أكاديمية الإمارات الدبلوماسية
EMIRATES DIPLOMATIC ACADEMY

EDA INSIGHT

RESEARCH & ANALYSIS

NOVEMBER 2018

The Economic, Security and Military Implications of Artificial Intelligence for the Arab Gulf Countries

Dr Jean-Marc Rickli

Dr Jean-Marc Rickli

Head of Global Risk & Resilience at the Geneva Centre for Security Policy (GCSP)

Dr Jean-Marc Rickli is the Head of Global Risk and Resilience at the Geneva Centre for Security Policy (GCSP). He is also a visiting fellow at the Department of Defence Studies, King's College London and an advisor for the Artificial Intelligence Initiative at the Future Society, Harvard Kennedy School. He is the co-chair of the NATO Partnership for Peace Consortium Working Group on Emerging Security Challenges and an expert on autonomous weapons systems within the framework of the United Nations Convention on Certain Conventional Weapons. He is also a non-resident fellow in modern warfare and security at TRENDS, Abu Dhabi and an advisor at Gulf State Analytics, Washington. Prior to these appointments, Dr Rickli was an assistant professor at the Department of Defence Studies at King's College London and at the Institute of International and Civil Security at Khalifa University in Abu Dhabi. Dr Rickli received his PhD in International Relations from Oxford University.

Executive Summary

- Artificial intelligence (AI) since the early 2010s has witnessed a series of technical breakthroughs due to the increase in computing power, the amount of data generated and the application of machine learning techniques.
- Artificial intelligence will have major economic impacts by increasing productivity worldwide. However, many jobs, both blue- and white-collar workers, are at risk of being automated. This implies that important efforts in terms of education and training will have to be undertaken to keep these people on the job market.
- Artificial intelligence will also have major impacts on international and national security. It will rebalance the international balance of power, empower individuals and shift the global strategic balance towards those states that have a strong AI industrial base and heavy investment, both public and private, in AI research and development.
- The Arab Gulf countries will also be faced by the economic and security implications of AI. It has the potential to profoundly change the economic structure of Gulf societies. Expats will be the hardest hit by automation, but AI is also expected to profoundly affect governmental jobs. This implies that Gulf countries governments have to massively invest in education to best prepare future generations for this transformation. Continuing education programmes also have to be put in place to provide national workers with re- and upskilling opportunities.
- In terms of military and security consequences, self-organised collective decision-making in swarms of autonomous agents will likely become a defining feature of future battlefields. The impact of swarming strategies has the potential to upset the offense-defence balance and impact strategic stability both regionally and globally accordingly. It will also act as a force multiplier for non-state actors that could directly impact the Gulf countries' military forces operating in Middle Eastern theatres of operations.
- The cyber domain will be very conducive for the development and engagement of fully autonomous weapons as surrogates. Given the Gulf region's past record with regard to cyber-attacks, one cannot exclude that AI will magnify instability in the region.
- The use of artificial intelligence for massive manipulations through the forgery of images, films or voices is already a reality. Its use by malicious actors has the potential to magnify the tensions in the Gulf region and increase its instability.
- The broadening of the scope of threats, vulnerabilities and potential mis- and malicious uses of AI, but also of other emerging technologies, calls for a rethinking of global governance mechanisms so that they can better deal with dual-use technologies.

The Issue

Artificial intelligence (AI) has long been the subject of science fiction but only recently has its profoundly disruptive potential seemed near to realisation. Advances in artificial intelligence have grown exponentially since the early 2010s. While Moore's law relies on the processing power of computers doubling every 18 months, the amount of compute used in the largest AI training runs has been doubling every 3.5 months from 2012 to 2018. This represents a more than 300,000-times increase compared to a 12-times increase based on Moore's law for the same period.[1] Such an exponential growth is transformative for every sector of activity and this causes hopes but also serious concern among its developers and the international community.

On the one hand, faced with pressing global challenges associated with overpopulation, environmental challenges, health and inequality, the world stands to benefit enormously from the development of AI. For instance, AI can contribute to making sense of the big data gathered to monitor climate change, predict pollution or be more accurate and faster than doctors at diagnosing certain illnesses.[2] A recent study showed that an AI trained to diagnose skin cancer achieved 95% detection rate compared to 86.6% for human doctors.[3] The International Telecommunications Union acknowledged the positive contribution of AI and organised the second edition of the AI for Good Global Summit with the focus on "impactful AI solutions able to yield long-term benefits and help achieve the Sustainable Developments Goals." in Geneva in May 2018.[4]

On the other hand, a myriad of security concerns and risks accompany the wide-ranging solutions that AI can bring. A recent study by an interdisciplinary group of AI experts, philosophers and political analysts warned against the malicious uses of AI in three security domains: digital, physical and political security.[5] The economic impacts of the increasing use of AI provide optimistic prospects in terms of productivity but also raises concerns about the human costs of this transformation, especially for those who will not be able to adapt fast enough or adapt at all. This added to the existing public warnings about the development of AI from leading personalities such as Stephen Hawking and Elon Musk.

Against this backdrop, this EDA Insight reviews some of the economic and security implications of AI for the Arab Gulf countries. It first defines and reviews recent breakthroughs in AI, then looks at the economic implications of AI in terms of productivity growth but also jobs destruction and displacement. The security implications are then analysed by focusing on autonomous weapons system and their impact on strategic stability. It is followed by analysis of some uses of AI in the cyber domain and argues that cyber AI-supported offensive operations and manipulations are likely to be the biggest challenge that the Gulf countries will face in the near future. It concludes by looking at the issue of the global governance of AI.

What is AI?

While there are numerous debates about the meaning of intelligence, artificial intelligence, simply put, is the use of computers to perform tasks that normally require human analytical skills. There are three classes or levels of AI.

The most basic class of AI is artificial narrow intelligence (ANI) which encompasses technologies that are designed for specific, limited purposes. ANI examples include: the algorithm behind Google Translate, anti-lock brake systems, or facial recognition technology.

The second class of AI, which has not yet been realised, is that of artificial general intelligence (AGI), which would be capable of operating across all areas, including cognitive, that the human brain does. In a recent survey of AI experts, the median timeframe predicted for the achievement of AGI is 45 years from now.[6]

The most distant class of AI, and also its final incarnation, is considered artificial super intelligence (ASI). This form of AI, which will be by far the most challenging to achieve, describes intelligence that exceeds the capacity of the human brain. It is difficult to fathom exactly how such an AI would behave and what implications it might have for the world, but it is fair to assume that an AI more powerful than human beings would have consequences for the existing world order and potentially represent an existential threat to humanity.[7] However, the focus of this Insight is on ANI exclusively.

Recent Breakthroughs

Although the term artificial intelligence was coined in the 1950s, lack of progress in the field led to a long period of AI winter. Since the 2010s however, AI research has passed a couple of milestones. In the words of Sergey Brin, co-founder of Google, "the new spring in artificial intelligence is the most significant development in computing in [his] lifetime."[8]

This revival of AI is due to developments in two fields. To make algorithms work, significant computing capacities

and huge sets of data are needed. Thanks to Moore's law, a mobile phone nowadays has more computing power than the best supercomputer in 1999.

Similarly, with the rise of the Internet of Things (IoT) the increasing number of computers and connected devices generate an exponential growth of data. It is estimated that 23.14 billion connected devices are in use worldwide in 2018 and 30.73 billion will be by 2020.[9] These will generate 44 zettabytes of data,[10] or the equivalent of 5,200 gigabytes for every individual. This represents more than half of the printed collection of the entire Library of Congress.[11] By 2025 it is estimated that the world will be creating 163 zettabytes a year and will lead to every connected person anywhere in the world interacting with a connected device every 18 seconds.[12]

The combination of increasing computing power and available data has enabled recent breakthroughs in AI, notably by the application of various machine learning approaches. In March 2016, Google Deepmind, created the AlphaGo algorithm and defeated the second-best player of the game 'Go', Lee Sedol, in four out of five games. Go is considered the most complex board game as there are more positions (2x10p170) than atoms in the universe (10p80).[13] In October 2017, the new version of AlphaGo, AlphaGo Zero, defeated AlphaGo 100 games to 0 after three days of training.

Two months later, building on the previous successful experiences, a general-purpose reinforcement learning algorithm, AlphaZero, was developed. AlphaZero was given no prior domain knowledge except the rules of each game.[14] It achieved in 24 hours superhuman performance in the games of chess, shogi and Go, by defeating a world-champion computer program of each game in each case.[15] Kasparov hailed AlphaZero as "a remarkable achievement" which underlines "a human-like approach to machine chess (…) instead of brute force."[16]

The Alpha-class algorithms represent breakthroughs in terms of the speed of learning as well as the ways of defeating human beings at games they have been playing for more than 2000 years. AlphaGo, for instance, in game two played a move that Fan Hui, three-time European Go champion and who had lost five straight game against AlphaGo in 2015, qualified as "so beautiful" but added "it's not a human move. I've never seen a human play this move."[17]

In January 2017, Libratus, an algorithm developed by Carnegie Mellon University, played more than 120,000 hands in no-limit Texas Hold 'Em Poker against four of the world's best human players.[18] In the end, Libratus won $1,776,250. The player who lost the least lost $85,649 and the biggest loser lost $880,087.

Unlike all board games, Poker is a game of incomplete information because players can bluff and thus have private information. Libratus has thus demonstrated the ability of algorithms in defeating human beings in real world strategic interactions similar to negotiations, business or military strategy, security interactions or auctions.

Economic Impact of AI in the Gulf

The global economy, the right to privacy, and our values as human beings will all be tested by the continued development of AI. When it comes to the impact of AI on the global economy, there is so far no consensus among analysts. Yet, two observations seem to be shared: that productivity will increase and that AI will lead to profound transformations of employment with the destruction of traditional and the creation of new jobs. The balance of these transformations however is unknown and left to various speculations. This section presents the most relevant conclusions of these findings.

A study by Accenture estimates that AI technologies could boost labour productivity by up to 40% in 2035.[19] A recent report from the McKinsey Global Institute argues that "AI could potentially deliver additional economic output of around $13 trillion by 2030, boosting global GDP by about 1.2 percent a year."[20] Another study from Pricewaterhouse Coopers shows that global GDP could be up to 14% higher in 2030 while Accenture finds that AI has the potential to double the annual economic growth rates of 12 developed economies.[21] The rate of AI adoption and integration in the economy has however the potential to increase the digital divide between advanced and developing economies. The gap between these countries in terms of net GDP impact could widen from "three percentage points in 2025 to 19 percentage points in 2030."[22]

The inherent consequence of the spread of AI and automation across a range of sectors, will also provoke profound changes in the employment structure and likely lead to the rise of social inequality. McKinsey estimates that up to 800 million jobs could be displaced worldwide by 2030 due to automation.[23] Job profiles which are "characterized by repetitive tasks and activities that require low digital skills may experience the largest decline as a share of total employment, from some 40 percent to near 30 percent by 2030" and that in return, jobs which involve "nonrepetitive activities and those that require high digital skills" can rise from "40 percent to more than 50 percent by 2030."[24]

If one considers ten-percent unemployment as a major

recession, and 20% as a global emergency, then the figures from various studies, where up to 15% of the global workforce will have to change their employment, - and some will not manage the transition – then it is clear that the digital revolution supported by AI will have profound socio-economic consequences.[25]

This revolution will also profoundly challenge domestic and international governance systems as, unlike the Industrial Revolution that took more than 100 years to unfold, the current revolution is extremely rapid due to the phenomenal rate of digital diffusion which is sustained by the private sector especially start-ups and the world's largest technology companies.[26]

When it comes to the Middle East, Pricewaterhouse Coopers has evaluated that AI will have a powerful impact on Middle Eastern economies.[27] They estimate that by 2030, AI could generate 10 million new jobs only in the Gulf region. They also predicted that by 2030, the impact of AI in developing non-oil sectors in the Middle East could amount to US$320 billion.

In the study, AI is predicted to have a positive effect on productivity in the Middle East. While the largest impact is expected to be on the UAE, with a projected 14% increase in its GDP, Saudi Arabia follows with an expected US$135.2 billion accrual in the next decade, equivalent to 12.4% of its GDP. The study predicts that the most significant economic impact of AI will be in the financial sector, to which an estimated 25% of all AI investment in the region will be directed by 2021, followed by the education, healthcare, and manufacturing sectors. The International Data Corporation expects the sectors that will see the fastest growing use of cognitive/AI systems to be defence, counter-terrorism and government intelligence.[28]

According to the latest McKinsey & Company's report on The Future of Jobs in the Middle East, the region should embrace the transition into the new age of automation, especially in sectors that consist of mostly routine tasks such as transportation and manufacturing.[29] They also found that over 93% of the automation will apply to jobs held by expat workers, resulting in nearly US$366.6 billion worth of automatable wage income. The resulting gains could be used to reduce the dependence on foreign workers and invest in developing and educating domestic workforces.

Although workforce automation will mainly affect expats, one area for GCC nationals that will however sizeably be affected by automation is the government sector. The rentier state model of the Gulf countries favours governmental jobs for nationals. According to the 2016 Arab Youth Survey, 70 percent of GCC youth prefer public sector jobs over private sector employment.[30] In order to guarantee future employment of their domestic workforce, GCC governments should promote digital jobs, especially those related to emerging technologies in information technology, data analysis, artificial intelligence, nanotechnology, neuroscience or biotechnology because they are more adaptable to technological disruption. These jobs will also contribute to moving from "administrative jobs in the government sector to higher-value-added roles in industries with future importance."[31]

This will require major changes in basic, superior and continued education. With advances in machine intelligence, more work will be offloaded to machines. Thus, humans will have to adapt, up- and reskill and focus on work that can only be done by humans. In order to achieve this, agility and a change of mindset towards flexibility will be required. Moreover, people will have to be prepared to develop partnerships between machine intelligence and human workers to accurately perform traditional and new jobs.[32]

For current workers, the World Economic Forum estimates that globally by 2022 no less than 54% of all employees will require significant re-and upskilling and that companies will prioritise these efforts on employees currently performing high-value roles.[33] Hence, the education of the future generation will be key to deal with future disruptions.

Adaptation of education systems towards more agility should not only focus on fostering sharp academic knowledge but also on developing technological and vocational training. Likewise, proficiency in new technologies will be needed but human skills such as social and emotional intelligence, creativity, empathy, originality and initiative, critical and divergent thinking (to find and frame problems not yet known), persuasion or complex problem-solving will be as important. This is all-the-more important in the Gulf as 60% of the population is currently under the age of 25 but the region has one of the world's highest rates of youth unemployment (30%), which is double the world's average.[34]

The economic impact of AI in the Gulf will therefore be transformative from a productivity point of view in a region characterised by weak productivity levels. AI-driven productivity gains will however have to be invested in strategic diversification across different sectors to guarantee the sustainability of Gulf economies.[35] The domestic labour market, on the other hand, will require major structural adjustment of traditional workers in services, administrative and support, government, manufacturing, construction and trade. AI will massively cut down "the amount of labor for repetitive tasks thereby

leading to increased return on capital investment" but will also require drastic adaptation of education and training systems so as to maintain the national workforce relevant.[36]

Current State of AI Integration in the Arab Gulf Economies

The UAE and Saudi Arabia are currently at the forefront of embracing AI as a new driver of economic change in the Gulf. Dubai has made major efforts in the application of emerging technologies and AI in futuristic urban infrastructure (some being realised and others still in the making). This includes a hyperloop system, a robot police force, a store that changes shape, self-driving electric vehicles, flying taxis, a space agency, and the Dubai Future Accelerators, a programme where the government pairs with the private sector to facilitate innovation.

The UAE also launched the US$270 million Dubai Future Endowment Fund to help organisations leverage disruptive technologies while the Abu Dhabi-based investment company Mubadala works with IBM Watson to create a local ecosystem of entrepreneurs and start-ups applying cognitive computing in new and innovative ways. The UAE government has also identified sectors in which AI could be implemented, such as the police, to develop AI-based forensics solutions and facial recognition systems, in the medical sector by developing autonomous digital mobile booths designed to replicate doctors' surgeries or in education using machine learning to predict students at risk of dropping out.[37]

Saudi Arabia is planning to build a US$500 billion new, hi-tech city, Neom, on the Red Sea Coast. In the words of Saudi Arabia's Crown Prince, Mohammed bin Salman Al Saud, "everything [in Neom] will have a link to artificial intelligence, to the Internet of Things – everything."[38] During his visit to the United States in March 2018, AI was at the heart of several agreements signed with leading American companies including a memorandum of understanding between Saudi Arabia and Microsoft to contribute to the "transfer of knowledge and acquisition of systems related to artificial intelligence."[39] Mohammed bin Salman thereafter also approved the establishment of a college on AI and cyber security named after him: the Prince Mohammed bin Salman bin Abdulaziz College of Cyber Security, Artificial Intelligence and Advanced Technologies.

With the creation of a Council for Artificial Intelligence as well as the appointment of a Minister of State for Artificial Intelligence, Omar bin Sultan Al Olama, in 2017, the UAE has been a pioneering country in developing domestic institutions for the governance of AI. According to Al Olama, the reasons why the Muslim world stagnated while the rest of the world was progressing was because of technology. Thus, for him, among the technologies that "will shape the next century, AI is at the forefront" and therefore "if we (the UAE) don't embrace it, we'll be in the Dark Ages compared to countries that are."[40] It follows that the UAE has developed a national Strategy for Artificial Intelligence, a first of its kind in the world, that offers a roadmap to leverage AI in the sectors of transport, health, space, renewable energy, water, technology, environment, traffic and education.[41] The latter is especially important as it aims at creating a generation of tech-savvy citizens with knowledge of AI.

Thus, the impact of AI on the global and Gulf economies provides both optimistic prospects in terms of productivity and pessimistic perspectives with the potential destruction of traditional jobs that it will entail and the uncertainty related to the creation of new jobs. These transformations will have serious socio-economic consequences and potential security implications in terms of national stability, as the greater the share of people losing their job and being unemployed or unable to adapt to these changes, the more national welfare systems will be impacted.

Also, and particularly in the Gulf region, the education of the young generation to new jobs that will increasingly integrate human intelligence with AI, will be essential in order to avoid significant unemployment in the next generations. If harnessed well however, the adoption of AI could be a major determinant to diversify the GCC economies and reduce their dependence on oil and gas exports.[42]

Setting the Stage for AI and International Security

AI will alter international security by rebalancing the international balance of power, empowering individuals and shifting the global strategic balance. Two states, China and the United States, are currently dominating the AI market and innovations. Beyond fuelling great power rivalries, AI also potentially diffuses power to transnational actors such as multinational companies as well as individuals and non-state actors.[43] AI and other emerging technologies such as additive manufacturing, synthetic biology or cognitive neuroscience, indeed are dual-use technologies that are primarily developed in the private sector and for some increasingly relying on open-source developments.[44]

These new technologies offer tremendous opportunities for beneficial developments but their rapid diffusion also provides room for mis- and malicious uses. For instance, the Cambridge Analytica scandal demonstrated how a group of scientists and businessmen could leverage big data, a social network (Facebook) and algorithms to influence people's opinions in democratic elections.[45] In the military, the increasing autonomy of machines and robots afforded by artificial intelligence together with the AI-related technologies that contribute to human enhancement such as brain-computer interface, represent the new silver bullet of future conflicts.

The Militarisation of Artificial Intelligence

The growing militarisation of AI will have major consequences for both national and international security. The UN, through the Convention of Certain Conventional Weapons (UNCCW), has debated the issue of autonomous weapons systems (AWS) since 2014. No consensus has so far emerged on a definition of these weapons nor on the issue of their limitations or even a ban. The only agreement among states seems to be on the requirements of guaranteeing meaningful human control in the use of these weapons. However, no agreement has yet been reached on the definition of what meaningful human control means nor on the practicalities of implementing this concept operationally.

To qualify as a fully autonomous system, a weapon should fulfil at least three core functions of its engagement cycle autonomously: the search of the objective, the decision to engage and the engagement of the target. Such a weapon should be able to move independently through its environment to arbitrary locations; select and fire upon targets in their environment and create and or modify its goals, incorporating observation of its environment and communication with other agents.[46]

There is also no agreement on whether these weapons already exist or not. Paul Scharre, who has written the most compelling book on the subject so far, considers that only the Israeli Harpy drone would qualify as AWS.[47] The Harpy is an anti-radiation loitering weapon capable of finding and attacking radar installations autonomously. The Stockholm International Peace Research Institute (SIPRI) on the other hand, has identified 381 weapons with autonomous functions. According to SIPRI however, the British Dual Mode Brimstone guided missile is currently the only operational guided munition with target selection autonomy while the Harpy is the oldest system that can operate in complete autonomy.[48]

Irrespective of whether fully autonomous weapons systems already exist or not, with the improvements in machine learning we see that technologies developed in the private sector can be used for military purposes. Dual-use technologies represent the core technologies for the development of AWS. This is, for instance, the case with computer vision. In 2015, algorithms have equalled human beings in image recognition error rate (5%). These days algorithms are much better at identifying patterns than human beings.

The US Department of Defense partnered with Google to automate real-time image recognition on drone footage in April 2017. Project Maven reached promising results with more than 80% identification accuracy.[49] The goal was to equip armed drones such as the Predator or the Reaper, eventually. However, 3000 Google employees signed an open letter to Google CEO Sundar Pichai to advise the company to pull out of any contract that involves any military applications of Google software, in April 2018. On June 1st, Google announced that it would not renew the contract with the US DoD that is due to expire in 2019.[50]

One of the defining characteristic of AI is its ability to process information at machine speed that far outstrips human capacities. The application of AI in command and control or in decision-support systems is increasingly becoming a reality in the military. In order to cope with the speed of decision-making, the soldiers of the future will progressively be enhanced in their cognitive, biological and analytical functions by synthetic and artificial systems.[51] The Director of the US Defence Intelligence Agency, Lt. Gen. Robert Ashley, recently expressed concerns about China's research into "human performance enhancement including efforts to merge human and machine intelligence."[52]

AI through collective autonomy also allows the simultaneous control and coordination of a multitude of platforms. In terms of military applications, AI makes swarming tactics an emerging feature of future battlefields. Swarming relies on overwhelming and saturating the adversary's defence system by synchronising a series of simultaneous and concentrated attacks.[53] In October 2016, the US Department of Defense conducted an experiment that saw 103 Perdrix micro drones autonomously deal with four different objectives. In May 2018, the Chinese drone manufacturer, Ehang, broke the world record established at the Pyeongchang Winter Olympics, by flying a swarm of 1,374 drones simultaneously over the city wall of Xi'an. This record was then broken by the company Intel to celebrate its 50th anniversary on 15 July with the flight of 2018 drones.[54]

Swarming combines the military principles of mass,

coordination, speed and concentration of forces at new levels. Autonomous swarms will allow the concentration of large numbers of military assets with very few or no human controllers and with far quicker reaction times to constantly changing situations. Swarms rely on collective intelligence. Some posit that the development of AWS and the proliferation of their use in swarms will probably have a destabilising impact on strategic stability in the future through the neutralisation of defence systems, thereby giving an advantage to the offensive.[55] It follows that deterrence would be replaced by pre-emption, a very unstable international configuration that encourages escalation and arms races.[56]

Drones equipped with autonomous technologies are relatively easy to obtain. Unlike weapons of mass destruction, autonomous drones are accessible to less technologically advanced states. It is now possible to convert a "remotely controlled combat drone to autonomously fire a weapon in response to a simple pattern-recognising algorithm".[57] The proliferation of such weapons however, could be used to increase anti-access and area denial capabilities but also to conduct offensive operations against more powerful adversaries and thus have an impact on regional and strategic balances.[58]

Similarly, non-state actors could also get access relatively easily to autonomous drones. It is now possible for anyone to 3D-print micro drones.[59] Similarly, collective intelligence algorithms and trained neural networks are available on open source AI library liked TensorFlow developed by Google. Non-state actors such as Hamas, Hezbollah, Daesh or the Houthi rebels have all acquired off-the-shelf unmanned aerial vehicles. These have been used for intelligence, surveillance and reconnaissance, but also offensive purposes. For instance, Daesh mounted high-definition cameras under drones to acquire ISR capabilities and situational awareness. They also mounted makeshift 40mm grenades to drop them on Iraqi positions. During the battle of Mosul in 2017, Daesh's air capability had significant tactical impact as they killed up to 30 Iraqi soldiers in a single week.[60] These developments are a game changer for militaries as they now have to prevent non-state actors from acquiring tactical air superiority for the first time.

With autonomous drones, terrorist organisation will be able to conduct saturation attacks and targeted assassinations with very low or no human costs on their sides. Artificial intelligence will reinforce targeted killing as a dominant operating mode for both states and non-state actors.[61] Yet, non-state actors, less constrained by organisational culture and bureaucratic resistance than states, might adapt faster to new concepts of operations relying on AI.[62] Critics of the strategic impact of drones used in swarm, point out that current costs of drones make this tactic too costly to be effective.[63] The cyber domain, however, removes the physical costs of weapons manufacturing and maintenance.

Cyber Autonomous Weapons Systems

While most people tend to think of autonomous weapons in terms of robots or autonomous vehicles, AWS also operate in the cyber domain. Because of the low cost of developing an algorithm compared to physical AWS, autonomous cyber weapons are very likely to be developed earlier and spread faster than their counterparts in the physical world.

The Middle East has been a testing ground for cyber offensive operations.[64] Since the 2010 Stuxnet attack that caused irreversible harm to nearly 1,000 centrifuges used for Iran's nuclear programme, a cyber arms race was triggered in the region.

In 2011, Ayatollah Ali Khamenei authorised the establishment of Iran's Supreme Council of Cyberspace to coordinate efforts for both offensive and defensive operations. Similar initiatives were then adopted by the UAE in 2012, Saudi Arabia, Kuwait, Qatar and Bahrain in 2013.[65] In 2012, Saudi Arabia's Aramco company and Qatar's RasGas suffered a cyber attack by a virus called Shamoon that erased data from several thousand computers.[66] Shamoon resurfaced through three distinct waves between November 2016 and January 2017 targeting again Saudi Arabia. In August 2017, a petrochemical plant in the Kingdom was attacked by a malware that aimed to trigger an explosion but failed due to a bug in the code.[67]

This series of events demonstrates a worrisome escalation in the use of cyber weapons in the Gulf.[68] Saudi Arabia is the Arab country that faces the largest number of cyber-attacks in the Middle East and the 17th highest worldwide followed by the UAE, ranked 18th globally. Algeria, Egypt and Morocco then follow.[69]

The use of AI in cyber attacks offers destabilising perspectives for the Middle East. Due to its low barrier of entry, the cyber domain provides an offensive advantage over defence. With the development of generative adversarial networks (GANs) - which are algorithms pitting neural networks against each other - it is possible to manipulate the data of its adversary and therefore fool its defence system. These are known as black box attacks in which "GANs are used to figure out the machine-learning models with which plenty of security programs spot malware."[70]

Similar to the data corruption that Stuxnet relied upon to manipulate the operator of the Natanz centrifuges, malware relying on synthetic data produced by AI will be able to do this, however, autonomously and at machine speed. Unlike Stuxnet, such an offensive autonomous cyber weapon will not rely on a human operator to code the behaviour and plan of attack of the malware, it will learn on its own.

In August 2018, IBM presented a proof of concept called "DeepLocker" at the Black Hat USA conference. DeepLocker is an AI-powered malware "highly targeted and evasive" because unlike traditional malware, it hides its malicious payload in a benign carrier application such as a video application and uses AI to create unique trigger conditions that can only be unlocked if the intended target is reached.[71] A neural network is indeed trained to recognise the target, for instance a person, that will trigger the attack once identified. This type of attack opens the possibility for hyper discriminate attacks that can be reproduced easily by training neural networks to identify new targets.

To defend against the increasing threat of complex cyber attacks, in 2016 the DARPA (Defence Advanced Research Projects) organised the Cyber Grand Challenge whose aim was to enhance cyber security through machine learning. Seven machines competed to automatically heal their system while simultaneously scanning and attacking the vulnerabilities in adversary systems. A year later, the winning team, ForAllSecure, was offered a contract by the Pentagon to secure US military systems.[72] Similar to high frequency trading, the trend in cyber security will be to increasingly rely on algorithms as both offensive and defensive tools.[73] Considering the importance of cyber security, the Gulf region will most likely embrace this trend.

The use of AI for subversive purposes is a trend that will likely hit the Middle East and the Gulf as well. The spread of deep fake technology such as FakeApp, which uses AI deep learning techniques to swap a person's face onto someone else's, has democratised the ability to create perfect visual manipulations.[74] Voice mimicking software such as Lyrebird or Baidu's Deep Voice can clone anyone's voice. The Chinese tech giant application only needs 3.7 seconds of audio of a voice to reproduce it.[75] The combination of voice and image forgery will make any piece of media on the internet suspicious.

The automation of political manipulation by algorithms, that are increasingly able to learn by themselves and share information in "hivenet", will trigger the development of increasingly adaptive malware[76] and allow for the rise of true technological surrogates waging psychological and disinformation operations in the cyber domain with extensive disruptive effects in the real world.[77] As citizens of the GCC countries are amongst the biggest users of the internet and social media in the world and because the Middle East is a fertile ground for conspiracy theories,[78] the risk of mass and targeted manipulations through AI systems is non-negligible in the Arab Gulf countries in the future.

Overall, the international threat pictures will be dramatically altered by AI and autonomy in the near to medium term future. It follows that current international governance structures have to be adapted and some new ones probably created in order to face these new challenges.

The International Governance of AI

In his newly released report on disarmament, the UN Secretary General raises awareness about "the dangers posed by the weaponisation of artificial intelligence and autonomous systems" and recommends states to "exercise restraint in the development and acquisition" of these weapons.[79] However, states are unlikely to relinquish seeking leadership in AI and its many applications.[80] For instance, in July 2017, China set itself the goal of becoming the leader in the field of AI by 2030, to challenge US dominance.[81] A race regarding autonomous technologies between the great powers but also among non-state actors has already started.

It follows that the efforts at regulating AI have been very disparate and uncoordinated. Regarding the weaponisation of AI, the UN through the UNCCW has not been able to bring states to a consensus about the regulation of lethal autonomous weapons systems since 2014. Various initiatives in the private sectors have tried to compensate for the lack of international governance. For instance, in December 2017 IEEE, the largest professional engineers organization, published a code of conduct whose primary goal is to ensure that every technologist prioritises ethical considerations in the design and development of autonomous and intelligent systems.[82] The Partnership on AI, a non-governmental organisation founded by a coalition of tech giants, aims to share best practices in the research, development and fielding of AI technologies while OpenAI, a non-profit AI research company, seeks to build safe artificial general intelligence.

Faced with potential daunting economic and security consequences of the use of AI, the international community should be serious in creating a governance system that brings together governments, international organisations, the scientific community, the private and

commercial sectors as well as civil society.[83] The Gulf countries could play a pivotal role in this by bringing the Arab voices to the table as well as by favouring multilateral diplomacy. The recent appointment of the UN Secretary General of a "High-Level Panel on Digital Cooperation," where the UAE through its Minister of Cabinet Affairs and the Future, Mohammed Al Gergawi, is the only Arab state representative, is a step in the right direction.[84]

Conclusions

The Gulf countries will not be immune to the developments and consequences of AI. Economically the productivity of the Gulf economies is most likely to benefit from AI. Artificial intelligence will allow the automation of many sectors of activities. This will reduce the need for foreign labour and thus free financial resources to diversify the Gulf economies in order to move beyond their rentier state model. AI, however, will require the re-skilling of the domestic populations and the education of the younger generation towards more creative and critical thinking as well as the development of more tech-savvy future workers in order to avoid them being side-lined by automation.

AI will alter international security and the international balance of power. President Putin noted last year that "whoever becomes leader in this sphere [AI], will be the ruler of the world."[85] An AI race is taking place among the three largest military powers, USA, China and Russia. Since AI is a dual-use technology that can proliferate very quickly, it also empowers individuals and non-state actors who can find ways to leverage this technology. In security terms, the world has moved from 195 states as referent of security towards potentially more than 7.5 billion sources of insecurity.

The character of war will also be affected by the growth of autonomy and autonomous weapons systems as well as the growing fusion between human soldiers and enhancement technologies. It is very likely that states and non-state actors alike will increasingly resort to technological surrogates to fight wars in the future.[86] The chaotic and unregulated nature of the cyber domain offers a glimpse of things to come and AI will very likely magnify the advantage of the offensive. Based on previous records of cyber attacks in the Gulf, one can infer that AI could act as a destabilising factor for the region unless AI can be leveraged to reinforce autonomous cyber defence.

It is too early to have an accurate picture of the full socio-economic and politico-strategic consequences of AI. However, while AI technology advances rapidly and becomes increasingly integrated into our lives, it is critical that the international community establishes a system of global governance to assure that it develops in a way that is beneficial to societies. The appointment of an AI minister in the UAE is a recognition that this technology is transformative in itself. The other Gulf countries would be inspired to follow the Emirati example but also to push and support the establishment of a global AI governance system.

Endnotes

1. Dario Amodei and Danny Hernandez. "AI and Compute," *OpenAI Blog,* 16 May 2018, https://blog.openai.com/ai-and-compute/
2. Bernard Marr. "The Amazing Ways We Can Use AI to Tackle Climate Change." *Forbes,* 21 February 2018, https://www.forbes.com/sites/bernardmarr/2018/02/21/the-amazing-ways-we-can-use-ai-to-tackle-climate-change/#1e7dcf4a357e, Alex Gray. "7 Amazing Ways Artificial Intelligence is Used in Healthcare.". *World Economic Forum,* 20 September 2018, https://www.weforum.org/agenda/2018/09/7-amazing-ways-artificial-intelligence-is-used-in-healthcare/
3. Agence France Press, "Computer Learns to Detect Skin Cancer More Accurately than Doctors." *The Guardian,* 29 May 2018, https://www.theguardian.com/society/2018/may/29/skin-cancer-computer-learns-to-detect-skin-cancer-more-accurately-than-a-doctor
4. ITU, "AI Good Global Summit 2018", *International Telecommunication Union,* https://www.itu.int/en/ITU-T/AI/2018/Pages/default.aspx
5. Miles Brundage, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention and Mitigation,* University of Oxford: Future of Humanity Institute, February 2018, https://arxiv.org/pdf/1802.07228.pdf
6. Katja, Grace and *al.*. "When Will AI Exceed Human Performance? Evidence from Experts." arXiv:1705.08807, 24 May 2017, https://arxiv.org/pdf/1705.08807.pdf
7. WEF. *The Global Risks Report 2017.* Geneva: The World Economic Forum, 12th Edition, 2017, http://www3.weforum.org/docs/GRR17_Report_web.pdf
8. Tom Simonite. "Google Cofounder Sergey Brin Warns of AI's Dark Side", Wired, 27 April 2018, https://www.wired.com/story/google-cofounder-sergey-brin-warns-of-ais-dark-side/amp?__twitter_impression=true
9. Statista. "Internet of Things (IoT) Connected Devices Installed Base Worldwide from 2015 to 2025 (in Billions), *Statista,* 2018, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
10. Lucas Mearian. "By 2020 there will be 5'200 GB of data for every person on Earth", *Computer World,* 11 December 2012, http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html
11. What's a Byte. "Megabytes, Gigabytes, Terabytes… What are They?," *Whatsabyte.com,* accessed 30 Septembre 2018, https://whatsabyte.com
12. David Reinsel, John Gantz and John Rydning. *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big.* Framingham, MA: International Data Corporation (IDC), p. 3, https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf
13. Leon, Lei. "Go and Mathematics", *The American Go Foundation, 2017,* http://agfgo.org/downloads/Go%20and%20Mathematics.pdf
14. Critics of AlphaZero's achievement point out that many real-life situations cannot be simplified to a fixed predefined set of rules. See, Jose Camacho Collados. "Is AlphaZero Really a Scientific Breakthrough in AI?", *Medium,* 11 December 2017, https://medium.com/@josecamachocollados/is-alphazero-really-a-scientific-breakthrough-in-ai-bf66ae1c84f2
15. David Silver and al. "Mastering Chess and Shogi by Self-Play with a General Reinforcement Algorithm," *arXiv,* 550, 2017, pp. 354-359, https://arxiv.org/pdf/1712.01815.pdf
16. Quoted in Mike Klein. "Google's AlphaZero Destroy Stockfish in 100-Game Match," *Chess.com,* 6 December 2017, https://www.chess.com/news/view/google-s-alphazero-destroys-stockfish-in-100-game-match
17. Quoted in Cade Metz. " How Google's AI Viewed the Move No Human Could Understand," *Wired,* 14 March 2016, https://www.wired.com/2016/03/googles-ai-viewed-move-no-human-understand/
18. Noha Brown and Tuomas Sandholm. "Libratus: The Superhuman AI for No-Limit Poker", *Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-2017),* 2017, https://www.ijcai.org/proceedings/2017/0772.pdf
19. Mark Purdy and Paul Daugherty, *Why Artificial Intelligence is the Future of Growth,* Accenture, 2016, p. 17, https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-33/Accenture-Why-AI-is-the-Future-of-Growth.PDF#zoom=50
20. Jacques Bughin and all. *Notes from the AI Frontier: Modelling the Impact of AI on the World Economy.* McKinsey Global Institute, September 2018, p. 3, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
21. PricewaterhouseCoopers, *Sizing the Price: What's the Real Value of AI for your Business and how can you Capitalise.* PwC, 2017, https://www.pwc.com/gx/en/issues/analytics/assets/pwc-ai-analysis-sizing-the-prize-report.pdf and Mark Purdy and Paul Daugherty, *Why Artificial Intelligence is the Future of Growth,* Accenture, 2016, p. 3, https://www.accenture.com/t00010101T000000__w__/gb-en/_acnmedia/PDF-33/Accenture-Why-AI-is-the-Future-of-Growth.PDF#zoom=50
22. Jacques Bughin and all. *Notes from the AI Frontier: Modelling the Impact of AI on the World Economy.* McKinsey Global Institute, September 2018, p. 34, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
23. James Manyika and al.. *Jobs Lost, Jobs Gained: Workforce Transition in a Time of Automation,* McKinsey Global Institute, p. 11, December 2017, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi%20jobs%20lost-jobs%20gained_report_december%202017.ashx
24. Jacques Bughin and all. *Notes from the AI Frontier: Modelling the Impact of AI on the World Economy.* McKinsey Global Institute, September 2018, p. 4, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy
25. James Manyika and al.. *Jobs Lost, Jobs Gained: Workforce Transition in a Time of Automation,* McKinsey Global Institute, p. 1, December 2017, https://www.mckinsey.com/~/media/mckinsey/featured%20insights/future%20of%20organizations/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20

skills%20and%20wages/mgi%20jobs%20lost-jobs%20gained_report_december%202017.ashx

26. Kevin Drum. "Welcome to the Digital Revolution," *Foreign Affairs,* July/August 2018, https://www.foreignaffairs.com/articles/world/2018-06-14/tech-world
27. PWC. *The Potential Impact of Artificial Intelligence in the Middle East.* PwC Middle East, 2018, https://www.pwc.com/m1/en/publications/documents/economic-potential-ai-middle-east.pdf
28. IDC, "Spending on Cognitive and Artificial Intelligence Systems to Undergo Sustained Period of Growth in the Middle East and Africa, says IDC", Dubai, International Data Corporation, 24 October 2017, https://www.idc.com/getdoc.jsp?containerId=prCEMA43173217
29. Jan Peter aus dem Moore and al, *The Future of Jobs in the Middle East,* World Government Summit in collaboration with McKinsey&Company, January 2018, http://www.lsce-mena.org/uploads/resources/mckinsey-Full_Report.pdf
30. *The National*." Survey Shows 70% of GCC Youth Prefer Governmental Jobs." 12 October 2016, https://www.thenational.ae/uae/government/survey-shows-70-of-gcc-youth-prefer-government-jobs-1.162857
31. Samer Bohsali and all. *Empowering the GCC Digital Workforce: Building Adaptable Skills in the Digital Era*. Strategy and LinkedIn, Ideation Center Insight, 2017, p. 8.
32. Proceedings of the conference organized by the PfP Consortium Emerging Security Challenges Working Group and the Global Challenges Forum Foundation "Innovation in the Age of Accelerations: Global Resilience and Cyber Knowledge Networking", Manassas, VA: George Mason University, 26-27 April 2018.
33. Centre for the New Economy and Society. *The Future of Jobs Report 2018.* Cologny: World Economic Forum, 2018, p.ix.
34. Caline Malek. "The Automation Game in the Gulf…It's Time to Crack the Code," Arab News, 3 October 2018, http://www.arabnews.com/node/1381651/middle-east
35. Rasmus Gjedsso Bertelsen, Neema Noori and Jean-Marc Rickli (eds.). *Transnational Knowledge Relations for Building Knowledge-Based Societies and Economies in the Gulf.* Berlin : Gerlach Press, 2017.
36. Suparna Dutt D'Cunha, "Oil-Rich Middle East Edging into AI to Future-Proof Its Economy," Forbes, 13 March 2018, https://www.forbes.com/sites/suparnadutt/2018/03/13/how-artificial-intelligence-is-edging-its-way-in-the-oil-rich-middle-east/#3eebc05a6ed7
37. See Arabian Business."Why the UAE and Saudi See Artificial Intelligence as an Investment in the Future", 8 February 2018, https://www.arabianbusiness.com/technology/389533-why-the-uae-saudi-see-artificial-intelligence-as-an-investment-in-the-future, James Langton. "Dubai Police Considers Blimp in Fresh Strategy to Help Fight Crime Without Police Officers,"*The National,* 12 March 2018, https://www.thenational.ae/uae/government/dubai-police-considers-blimp-in-fresh-strategy-to-help-fight-crime-without-police-officers-1.712472 and MR Raghu. "How AI will Disrupt the GCC," *Gulf Business,* 8 July 2018, http://gulfbusiness.com/ai-will-disrupt-gcc/
38. Vivian Nereim and Alaa Shahine, "Saudi Arabia Crown Prince Details Plans for New City: Transcript," *Bloomberg,* 26 October 2017, https://www.bloomberg.com/news/articles/2017-10-26/saudi-arabia-crown-prince-details-plans-for-new-city-transcript
39. Al Arabiya English, "Artificial Intelligence Among the Key Topics of Saudi Crown Prince's Agenda to US," *Al Arabiya,* 26 March 2018, https://english.alarabiya.net/en/business/technology/2018/03/26/Artificial-intelligence-among-key-topics-of-Saudi-Crown-Prince-s-agenda-to-US.html
40. Quoted in Caline Malek. "The Automation Game in the Gulf…It's Time to Crack the Code," *Arab News,* 3 October 2018, http://www.arabnews.com/node/1381651/middle-east
41. UAE Government, "UAE Strategy for Artificial Intelligence", October 2017, https://government.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/uae-strategy-for-artificial-intelligence
42. World Economic Forum. *The Future of Jobs and Skills in the Middle East and North Africa*. Cologny, May 2017, http://www3.weforum.org/docs/WEF_EGW_FOJ_MENA.pdf
43. Nicholas Davis and Jean-Marc Rickli. "Submission to the Australian Council of Learned Academies and the Commonwealth Science Council on the Opportunities and Challenges Presented by the Deployment of Artificial Intelligence." Geneva, 25 July 2018.
44. Philip Chertoff. "Perils of Lethal Autonomous Weapons Systems Proliferations : Preventing Non-State Acquisition," *Geneva Center for Security Policy,* Strategic Security Analysis Paper, Issue 3, May 2018.
45. Alex Hern. Cambridge Analytica : How did it Turn Clicks into Votes ?, *The Guardian,* 6 May 2018, https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie
46. Heather Roff and Richard Moyes. "Autonomy, Robotics and Collective Systems", *Global Security Initiative,* Arizona State University, 2016, https://globalsecurity.asu.edu/robotics-autonomy
47. Paul Scharre. *Army of None: Autonomous Weapons and the Future of War.* New York, W.W. Norton and Company, 2018, p. 53.
48. Vincent Boulanin, and Maaike Verbruggen. *Mapping the Development of Autonomy in Weapons Systems.* Stockholm: Stockholm International Peace Research Institute (SIPRI), 2017, pp. 50 and 54.
49. Paul McLeary. "Pentagon's Big AI Program, Maven, Already Hunts Data in the Middle East, Africa." Breaking Defense, 1st May 2018. https://breakingdefense.com/2018/05/pentagons-big-ai-program-maven-already-hunts-data-in-middle-east-africa.
50. Kate Conger. "Google Plans Not to Renew Its Contract for Project Maven, a Controversial Pentagon Drone AI Imaging Program." *Gizmodo.com,* 1st June 2018, https://gizmodo.com/google-plans-not-to-renew-its-contract-for-project-mave-1826488620
51. Joelle Thorpe, Kimberly Girling and Alain Auger. "Future Military Dominance and Human Enhancement Strategy for Soldier Resilience," *Small War Journal,* 13 July 2017, https://www.dsiac.org/resources/news/future-military-dominance-and-human-enhancement-technology-soldier-resilience
52. Patrick Tucker. Defense Intel Chief Worried about Chinese Integration of Human and Machines, *Defence One,* 10 October 2018, https://www.defenseone.com/technology/2018/10/defense-intel-chief-worried-about-chinese-integration-human-and-machines/151904/

53. Paul Scharre P *Robotics on the Battlefield Part II: The Coming Swarm,* Washington, Center for a New American Security, October 2014.
54. Darren Weaver and Erin Black. "How Intel Made its World Record-Breaking Drone Show,"*CNBC,* 18 July 2018, https://www.cnbc.com/2018/07/17/intel-breaks-world-record-2018-drones.html
55. Jürgen Altman and Frank Sauer. Autonomous Weapons Systems and Strategic Stability. *Survival,* Vol. 59, issue 5, 2017, pp.117-142.
56. Jean-Marc Rickli. "The Impact of Autonomy and Artificial Intelligence on Strategic Stability", *UN Special,* July-August 2018, pp. 32-33, https://www.unspecial.org/2018/07/the-impact-of-autonomy-and-artificial-intelligence-on-strategic-stability/ and Jean-Marc Rickli. "The Impact of Autonomous Weapons Systems on International Security and Strategic Stability," in Ladetto, Quentin, *Defence Future Technologies: What We See on the Horizon.* Thun: Armasuisse, 2017, pp. 61-64. https://deftech.ch/What-We-See-On-The-Horizon/armasuisseW%2BT_Defence-Future-Technologies-What-We-See-On-The-Horizon-2017_HD.pdf
57. Jürgen Altman and Frank Sauer. Autonomous Weapons Systems and Strategic Stability. *Survival,* Vol. 59, issue 5, 2017, p. 126.
58. Paul Scharre. "Unleash the Swarm: the Future of Warfare," *War on the Rocks,* 4 March 2015, https://warontherocks.com/2015/03/unleash-the-swarm-the-future-of-warfare/
59. Greg Allen and Taniel Chan. "Artificial Intelligence and National Security", Cambridge: Belfer Center.for Science and International Affairs, 2017.
60. Pablo Chovil. "Air Superiority under 2000 Feet : Lessons from Waging Drone Warfare against ISIL", *War on the Rock,* 11 May 2018, https://warontherocks.com/2018/05/air-superiority-under-2000-feet-lessons-from-waging-drone-warfare-against-isil/
61. Michael Carl Haas, and Sophie-Charlotte Fischer. "The Evolution of Targeted Killing Practices: Autonomous Weapons, Future Conflict and the International Order", *Contemporary Security Policy,* Volume 38, No. 2, 2017, pp. 281-306
62. Michael Horowitz. "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review,* 15 May 2018, https://tnsr.org/2018/05/artificial-intelligence-international-competition-and-the-balance-of-power/
63. Shmuel shmuel. "The Coming Swarm Might be Dead on Arrival,"*War on the Rocks,* 10 September 2018, https://warontherocks.com/2018/09/the-coming-swarm-might-be-dead-on-arrival/
64. Sameh Aboul Enein. Cybersecurity Challenges in the Middle East, *Geneva Papers,* Geneva Centre for Security Policy, 2017.
65. James Andrew Lewis. "Cybersecurity and Stability in the Gulf", *Gulf Analysis Paper,* Washington Center for Strategic and International Studies, January 2014.
66. Elen Nakashima. "Cyberattack on Mideast Energy Firms was Biggest Yet, Panetta Says," *Washington Post,* 11 October 2012, https://www.washingtonpost.com/world/national-security/cyberattack-on-mideast-energy-firms-was-biggest-yet-panetta-says/2012/10/11/fe41a114-13db-11e2-bf18-a8a596df4bee_story.html?noredirect=on&utm_term=.eb7de19390ef
67. Nicole Perlroth and Clifford Krauss. "A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," *New York Times,* 15 March 2018, https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html
68. Khalid Al-Mezaini and Jean-Marc Rickli (eds.). *The Small Gulf States: Foreign and Security Policies Before and After The Arab Spring.* London: Routledge, 2017.
69. Nermeen Abbas. "Arab Countries Facing The Highest Number Of Cyber Attacks." *Forbes Middle East,* 28 March 2018. https://www.forbesmiddleeast.com/en/arab-countries-facing-the-highest-number-of-cyber-attacks/
70. Martin Giles. "The GANfather : The Man Who's Given Machines the Gift of Imagination," *MIT Technology Review,* 21 February 2018, https://www.technologyreview.com/s/610253/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination/
71. Marc Ph. Stoecklin. "DeepLocker: How AI Can Power a Stealthy New Breed of Malware", *Security Intelligence,* 8 August, 2018, https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/
72. Chris Bing. "The Tech Behind the DARPA Grand Challenge Winner Will Now Be Used by the Pentagon," *Cyberscoop,* 11 August 2017, https://www.cyberscoop.com/mayhem-darpa-cyber-grand-challenge-dod-voltron/
73. Adam Stone. "How DARPA Sparked Dreams of Self-Healing Networks," C4ISRNET, 26 December 2017, https://www.c4isrnet.com/it-networks/2017/12/26/how-darpa-sparked-dreams-of-self-healing-networks/
74. Alessandro Cauduro. "Live Deep Fakes – You Can Now Change Your Face to Someone Else's in Real Time Video Applications", *Medium,* 4 April 2018, https://medium.com/huia/live-deep-fakes-you-can-now-change-your-face-to-someone-elses-in-real-time-video-applications-a4727e06612f
75. Samantha Cole. "Deep Voice Software Can Clone Anyone's Voice with Just 3.7 Seconds of Audio," *Motherboard,* 7 March 2018, https://motherboard.vice.com/en_us/article/3k7mgn/baidu-deep-voice-software-can-clone-anyones-voice-with-just-37-seconds-of-audio
76. Derek Manky. Rise of the "Hivenet": Botnets that Think for Themselves,", *DARKReading,* 16 February 2018, https://www.darkreading.com/vulnerabilities---threats/rise-of-the-hivenet-botnets-that-think-for-themselves/a/d-id/1331062?
77. Andreas Krieg and Jean-Marc Rickli, "Surrogate Warfare: the Art of War in the 21st Century?," *Journal of Defence Studies*, Vol. 18, Issue 2, 2018, pp. 113-130, and Tim Maurer. *Cyber Mercenaries: The State, Hackers, and Power.* Cambridge: Cambridge University Press, 2018.
78. Bethan McKernan. "Fake News in the Middle East is a Power Keg Waiting to Blow," *The Independent,* 10 September 2017, https://www.independent.co.uk/news/world/middle-east/middle-east-fake-news-consequences-israel-saudi-arabia-syria-lebanon-hezbollah-mossad-qatar-uae-a7936621.html and Matthew Gray. "Explaining Conspiracy Theories in Modern Arab Middle Eastern Political Discourse: Some Problems and Limitations of the Litterature," Critique: *Critical Middle Eastern Studies,* Vol. 17, No. 2, pp. 155-174, Summer 2008.
79. Office for Disarmament Affairs. *Securing our Common Future: An Agenda for Disarmament.* New York: United Nations, 2018, pp. 54-55.
80. Michael Horowitz and al.. *Strategic Competition in an Era of Artificial Intelligence.* Washington, CNAS, 25 July 2018, https://www.cnas.org/publications/reports/strategic-competition-in-an-era-of-artificial-intelligence

81. Cate Cadell and Adam Jourdan. "China Aims to Become the World Leader in AI, Challenges U.S. Dominance," Reuters, 20 July 2017, https://www.reuters.com/article/us-china-ai/china-aims-to-become-world-leader-in-ai-challenges-u-s-dominance-idUSKBN1A5103
82. IEEE. *Ethically Aligned Design : a Vision Prioritising Human Well-Being with Autonomous and Intelligent Systems,* Version 2, December 2017.
83. Jean-Marc Rickli. "International Governance and The Malicious Uses of Artificial Intelligence", *Swissfuture Review,* Summer 2018, https://www.gcsp.ch/News-Knowledge/Global-insight/Malicious-Uses-of-Artificial-Intelligence-Is-it-Time-for-international-Governance
84. UN. "Secretary-General's High Level Panel on Digital Cooperation," *United Nations,* 12 July 2018, http://www.un.org/en/digital-cooperation-panel/
85. Edoardo Maggio. Putin Believes that Whatever Country has the Best AI will be the Rule of the World," *Business Insider,* 4 September 2017, http://uk.businessinsider.com/putin-believes-country-with-best-ai-ruler-of-the-world-2017-9.
86. Andreas Krieg and Jean-Marc Rickli. *Surrogate Warfare: The Transformation of War in the Twenty-First Century.* Washington: Georgetown University Press, 2019.