to separate real human users from automated algorithms communicating via software, then this undermines the public sphere, eroding the trust necessary to forge common ground and compromise between rival parties, beliefs, or faiths. Couple this with the increased speed of communication and the psychology of deep immersion into new tools such as VR — or AR, which, as an overlay upon the existing world, would lead to even deeper levels of disintermediation from objective reality — and we open a landscape of new vulnerabilities for public discourse.

The result of today's bot armies for amplifying digital propaganda has been theorized as a step away from traditional media propaganda, such as radio, television, or fliers, and into "participatory propaganda[36]", the production of deliberately belligerent computerized interactions with humans with the sole intention of creating frustration, amplifying emotions, and making civil dialogue feel hopeless. One function of today's online social media disinformation campaigns is the capacity for actors to measure success through a variety of marketing metrics — clicks, likes, shares, responses. Combined with NLP, these actions could be further manipulated to "learn" messages that evoke hostility, shares, and responses, essentially co-creating propaganda with a target audience.

From Black Box to an Explainable AI

Beyond the capacity to speak to us, the next generation of AI is likely to include some kind of self-awareness. Far from the sophisticated robots of science fiction, an emerging field — Explainable AI, or XAI — focuses on creating systems that can give accountability to algorithms and their outputs.

Today, algorithms used in artificial intelligence suffer from a "black box" phenomenon, in which the machine analyses patterns, uses those patterns to predict output, and shares that output with a user. The process that takes the machine from pattern analysis to prediction are often obscure — a methodology that is influenced by the machine's

pattern-finding process, by enormous sets of data, by code that is often constructed by teams of engineers or researchers working independently of one another on modules of a larger system. As a result, AI has been known to present incorrect, unreliable, and/or biased output, often in ways that humans are not immediately capable of recognizing.

The solution, XAI, is envisioned as a parallel process to the data analysis work of an AI. It has been conceived either as an aspect of tools that can create an outline of the logic that was used, or an outside tool that can "reverse-engineer" the output of another machine and break down why it came to a particular conclusion. DARPA has eyed XAI[37] as a means of creating a "second opinion" on the recommendations of automated systems. But it could also serve enterprises, where understanding the machine's models would give engineers an opportunity to adjust the logic of the machine's correlations, based on a real-life understanding of the world. This is essential if AI is to become truly autonomous in a broader range of situations — for example, the deployment of self-driving vehicles. If even a small number of self-driving cars accelerate towards a road barrier (as a Tesla model did in 2018[38]) this is an unacceptable risk that would be extremely difficult to identify in a black-boxed algorithm. An XAI process would have been able to create a human-comprehensible readout of why it made the decision.

With artificial intelligence processes taking up vast amounts of hardware and data processing power, creating redundant or parallel processes is difficult. The future of XAI will be limited until more of that power becomes available. As pressure mounts for algorithmic accountability in policy, as in the "right to an explanation[39]" provisions of the GDPR[40], XAI is likely to become an even greater priority for industry.

The Future of Facts

To understand the future of falsehood, we can look to the phenomenon of "fake news" — the behaviour of sharing of deliberately incorrect information online. A Knight Foundation survey[41] suggests that when fake news is shared, a majority of users (84%) did so to call attention to it being false. However, 27% of "fake news" was shared deliberately and knowingly in a bid to amplify its message or to antagonize those they saw as its targets.

While not everyone sharing or reading fake news believes it, widely circulated falsehoods do have consequences on understanding of facts. Exposure to repeated falsehoods been shown to create a willingness to negotiate a compromise[42] between proven facts and an often-repeated[43] lie. Studies have shown that partisan reasoning[44] can bias our information processing ability.

IBM's Quantum Computer (the "Q") on display in Germany.

Some have proposed a number of technological solutions. In the case of AI-generated "deepfake videos," for example, Amnesty International — which has an interest in legitimating video documentation of human rights abuses, has created a lab designed to quickly evaluate whether videos show what they claim[45]. Using traditional techniques combined with data available online — geotagged photos, Google Street View and Maps, for example — the NGO is able to ascertain the credibility, or lack thereof, of a video as evidence.

In the US, news giant The New York Times is working to solve this problem through authentication of news items through blockchain technology. Based on the belief that "news consumers [who] are deceived and confused...eventually become fatigued and apathetic to news," the newspaper has launched a project to research new ways to verify information online[46]. The project aims to transmit images and video through a secure blockchain, a traceable ledger that would track the transfer of images between parties. Editing the image would remove the image from its associated line of transfer, at which point readers could reference (and see) the original to determine how it might have been doctored, and by whom. Others are examining whether visually imperceptible but machine-readable watermarks[47] could be inserted into original images in such a way that any disruption of the watermark could be seen as proof of tampering. Amber also secures these watermarks through a blockchain ledger-based technology.

Curiously, one challenge to blockchain-based solutions for establishing provenance is the rise of quantum computing, which can be used to overcome the complex encryption that blockchains use to ensure security and accuracy. A quantum computer could easily overcome the security apparatus[48] that keeps a blockchain secure and reliable. Given the arms-race-nature of cryptography, however, "quantum blockchains[49]" have already been theorized as a solution.

Likewise, tools[50] can already identify text created by the OpenAI with a high degree of certainty, by recognizing patterns in GPT2 output. Others are turning to NLP to quickly discover patterns and correlations[51] in the automated propaganda being produced on social networks, analysing known cases of "fake news" to discover tell-tale signs (emotional language, for example) and to create an autonomous machine-learning algorithm that could identify and flag new examples even as they are first produced.

For images, altered material could be identified by comparing it to a database[52] of image data. Today technology is being used to identify images of human trafficking victims but could eventually identify similarities between suspicious images or videos and pre-existing content, assuming these sources are online.

The Future of Facts

Complex data streams are a requirement for AI and other systems that promise the benefits of more organized societies, from traffic control of smart cars to energy-efficient smart homes. But each advantage comes with a trade-off[53], creating a new kind of cyborg, in which, rather than becoming one with a machine, we immerse ourselves in a kind of data surveillance that surrounds us like an invisible second layer of skin. This creates databases of sensitive data, networks that could be accessible to hackers or institutions.

As we have discussed in our communications chapter, the protection of data from malevolent actors may come down to advances in quantum encryption[54], in which information quite literally collapses if it's intercepted by an unanticipated observer.

What's Next?

It is safe to say that data is the backbone of our future society. AI and algorithms, which can sort through vast quantities of data to make decisions on a mass scale, promise to create the space for more complex societies. To understand the future of data, we might look to the principle of induced demand: related to the construction of highways, induced demand suggests that the more we make something available, the more it is used. As we approach a capacity, products become more efficient, but in the end, this means we only do more with the capacities we have. As AI becomes capable of processing more data, faster, we will likely produce more data — and more complex AI to sort it. If XAI offers us insights into the decisions of the machines, paired with a means to digitize our own ability to process even more complex "explanations," we may increase the complexity of infrastructures, societies, and communication even further.

The design and implementation of technologies to manage this spiralling complexity is crucial to which future we have. Toward dystopia, we could ignore algorithmic reproductions of bias and dehumanization, which become further embedded and obscured into evermore complicated systems, amplified as machines make decisions that humans cannot understand. Or we can embrace the utopian view: a world in which machines are firmly in our control, designed to accomplish human-centred tasks through thoughtful engineering.

New, broadly interdisciplinary research fields are emerging to address these issues. The field of "machine behaviour[55]" is the study of algorithmic influence on the real world; whereas "applied cybernetics[56]" is the study how small design considerations can affect these systems at scale. This approach is limited, in some ways, to observable consequences of algorithms only after they are deployed, but they point toward new tools to better understand and uncover flaws in artificial intelligence technologies before and after they are deployed.

Whether we confront a utopian future of leisure and seamless societies, or a dystopian image of humanity losing its way to binary operations, is perhaps — to put a twist on the old adage — in the digital contact lens of the beholder.

You'll find on the next page the list of the links included in the article >

List of links included in the article

1. https://www.nytimes.com/2019/05/07/opinion/data-privacy.html
2. https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/
3. https://www.theatlantic.com/technology/archive/2018/11/google-sidewalk-labs/575551/
4. https://www.hpe.com/us/en/newsroom/press-release/2018/07/hpe-helps-epfl-blue-brain-project-unlock-the-secrets-of-the-brain.html
5. https://www.humanbrainproject.eu/en/brain-simulation/brain-simulation-platform/
6. https://en.wikipedia.org/wiki/In_silico
7. https://engineeringbiologycenter.org/
8. https://www.wired.com/story/live-forever-synthetic-human-genome/
9. https://dnasec.cs.washington.edu/
10. https://www.theverge.com/2016/7/7/12114480/dna-storage-ok-go-microsoft-university-washington-twist-bioscience
11. https://wyss.harvard.edu/technology/digital-information-storage-in-dna/
12. https://nectome.com/
13. https://www.media.mit.edu/posts/the-media-lab-and-nectome/
14. https://www.statnews.com/2019/01/30/nectome-brain-preservation-redemption/
15. https://www.frontiersin.org/articles/10.3389/fninf.2018.00002/full
16. https://www.nidcd.nih.gov/health/cochlear-implants
17. https://www.blog.google/products/hardware/glass-enterprise-edition-2/
18. https://www.spectacles.com/
19. https://advances.sciencemag.org/content/4/1/eaap9841
20. https://www.telegraph.co.uk/technology/2019/08/06/samsung-patents-smart-contact-lenses-record-video-let-control/
21. https://futurism.com/darpa-augmented-reality-contact-lens
22. https://www.wired.com/story/this-diy-implant-lets-you-stream-movies-from-inside-your-leg/
23. https://www.sciencedaily.com/releases/2019/04/190416081416.htm
24. https://www.sciencemag.org/news/2017/03/dna-could-store-all-worlds-data-one-room
25. https://ethz.ch/en/news-and-events/eth-news/news/2015/02/data-storage-for-eternity.html
26. https://openai.com
27. https://openai.com/blog/better-language-models/
28. https://venturebeat.com/2018/11/06/microsoft-researchers-develop-ai-system-that-can-generate-articles-summaries/
29. https://ai.googleblog.com/2017/11/understanding-medical-conversations.html
30. https://replika.ai/
31. https://www.x2ai.com/
32. https://woebot.io/
33. https://www.washingtonpost.com/technology/2018/07/06/twitter-is-sweeping-out-fake-accounts-like-never-before-putting-user-growth-risk/
34. https://www.marketwatch.com/story/facebook-removes-a-record-3-billion-fake-accounts-2019-05-23
35. https://comprop.oii.ox.ac.uk/
36. https://jods.mitpress.mit.edu/pub/jyzg7j6x
37. https://www.darpa.mil/program/explainable-artificial-intelligence
38. https://www.ntsb.gov/investigations/AccidentReports/Pages/HWY18FH011-preliminary.aspx
39. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3196985
40. https://www.law.ox.ac.uk/business-law-blog/blog/2018/05/rethinking-explainable-machines-next-chapter-gdprs-right-explanation
41. https://kf-site-production.s3.amazonaws.com/publications/pdfs/000/000/254/original/KnightFoundation_Misinformation_Report_FINAL_3_.PDF
42. https://www.poynter.org/fact-checking/2019/why-is-fake-news-so-prevalent-researchers-offer-some-answers/
43. https://www.researchgate.net/publication/317069544_Prior_exposure_increases_perceived_accuracy_of_fake_news
44. https://www.ncbi.nlm.nih.gov/pubmed/29475636

45. https://www.amnesty.org/en/latest/news/2018/09/digitally-dissecting-atrocities-amnesty-internationals-open-source-investigations/
46. https://www.newsprovenanceproject.com/
47. https://ambervideo.co/
48. https://www.nature.com/articles/d41586-018-07449-z
49. https://arxiv.org/abs/1804.05979
50. http://gltr.io/dist/index.html
51. https://marvelous.ai/marvelousai/
52. http://www.ee.columbia.edu/ln/dvmm/memex/index.html
53. https://www.weforum.org/whitepapers/data-policy-in-the-fourth-industrial-revolution-insights-on-personal-data
54. https://www.technologyreview.com/f/614209/a-super-secure-quantum-internet-just-took-another-step-closer-to-reality
55. https://www.quantamagazine.org/iyad-rahwan-is-the-anthropologist-of-artificial-intelligence-20190826/
56. https://www.igi-global.com/book/handbook-research-applied-cybernetics-systems/176081

The future of information in Switzerland

A stronghold of AI technology for a long time, Switzerland pursues ambitious goals in the digital and information revolution. Its research centres are advanced in multiple information-related domains and numerous companies are already active in digitalisation technologies, especially for medical applications. Despite the lack of an "anti-deep-fake" legal plan, Switzerland is well equipped to stand at the forefront of the future of information.

S Start: no real activities | T Trend: Early activities | A Advanced | R Ready | S T A R

Digital twins

S T **A** R

Switzerland has a strong position in Digital Twins-related technologies. EPFL (VITA[1]) and ETHZ are worldwide key players in research. These leaders with more than 25 laboratories in the Health EU project[2] dedicated to combine customized medicine with digital technology apply the latest technological developments such as connected objects, Artificial Intelligence and the concept of "digital twins[3]". EPFL's activity extends beyond medicine towards Industry 4.0 with the Horizon 2020 project QU4LITY (Digital Reality in Zero Defect Manufacturing[4]). This project also involves Swiss company Agie Charmilles. Several companies are active in this field: Akselos[5,6,7,8] (world leader in digital twin technology), Biovotion's Everion[9,10] (specialised in wearable devices which combine advanced machine learning with physiology biomarkers to monitor and analyse patient data) and Nomoko[11,12] (digital twins of geographical locations). Some academic work on ethical and policy challenges, which come with the development of digital health in Switzerland, was jointly undertaken by ETHZ and the University of Cambridge in 2018[13].

Digital Genetics

S **T** A R

In 2015, ETH Zurich stored the text of the Swiss Federal Charter from 1291 in DNA as a proof of concept[14], using a proprietary technology. In 2017, EPFL in association with the US company Twist Bioscience, Microsoft and the University of Washington safeguarded two songs in DNA strands as part of the Montreux Jazz Digital Project[15]. In 2018, ETH Zurich's Functional Materials Laboratory stored an entire music album (15 megabytes) by Massive Attack in the form of DNA molecules poured into tiny glass beads[16] with the help of its Zurich-based spin-off: TurboBeads[17]. ETHZ has also very advanced capabilities in computer-generated genomes[18].

Digital backups of the human mind

S T A R

Transhumanism is not yet a real topic in Switzerland, neither is digital backup of the human mind. The closest research to this topic is the Blue brain project[19] that intends to build and simulate digital reconstructions of the brain.

Human brain simulation

S T **A** R

Switzerland is a top spot for human brain simulation. The country hosts the Blue brain project[20] aiming to build biologically detailed digital reconstructions and simulations of the rodent, and ultimately the human brain. Blue Brain is run by IBM and the EPFL. The project involves more than 80 researchers since 2005 and has seen publication of more than 160 scientific papers[21]. Based on the research strategy developed in the Blue Brain Project, the European Human Brain Project (HBP)[22] was launched in 2010. It is a consortium of 131 European and international partners in which EPFL occupies a central place[23].

Cyborg

S T **A** R

Swiss research centres are massively involved in this topic. Projects cover brain-machine interface (EPFL[24,25,26], ETHZ, Bern University[27]), exoskeletons (EPFL[28,29], ETHZ[30,31], HSR University[32]) and powered prostheses (EPFL[33], ETHZ[34], Bern University[35], HES-SO[36]). Opened in 1st December 2010, the National Centre of Competence in Research (NCCR) Robotics is a Swiss nationwide organisation funded by the Swiss National Science Foundation that brings together experts from EPFL, ETHZ, UZH[37], IDSIA[38], UNIBE[39] and Empa[40] with the objective of creating exoskeletons and prosthetic limbs that can be controlled by the brain. Multiple start-ups have already been spawned: Fes-ability[41], Intento[42], MyoSwiss[43], Noonee[44], SenArs[45] and TWIICE[46]. The country also hosts organizations such as SwissLimbs[47] and Project circleg[48],

that promote actively the use of powered leg prostheses.

Smart contact lenses

S T A R

Smart contact lenses developments in Switzerland are mainly related to the medical field. Several Swiss companies are developing smart lenses for medical monitoring (to treat glaucoma): Sensimed[49], Tissot Medical Research[50,51] and Fabrinal[52]. EPFL[53,54] and ETHZ[55] both have smart-lenses-related projects. In 2014, Novartis (Alcon eye-care division) announced its collaboration with Google (Verily) to develop high-tech contact lenses that can monitor glucose levels in real time to help diabetes patients. After 5 years of development, the "duo" decided to pause the project as first results were not conclusive. They decided to explore new leads like smart contact lenses to improve patient sight after cataract surgery or contact lenses specially designed to treat presbyopia.

Body storage

S T A R

ETHZ has created a biosynthetic dual-core cellular computer, "the first cellular computer with more than one core processor[56]". ETH researchers have integrated two CRISPR-Cas9-based core processors into human cells, with potential applications in biological signal detection as well as in cancer treatment. The department of Biosystems Science and Engineering is exploring the application of information-processing diagnostic circuits in cell therapies or tissue engineering to monitor current cell state[57,58].

Artificial intelligence

S T A R

Switzerland has a long history of research in AI. In 1971 the world's first IA centre was created in Manno, in the suburbs of Lugano, then two other centres followed: ISSCO at the University of Geneva (semantics) and in 1991, IDIAP[59] in Martigny, specialised in perception[60]. These "natives" were joined later by technology giants Google (2'500 data scientists in Zürich), Facebook, which acquired Zurich Eye (ETHZ Spinoff) in 2016[61], IBM[62] and Microsoft[63]. The country is now at the forefront of AI research with several top academic institutions in the field: ETHZ[64], EPFL[65], University of St. Gallen[66], IDIAP[67] and IDSIA[68]. Switzerland is considered "a hub for AI" by a 2019 SGE's report[69]. The 2017-Asgard's European AI landscape stated that Switzerland has the most AI companies per citizen[70]. Key AI-related Swiss companies are: NVISO[71], Spinningbytes[72] and MindMaze[73].

Chatbots

S T A R

A lot of Swiss companies already use chatbots for their customer service[74,75] (Helvetia[76,77], SBB[78], Postfinance[79], Swiss[80,81], Swisscom[82]). Several companies propose chatbot design and implementation services, some of them are: Obeeone[83] (developed with HES-SO), Dermintel[84], Siropbot[85], Enterprise bot[86], ELCA[87], AdNovum[88], Paixon[89] and Spinningbytes[90]. ETHZ, St Gallen University and the Swiss Research Institute for Public Health and Addiction developed an open source behavioural intervention platform (chatbot) for fully automated digital interventions named MobileCoach[91]. In politics, the Swiss government uses this technology[92] but political parties are still very modest when it comes to social media and technology[93].

Fake news prevention

S T A R

In June 2018[94], the Swiss government recognized fake news as a possible threat to the national political system which is based on direct democracy: an opinion shared by 75% of the population[95]. Despite this possible threat, no "anti-deep-fake" legal plan is considered in Switzerland. Harder legislation, such as the one that France considers adopting, is regarded a risk since transferring political debate to courts may reduce freedom of speech and freedom of the press. The existing legislation is considered strong enough. Quantum Integrity, an EPFL start-up, is developing a software that will detect deepfake videos. It may be operational in 2020[96]. Another similar project exists at Idiap[97]. Prof. Monti, of the University of Lugano, co-founded Fabula in 2018, a Twitter-owned London-based fake-news detection Deep Learning company[98].

Digitalisation & Privacy

S T A R

The Swiss federal government recognized[99] that *"digital content is one of the most important drivers of growth for the digital economy [...]. However, it is also necessary to address the risks of increasingly data-based decision-making, including the lack of transparency of computer-based conclusions and possible unequal treatment of people."* To answer these challenges, the Federal Office of Communications (OFCOM) established the "Switzerland Digital Strategy[100,101]", a set of principles and actions that "guarantee security, trust and transparency" when it comes to data collection, storage and use. Its objectives are legal[102], economical[103], technological[104] and the protection of privacy[105]. More than 150 leading companies, organisations, academia and politics joined forces in the Digitalswitzerland[106], a multi-stakeholder initiative created to strengthen Switzerland's position as a leading innovation hub. >>

Conclusions

Switzerland's strengths	Switzerland's weaknesses
• Academia developing a lot of advanced projects • Switzerland's Digital Strategy • Switzerland is considered "a hub for AI" • A well-developed medical-related "cyborg" activity	• Vulnerable to fake-news and AI-driven disinfomation
Opportunities	**Threats**
• Blue Brain and Digital Twins projects give the country a head start in these fields • World premiere in digital genetics opens potential leader position in this technology	• No digital backup of human brain project

List of links included in the article

1. https://www.epfl.ch/labs/vita/
2. https://www.health-eu.eu/
3. https://actu.epfl.ch/news/with-health-eu-everyone-will-have-an-avatar-to-man/
4. https://cordis.europa.eu/project/rcn/220162/factsheet/en
5. https://akselos.com/blog/akselos-rb-fea-is-the-digital-twin-gold-standard-by-dr-knezevic/
6. https://akselos.com/news/akselos-to-create-worlds-first-digital-twin-of-hydroelectric-power-station/
7. https://www.zdnet.com/article/this-power-station-the-size-of-a-cathedral-is-getting-a-digital-twin/
8. https://www.ictjournal.ch/articles/2019-07-10/digital-twins-des-clones-virtuels-au-service-du-reel
9. https://www.biovotion.com/everion/
10. https://www.startupticker.ch/en/news/august-2018/pain-management-solution-with-swiss-wearable-technology
11. http://nomoko.world/
12. https://www.switzerland-innovation.com/node/326
13. https://smw.ch/article/doi/smw.2018.14571
14. https://www.nature.com/articles/518276b
15. https://actu.epfl.ch/news/two-items-of-anthology-now-stored-for-eternity-in-/
16. https://ethz.ch/en/news-and-events/eth-news/news/2018/04/entire-music-album-to-be-stored-on-DNA.html
17. http://www.turbobeads.com/
18. https://ethz.ch/en/news-and-events/eth-news/news/2019/03/bacterial-genome-created-with-computer.html
19. https://www.epfl.ch/research/domains/bluebrain/blue-brain/research/
20. https://www.epfl.ch/research/domains/bluebrain/blue-brain/research/
21. https://www.epfl.ch/research/domains/bluebrain/blue-brain/publications/
22. https://www.humanbrainproject.eu/en/
23. https://www.humanbrainproject.eu/en/open-ethical-engaged/contributors/partners/
24. https://cnbi.epfl.ch/
25. http://ieeexplore.ieee.org/document/7109829
26. http://www.project-rewalk.com/fr/home
27. https://www.bfh.ch/ti/fr/recherche/domaines-de-recherche/institut-rehabilitation-technologie-performance-irpt/
28. https://www.youtube.com/watch?v=PphYGkNENGw
29. https://lsro.epfl.ch/
30. https://www.varileg-enhanced.ch/

31. http://www.robo-mate.eu/
32. https://www.hsr-enhanced.ch/
33. https://www.youtube.com/watch?v=QtPs8d4JbwY&feature=youtu.be
34. https://neuroeng.ethz.ch/
35. https://www.bfh.ch/ti/en/research/research-areas/microlab/
36. http://ninapro.hevs.ch/ProHand/
37. https://www.uzh.ch/
38. http://www.idsia.ch/
39. https://www.unibe.ch/
40. https://www.empa.ch/
41. https://fes-ability.ch//
42. https://www.intento.ch/
43. https://myo.swiss/en/
44. https://www.noonee.com/en/
45. https://www.sensars.com/
46. http://twiice.ch/
47. http://www.swisslimbs.org/products-and-services/
48. https://projectcircleg.com/
49. https://www.sensimed.ch/
50. https://actu.epfl.ch/news/an-innovative-contact-lens-for-glaucoma/
51. https://www.youtube.com/watch?v=u1ck8Fg7nhg
52. http://fabrinal.ch/en/
53. https://infoscience.epfl.ch/record/189508?ln=fr
54. https://www.dezeen.com/2015/02/17/telescopic-contact-lenses-zoom-in-and-out-with-right-and-left-winks/
55. https://ethz.ch/content/dam/ethz/special-interest/mavt/energy-technology/nets-dam/documents/publications/Choi_Park_Graphene.pdf
56. https://ethz.ch/en/news-and-events/eth-news/news/2019/04/biosynthetic-dual-core-cell-computer.html
57. https://bsse.ethz.ch/synbio/research/InVivo.html
58. https://www.nature.com/articles/ncomms5729
59. https://www.idiap.ch/en/about/overview#idiapataglance
60. http://www.manufacturethinking.ch/blog/2018/10/17/les-maitres-de-lia-en-romandie/
61. https://www.swissinfo.ch/eng/social-media_-facebook-to-double-numbers-in-zurich-office/45251896
62. https://www.zurich.ibm.com/
63. https://www.microsoft.com/en-us/research/event/mixed-reality-and-ai-zurich-lab-launch/
64. https://ml.inf.ethz.ch/
65. https://www.epfl.ch/schools/ic/fr/recherche/intelligence-artificielle-apprentissage-automatique/
66. https://www.es.unisg.ch/en/programme/cas-hsg-big-data-and-artificial-intelligence-managers
67. https://www.idiap.ch/en/scientific-research/machine-learning
68. http://www.idsia.ch/
69. https://www.s-ge.com/sites/default/files/publication/free/factsheet-artificial-intelligence-switzerland-s-ge-en-2019_0.pdf
70. https://www.linkedin.com/pulse/european-artificial-intelligence-landscape-more-than-400-westerheide/
71. https://www.nviso.ai/en/about-us
72. https://www.spinningbytes.com/services/
73. https://www.mindmaze.com/
74. https://www.letemps.ch/economie/chatbots-percent-suisse
75. https://www.pwc.ch/en/publications/2017/Chatbot-survey_eng_final_web.pdf
76. https://www.helvetia.com/ch/web/fr/notre-profil/a-propos-helvetia/informations/chatbot-service.html
77. https://www.helvetia.com/ch/web/en/about-us/about-helvetia/information/chatbot-service.html

78. https://www.startupticker.ch/en/news/april-2019/sbb-answers-ticketing-questions-via-chatbot
79. https://www.postfinance.ch/fr/notre-profil/medias/newsroom/communiques-presse/le-chatbot-de-postfinance-disponible-en-francais.html
80. https://www.ictjournal.ch/news/2019-05-17/le-chatbot-nelly-va-parler-aux-passagers-de-swiss-via-facebook-messenger
81. https://www.swiss.com/switzerland/EN/chatbot-nelly
82. https://www.swisscom.ch/en/business/enterprise/themen/digital-business/des-2017-008-servicesmit-kuenstlicher-intelligenz.html
83. http://www.obeeone.com/3139/
84. https://dermintel.com/
85. https://www.siropbot.ch
86. http://www.enterprisebot.ai/technology
87. https://www.elca.ch/fr/chatbots-et-agents-virtuels
88. https://www.adnovum.ch/en/innovation/chatbots.html#contact
89. https://paixon.ch/
90. https://www.spinningbytes.com/
91. https://www.mobile-coach.eu/
92. https://www.parlament.ch/Documents/parli-f.html
93. https://sawisms.blog/2017/05/30/en-politique-suisse-les-reseaux-sociaux-se-professionnalisent-timidement/
94. https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183448
95. https://www.arcinfo.ch/articles/suisse/medias-les-suisses-considerent-les-fake-news-comme-un-danger-pour-la-democratie-789913
96. https://actu.epfl.ch/news/un-logiciel-pour-demasquer-les-deepfake-prend-form/
97. https://www.ictjournal.ch/news/2019-06-21/une-ia-nee-a-martigny-identifie-les-videos-truquees
98. https://en.wikipedia.org/wiki/Fabula_AI
99. https://www.bakom.admin.ch/bakom/en/homepage/digital-switzerland-and-internet/strategie-digitale-schweiz.html
100. https://strategy.digitaldialog.swiss/en/strategie-digitale-schweiz-pdf
101. https://strategy.digitaldialog.swiss/
102. https://strategy.digitaldialog.swiss/en/data-digital-content-and-artificial-intelligence#objective-1
103. https://strategy.digitaldialog.swiss/en/data-digital-content-and-artificial-intelligence#objective-2
104. https://strategy.digitaldialog.swiss/en/data-digital-content-and-artificial-intelligence#objective-3
105. https://strategy.digitaldialog.swiss/en/data-digital-content-and-artificial-intelligence#objective-4
106. https://digitalswitzerland.com/

Information

INTRODUCTION

Critical Sci-Fi movies and literature in the tradition of George Orwell often warn about total surveillance by state authorities. However, in order to succeed militarily in future urban wars, information about what happens on and beside the battlefield is crucial. Without knowing every movement of enemy forces, troop locations or communication channels within a city, the soldier of the future will not be able to accomplish his mission.

Information is a general term that covers all kinds of meanings. In the context of future urban warfare, it stands for data as in information that is picked up by sensors and then being processed. It also stands for the information domain, which includes the dynamics of social networks, digital communication systems, misinformation campaigns or propaganda.

Network Operations Center: Artificial Intelligence will support real-time analysis and mission planning
Source: IABG

CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Information gathering

Mapping applications have made it quite easy to navigate within a large city for almost anyone. People do not buy maps anymore, they simply take out their phones to cope in a new environment. For the soldier of the future, things are not going to be as easy. The requirements of the future urban battlefield call for a fundamentally different approach to the use of available information.

Gathering and analysing information is key in future warfare. Because large urban areas are very complex and difficult to grasp, soldiers need to be well prepared in order to operate effectively. A clear and comprehensive situation picture needs to be provided to military operators. Data gathered by all available sensors, civil as well as military, has to be aggregated into a holistic situational overview.

When required, armed forces have to be able to fall back on civil infrastructures and sensor technology. Surveillance cameras, Internet of Things devices, cellular data and even sensors of offshore wind farms or animal monitoring instruments are assets to assess enemy forces and civilian movements on the battlefield. At the same time, these sources of information need to be protected from hostile access to sustain advantage.

Urban warfare will be fought on all levels of a city, from the air via drones and aircrafts, on the ground level and on the subsurface. Simply accessing many sensors will not be enough to build a comprehensive situational picture. Military intelligence has to find ways to connect and combine all available sensors. Prospectively, Artificial Intelligence will support this process by automatically putting together the necessary pieces of information.

Sensors do not have to be physical, as digital surveillance and the monitoring of civil and military communication will contribute to the situation picture. Especially internal conflicts and riots are typically organized through social media. Early warning systems relying on text analysis within the information domain become even more important.

Information analysis

While all of us have seen movies with futuristic war rooms where all available information is displayed on a large screen and the commander only needs to wave his hand in the air to restructure the elements, this is not realistic in today's mission planning. The status quo for most conventional armies is rather that information is not collected centrally and that the analysis of available data takes a lot of time.

Recent terrorist attacks on large cities like Paris and Berlin show how all kind of information just starts swirling around the information sphere as soon as something unforeseen happens. Cellphone videos of bystanders and victims, tweets of civilians and rescue teams, gathered information by police, military and intelligence personnel – all

this needs to be structured and analysed in real time. While this is true even for singular events like a terrorist attack, this is all the more evident on an urban battlefield within an enduring conflict. Future conflicts will consist of many different actors linked in fragile alliances and shifting intentions. Discrimination and specification of actors on the battlefield will be a major capability in future urban warfare. To prevent civilian casualties and to protect own forces, conventional armies need to be aware of any movement on the battlefield.

Simply gathering a huge amount of information will not help to overcome an enemy within a densely populated area. One also needs to be able to structure, analyse and present the incoming data in order to use it properly. Because of the large number of sensors and the mass of raw data collected by them, human analysts will not be capable of analysing all of it. Artificial Intelligence and automated systems are necessary to process data and provide military decision makers with recommended options. Creating and building self-learning systems takes a long time and soldiers working on them require special training. Therefore implementation of centralized processes and acquisition of new technologies combined with new concepts of mass data analysis need to start sooner rather than later.

Information sharing

In the aftermath of 9/11, failed cooperation and sharing of information between intelligence agencies and government institutions was made out to be the most severe mistake committed by the US government. If NSA, CIA and the DoD had cooperated on the matter, the terrorist attack on the World Trade Centre might have been handled much more effectively. What proved to be difficult even within a single government becomes more challenging when more actors are involved.

In urban warfare, information sharing with allies as well as with the local population is of great importance. Local organizations and civilians are vital human intelligence assets which can be used to get a better understanding of a city's infrastructure and culture. They often know more about strategic points of interests, frequently used supply routes and possible hideouts than official government sources. If the recruitment of human sensors is successful, it will result in advantages concerning situational awareness. Usually, this does not remain a one-way road. In cities with high population density, it is vital to warn the civil population of danger to avoid large casualties. Warning systems and information channels need to be implemented and tested in the area of crisis.

The combination of sensors and sources with allies is another element of information sharing, which will become increasingly important. While different laws and rules of engagement often complicate direct cooperation within international missions, sharing of information and data contributes to a joint situational picture everyone can profit from. Especially countries with a cautious security policy who are not willing to send soldiers into an area of crisis can do their part from the distance by providing intelligence and helping with data analysis.

Still, sharing of information always comes with certain risks. Civilian organizations and non-state actors like militias or rebel groups in particular, need to be vetted before they receive classified data. In addition, volatile alliance structures complicate the selection of trustworthy partners.

Information domain

During the annexation of Crimea in 2014, Russian paramilitary forces used an insidious method to intimidate Ukrainian soldiers. They went online, scanned the social media profiles of soldiers and their families and took photos off these profiles to show their enemies how much they know about them. This weakened the morale of Ukrainian fighters and contributed to the victory of Pro-Russian militias.

Between 2010 and 2012, the revolutionary wave of social uprisings and protests during the "Arab Spring" showed the significant role of social media in today's world. Social media was used to shape political debate, mobilize and empower protests and disseminate information. Beginning in 2010 in Tunisia, demonstrations spread to several Arab countries like Egypt, Bahrain, Libya and Yemen – and thereby proved the power of information and social media.

Helicopter Cockpit: Soldiers will be provided with holistic, real-time situation pictures
Source: IABG

Both examples indicate the relevance of digital information exchange. In the wake of digitalization, information travels faster, farther and is getting harder to verify as well as to secure. Besides the use of information platforms to organize social uprisings, actors exploit the advantages of reaching large audiences for their own purpose. Propaganda of terrorist organizations, fake news distributed by state actors or misleading information on actual incidents confront various actors with new challenges in the information sphere.

In the information sphere, great impact can be made with relatively simple means (resources, equipment). Actors with

little resources can perform successful attacks against individuals, large companies, militaries or states. The attribution of attacks of this kind proves to be nearly impossible. Asymmetric actors or state actors using proxies benefit the most by using the information domain as hybrid war tactics.

The challenge for conventional armies consists of owning the narrative. Every kinetic action is accompanied by pictures and headlines, available to anyone around the world. The interpretation of any military action in the eyes of the global public is dependent on the narrative that goes with it. "NATO forces bomb Syrian children's hospital" sounds a lot different than "IS uses empty hospital to hide weapons". It does not matter which of these headlines is actually true, what matters is who can be more convincing in the information sphere. Especially in urban areas, where many sensors carry information out in the world and where the civilian population is most vulnerable, owning the information domain is significant to a mission's success.

IMPLICATIONS FOR THE MILITARY

The concept of information

Information has been and always will be the foundation of good military mission planning. This does not change. What does change is the sheer mass of data that can be collected today. Conventional armies like the Swiss military need to use their economic and technological advantages to process as much information in as little time as possible. A clearly structured overall situation picture is absolute key to success in (urban) warfare. To be aware of this fact is the first step in developing a military concept of information.

A national information concept has one crucial objective: combine all available information into a single situational picture. Every piece of data that can possibly be collected must flow through one outlet. It is the task of all government institutions to work together on this information concept:

- Coordination of government institutions and appointing of responsibilities
- Setting uniform standards for format and language of shared data
- Creating a platform for communication
- Implementing training and education
- Evaluating and exploring opportunities for sensor sharing
- Evaluating and exploring opportunities of civilian new-information technologies in the military domain

The information concept will not only benefit the military, it can also be used to analyse economic, financial or environmental topics. All the same, military analysts and planners have to rely on all government institutions to work together.

Implementing a new technology

When it comes to the analysis of big data, one technological implication always comes to mind – Artificial Intelligence (AI). And as stated earlier, this assumption is not incorrect. However, AI is not simply a ready-to-use tool that governments can use for military purposes. Developing and implementing automated systems that are supported by AI is intensive in terms of time and financial resources. Eventually, it is not free of risks and ethical restrictions.

As soon as something happens automatically and a computer makes decisions, the responsibility for mistakes is unclear and needs to be regulated. Who is responsible if the AI misses a crucial piece of information? How can you control an automatic system? These questions need to be answered before implementing AI into processes of information analysis. Moreover, "training" automated systems takes time and manpower. Analysis of raw data has to be "taught" to the system and evaluated carefully. Conceptual guidelines need to be considered and the necessary hardware supplied. Once all these requirements are met, automated systems for multiple military purposes in the information domain:

- Analyse mass data in real time and detect anomalies
- Identify actor-specific differences in behaviour and conduct for potential enemies and allies
- Formulate counter measures customized to the threat
- Minimize risk of civilian casualties through precise target discrimination
- Analyse own weaknesses (Red Teaming Function)
- Develop alternative mission plans
- Choose the measures of force effect

Use of strategic communication

Every military action needs to be supported by a communication strategy. This starts with the acquisition process of new weapons systems and technologies. What is the purpose of new fighter jets? What threats counters a missile

defense system? If you do not develop a narrative, somebody else will do it for you. Strategic communication has to be implemented in the training and education of soldiers and into the concepts and doctrines of the army. Every soldier has to understand that he or she is part of something bigger and that any action of a single part of the entity "military" falls back on the institution as a whole.

Moreover, it is important to use strategic communication to increase resilience against opposing narratives. Mistrust and hostility against foreign troops need to be met with building confidence and reliability by translating own narratives into reality.

CONCLUSION

The importance of information to the military appears immediately obvious. Gathering and analysing information before starting a mission is not new, neither is it groundbreaking or innovative. It is the perception of military missions and the technology that is used to gather and analyse information which is innovative in the information domain. As we have learned, every action on the battlefield, especially in urban areas, must fit into a larger narrative – as everything can potentially be broadcasted around the globe. Casualties among civilians and own forces must be avoided at all costs. To be able to do so, military planners and operators need a flawless situational picture they can rely on. Combining sensors, falling back on human intelligence, using AI and automated systems to process big data and training soldiers to handle all this will be key to succeed in future (urban) wars. >>

SWOT-ANALYSIS for swiss military planners

Strengths • Development of information strategies • Skilled reconnaissance personal • Understanding of the importance to detect false information in the military and societal domain"	**Weaknesses** • Missing technological support of analysts • Late start to identify propaganda, false information and how to handle it • Allegedly transparent warzones
Opportunities • Development of technical AI-based analytical systems • Cooperation with partners, allies and economic enterprises)	**Threats** • Hybrid attacks on information systems • Destabilization of societies

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

Communication

Communication of data and information from human to human, machine to machine or human to machine, is expected to be permanent and ubiquitous. Reliability is expected irrespective of whether communication takes place via wired or wireless networks, in the terrestrial or space domain. As such reliable infrastructure and transparent service is paramount for autonomous systems to operate, resilience and security must be guaranteed, but is it so? When we consider augmented and virtual realities, avatars and holograms, new forms of communication in the real world or in parallel virtual worlds are seen to emerge. How to stand back in such a world of immediacy?

Emitting out black holes?

Communicating for the communication's sake

In the previous text we have demonstrated that we live in an information society, in particular because we are, according to Norbert Wiener and the apostles of cybernetics, complex systems, which, in the same way as animals and machines, are continually exchanging information with our environment. This omnipresence of the exchange of information – which is also self-regulating *(feedback loop)* – also enables the understanding that the information society has very rapidly doubled, already with Norbert Wiener, from a communication society: the more we exchange information - the more we communicate therefore - the closer we are to our intimate nature. How can one not grasp here, that the epistemological monism at the heart of cybernetics – information, the mode of being for complex systems – leads to an ideological reworking of society, suddenly reoriented towards the exploitation of that which is at the basis of the biological and mechanical reality? The reasons for this reworking, apparently rational, because they are scientific, are not so much so, when we remember that Norbert Wiener, after the atrocities of the Second World War, effectively founded a new *theology* – information assumed the place of the god of the revealed religions –, a new *utopia*. The scientific is in effect intimately undermined by the responsibility of scientists in nightmares such as the atomic bomb and the concentration camp; this is why the American mathematician, combining in this the hatred of the body promoted by certain strands of Christianity, seeks to flee matter, and to put it behind him, to impute all crimes to it, all passions and all violence – as shown very clearly in his letters of 1945. Cybernetics, in consequence, is from the outset conceived as the remedy to human abuses, like the new utopia which will enable the avoidance of the past repeating itself: as information is not material – even if it does transit via physical interfaces (body, mind) –, creating a society around this postulate, particularly by emphasising the value of communicational interactions, is the road to follow so that the human avoids the fate of foundering in the follies dictated by its body. In other words, it is not as rare as one might imagine, we notice that the scientific theory founded by Wiener – and more active than ever in our contemporary society – is a lay utopia based upon a theological paradigm.

Utopia, and since Thomas More's (1516) *Utopia*, is a fictional narrative which invents an alternative world by articulating it around a rational principle that is different from that of the empirical world; however, while in the fictions this procedure enables one to reflect upon the dysfunctionalities of the real – utopia is a hermeneutic mirror –, Wiener and all those who sought to establish a utopia imagine it as something possible, the section of its mirrored nature. Cybernetics is not, in this sense, considered as an image reflecting our aberrations, but as an ideal *to be attained*; and this is the crux of the matter. In fact, it is possible to learn a lesson from the classical narrative utopias: the utopic world is painted as perfect, but as soon as one begins to live it, one follows a personality evolving in this clock-maker's mechanics, while the alienating nature in this ideal reveals itself and the world becomes nightmarish, dystopian. In other words, *1984* by George Orwell (1949) is a utopia seen from the inside; the same for Nous autres *[We others]* (Eugène Zamiatine, 1920) or *Brave New World* (Aldous Huxley, 1932). There is no difference in nature between the utopias and dystopias: they are the same systems, but perceived differently; they are the same worlds, but the one speaks to us of the dysfunctionalities of society, while the other marks out the dysfunctionalities of ... our utopias.

Strangely, today we live in the era of information and communications: we need to communicate, never to stop, to continue, to multiply the resources available to achieve this, owning a smartphone, never turning it off, communicating via SMS, emails, social networks; but also never forgetting to exchange, with gluttony, endlessly, and fearlessly, all the information we can, everywhere, all the time, even if it enriches the servers of GAFAM (Google, Amazon, Facebook, Apple, Microsoft). This injunction to communicate – but also to consume, because in the information era, information is a precious asset – also explains the choices operated by marketing strategies: advertising needs to be everywhere, solicitations are just not supposed ever to stop. It is scarcely surprising that science fiction, a recent avatar of utopia (in this case science fiction spends its time reflecting upon our techno-scientific utopias), has taken this societal reality in order to reflect its consequences upon human beings: cyberpunk narratives – films such as *Blade Runner* (Ridley Scott, 1982) or *Strange Days* (Kathryn Bigelow, 1995) come to mind – always take place in dark worlds where advertising information carpets the building facades and imposes itself upon our gaze without our opinion being sought. Given that most science fiction narratives construct their worlds on the same principles as the real world – which can be understood due to the necessity of proposing a realist reading pact –, it is logical to see a quantity of intrigues being exploited, to nonetheless varying degrees, the effects upon human beings of this avalanche

of information and the implicit obligation of being required to communicate on a permanent basis. Philip K. Dick shows us with a morbid jubilation how, in "Sales Pitch" (1954), the character in the short story becomes crazed through living in a futuristic world where advertising is omnipresent. Another particularly powerful example is given to us in the short story "So phare away" (2007) by Alain Damasio, in which the lighthouse keepers have the mission of emitting coloured light in order to communicate with others. The light of the lighthouses then suddenly becomes the metaphor for information that we communicate left right and centre, without pausing to consider the quality of the information:

> The lighthouses express themselves of course. Often copy each other, mutually decode and trace each other. They give out their personal light. *Express your moi, be yourself* – as everyone does. I stopped doing this long ago. They call me bitter. [...] Who says what? That in a world where everyone thinks they are supposed to express themselves, no illumination is possible. Nothing can be *enlightened* in a context of total luminance. A lot of silence is needed to hear a single note. A lot of night is needed for a flash of light to shine out, for a new colour to be seen, or received. If I had the power to do it, what I would do now is to emit a black hole. Something like an extinction cone boring through the stomach of the thickness of the daylight. To re-open space. What terrifies me is not this chaos of brightness that scrambles the city like an avalanche of suns. It is that there is no more shadow anywhere. Everything is ferociously over-exposed. But nothing is established. Or distinct.

The criticism is acerbic, the voice speaking to us is vindictive: when too many lights are being emitted simultaneously – when there is too much information –, the "statement" fades, disappears, no longer articulates: there is *"no more shadow anywhere"*, *"Everything is ferociously over-exposed"*, whereas this shadow – this separation between the messages – and this sense of propriety are necessary for the communication to make sense. A ferocious assault against a logorrhoeic society in which information dis-informs, "So phare away" fascinates, and proves just how far Damasian science fiction reflects, and reflects upon our identity...

Conclusion

As a worthy successor to the classical utopian narratives, science fiction has the virtue of interrogating our techno-scientific utopias and questioning the passivity with which we accept them, while they model us, inform us, reduce us. When the utopia of communication is involved – based upon the central role occupied by information in the human condition –, the authors of science fiction really go to town on this, but the intrigues they offer us cause us to gnash our teeth: mankind sees its exterior and interior space saturated by information; mankind discovers that it no longer has the choice but to be permanently involved in communicating. Democratic freedom, so hard won, is then no more than a pious hope: how can one think, choose, or reflect, if every instant of our existence is saturated? How can we be hungry if we are force-fed? How can we not want to cry out with our entire being, like Damasio's character, *"If I had the power to do it, what I would do now is to send out a black hole"*? Because without these black holes, communication communicates nothing to us: it simply emits information whose content is of little consequence, because all that matters is that it should be emitted.

The Widening Stream: The Future of Communications

The world today is already perceived as a rush of non-stop communication. The world of tomorrow looks to be more of the same: faster and invisible, enabling humans to communicate with one another, but also facilitating human-to-machine and machine-to-machine interactions. It could be that the future of communications enables a utopia where needs are instantly met and anticipated, but the shadow of this is a world in which humans are ceaselessly monitored and analyzed even faster than we can make decisions for ourselves, all for the benefit of the machines envisioned to serve us.

This faster world is more than a metaphor: today's cell phones communicate with one another over the 4G network, reaching peak speeds of 3mb per second. Next generation (5G) devices are already coming to areas of the United States, Canada, Japan, and China, capable of transfers of 1gb per second: what would be a seven-minute download today could take just six seconds. That shift heralds an era wherein so-called "landline" speeds and cellular speeds will be evenly paired, bringing the benefits of fibre-optic cable speeds to portable devices.

5G has long-term potential to accelerate not just how humans communicate with each other, but how we communicate with machines. Where today's 4G devices experience a nearly imperceptible 20-60ms lag between data being transmitted and received, 5G would eventually be capable of transmitting higher quality video with less than 1ms delays, allowing near-real-time telepresence between any location with access to the network. This stream is not only faster, but is in a sense wider, allowing larger files and multiple sources of data to be accessed at the same time.

Ericsson, a mobile manufacturer, predicts 1.9 billion users[1] would have access to 5G services by 2024. In contrast, Deloitte estimates a significantly lower adoption rate of 1.2 billion subscribers[2] by 2025, densely concentrated in North America, Europe, and Japan/China. The tech is not only for cellular phones, but could spark an era where 5G antennas could be deployed in rural areas, offering high-speed broadband anywhere it is needed, connecting laptop computers, machinery, drones, self-driving cars, tractors, and robotics to the so-called "Internet of Things" in ways that transcend today's imagination.

This transformation is already underway. In Switzerland, Swisscom has "switched on" 5G networks across the country, claiming 90% coverage by the end of 2019[3] — far ahead of the market for 5G-capable devices. In the US, 13,000 satellites have been approved to launch[4] for 5G capacity. This year, the US Department of Defense has announced that it will begin trials for 5G services on military bases[5]. That comes on the heels of the U.S. Federal Communication Commission's approval of a SpaceX plan to launch 4,425 5G satellites[6]; data giant Amazon has requested to launch 3,236 5G satellites of its own[7] — satellites that come pre-packaged not only with 5G, but with 6G capabilities. Other companies in the new space race include Japan's SoftBank and the UK's Virgin Group. Such plans for satellite launches do not come without consequences — the European Space Agency recently had to force an emergency manoeuvre of a weather satellite to avoid a collision with a so-called "mega constellation" of SpaceX satellites[8] already in orbit, and many fear it is only the first to come as we enter a new era of these objects in space[9].

Communications: Machine to Machine

Already, these networks are being eyed as ways to shift processing power from an internal device to an external, even cloud-based, server. By allowing nearly-instantaneous communication between devices, the weight of objects, such as virtual or augmented reality headsets, can be streamlined by offloading processing to smaller devices (sometimes called "cloudlets[10]"). This way, the device doesn't need to have processors built in, but could rely on external computers to do the heavy lifting of computation, sending signals back to a headset, screen, or wearable device. In essence, the heaviest hardware can be reduced to the bare minimum: a robot doesn't need a full camera on board to see objects in front of it; it only needs the camera lens, connected remotely to anything from a cell phone to a warehouse-sized supercomputer.

This has implications for so-called "Cloud Robotics," long imagined by engineers but rarely applied in the absence of 5G coverage[11]. Cloud Robotics allows complicated computational decisions to be processed and communicated wirelessly between a computer and a robot. 5G allows near-instantaneous decision-making by the device as it gives instructions to the mobile robot, but also allows the computer to share information near-instantaneously with other robots anywhere in the world, guiding software updates, avoiding glitches, and creating opportunities to replicate "learnings" on one site across the entire network, instantly.

The CloudMinds XR-1 robot performs for visitors at the Mobile World Congress in Barcelona in February 2019.

The global robotics startup Cloudminds[12] offers an example of this approach. The XR-1 robot is mostly hardware — a shell, of sorts — with access to a cloud-based library of scripts developed internally and by independent developers. When an XR-1 is asked to do something it hasn't done before, it searches the Cloudminds library for instructions on how to complete that task. With a 5G connection, this could happen nearly in real-time, creating a network of robots that is instantly interchangeable and constantly communicating real-world feedback.

Other proposals for 5G include its use in self-driving vehicles, which could become transmitting stations broadcasting locations to roadside transmitters, eliminating the need for complex on-board navigation machinery[13]. This would require widespread improvements in the speed, reliability and ubiquity of sensors. Connecting IoT technology to vehicles would allow them to anticipate and react to their environment, from immediate lane changes to broad traffic trends and road outages.

Communications: Human to Machines

Near-real-time, low-latency communication could accelerate the transformation of the smartphone from an active communication device to a passive one. Already, reams of data are collected about movements and behaviours, with a recent expose showing 5,400 trackers communicating data from your phone overnight[14]. Today, it is possible[15] to measure the success of analogue advertising such as billboards[16] based on smartphone tracking, and the "datafication" of non-digital experiences is likely to expand. If so, it could point to a future in which the scope of advertising, media monitoring, and influence campaigns could be tracked and adapted in real-time, in real space, based on the understanding of who looks to the digital billboard at any given moment: a world in which it becomes increasingly difficult to "unplug the phone."

Turning the smartphone into a data collection tool would have benefits, of course. For example, 5G could connect real-time sensors for information gathering at sites of crisis — allowing first responders, police, or military to have a synchronized understanding of the aftermath of a catastrophic event[17] — while recording and transmitting information about environmental hazards, health status, and actions of first responders.

However, the experience of a centralized "phone" or other object for communication may itself be outpaced by the possibilities of smaller sensors in a 5G era. Sensors embedded into the fabric of a shirt could communicate with the sensors in a car, for example, to let the car know that you are approaching and that it should prepare for you. Credit company MasterCard is proposing a world where devices learn from your spending habits, shares that information between other devices, and anticipates or encourages those habits[18].

Reducing the processing burden on devices could also create more functionality for Augmented Reality in technologies such as Google Glass, which failed on launch but have recently been re-introduced as a product for the workplace[19].

Photo: A Google Glass Wearer, by Loïc Le Meur - Flickr: Loïc Le Meur on Google

Glasses rely on a user experience which combines eye tracking, voice, and gesture commands, transforming the way we interact with information. The user experience in the 5G era would include real-time feedback embedded into the environment, and in the long term could create an interface with other devices embedded into other objects.

The possibilities for such uses include live 360-degree vision, shared vision, and real-time interaction with avatars made to appear in the local environment. This could provide real-time AR for first responders that could show the perspective of a drone camera for real-time "eagle's eye" vision that could help coordinate rescue actions[20].

Communications: Human to Human

5G networks are also poised to transform communication between people, creating new opportunities for telepresence and immersive chats. Paired with Virtual Reality, 5G would make it possible for virtual participants not only to see a room from a fixed position, but also to "move around" based on the positions of multiple, interconnected cameras — a holy grail for VR known as "six degrees of freedom," that is, six possible paths of motion for a user. If successful, this kind of technology could pave the way to real-time presence in remote locations, transforming the concept of "telecommuting employees."

Such telepresence is poised to bring new possibilities to a range of activities now assumed to require a local presence. For example, surgery: China set the milestone for first telepresence surgery in 2019, when a surgeon in Beijing performed an operation on a patient 3,000 miles away using Huawei's 5G network, according to Chinese media reports[21]. 5G medical telepresence would allow physicians and surgeons to offer real-time expertise anywhere in the world[22], potentially expanding access to advanced medical procedures and training for those in remote areas.

High speed communications technology would eliminate the lag and interruptions that mar much of today's video conferencing. With faster, larger data transfer speeds over 5G and 6G networks, the future of "holographic" video conferencing will no longer restricted by the network, but by the challenge of optics. Today, holographic telepresence is possible using multiple cameras and projectors within a cylinder[23]. However, these machines are bulky and the viewing radius is limited, causing the image to disappear from certain positions around a room. Research continues into volumetric displays[24], which use high-speed lasers to create the illusion of an object in three-dimensional space, but as of today, these are limited to a single colour projection.

5G: Constraints and Concerns

The rollout of 5G will require heavy investment in infrastructure upgrades, estimated to total between $500 billion and $1 trillion globally[25], while the transformation of supporting systems (to ensure devices, supply chains, and other

systems can make use of 5G) is even higher, bringing global cost estimates to be 2.7 trillion dollars in the first year of rollout alone. This limits the 5G rollout to a handful of stakeholders already operating in telecommunications.

A key geopolitical player in 5G is Huawei, the Chinese communications giant that has dominated the market to the chagrin of the United States. The US Department of Defense, in its list of recommendations for 5G adoption[26], outlined fears that Chinese-produced equipment would permit the same access to data through Huawei devices shipped abroad that are maintained for devices distributed inland. European competitors such as Nokia and Ericsson are regulated by the strict data privacy standards of the GDPR; however, they are seen by some to lack the competitive advantage, and manufacturing capacity, of their Chinese rival[27]. Regardless, the companies have made inroads amidst the security controversy, with Nokia announcing it has signed more contracts for 5G systems than Huawei[28].

Despite US[29] (and Czech[30]) concerns over the security threats posed by using Chinese platforms for communications — citing a Chinese intelligence law which states that "the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings" – Huawei has made rapid inroads into the market, from Brazil[31] to the United Kingdom[32]. Nations including Australia, New Zealand, and Japan have followed the US ban, though the US position has been flexible[33]. It seems clear, however, that regulatory and cybersecurity concerns loom large on the geopolitical sphere for the pace and scale of 5G adoption globally.

Other constraints on the adoption of 5G include a number of local regulatory hurdles, including public perceptions about health effects tied to radiation, a fear that has been promoted by disinformation campaigns[34]. The World Health Organization has found "no evidence to date" that the radiation associated with 5G poses a public health risk[35], in alignment with several independent research studies[36]; the US-based Center for Disease Control suggests "there is no definitive answer" to the question of whether cell phone use and dangerous radiation exposure are linked[37], while the US Federal Communications Commission announced that current safety precautions[38] for cell phones were stringent enough for 5G networks.

A Vodafone 5G tower in Germany. By Fabian Horst, CC BY-SA 4.0, via Wikimedia Commons.

Nonetheless, citizen concerns have lead the government in Switzerland to create a monitoring project for 5G radiation[39]; the canton of Vaud has frozen 5G rollout[40]. In Silicon Valley, Bay Area cities Mill Valley, Sebastapol[41], and San Rafael[42] have blocked the construction of 5G towers, awaiting more information about their health effects.

5G services also face technical limits, depending on the portion of the radio spectrum they occupy. A 5G rollout makes use of ultra-high-frequency millimetre waves (mmWave) that can transmit dense amounts of data in very short distances — up to 1,000 feet. These waves are in the 24GHz to 300GHz range. This 5G signal requires denser placements of antenna, with reliable signal requiring placement every 150 meters (500 feet). The impact of these antenna on local neighbourhoods has also lead to citizen resistance to their placement[43]. mmWave technology also poses challenges from a materials perspective — global demand for 5G could place incredible strains on the availability of 5G semi-

conductors, as well as the expertise — and energy — needed to build and maintain them.

Alternatively, so-called "sub 6" frequencies (below 6Ghz) make use of longer waves already in use for communications services in military, emergency, and some commercial applications. These are more readily accessible to a broader base of consumers but pose risks to the security of transmissions already taking place on these channels; and due to limited availability, interference between overlapping users poses a greater reliability threat on sub-6 frequencies.

Beyond 5G: Quantum Communications

Looking to a more distant horizon, scientists today are working on quantum technologies that could transform communication. Quantum technology relies on a deeper understanding of physics at the atomic level, in which rules of the macro world operate differently. For example, light can be harnessed as a particle and a wave simultaneously, creating a "superposition" of both. In essence, this transforms the possibilities of computing by moving machines away from the binary logic of bits — 0 and 1 — to the quantum logic of qbits, in which data can be stored at infinite points between 0 and 1.

Quantum computing has been realized in labs, and are even being commercialized through ventures such as IBM's Q[44], which recently announced a partnership with diverse stakeholders, from the physics researchers at CERN[45] to the energy giant Exxon-Mobil[46].

Though largely theoretical, researchers suggest that quantum technology would point to a radical shift in cryptography. Considering the physics law that you cannot observe the speed and location of a particle at the exact same time, quantum computing could create communications sensitive to external observation — in essence, messages that scramble into incoherence the moment an unauthorized viewer tries to read them.

Theorized as early as 1984, quantum encryption was deployed in 2007 as a means of securing the transfer of polling station votes to Geneva[47] during a Swiss federal election. Today's encryption relies on quantum data to be encrypted at a start point — a lock — and decoded at the reception point — a key — independent of the message the key decodes. This is called quantum key distribution (QKD), and is a promising first step to full quantum encryption of the data stream. QKD works by replacing large strings of numbers, as is used in traditional encryption, with a kind of "snapshot" of the exact states of a range of qbits. This is typically done through fibre-optic cables identical to what is used in today's internet infrastructure.

The constraint on this technology is distance: as a dense quantum key is transferred further away from its source, the stability of the data collapses, introducing variations into the copy of the key, blurring the copy's ability to confirm the original, and reducing the certainty of holding the same key. This compromises the security of the transmission — and begins as the qbits approach 200km of distance from the source. Companies such as Raytheon have been working on methods[48] to send a key from the source point to the receiver of the transmission that can transcend this constraint.

Most promisingly, Chinese researchers were able to create a quantum-entangled video stream from Vienna to Shanghai (7,600km) in 2018[49] using an orbiting satellite that transmitted quantum-secure decryption codes to both sides of the broadcast. This proof of concept was able to transmit 2gb of secure data over 75 minutes. However, it relied on 32 additional nodes to "repeat" the signal, meaning the strength of the transmission remained relatively limited.

The prospect of building these more powerful tools for encryption could diminish the strength of today's security protocols. Because quantum computers are capable of processing larger ranges of numbers simultaneously, their ability to "hack" encryption codes is significantly faster than traditional computers: imagine trying to open a combination lock by trying each number combination individually, and compare it to having a room full of people with identical copies of the lock working on the problem simultaneously. This is roughly the difference between traditional hacking methods, which can try one series of numbers at a time, and quantum computing, which can attempt multiple number combinations simultaneously. This year, the US Defense Information Systems Agency at the Pentagon issued a call for quantum-resistant encryption methods[50].

But perhaps the most startling future of communication will come in the form of a Quantum Internet, in which the most sensitive data can be transmitted securely and in real time through a process called "quantum entanglement." Entanglement refers to the phenomenon, which occurs only at the smallest scales of physics, in which a particle's behaviour is instantly influenced by another particle, regardless of their distance from one another. The constraint on quantum communication through entanglements is the immense difficulty of sustaining these entanglements; currently, the process is restricted to 10 qbits, with recent progress heralding a sustained 10-qbit string[51] within a 20-qbit chain.

Harnessing this force for data transmission could mean instant, secure communication anywhere in the world or space: imagine a computer that not only transmits data, but transmits those computations instantly onto a machine in another part of the world, or to a satellite or spacecraft, as was achieved by Chinese researchers in 2017[52]. >>

What's Next?

The expansion of the 5G signal means faster services, greater simultaneity in our communications, and a widening stream of data being delivered and collected about the human users of a network. Through the passive, ambient collection of data, such communication will take place even when one "opts out." The impact of 5G may be a test to the human mind's ability to adapt to the challenge of today's information landscape — social media pings, phone alerts, and news updates have already shortened attention spans, challenged our social interactions, and reduced memory[53]. Widening this stream, at a faster pace, would turn a digital deluge into a maelstrom.

The solution to this may well lie in more technology — technology that can slow down the information to a level most comfortable to human perception, machines analysing data to predict and anticipate needs before we ever think to ask. If so, the question of a utopia or a dystopia both rely on whether we design these solutions to comfort the passive consumer of information, or to facilitate greater agency and control over the choices of our lives.

List of links included in the article

1. https://www.ericsson.com/en/mobility-report/reports/june-2019
2. https://www2.deloitte.com/insights/us/en/industry/technology/technology-media-and-telecom-predictions/5g-wireless-technology-market.html
3. https://www.swisscom.ch/en/about/news/2019/04/17-erstes-5g-netz-live.html
4. https://www.latimes.com/business/la-fi-amazon-spacex-space-internet-20190705-story.html
5. https://fcw.com/articles/2019/07/05/dod-preps-bases-5g.aspx
6. https://www.fcc.gov/document/fcc-authorizes-spacex-provide-broadband-satellite-services
7. https://www.latimes.com/business/la-fi-amazon-spacex-space-internet-20190705-story.html
8. https://twitter.com/esaoperations/status/1168533241873260544
9. https://www.technologyreview.com/s/613239/why-satellite-mega-constellations-are-a-massive-threat-to-safety-in-space/
10. https://en.wikipedia.org/wiki/Cloudlet
11. https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2016/etr-5g-cloud-robotics.pdf
12. https://www.en.cloudminds.com/
13. https://venturebeat.com/2019/05/08/waymo-cto-5g-will-be-a-self-driving-car-accelerator-and-enabler/
14. https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/
15. https://www.cuebiq.com/location-intelligence/attribution/
16. https://www.mediavillage.com/article/perfecting-out-of-home-measurement-an-interview-with-clear-channels-andy-stevens/
17. http://www.blueforcedev.com
18. https://www.mastercard.us/en-us/consumers/payment-technologies/connected-commerce.html
19. https://www.blog.google/products/hardware/glass-enterprise-edition-2/
20. https://www.verizon.com/about/news/5g-and-mixed-reality-glasses-help-change-how-we-see-world
21. http://www.chinadaily.com.cn/a/201903/18/WS5c8f0528a3106c65c34ef2b6.html
22. https://www.proximie.com/
23. http://www.humanmedialab.org/blog/telehuman2
24. https://www.nature.com/articles/d41586-018-01125-y
25. https://www.greensill.com/whitepapers/financing-the-future-of-5g/
26. https://media.defense.gov/2019/Apr/04/2002109654/-1/-1/0/DIB_5G_STUDY_04.04.19.PDF
27. https://www.aspistrategist.org.au/huawei-and-5g-what-are-the-alternatives/
28. https://www.reuters.com/article/us-nokia-5g/nokia-says-it-has-moved-ahead-of-huawei-in-5g-orders-idUSKCN1T428W
29. https://www.nytimes.com/2019/07/05/technology/huawei-lawsuit-us-government.html
30. https://www.nytimes.com/2019/02/12/world/europe/czech-republic-huawei.html
31. https://www.reuters.com/article/us-huawei-tech-brazil-idUSKCN1U42GA
32. https://www.theguardian.com/technology/2019/jul/06/huawei-uk-mobile-5g-networks-operators-gamble-security-concerns
33. https://www.nytimes.com/2019/07/09/business/huawei-donald-trump.html
34. https://www.nytimes.com/2019/05/12/science/5g-phone-safety-health-russia.html
35. http://www.emfexplained.info/?ID=25718
36. https://sp.ehs.cornell.edu/lab-research-safety/radiation/rf-microwaves/Documents/RF_microwave_safety_program.pdf
37. https://www.cdc.gov/nceh/radiation/cell_phones._faq.html
38. https://www.fcc.gov/document/chairman-pai-proposes-maintain-current-rf-exposure-safety-standards
39. https://www.reuters.com/article/us-swiss-5g/switzerland-to-monitor-potential-health-risks-posed-by-5g-networks-idUSKCN1RT159
40. https://lenews.ch/2019/04/11/swiss-canton-blocks-5g-mobile-rollout/

41. https://www.marinij.com/2018/09/09/mill-valley-joins-effort-to-constrain-5g-proliferation/
42. https://www.marinij.com/2018/08/21/san-rafael-residents-take-pre-emptive-strike-against-5g-installations/
43. https://www.citylab.com/life/2019/05/fast-internet-wireless-service-provider-wifi-5g-boxes-fcc/587269/
44. https://www.research.ibm.com/ibm-q/
45. https://www.ibm.com/blogs/research/2019/03/cern-ibm-quantum/
46. https://newsroom.ibm.com/2019-01-08-ExxonMobil-and-Worlds-Leading-Research-Labs-Collaborate-with-IBM-to-Accelerate-Joint-Research-in-Quantum-Computing
47. https://www.economist.com/technology-quarterly/2019/02/18/the-promise-of-quantum-encryption
48. https://www.raytheon.com/capabilities/products/quantum#q-key
49. https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/
50. https://www.fbo.gov/index.php?s=opportunity&mode=form&id=95f46419bef0eb24a69e15771e722cb2&tab=core&_cview=1
51. https://science.sciencemag.org/content/364/6437/260
52. https://arxiv.org/abs/1707.00934
53. https://www.sciencedaily.com/releases/2019/06/190605100345.htm

The future of communication in Switzerland

Even though it has no network technology provider, Switzerland is amongst the most advanced countries in 5G deployment. The mature but also well-developed sensor and microtechnology industry, linked to world-class academic research centres and top robotics development can potentially place Switzerland at the forefront of next-gen communication industry. The very strict legislation and growing popular opposition to 5G may prevent the country from taking the leading role in this field. Switzerland is notably a key player in quantum communications, a beyond-5G technology.

S Start: no real activities | T Trend: Early activities | A Advanced | R Ready | S T A R

HUMAN TO HUMAN COMMUNICATION

Telepresence

S T A R

Telepresence is a major trend of human to human communication. There is no local production of telepresence robots in Switzerland but We-secure.ch commercialize Double robotic products[1] and CISCO has a development team at the EPFL dedicated to telepresence visual conferencing systems[2] (2 patents applied). Academic research is well developed with both EPFL and ETHZ working on telepresence programs. EPFL has an active group working on this topic, especially brain-controlled telepresence robots[3], with 184 publications. ETHZ's CGL (Computer Graphic Laboratory) works on software component such as display, gaze awareness and acquisition algorithms[4]. According to Forbes[5], Switzerland is a frontrunner in worldwide robotics development. This could offer an interesting position for further telepresence development..

Holographic video & volumetric display

S T A R

ETHZ developed HoloPort in 2006[6], a device for simultaneous video and data conferencing featuring gaze awareness. Since then, several Swiss companies commercialize holographic video systems, such as Hologtech SA[7], Wayray[8], Amethys Technologies & Consulting Sàrl[9] and Olomax[10]. EPFL develops a head worn holographic display[11].

HUMAN TO MACHINE COMMUNICATION

Smaller sensors

S T A R

Switzerland has a rich R&D history in small sensor technology, mainly designed for the specialized watch industry with low size/low power components. Some of the world's top R&D institutes in this area are located in the country: the CSEM and the EPFL. The country has a strong ecosystem of sub-contractors and companies dedicated to low CSWaP devices (Costs, Size, Weight and Power) such as EM Microelecronic, Melexis, Sensirion, STMicroelectronics. As an example of national achievement in this field, Sensirion offers the world's smallest humidity and temperature sensor that can be very easily integrated in consumer electronic and wearable sectors[12].

Sensors in garments

S T A R

There is a well-developed activity in Switzerland for sensors-in-clothing technology. Several actors propose technologies that are "garment-compliant", such as EMPA[13], EPFL[14,15] (also in collaboration with the MIT[16]), ETHZ[17], CSEM[18] and STMicroelectronics[19]. A start-up was created in 2015, SensCore[20] but it stopped its activities. The country still needs a first consumer-related company to be considered as "ready".

AR glasses technology

S T A R

Magic Leap, a start-up specialized in Augmented Reality (AR), acquired in 2018 the teams of Lemoptix, a former EPFL spin-off. Magic Leap expands its presence in Switzerland with a new Centre of Excellence in Lausanne. This centre focuses its efforts on advancing Magic Leap's optics and photonics work for future devices[21]. Swiss-based STMicroelectronics[22] offers a number of products and ICs for AR devices in order to achieve the best integration while offering

the right autonomy and accuracy. Key products include high-accuracy motion sensors, proximity sensors, ultra-low power, high performance microcontrollers, power management and wireless charging, as well as Bluetooth and NFC connectivity. Several Swiss companies are active in the field of virtual reality and AR, such as Virtual Tomato[23], Bandara[24], and Necio[25].

Immersive video

S T A R

According to DFAE's "House of Switzerland" website[26], Swiss start-ups are gaining increasing interest for the Virtual Reality industry. Several start-ups from EPFL and ZHdK are attracting attention from major AR/VR companies: Somniacs SA and its birdly product[27] or Artanim[28], Apelab[29]. The Swiss reference in this technology is Mindmaze, a one-billion USD start-up based in Lausanne that applies VR to medical field.

MACHINE TO MACHINE INTERACTIONS

Internet of things

S T A **R**

Switzerland hosts some of the early promoters and main driving companies of LoRa Alliance[30], an open, non-profit association that has grown to more than 500 members since its inception in March 2015. LoRa promotes the LoRaWAN, a Low Power, Wide Area (LPWA) networking protocol designed to wirelessly connect battery-operated 'things' to the internet in regional, national or global networks, but it also targets key Internet of Things (IoT) requirements such as bi-directional communication, end-to-end security, mobility and localization services. One of the major alliance members is the Swiss-based company Semtech[31]. Beside various academic research teams (EPFL, EPFZ, He-Arc[32], CSEM), many companies already provide services for Internet of Things along with smart services such as Axians[33], Ebeewan[34], Geboa[35], MTF[36].

Cloud Robotics

S T A R

ETHZ was part of the ECRP CTI project[37] - Enterprise Cloud Robotics Platform. It created Rapyuta Robotics[38], an ETH Zurich spinoff in 2014[39]. This start-up raised 9.5 million USD in 2018. It is one of the 11 world companies listed under "cloud robotics" Wikipedia's page.

Self-driving vehicles

S T **A** R

The STAR report dedicated to future mobility in Switzerland states that the country is on an advanced state for terrestrial autonomous vehicles and a trend state for aerial ones.

5G CONSTRAINTS AND CONCERNS

Geopolitical

S T A R

NATO believes that 5G in Huawei's hands is a threat. The United States and several other Western countries have excluded Huawei from bidding for ultra-fast 5G networks because of its close links with the Chinese government. If Huawei's technology were used by countries in their defence communications systems, the US military would no longer communicate with them, General Scaparrotti warned[40]. In telecommunications, the United States and China dominate the world. According to a report of the Montaigne Institute, Europe must develop its own network. This report presents all the risks associated with American and Chinese domination in communication networks[41]. The benefits of controlling 5G networks are not only measured in commercial terms, because controlling the physical layer (antennas, networks) effectively controls traffic and therefore the availability and confidentiality of data that flow over these networks[42]. Switzerland cannot currently provide alternatives to the dominant solutions of the major players in the telecommunications market. Nevertheless, Switzerland can benefit from its independence from security policy alliances that force some countries to take sides. The Swiss government must implement measures against cyber risks[43] but cannot influence private network operators in their choice of 5G technology provider. It is the operator's responsibility to guarantee telecommunication privacy and data protection.

Cyber Security

S T A R

The Switzerland's "National Strategy for the Protection of Switzerland against Cyber Risks 2018-2022[44]" outlines the need for experts in Cyber Security[45]. In March 2019, EPFL and ETHZ introduced a joint Master's degree in Cyber Security with the support of the federal government. This is Switzerland's first university-level degree program in this field despite the fact that EPFL has been investing in cyber security research for over ten years. A Deloitte study showed that, while the majority of internationally-oriented companies assess the risk of cyber threats as high, Swiss businesses oriented to the home market generally rate these threats as low[46]. The Swiss Army has a Cyber Defence branch[47] but unlike the French ANSSI[48] it doesn't help private companies. Switzerland counts multiple private Cybersecurity-related companies. One of them is ProtonMail[49], an end-to-end encrypted email service founded in 2014 at the CERN research facility. >>

Public perceptions

S T A R

Switzerland was among the first countries to begin deploying 5G, but health fears over radiation from the antennas that carry the next-generation mobile technology have sparked a nationwide concern[50]. Several cantons including Geneva, Vaud, Fribourg and Neuchâtel have buckled to pressure from online petitioners and put the construction of the 5G infrastructure on hold[51]. The Swiss press regularly publishes articles related to 5G-related issues[52, 53].

Public health risk

S T A R

In 2017, 4 Swiss scientists and doctors participated in a call for a moratorium on 5G roll-out, known as "The 5G appeal[54]". In April 2018, Switzerland decided to introduce a monitoring system to assuage concerns about the potential health impact of 5G emissions and smooth the cutting-edge technology's rollout[55]. Private initiatives try to deliver a reassuring message[56, 57]. Despite these measures, the country faces strong opposition from various groups[58, 59]. In 2019, an online petition against 5G was signed by more than 42'000 citizens[60].

Technical & legal limits

S T A R

Due to the lack of a national network hardware producer, Switzerland relies on foreign providers and commercially available technologies. The 700 MHz bands (allowing building penetration) have been acquired by three operators (Swisscom: 3, Salt: 2 and Sunrise: 1), creating a disbalanced offer for quality "in-house" networks[61]. The Swiss topology is a real challenge for a global 5G coverage. The government (ComCom) requires 50% of population coverage by each operator, leading to 5G blind spots in the less populated areas. Another technical limitation on the 5G deployment in Switzerland is the Non-Ionising Radiation Ordinance (ORNI)[62], that sets a limit ten times stricter than in the European Union[63], a value already reached by previously existing networks in the most populated areas. A task force comprising representatives from several federal departments, cantons, operators and the health sector, was set up in 2018 in order to see if and how to change the legislation.

BEYOND 5G

Quantum Communications

S T A R

Switzerland is very well positioned in the field of quantum technology. The Swiss National Science Foundation has supported quantum science and technology since the field started to take off around the year 2000[64]. The National Centre of Competence in 'Quantum Science and Technology Research' (NCCR QSIT) consists of 32 research groups from different institutions located in all over Switzerland. Swiss company ID Quantique (IDQ) is the world leader in quantum-safe crypto solutions, designed to protect data for the long-term future. The company provides quantum-safe network encryption, secure quantum key generation and quantum key distribution solutions as well as services to the financial industry, enterprises and government organisations globally[65].

Conclusions

Switzerland's strengths	Switzerland's weaknesses
• Sensor industry is mature and well-developed. • Sensors miniaturization and integration. • At the forefront of holographic development. • The country is "IoT-ready". • Key player in quantum communications.	• Very restrictive network legislation. • No native network hardware provider
Opportunities	**Threats**
• Emerging start-ups in immersive video. • Active academics in cloud robotics and telepresence. • Advanced in autonomous vehicles.	• Cybersecurity and hacking • Strong public resistance toward 5G

You'll find on the next page the list of the links included in the article >

List of links included in the article

1. https://www.we-secure.ch/product-category/robotics/double-robotics/
2. https://www.20min.ch/ro/multimedia/stories/story/La-telepresence-passe-en-toute-discretion-31313510
3. https://infoscience.epfl.ch/record/168292?ln=fr
4. https://cgl.ethz.ch/research/telepresence/
5. https://www.forbes.com/sites/andrewcave/2017/09/26/how-switzerland-became-the-silicon-valley-of-robotics/#71d-da27d200d
6. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/150830/eth-31064-01.pdf;jsessionid=EB2C8CA56B-5C14A59BD5EF6588ABFF3E?
7. https://hypervisual.ch/
8. https://wayray.com
9. https://amethys3d.com/en/holographic-display/
10. http://www.olomax.com/
11. https://actu.epfl.ch/news/curved-holographic-combiner-for-color-head-worn-di/
12. https://www.sensirion.com/en/about-us/newsroom/sensirion-specialist-articles/ultra-small-humidity-sensors-for-consu-mer-electronics/
13. https://www.empa.ch/web/s401/selected-projects
14. https://actu.epfl.ch/news/une-fibre-inedite-pour-des-textiles-intelligents/
15. https://lmts.epfl.ch/lmts-research/enviromems/page-129698-en-html/
16. https://www.designnews.com/electronics-test/wearable-semiconductor-cloth-eyed-new-designs-smart-clo-thing/200209251159586
17. https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/13843/eth-30914-02.pdf
18. https://www.csem.ch/Doc.aspx?id=39052
19. https://www.st.com/en/applications/wearable/sports-equipment.html
20. https://www.arcinfo.ch/articles/regions/canton/les-dernieres-nees-121035
21. https://www.letemps.ch/economie/startup-magic-leap-installe-un-centre-recherche-lausanne
22. https://www.st.com/en/applications/virtual-augmented-reality/ar-headset-and-glasses.html
23. https://virtual-reality-app.ch/fr/
24. https://www.bandara.ch/
25. https://www.necio.ch/necioar/
26. https://www.houseofswitzerland.org/fr/swissstories/science-education/la-touche-suisse-dans-la-realite-virtuelle
27. https://www.somniacs.co/
28. http://artanim.ch/
29. https://www.apelab.io/
30. https://lora-alliance.org/
31. http://www.semtech.com/
32. http://projets.he-arc.ch/stemys-io/
33. https://www.axians.ch/fr/portfolio/internet-of-things/
34. https://ebeewan.com/
35. https://www.geboa.com/
36. https://www.mtf.ch/fr/solutions/numerisation/
37. https://www.zhaw.ch/no_cache/en/research/research-database/project-detailview/projektid/1572/
38. https://www.rapyuta-robotics.com/
39. https://www.startup.ch/index.cfm?page=129367&profil_id=13147
40. https://www.bilan.ch/economie/lotan-estime-que-la-5g-entre-les-mains-dhuawei-est-une-menace
41. https://www.institutmontaigne.org/ressources/pdfs/publications/leurope-et-la-5g-le-cas-huawei-partie-2.pdf
42. https://omc.ceis.eu/la-5g-enjeux-politiques-et-strategiques-dune-revolution-technologique/
43. https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051

44. https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
45. https://actu.epfl.ch/news/l-epfl-et-l-epfz-lancent-un-master-conjoint-en-c-2/
46. https://www2.deloitte.com/content/dam/Deloitte/ch/Documents/audit/ch-en-audit-advisory-cyber-security-in-switzerland-08052014.pdf
47. https://www.vtg.admin.ch/fr/actualite/themes/cyberdefence.html
48. https://www.ssi.gouv.fr/
49. https://protonmail.com/fr/
50. https://news.yahoo.com/health-fears-prompt-swiss-5g-revolt-050428328.html
51. https://www.avenir-suisse.ch/fr/5g-le-danger-de-signaux-contradictoires/
52. https://www.swissinfo.ch/fre/bonnes-ou-mauvaises-ondes-_la-suisse--%C3%AElot-de-r%C3%A9sistance-%C3%A0-la-5g/44939236
53. https://www.illustre.ch/magazine/5g-sentons-cobayes?utm_source=facebook&fbclid=IwAR1kXKK1yWBDKoaZRVOQB7gR-vC8o-1a3GyVbQHJPyPkAzzpl73iKYtaiA6Q..
54. http://www.5gappeal.eu/signatories-to-scientists-5g-appeal/
55. https://www.reuters.com/article/us-swiss-5g/switzerland-to-monitor-potential-health-risks-posed-by-5g-networks-idUSKCN1RT159
56. https://asut.ch/asut/media/id/1621/type/document/asut_Faktenblatt_Mobilfunktechnologie5G_Gesundheit_A4_FR.pdf
57. https://itis.swiss/customized-research/exp-eval/5g-safety-evaluation/
58. http://www.pierredubochet.ch/appel-international-contre-la-5g.html
59. https://www.alerte.ch/images/stories/documents/normes/Document_general_fascicule_ARA_427%20pages.pdf
60. https://www.letemps.ch/economie/5g-sante-dix-points-comprendre
61. https://www.letemps.ch/economie/voici-5g-se-deploiera-suisse
62. https://www.admin.ch/opc/fr/classified-compilation/19996141/201906010000/814.710.pdf
63. https://www.letemps.ch/economie/voici-5g-se-deploiera-suisse
64. https://www.swiss-quantum.ch/SwissQuantum.pdf
65. https://www.idquantique.com/

Communication

INTRODUCTION

Imagine a bank robbery with a hostage-taking situation. The doors of the bank are barricaded, surveillance cameras destroyed, and every hostage has to hand over their mobile phone. Then, the bank robbers shut down all communication systems. In consequence, the criminals can establish a telephone connection to the outside world at their discretion. The police have lost the power to communicate with the bank robbers about a possible liberation of hostages. For the police there are only two options for action: waiting or risking casualties or resolving the situation with firepower. Apparently, loss of communication makes actors powerless and dysfunctional.

Communication Networks: Urban operations are highly dependent on working communication systems
Source: IABG

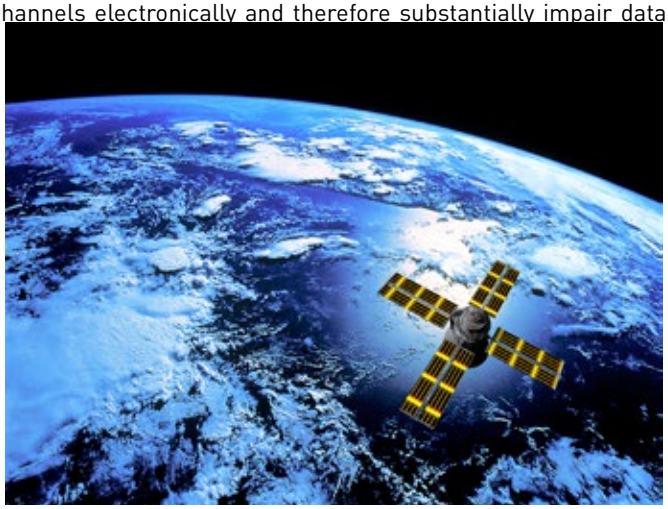
Today's world is highly dependent on communication systems. Especially in urban areas, people, infrastructures and public life rely heavily on communication. The same is true for military operations. If communication systems collapse, soldiers can only act on behalf of what they actually see and what the plan envisaged. This is quite dangerous, since there is no situational awareness of the wider surroundings and it cannot be confirmed that the operational plan is still in place. Particularly in urban operations communication is vital to survival. The complex nature of urban missions makes reconnaissance difficult. In the three-dimensional urban geography, technical advantages are not as relevant as on other battlefields and asymmetric actors can easily change places. Moreover, communication in urban areas is highly complex, since radio signals can be impaired by dense structures like massive and high buildings as well as by numerous electronic devices.

CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Vulnerability of communication

Communication can be disrupted. There are several possibilities to do that. First, radio signals can be impaired by dense structures, interfering transmitters or by the rapid movements of senders. Besides that, undersea cables can be cut or damaged either by malicious damage or natural hazard. The same is true for the destruction of contact wires of signal stations. Especially symmetrical actors – but also asymmetrical ones such as criminal or terrorist groups – are capable of disrupting communication channels electronically and therefore substantially impair data transmission.

Secondly, communication devices can be non-functional or destroyed. Moreover, communication devices can turn out technically inadequate for new theatres of war. To maintain stable and secure tactical communication in and between the multiple dimensions of urban areas is a challenging technological task. Due to urban structures, interference from numerous electronic devices and power constraints of human-portable radio wireless communications are significantly degraded. This is especially true for signal frequencies of about 100 MHz, which can lead to delayed reaction and double reception, becoming emergent for communication at brigade level and below. Besides that, new weapon systems, like Directed Energy Weapons, can cause damages on communication devices and signal transmitter. If an enemy attack was successful, soldiers can be isolated from their bases.



Satellite Dependency: Space forces can disrupt digital communication
Source: IABG

Thirdly, it is possible to intercept and manipulate communication. During the Second World War, British Y-stations (signal intelligence) intercepted German signals and decoded them with a special decoding device called "Enigma". Because of this decoded information, the allies had huge strategic advantages. Apart from intercepting signals, manipulation plays a major role in military operations. Especially in this highly interconnected world, the true origin of communication signals can be obfuscated. In help of new technologies, an incoming message of a friend can actually be a message of the foe, who has used signal technic to delude the origin.

In a future theatre of war, it is also thinkable that hostile space forces or DEWs will be able to destroy communication satellites. Private contractors already have a massive impact on space traffic and will continue to expand their influence.

Communication and technology

In times of digitalization, man-machine-communication will become increasingly important. Thus, besides communication between military actors, the interaction between humans and machines gains importance. Men-machine-connection is defined as the creation of meaning between humans and machines, with technology being understood as a communicator, a subject with which people communicate, instead of a channel through which humans interact with one another. In man-machine-systems, humans take the role of the operator and machines handle processing tasks. Capabilities which were formally reserved for humans (e. g., evaluation of options, analysing the situational picture) can now be taken on by machines with AI features. Moreover, people with handicaps can rely on exoskeletons, a mobile machine that allows the limb movements with increased strength and endurance. In order to profit from this new connection, complexities in the communication between men and machines have to stay within justifiable limits. Hence, to use man-machine communication successfully, user-friendly cooperative interfaces have to be developed as well as interfaces which account for human sensory, motor skills and cognitive capabilities. Examples of man-machine communication can be found in all different kinds of industries like electronics, entertainment, military or the medical sector. Using mobile phones, laptops or simply regulating temperature of the heating system, most of today's world is based on man-machine-communication.

Besides man-machine communication, "machine to machine" (M2M) communication gains importance in both the civilian and military sector. M2M is the direct communication between devices using communication channels, including wired and wireless – for instance, a self-refilling fridge ordering food if necessary, or sensors which communicate recorded information to an application software.

All in all, the communication between man-machine and machine-machine brings many advantages. Soldiers do not have to be on battlefields to monitor a situation, they can also sit in a safe command centre and control a surveillance drone. Especially in urban warfare scenarios, communication between men and machines can facilitate surveillance. This reduces vulnerabilities of armies and extends the possibilities without risking casualties. Thus, communication with machines or between machines can increase effectiveness, efficiency as well as performances in civil sectors as well as in the military. Nevertheless, it has to be kept in mind that new standards about decision-making competences and the handling of poor decision making in regard to men-machine and machine-machine communication have to be developed.

Integrated operation command

In times of diverse and variable threat scenarios of the 21st century, agility is important in order to react appropriately in any situation. In this regard, integrated systems are reaching their limits. One solution is a network-based approach of operation command. This includes the development of joined networks of single systems to transfer information. The challenge of the future will be to integrate different communication systems into a unified whole. If this can be implemented successfully, a system of systems approach enables synergetic effects and increases flexibility and adaptability. By transferring results of the communication between systems to a network which can be accessed by all involved entities a whole system approach can be developed. Besides the communication between systems, the communication between domains need to be enhanced. Sensors, commands and effectors have to be part of one single network. Different domains must be included in this network and have to coordinate their communication. If this domain-overlapping communication is successful, a common operational picture is the result.

A network operation command approach strengthens the communication with allies. This includes the harmonization of technical and operational aspects of network centric warfare and operations. For example, NATO's interoperability standards and profiles provide guidance to support joint missions. Generating joint situational awareness pictures brings along many benefits at all operational levels and minimalizes the possibility of friendly fire. In order to use connected communication systems and in order to improve communication between different domains and security concepts have to be developed. Integrity, accessibility and confidentiality of those communication systems has to be guaranteed.

IMPLICATIONS FOR THE MILITARY

Men-machine interaction

Since man-machine interaction is evolving, the military has to adapt to new circumstances and challenges. In order to communicate with machines, military personal has to be educated and trained. Therefore, highly specialized person-

nel has to be recruited. Besides that, it is important to recruit personal which can supervise communication systems between machines. Since, cyberattacks and manipulation of machines can occur, soldiers need to be educated in identifying changes in communication with machines. If an attack remains unrecognized, the communication can be target of manipulation which could lead to severe damages and casualties. If an attack is observed, soldiers should have the ability to develop solutions to defend the communication systems in order to secure a safe man-machine interaction. Fast-evolving technological innovations results in changing man-machine interaction. Therefore, armies should think of hiring development specialist to design communication surfaces which facilitates the operability.

Besides recruiting highly skilled personnel, rules, laws and ethical standards have to be considered. One example is a soldier who wears an exoskeleton which can shoot automatically in case of a threat. Who is responsible for killing this person? To answer those relevant questions, it is important to develop general rules, regulations and ethical guidelines. If it were possible to replace all human soldiers by machines, how could a state advocate a single death of a soldier? Why deploy vulnerable soldiers if a machine could do the same job? And what are tasks and decisions only human beings can decide? Not only is it important to develop those laws to have a code of conduct, but moreover to justify further developments to the society as well as to the members of the army.

Communication devices

Because some wars will evolve in an asymmetric manner, future theatres of war will be highly complex. Therefore, communication was and will be of great significance for any operation. Especially in war areas such as deserts, urban areas or outer space, communication is key to guarantee situational awareness. Line-of-sight problems and transmission and reception problems caused by fading and path loss pose challenges that need to be solved. Material of transmitters, satellite phones and radio devices must be adjusted to new theatres of war (e. g., high temperature, disruption or interference issues). Modern devices, especially man-portable radios, have to ensure an outstanding performance, long lifespans and full interoperability.

The concept of supply and demand has to be the basis of decision-making for the use of communication devices. The more information is claimed on different communication channels, the more information must be provided via these channels. Additionally, communication channels need to be kept stably open and secured. Hence, it needs to be evaluated how demand for information and the use of communication channels can be minimised.

Furthermore, a modular structure of communication systems can help to avoid total system breakdowns. Networks of systems need to function alone as well as in a network connection to be on alert. For communication issues, different physical data transmission processes should be used for the purpose to maintain the lines of communications if an attack of one transmission system occurs. Moreover, future technologies should be critically reviewed and procured if it can develop other ways of communication. For example, scientists of the University of Washington claim that they developed a way to communicate via a BrainNet system, a brain-to-brain network. Today, scientists use interconnected head gears to communicate via brain-to-brain communication. Hypothetically spoken, at some point in time BrainNet systems could be deployed without using interconnected head gears, so that future soldiers will communicate by thinking about something and another soldier or commander can receive those signals. This could be especially helpful in new warfare terrains, which are highly complex and in which conventional communication devices reach a limit.

CONCLUSION

Without communication, life as we know it would stop to exist. Ultimately, as the world is dysfunctional without communication, it is of special significance to secure communication systems. Therefore, both the state and its military must rethink their communication concepts, their own capabilities and their procurement politics as well. To counter future threats, the vulnerability of communication devices must be critically reviewed. Besides that, developments like men-machine interference has to be considered by personal planning as well as in regard to ethical questions. Moreover, domain overarching communication has to be deepened, should be structured in a modular sense and should use different kinds of communication transmitter techniques. In the future, new communication techniques will evolve – their military impact should be evaluated today.

SWOT-ANALYSIS for swiss military planners

Strengths • Operational agility • Several Awareness pictures • More intelligence for fewer resources	**Weaknesses** • High costs of new materials • High training costs of new personal • Development of rules and ethical standards
Opportunities • Decrease of casualties • Facilitation of communication between allies	**Threats** • High destructive impact • Target of manipulation

HIGH LIGHTS
THE DEFTECH PUBLICATION
ABOUT FORESIGHT IN DEFENCE

URBANITY

Force-Effect

Artificial Intelligence, drones, deep fakes, hacking, 3D printing, Internet of Things, social media, etc. the list is not exhaustive, but all these technologies, developed and mastered in the industry will play an important role in the future technology landscape of the armed forces. More than an opportunity, dual-use technology has become a strategy. In parallel, hypersonic and space-based weapons present disruptive and new dissuasive military capabilities. Innovation and creativity will more than ever affect the military landscape. How will the opportunities they represent in the civil society compensate for the threats they pose in defence and security?

The warring worlds of science fiction

Arms and the man

Science-fiction, as we have been able to determine in the previous texts, is a narrative technique that exploits motifs established by the techno-scientific world and, in order to transform them into images – into metaphors – that enable one to grasp the changes undergone by the human condition in a world informed by scientific and technological utopias. The robot evokes our tendencies to instrumentalise and to be instrumentalised (cf. the film *Ex Machina* by Garland, released in 2015); the cyborg, our dependencies upon technology (which is the subject of the excellent novel *Neuromancer* by William Gibson, published in 1984); artificial intelligence, our desires to quit our bodies to evolve freely in virtual networks (is this not what the film *Her* by Spike Jonze says to us, which was released in 2013?). In this sense, la science fiction can reasonably be compared to a "sounding board" which demonstrates, through the twists and turns of the narrative, just how far our techno-scientific utopias, far from being solely representations of an imaginary future, profoundly modify our mode of existence in the world: reading science fiction novels or watching futuristic films consequently enables the deciphering – so long as we do not interpret them at the first level – of what we have become, or what we are in the process of becoming, in a techno-capitalist world.

I would like to conclude this tour, by reflecting, briefly, on one of the motifs that runs through the history of the science fiction genre – that appeared at the end of the 19th century, from the pen of the English writer Herbert George Wells –, and which one can readily comprehend by bearing in mind that the technological society, other than the profound changes it has had to undergo in the West (industrialisation, public health, etc.), has also led to the unprecedented development of technological armaments of devastating power. While science fiction incorporates such arms in its narratives, it is not so much for the purpose of some kind of apologia for them or in order to criticise them naively, but more to express, symbolically, the underlying values of our society and the effects that these values produce for human beings. For example, while the Martians in *The War of the Worlds* (H.G. Wells, 1898) invade earth on tripods equipped with luminous rays destroying everything in their path this is above all a literary artifice to sketch out a paradox: the Martians have a powerful technology, but they are also very fragile because they had to leave their dying plant to colonise the solar system (Earth first of all, then Venus, in the novel's epilogue). This paradox, in a way that is more interesting than the tripods or the death rays, enables Wells to construct a questioning of Victorian Society, proud of its technical power, but fragile, because it has to draw upon the resources of other continents. In other words, the Martians' armaments are above all to be considered as a fictional exaggeration, highlighting the weakness of all colonising peoples: they are without question endowed with incredible firepower, but they need to be "nourished" elsewhere in order to avoid decline. This example, which I cannot unfortunately develop here further, is sufficiently significant to help us to understand how science fiction generally relates to arms and military artefacts: it only calls upon them to place them in relation to other elements, by this same token, inducing a reflection that encompasses the question of the armament in a wider consideration. One could thus find many examples, and find, always somewhat differently, what has just been postulated; the main thing, in my opinion, lies in the need to read the texts other than as futurological fictions, and to discover in them a particular "reading" of our identity and a singular "interpretation" of the bases upon which the society in which we live has been constructed.

This is why – another example that is closer to home, and certainly more eloquent – science fiction, since the end of the 1940s has sought to represent the nuclear threat in its novels: the bombs are bigger, and the levels of destruction correspondingly more extreme. It is clear that this exaggeration is merely a device with which to highlight other elements, to place the accent on other values: the arms race – responsible for the proliferation of arms and their refinement – enables, in particular a consideration of the damaging imperialism of a Western civilisation that evaluates itself only in terms of performance, even if this means eternally committing the same mistakes, given its incapability of seeing any other way of constructing a society (see *A Canticle for Leibowitz* by Walter M. Miller, published in 1961); or the blinding of a humanity that only congratulates itself in terms of superlatives and which, by so doing, has lost its soul (I am thinking in this case of the novel Dark Universe by Daniel F. Galouye, which was published in 1961). As for the detective robots in *Fahrenheit 451* (Ray Bradbury, 1953), these symbolise the imperative of surveillance, which seems inevitably to accompany modern powers. Contemporary narratives are not to be outdone, although the nuclear bomb has given way to other arms, and by extension, to other criticisms: the child soldiers in *Ender's Game* (Orson Scott Card, 1985), for example, play with new armaments – this time digital weapons, but the reader understands

that while these children became soldiers, in other words compliant beings, it is the video game and computer simulations that are in fact "tools" constructing reality and modifying it, particularly when operated blind ...

One might believe, in reading the above, that science fiction is technophobic; however, this is far from being the case (it would be strange to write a novel involving the sciences and technologies in order to convey some kind of technophobia). On the other hand, it is critical, and, above all, it invites us to think that which has not yet be thought, or, more precisely, to think that which habitually one does not think, in other words, the correlations can be woven around motifs such as armaments and other elements, the one elucidating the other. Humanity has always constructed arms – to defend itself, to conquer –, but these arms are only a reflection of values of civilisation, the indices of our utopias. And this is why science fiction should not, as is the case for any artistic discourse, allow itself to be limited by the alleged transparency of reality: arms are not, firstly, signs of our warlike impulses, but the signs of values upon which we construct ourselves. It is furthermore certainly because authors think – perhaps rightly? – that humanity has a greater chance of constructing itself other than by bellicose means, that they are so critical – even ironic (cf. the film Mars Attacks! By Tim Burton, released in 1996) – in the face of the unprecedented development of the military industry. There is lots of fighting in science fiction, but the battle is above all against the harmful tendencies that alienate us and enclose us in self-destructive or paradoxical rationales.

Conclusion

At the conclusion of this tour structured around a number of motifs, it seems to me important to emphasis what I have sought to set out here: science fiction incessantly dialogues with our world, and seeks, through this dialogue, to offer us different perspectives of this same world. We are, in effect, and this is quite normal, incapable of thinking and reflecting about everything; our lives are taxing enough in themselves. In a democracy, it is imperative that we can position ourselves in that which surround us, and in respect of the choices we make, without which, our votes, for example, are empty of substance and are only evidence of the parties we uncritically follow. Science fiction, like all forms of fiction, is an opportunity, because it suggests that we should stop, inviting us to consider our identity, the forces that pull at us, and to reflect at two levels: who are we in this techno-capitalist world? Are we as free as we think? How are technologies – or the sciences – modelling us, changing us, and alienating us? These questions, which are seemingly complex, must necessarily be asked if we wish to remain master of our decisions and of our humanity; is it not this that we have incidentally chosen when we left the darkness of feudalism to enter into the light of democracy? Let us hope so, and science fiction has been setting out this hope for over a hundred years, that this enlightenment will prefer the rich nuances of potential transformers of an imperfect society to the reductive glitter of a utopic future...

Shadows of Utopia: Threats & Vulnerabilities of Tomorrow's Tech

Paul Virilio posed a bleak, but crucial insight into the unintended consequences of technology: "When you invent the ship, you invent the shipwreck; when you invent the plane you invent the plane crash; and when you invent electricity, you invent electrocution... Every technology carries its own negativity, which is invented at the same time as technical progress."

The research labs of universities and corporations aren't seeking catastrophe, but sometimes they find it anyway. Such risks are inherent in benign applications — when researchers created the World Wide Web to share physics research in 1989, they could not have anticipated its role in spreading disinformation on a mass scale by 2019. Emergent technologies cast a shadow from their ideal purpose, creating new risks and vulnerabilities.

These risks include the design of new forms of weaponry, but physical warfare is far from the only security threat posed by tech such as AI, drones, and autonomous vehicles. In the future, cyberwarfare looms large, as entire cities can be attacked from an anonymous computer thousands of miles away, its location and motives obscured. From terrorism to cybercriminals, the threats of tomorrow require an awareness of vulnerabilities — and an investment in solutions. Technologies do not evolve in a vacuum, and each threat could spark new, innovative approaches to contain them.

We begin by looking at the role of artificial intelligence as it drives autonomous weapons, but also explore possible roles for machine learning in the prevention of armed conflict. We will look at potential future risks of social media, and how companies and researchers are working to minimize them. Finally, from smart grids to smart cities, how might technologies such as edge computing, 5G, and IoT create new security challenges?

Artificial Intelligence: From the Database to the Battlefield?

Dystopian scenarios about AI abound, from the sentient AI that takes over human weapons systems, to the controversies surrounding the use of unmanned — and possibly, computer-piloted — drones. Artificial Intelligence in warfare[1], such as the automation of smart weapons which can work together autonomously, could minimize human casualties for those who deploy them, but widespread innovation over traditional weaponry presents unprecedented strategic challenges[2].

The Blowfish A3, a new helicopter drone equipped with a light machine gun. Photo: Courtesy of Ziyan UAV

Reported projects for autonomous weapons systems include a UK drone project[3]; Russia's autonomous tanks with drone scouts[4]; the US Navy's unmanned battleships[5]; China's Blowfish A3 "swarming" drones[6] equipped with machine guns — all from countries working to create global guidelines[7] to limit the capacity of autonomous weaponry. China's initiatives in AI have pushed an "integrated development[8]" strategy with defence, building cooperative agreements with research labs and industry partners. In the US, employees have created constraints on the viability of such public-military partnerships — as in 2018, when Google ended a partnership[9] with the defense department to create video-identification software that could be used in drone strikes. But tech giants may not be required to weaponize new technologies: a $35 device[10] installed onto a $25 drone can run an AI capable of outmanoeuvring top US Air Force pilots. Meanwhile, machine learning development has shown the technique is capable of creating novel solutions to problems[11] which may evade the imagination of those who give it orders. Novelty and surprise on a battlefield threaten lives of soldiers and civilians. It also undermines the strategy of military command, who operate on the assumption that machines will follow orders, rather than creatively circumvent[12] them without regards to arching strategy — or human rights.

While battlefield deployments of AI could be constrained by objections from engineers and employees with the expertise to develop them, such a constraint may lead to more investment in less controversial military uses of machine learning, such as intelligence analysis. If so, the most powerful use of artificial intelligence on the horizon may not

be in the conflict zone, but on the desktop computers of strategists and diplomats. For example, a project from US Defense Agency DARPA, KAIROS[13], aims to create schemas of events on a geopolitical scale. It has eyed AI as a way to empower deeper analysis of increasingly complex events, and to predict possible scenarios and test effective response strategies. The ramifications of a project would allow military strategists to take in real-world data and recalculate an opponent's possible strategies in real time. But such a machine could also be a kind of prediction engine for diplomacy, being used to understand not only how to engage in armed conflict, but how best to avoid it.

To that end, a 2017 paper[14] from Chinese researchers suggested that a machine learning algorithm trained to analyze events in the Global Terrorism Database was able to predict attacks with 78% accuracy. That same year, American researchers were able to expand the training data to include patterns in social media activity[15], claiming to increase the prediction rate to 90%. This builds on decades of linguistics research[16]showing that terrorist social media activity tends to reflect less complexity as groups move closer to attacks. Other researchers have been far more sceptical, suggesting that the AI's results point to 100,000 false positives[17] for every successfully predicted attack. This raises concerns for civil liberties and does not allow full commitment to what the machine might flag.

Nonetheless, researchers in machine learning and social science are developing data collection practices[18] to further refine the prediction of conflict. Tactics include media analysis of newspaper reports, but acknowledge the limited frameworks for understanding the outbreak of conflict. Social and political realities may be hidden, obscuring the most crucial data required for conflict prediction. Machine learning research at the Virginia Military Institute, applied to massive databases centred on conflict, has been able to identify certain correlations of real-world data that help narrowly define conditions that spark violence. While these correlations may not prove to be predictive, they nonetheless resulted in 58 possible factors[19] where strong data could help refine future prediction models. These factors include variables such as past histories of conflict, GDP, and average education. Work on the conflict-prediction-model project is also being pursued at the Alan Turing Institute[20].

If conflicts could be predicted, could it lead to an AI declaring a "pre-emptive strike?" While such a policy discussion has yet to take place, the idea of an automated Doomsday Device[21] has been floated by researcher Herman Kahn at the outset of the Cold War, under the belief that mutually assured destruction would prevent the launch of a nuclear attack. The idea of leveraging autonomous AI systems to assess a doomsday situation and respond appropriately, without human intervention, was recently proposed[22] by researchers from Louisiana Tech and the Virginia Military Academy. But think tanks such as RAND have reacted with grave predictions that such moves could escalate the risk of nuclear war[23].

A bold research report anticipating AI vulnerabilities, and malicious use, was published in 2018[24], but advances in machine learning are moving quickly. Key threats for Artificial Intelligence systems are at the risk of manipulation — machine learning algorithms, which are at the heart of AI systems, require training data. As machines generate predictions, these models can be checked against real-world data to verify that the model is working correctly. The input of data also inserts vulnerabilities: a machine can learn on bad data, causing it to make bad decisions. Additionally, training data can be so complex that it can't be fully inspected by humans.

Researchers at MIT / CSAIL printed a toy turtle, pictured, that would be consistently be recognized as a rifle by artificial intelligence visualization systems. Such efforts could someday be used to deceive algorithms developed to predict armed conflicts

But if a model for pattern prediction was known to another AI, that AI could find exploitable gaps, a technique known as "adversarial machine learning." In 2017, Japanese researchers[25] were able to change just a single pixel in an image to radically transform what the AI "saw" in 74% of cases: for example, an image of a Stealth bomber was interpreted as a dog. MIT researchers 3D-printed a toy turtle[26] that was consistently interpreted as a rifle by Google's neural net for image detection; the researchers suggested that such techniques could be used in reverse, that is, to create weapons that would be undetectable as weapons.

Reverse-engineered data could also be manipulated to create certain outcomes or deliberately "trick" an AI into a specific interpretation — a kind of data camouflage that could be achieved through false reports, consistent leaks of fake or corrupt data, and even simple, physical camouflage of activities designed to confuse or trick data surveillance — for example, using a bot network to mimic heavy communication traffic to a strategically meaningless location could "train" an AI to include that location in its analysis.

Social Media: From Screens to the Streets

A dystopian scenario: Homemade bombs detonate at a climate change protest, simultaneous detonations injuring hundreds. Investigators discover that the "organizers" of the protest were in fact a series of fake accounts, with content generated by an AI under the control of a single user. An anti-climate-science terrorist scheduled "Facebook events" to bring passionate climate change activists to a single location — the site of the "fake protests" the terrorist had organized online, effectively bringing his victims to the detonations.

Though this scenario is a harrowing fiction, are such attacks possible? Using social networks to spread misinformation has been escalating, from spreading misinformation online to the real-world mobilization of activists. When Facebook shut down 32 pages for being "inauthentic operators," in 2018, the accounts were associated with a series of "events" with thousands of real-life activists[27] signed up to attend. These events were designed to protest white supremacist groups, and the attendees were verified as local activists, but the events were created and amplified by foreign agents. In 2017, Facebook announced[28] that a 2016 protest of an Islamic Center in Texas had been organized by an account associated with Russia's propaganda arm — and so had the counter-protest. The incentive seemed to be to bring hostile factions together, sewing division and possibly violence. The Facebook event, which lead to a confrontation of hundreds of protesters in Texas, cost only $200. A year later, a similar protest in Charlottesville, North Carolina, ended with the death of an activist[29].

An image from the scene of a 2016 protest of an Islamic Center in Texas, in which both protestors and counter-protestors had been organized by Russian agents using Facebook's "events" feature. Photo Jon Shapley, Houston Chronicle

Social media disinformation campaigns remain a knotty problem. The Department of Defense has called for software that can help it regulate online misinformation, with DARPA piloting a project[30] that could "unearth fakes hidden among more than 500,000 stories, photos, video and audio clips." This raises concerns[31] by activist groups over freedom of speech and political assembly. But detecting coordinated "bot" activity has become simpler, with dozens of security companies offering algorithms capable of tracking coordinated behaviour.

DeepFakes: From Boogeyman to Scapegoat?

It sounds like a story pulled from science fiction, rather than the headlines, but a recent series of events points to the dangers of hysteria over new technology.

Ali Bongo, the president of Gabon, had been receiving medical treatment abroad when public speculation about his health came full-pitch. After the Gabonese government released Bongo's New Year Address, a video in which the president spoke stiffly and awkwardly, speculation arose that the video was a deepfake — and that Bongo's face had been superimposed onto an actor, using artificial-intelligence tools. Political foes seized onto the theory that the video was faked by Bongo's party to conceal that he was gravely ill — or dead — to prevent an emergency election that could result in a shift of party control. The strangeness of the video was cited by the military in Gabon[32] as the driving

force for the nation's first coup in more than 50 years. Bongo appeared — alive, but ill — on a live television broadcast several months later, suggesting that the harm of a deepfake is not only what is shown in a video, but in empowering viewers to dismiss truth as fiction.

When evidence can be falsely discarded as "fake news," there is real harm to democratic discourse. But the evidence that misinformation campaigns are actually producing and deploying deepfake videos is scarce[33]. Software to detect deepfakes has already been deployed by companies such as Facebook[34]. Deepfake videos leave easily-detected digital fingerprints, which start-ups such as the Google-backed Deeptrace Labs[35] have used to detect the artefacts, glitches, and other details unique to AI-doctored videos. Meanwhile, teams from UC Berkeley and the University of Southern California have developed a digital forensic technique[36] that looks at how figures in a video move[37], which follow detectable patterns when generated by an AI.

Though creation and detection of these images and videos is like any other cat-and-mouse game, for now, the greatest threat of deepfake videos may be that they offer a scapegoat to deny the existence of damning visual evidence of wrongdoing, which itself is a powerful tool.

From Smart Fridges to Smart Bombs?
Smart Grids, which can allocate resources based on data about where they are needed most, could create efficient, clean energy networks, while also fuelling decisions for smart cities. But smart grids and cities require data: from generalities, such as peak use times, to specifics, such as which portable device is being charged in an outlet. Sophisticated machine learning models could inadvertently turn sensitive information gathered from electric grids into surveillance tools, including simple data such as whether a ratepayer is at home.

The largest single-site producers of energy would be institutions — those with large buildings or distributed real estate such as police, post, hospitals, or universities — whose data and energy would become powerful targets. Without careful attention to IoT security and regulation of the data these networks can collect, institutions could be vulnerable to both energy disruption and data theft through compromised elements of the smart grids.

These could be attacked remotely and without physical access to any power supply infrastructure through viruses or hacking attempts. A recent case in the US city of Baltimore[38] blocked utilities payments, among a host of other government services. San Francisco's public transit system was hacked in 2016[39], resulting in disruption of payment services — though the trains, which were not yet digitized, continued to function, highlighting one security benefit of analogue systems. Since then, ransomware attacks have only accelerated, with 40 attacks on municipal services[40] such as hospitals, police departments, courts, libraries, and schools in 2019.

These networked systems are exclusively for data and communication purposes today, granting access to records, files, and programs. The vulnerabilities of similar attacks on smart grids could create even more disruptive widespread service interruptions, such as black outs. With individualized recognition of objects and devices, they could also be used to target individuals. These problems — and their solutions — overlap with the risks inherent to the rise of interconnected devices, the so-called "Internet of Things."

The Internet of Things would link real-world objects into a communication grid, possibly yield enormous benefits, from self-driving cars that regulate their own traffic flow, to smart thermostats that operate seamlessly as consumers move from room to room. Communication across devices has security benefits, such as the ability to install security patches en masse. But the integration of data into everyday objects through RFID tags or similar tech presents strengths with shadows: patching all devices at once inevitably means that these devices share the same exploitable vulnerabilities. Data discovered or stolen by malicious actors could reveal weakest links in distribution chains, and simple physical attacks on a single device could be strategically implemented to affect entire networks.

For these reasons, IoT networks are a rich target for hackers. In the summer of 2019, researchers at Akamai cybersecurity reported an unidentified hacker claiming to be a 14-year-old boy had released a virus that wiped out 4,000 linked IoT devices[41] using default credentials installed by the manufacturer. More malware was discovered in 2018[42] after being dormant in routers for six years, which was capable of recording keystrokes and passwords. Nearly half of businesses who have deployed IoT systems have experienced breaches[43] as a result — and in the transportation sector, where supply chains and cargo shipments are targets, that number blossoms to 80%[44].

In March of 2019, the US Navy announced that compromised third-party vendors[45] were leaking information about military projects, in essence, collecting information about intellectual property from contractors in order to better understand the Navy's military production techniques and secrets. This kind of pattern recognition could escalate in an era of greater interconnectivity between devices, personnel, and supply chains as they move into coordinated, digital management systems through IoT.

From the personnel perspective, private data from fitness trackers[46] was used to identify the locations and layout of secret military bases in 2018 based on soldiers jogging while using Strava, a fitness app. As IoT becomes more ubiquitous, this kind of sensing of individual movements could be more localized and traceable for people and objects. With 28 billion devices[47] communicating with each other over insecure wireless networks by 2021 and 125 billion devices[48] by 2030, inadvertent data leaks on par with the Strava map are almost certain to be a headline in the next decade.

An image of a US military base in Afghanistan, as mapped by the fitness app Strava, which made global data about running routines public — inadvertently revealing the contours of running routes used in secret military bases across the world.

Already, Google's NEST devices have been compromised through simple methods for purely antisocial purposes; in one case a device was hijacked to repeatedly display pornography to a child[49] as a "prank." In 2019, Microsoft reported that hackers had accessed a corporate system through an office printer[50] and other benign devices, which was transmitting data from networked devices back to a Russian hacking group.

In worst case scenarios, vast numbers of interlinked devices could be hijacked based on a single vulnerability. IoT in electrical systems, heaters, or fire alarms could be tapped to create malfunctions that bring risk to life or property. These risks could be leveraged to create real-world "cyber-physical"[51] threats.

For example, just 42,000 networked water heaters could be hacked to create nationwide blackouts[52]. If an automatic door can be locked by an IoT device, it could be used to lock victims inside of a building or room before an attack, or create equipment failures that hinder first-responders. A nefarious actor would not need to disable a power plant during winter frosts if they could access smart heating systems en masse, and simply turn them off, as occurred in a small village in Finland in 2016[53].

Such crises may not even be the result of malicious actors. Simultaneous updates of devices in response to security threats could cause systems to require restarts or reboots, bringing critical services to a halt for the duration of the update. Likewise, glitches in one system can have widespread calamitous effects.

Nonetheless, security has been a low priority[54] as industry prioritizes convenience, adoption, and innovation. Solutions to this problem have been floated, including the widespread adoption of cryptographic tokens in IoT devices or security oversight by government agencies. California took a small step when it passed a bill[55] in 2018, set to take effect in 2020, that would require unique passwords for every device, reducing the possibility of using default settings from a single unconfigured device to access a network. The UK announced plans to implement security standards into "smart" devices in 2019[56], as has European Standards Commission ETSI[57]. But the standardization of security across nations, industries, and applications poses significant challenges.

Industry response to this security need includes third-party partitioning of IoT systems into smaller sub-networks, or micronets[58], which can limit the spread of malware or attacks through quarantines of linked devices. Promisingly, a Stanford-University of Illinois research study with Avast Software found that 90% of IoT devices came from 100 manufacturers[59], suggesting that regulation and standards could be simpler to implement than expected.

Beyond that, devices are always exploitable through human error — the threat to an entire network may be no further away than a disgruntled or careless employee. DARPA is developing an artificial intelligence to identify social engineering attacks, by creating digital "alter egos[60]" that can intervene and guide users through suspicious contacts, up to the point of identifying the attacker.

5G networks: An Imperfect Storm

Creating fast and reliable IoT networks is one of the justifications for the rollout of 5G networks, which would bring high-speed communication and sharing more data across existing IoT infrastructure. Whereas IoT is a broad interconnected system, 5G consists of the software and hardware these devices use to communicate. 5G networks, promising rapid speed and near real-time communication between devices, also carries risks.

In the US, two agencies — the space agency NASA, and weather agency NOAA — have expressed concern that so-called "mmWave" communications at the 24ghz frequency, like those recently auctioned to cell phone companies for 5G use, could impact weather forecasting. NOASS has suggested that 5G networks could set meteorology back nearly four decades, by interfering with the natural frequency of water dissolving in the atmosphere[61], which is tracked for activities such as hurricane forecasting.

From an information security standpoint, there is also the risk of data being compromised through backdoors in equipment, or the transmission of data through foreign networks. These concerns are at the heart of security concerns over Chinese technology firm Huawei, which the US and others contend is required, under Chinese law, to make data available by order of the government. But Huawei is not the only security issue at stake for 5G.

Other concerns include the widening of the stream of data, and corresponding increase in network activity and capacity, could make it even more difficult to discover irregularities such as cyberattacks through analysing network activity. However, unlike IoT more broadly, 5G is being driven by a handful of global vendors, centred on a product — smartphones — with heavy consumer demand for privacy. This seems to be spurring innovation in security measures in smartphones — for example, 29% of consumers[62] reported that they "expected" security protocols such as DNA authentication in a 5G cell phone. However, there are few incentives for private companies to invest in security, as the entire global network will only be as strong as the weakest player.

The vast speed and interconnectedness that results from the intersection of 5G and IoT technologies could spur the development of machine learning tools for cybersecurity[63], which would be capable of identifying threats and corresponding strategies to counteract them. But there is currently a skills shortage in AI, particularly AI focused on network security — there could be a shortfall of 1.8 million cybersecurity professionals[64] capable of working with AI by 2021.

What's Next?

Whether the future is full of dystopian moments, or utopian ones, will depend on how prepared we are for new technology. In an era where prosperity is increasingly networked and co-dependent, system failures can rapidly become global. Futures literacy — an understanding of coming changes, and a mindset of cautious deployment — is critical in ensuring that technological progress does not compromise public safety, democratic values, or human rights.

Today, investment into security from the private sector is relatively weak, as competitors jostle to be "first to market" rather than "last to be compromised." As discussed, there are few demands from consumers to drive safeguards in personal devices in IoT and 5G networks. In AI, challenges abound in the complexity of designing algorithms, creating a "black box" effect in which nobody understands the output of multiple algorithms working together, created by different teams, before they are deployed in the real world. As government intervention in industry — or the lack thereof — influences the development of these systems, we can envision a split not only of standards, but of ideological approaches and norms, compounded as systems are built upon systems. It is something of a paradox: a world which grows increasingly fractured, even as its systems become more interconnected.

List of links included in the article

1. https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12713
2. https://www.brookings.edu/research/ai-and-future-warfare/
3. https://www.theguardian.com/world/2018/nov/10/autonomous-drones-that-decide-who-they-kill-britain-funds-research
4. https://www.c4isrnet.com/unmanned/2019/03/04/russias-new-robot-is-a-combat-platform-with-drone-scouts/
5. https://www.defensenews.com/naval/2019/01/15/the-us-navy-moves-toward-unleashing-killer-robot-ships-on-the-worlds-oceans/
6. http://www.globaltimes.cn/content/1149168.shtml
7. https://time.com/5673240/china-killer-robots-weapons/
8. https://www.cfr.org/blog/civil-military-fusion-missing-link-between-chinas-technological-and-military-rise
9. https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html
10. https://www.newsweek.com/artificial-intelligence-raspberry-pi-pilot-ai-475291

11. https://blogs.icrc.org/law-and-policy/2018/08/29/im-possibility-meaningful-human-control-lethal-autonomous-weapon-systems/
12. https://www.wired.com/story/when-bots-teach-themselves-to-cheat/
13. https://www.darpa.mil/news-events/2019-01-04
14. https://ieeexplore.ieee.org/document/8078815
15. https://phys.org/news/2017-03-terrorist-behaviors-percent-accuracy.html
16. https://www.tandfonline.com/doi/abs/10.1080/17467586.2011.627932
17. https://firstmonday.org/ojs/index.php/fm/article/view/7126/6522
18. https://www.nature.com/articles/d41586-018-07026-4
19. http://visionofhumanity.org/economists-on-peace/predicting-civil-conflict-can-machine-learning-tell-us/
20. https://www.turing.ac.uk/research/research-projects/global-urban-analytics-resilient-defence
21. https://www.britannica.com/technology/doomsday-machine
22. https://warontherocks.com/2019/08/america-needs-a-dead-hand/
23. https://www.cnbc.com/2018/04/25/ai-could-lead-to-a-nuclear-war-by-2040-rand-corporation-warns.html
24. https://arxiv.org/pdf/1802.07228.pdf
25. https://www.bbc.com/news/technology-41845878
26. https://www.csail.mit.edu/news/fooling-neural-networks-w3d-printed-objects
27. https://www.washingtonpost.com/technology/2018/08/02/moment-when-facebooks-removal-alleged-russian-disinformation-became-free-speech-issue/
28. https://www.texastribune.org/2017/11/01/russian-facebook-page-organized-protest-texas-different-russian-page-l/
29. https://www.usatoday.com/story/news/2018/12/07/neo-nazi-convicted-murder-charlottesville-car-assault-killed-heather-heyer/2243848002/
30. https://news.yahoo.com/u-unleashes-military-fight-fake-134326896.html
31. https://www.commondreams.org/newswire/2019/06/12/social-media-platforms-increase-transparency-about-content-removal-requests-many
32. https://www.motherjones.com/politics/2019/03/deepfake-gabon-ali-bongo/
33. https://www.theverge.com/2019/3/5/18251736/deepfake-propaganda-misinformation-troll-video-hoax
34. https://newsroom.fb.com/news/2018/09/expanding-fact-checking/
35. https://www.deeptracelabs.com/
36. http://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf
37. https://www.technologyreview.com/s/613846/a-new-deepfake-detection-tool-should-keep-world-leaders-safefor-now/
38. https://www.baltimoresun.com/news/maryland/politics/bs-md-ci-it-outage-20190507-story.html
39. https://www.wired.com/2016/11/sfs-transit-hack-couldve-way-worse-cities-must-prepare/
40. https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html
41. https://blogs.akamai.com/sitr/2019/06/sirt-advisory-silexbot-bricking-systems-with-known-default-login-credentials.html
42. https://arstechnica.com/information-technology/2018/03/potent-malware-that-hid-for-six-years-spread-through-routers/
43. https://www.businesswire.com/news/home/20170601006165/en/Survey-U.S.-Firms-Internet-Things-Hit-Security
44. https://go.irdeto.com/connected-industries-cybersecurity-survey-report/
45. https://www.wsj.com/articles/navy-industry-partners-are-under-cyber-siege-review-asserts-11552415553?ns=prod/accounts-wsj
46. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
47. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5087432/
48. https://technology.ihs.com/596542/number-of-connected-iot-devices-will-surge-to-125-billion-by-2030-ihs-markit-says
49. https://www.washingtonpost.com/technology/2019/04/23/how-nest-designed-keep-intruders-out-peoples-homes-effectively-allowed-hackers-get/
50. https://arstechnica.com/information-technology/2019/08/microsoft-catches-russian-state-hackers-using-iot-devices-to-breach-networks/
51. https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8228.pdf
52. https://www.wired.com/story/water-heaters-power-grid-hack-blackout/
53. https://www.forbes.com/sites/leemathews/2016/11/07/ddos-attack-leaves-finnish-apartments-without-heat/#44bb1e5d1a09
54. https://www.wired.com/story/iot-security-next-step/
55. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327
56. https://www.gov.uk/government/news/plans-announced-to-introduce-new-laws-for-internet-connected-devices
57. https://www.etsi.org/newsroom/press-releases/1549-2019-02-etsi-releases-first-globally-applicable-standard-for-consumer-iot-security
58. https://www.ncta.com/whats-new/cablelabs-unveils-a-new-approach-towards-iot-security
59. https://press.avast.com/hubfs/stanford_avast_state_of_iot.pdf
60. https://gcn.com/articles/2017/09/12/darpa-bots-social-engineering-defense.aspx

61. https://www.wired.com/story/5g-networks-could-throw-weather-forecasting-into-chaos/
62. https://www.ericsson.com/en/trends-and-insights/consumerlab/consumer-insights/reports/5g-consumer-potential#key-consumerrealities
63. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/
64. https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx

Force-Effect

INTRODUCTION

Warfare has always led to ground-breaking technological inventions. Actors constantly strive to have the most advanced and capable force effect to protect their interests at home and abroad. The line between reality and science-fiction visions increasingly blurs. Are we going to hand over the battlefield to AI controlled combat robots? What about the use of Directed Energy Weapons firing microwave or laser beams? These kinds of questions need to be considered in preparation of future warfare scenarios.

As warfare developed, the distance between the fighting individuals increased. Starting from fists and maces over rifles and guns, we are now able to fight wars sitting in chairs in front of computers. The increased distance makes an enemy and warfare itself more and more "diffuse". By constantly increasing distances between enemies, new military and societal fears grow.

Drones and launching station: Dual- use-products and new technologies empower asymmetric actors Strava, which made global data about running routines public — inadvertently revealing the contours of running routes used in secret military bases across the world.
Source: Diehl

CHALLENGES OF THE FUTURE SECURITY ENVIRONMENT

Human Enhancement (HE)

In the future, methods and technologies of human enhancement (HE) will enhance the physical and mental capabilities of humans by natural or artificial means. Humans will be able to provide services more comprehensively and with greater range and perseverance. The social acceptance of HE from an ethical, political, social and legal perspective varies in different countries. HE applications can therefore be used by different actors in varying degrees of intensity. The military "value" of a human life differs equally – often depending on the political system of the country in which HE systems are deployed.

HE will help increase human performance, defensiveness, stamina and survivability. The HE application of "Human Self Repair Kits" ease the replacement of wounded body parts on the battlefield. Through the use of Health Monitoring Systems (HMS), the physical condition of deployed soldiers can be continuously monitored and health and performance-preserving measures can be initiated at an early stage.

The radical use of HE in security and defence will help increase the speed of operation at all levels. Technologically advanced players who specialize in the use of HE can therefore succeed to achieve significant effects on the battlefield not necessarily being reflected by their troop size. This can lead to even more complex asymmetrical warfare scenarios. Proven analytical methods for conflict assessment that are based on predictability and probability are no longer fully effective.

The use of HE likewise challenges societies, states and organizations by side effects of HE research and development. In addition to increased performance, the medical use of HE measures can lead to physical or psychological addiction. An unrestrained use of HE in the civilian world could promote over-dynamics and lead to vulnerability and seizures in society and the state. Additionally, HE creates insurance issues and the potential for the abuse of personal data gives cause for regulation by law.

AI and autonomous systems

In the future, the enforcement of global, comprehensive regulations for the use of AI in self-sufficient systems will remain difficult – especially in weapon systems. The use of autonomous weapon systems with AI therefore depends on the actor-specific political, ethical and legal framework conditions. In future warfare scenarios, actors who violate global guidelines (e. g., Geneva Convention) or apply other guidelines for the use of AI pose a fundamental challenge. The questions of "how much power do I want to give a machine to decide autonomously" and "at which point do I need a human actor to make a decision" needs to be discussed. A clear accountability needs to be implanted and ensured perhaps by sticking to the Man-in-the-Loop approach. The benefits of military AI usage consist in a quicker

decision-making process which leads to advantages on the battlefield. Furthermore, human resources can be saved due to automated tasks.

Directed Energy Weapon systems (DEW)

Laser weapons have always been part of science fiction novels and movies. "Star Wars" basically lives of the concept that sometime in the future, individual soldiers will fight each other with laser swords and canons. While the swords might not work so well in today's wars, a laser canon would. That is why military leaders have been working on and testing Directed Energy Weapons for years.

Directed Energy Weapons (DEW) strike military objectives with concentrated electromagnetic radiation. There are different types of DEW that will have a huge impact on future warfare scenarios. They can be categorized into electromagnetic interferers, high power microwave (HPM) weapons and high-energy laser (HEL) weapons. The use of HPM and electromagnetic interferers is primarily directed against sensors and communications, but can lead to collateral damage in electronic and digital systems. The impact can be on civilian as well as military systems and is difficult to scale, so tactical as well as unpredictable strategic and political implications may follow. HEL weapons counter a variety of military targets (e. g., enemy combat drones, approaching guided missiles and mortar shells). HEL weapons can be lethal and used against humans. Although international regulations may restrict an application against humans, they cannot prevent its use by irregular actors as a torture or killing weapon. It therefore remains a challenge to develop protective measures against HEL.

Significant advantages over conventional weapon systems are low ammunition costs, high precision and agility. DEWs are often based on technologies that are also used in the civilian area (dual use possibility). Therefore, there is a great danger that proliferation will give access to asymmetrical forces. DEWs can be used to defend against enemy threats. One of its major advantages is a DEW's "immediate" effect. Thus, DEWs are also suitable for combating targets with high air velocities (e. g., high velocity missiles). Due to the low costs per shot, DEWs are also meaningful in fighting miniaturized systems, which can attack in large quantities (e. g., swarms of combat drones).

Hypersonic weapon systems

A hypersonic weapon is a missile that travels at Mach 5 or higher, which is at least five times faster than the speed of sound. This means that a hypersonic weapon can travel about one mile per second. For reference, commercial airliners fly at subsonic speeds (just below Mach 1), while modern fighter jets can travel supersonically at Mach 2 or Mach 3.

"Sidewinder missile": conventional weapons are complemented by new systems like Directed Energy Weapons .
Source: Diehl

Hypersonic weapons as strategic assets with high destructive power and long range represent new threats that allow little time and resources for defensive measures. The risk of escalation may increase as new strategic equilibria occur. Deterrence, prevention and offensive thinking can become new strategic tools. The strategic unpredictability of the new weapon systems poses a high risk: A misperception can have catastrophic consequences as there is no time for deescalating measures. The stability of global security regimes, which could regulate the risk of a serious conflict with the use of strategic hypersonic weapons, is uncertain.

Biological warfare and biologized systems

Through technological progress, mankind is able to make increasingly use of nature. The mastery and control of biological systems in terms of warfare poses fundamental challenges. When it comes to "using nature" in terms of future technology, one can think of partial biological mini-weapon systems or reconnaissance systems on an insect basis, miniaturization and even controlling animals or plants. Furthermore, new forms of mobility can be researched as well as new protection methods of sensors and materials. Biologized detectors can help to spot B- and C-warfare agents, toxics and pathogens and biologized reactors can create new forms of those agents and be also used for food and energy supply.

Yet it needs to be considered that especially in the early stages biological warfare has a highly dangerous potential for accidents. Uncontrolled and unwillingly released B- and C-warfare agents do not identify friendly or hostile actors and do not stop at borders. This makes corresponding research facilities worthwhile targets for terrorist attacks.

IMPLICATIONS FOR THE MILITARY

Making use of human enhancement

The challenge of making good use of HE will be the combination of HE and existing skills. The question of necessity,

prioritization and synchronization of men and HE has to be constantly revised compared to traditional or basic procedures. Especially the application of dual-use applications and civil-military cooperation in HE developments lead to new challenges (e. g., interfaces, military use of civilian solutions).

Due to different socio-cultural attitudes toward HE, a core challenge will be to work together in a multinational military environment: If partners use HE applications with varying intensity, the social acceptance of the member states for multinational commitments will vary. The problem of interoperability poses a similar challenge in a multinational context.

Mission planning: The soldier of the future will face unexpected challenges
Source: IABG

Like other states, Switzerland must lead the debate on the opportunities and risks of HE impacts on the society and the military. Therefore, armed forces must develop an understanding that should be considered as part of the communicative strategy. Nevertheless, it must be ensured that the operational capability of the armed forces through training, aptitude and targeted training is maintained even without the use of HE.

Innovation of autonomous weapon systems

Even though there are national reservations regarding the use of autonomous weapons systems with AI integration, it is necessary to develop own innovative capabilities for the use of AI in this area. Causes of national reservations and public discussions can be eliminated by developing better solutions. The risk of missing out on the ability to innovate because of false expectations, fears and fixation on (alleged) legal or ethical difficulties should be considered.

Implications for directed energy weapon systems

In future warfare scenarios, it is necessary to reinforce own systems and structures against DEW threats and to reduce the vulnerability of own electronic systems. Electronic systems and sensors can be reinforced by being modular so that they can be inexpensively repaired after damage by opposing DEWs. The protection of own DEW systems is indispensable. In addition to passive ones, active defensive measures will be developed to be able to eliminate enemy DEW systems in a targeted manner (e. g., clearing up enemy DEW agents, anti-radiation missiles, anti-radiation UAVs). The protection against DEW-Friendly-Fire plays a superordinate role. The foundation for effective DEW defence measures is the creation of new deployment concepts, the review of own procedures and deployment principles.

- The ability to detect attacks with energy weapons and to identify attackers in the diffuse battlefield needs to be developed. That brings along new challenges.
- Electromagnetic interferers are directed against sensors that can reconnoitre them. Under interference conditions, these sensors can indeed clarify the direction of the interference, but not the distance of the interferer from the sensor. Therefore, at least a second sensor is needed, which performs a second direction detection from another position to determine the interferers' position.
- HPM weapons are directionally selective in order to achieve high energy densities in this area. They disrupt or destroy sensors that could enlighten them.
- HEL work with very short energy pulses that propagate at the speed of light. The time window for detection is thus extremely short.

Implications for hypersonic weapons

Because of the security significance of hypersonic weapons, armed forces have to build their own competencies for political and strategic consultation and assessment. Risk assessment of armament skills of own and opposing forces is necessary. On this basis, a discussion must be facilitated about the need for new weapons technologies and self-limitation in order to inform policy and society about their own capacity potentials and objectives.

The time frame for countermeasures to ward off hypersonic weapons is very short – making the challenge more difficult that human operators can no longer react fast enough. Therefore, the use of automated systems has to be checked. Detecting attacks by strategic hypersonic weapons requires an early warning system in the sensor network. For reconnaissance in depth, remote sensors are needed (air, space).

CONCLUSION

As technological advances change the world we know and offer different ways to make life easier, we also see military innovations leading to a changing security environment. This security environment sees itself endangered by various

highly destructive new forms of weapon systems. These risks need to be minimized by taking effective countermeasures to future threads. To what extent these countermeasures must be implied into existing military structures needs to be broadly discussed in terms of financial realization and ethical consequences. However, one must always keep in mind that hostile actors can come to a different conclusion which affects the safety situation even more adversely.

The challenge of dealing with technological innovations in the military sector is ambivalent – especially when it comes to force effect. In terms of defensive capabilities, one needs to react to technological advances, made by hostile actors to secure own forces and interests. Regarding offensive capabilities, the use of new weapons is addressed in broad social and moral discussions. To find the right path between securing own interest and staying in line with the political parameters will be one of the key challenges to military planners in the future.

SWOT-ANALYSIS for swiss military planners

Strengths • Research capabilities and technological advance • Permanent technological foresight mechanisms • High national innovation level • Strong civil tech industry	**Weaknesses** • Ehical consequences coming with future weapon systems • Restrictions on AI-based weapon system development
Opportunities • Broad public dialog • Deterrence through technological progress • Interoperability in a military defence community	**Threats** • Missing out on opportunities due to false implications with future technology • Very high damage potential of future weapon systems

armasuisse
Science and Technology S+T

Feuerwerkerstrasse 39
CH-3602 Thun

telephone: + 41 58 468 28 00
fax: + 41 58 468 28 41

email: wt@armasuisse.ch
web: www.armasuisse.ch/wt

ISBN: 978-3-9525175-0-5