National Defense

Strategic Annual Journal / Issued by National Defense College/ Issue 07 – June 2020

Jamal Al Suwaidi:

The Impact of Exponential Technological Development on Terrorist Operations

The Race to Dominate Space: Should the UAE Join?

Strategic Environment Analysis Is Vital For Decision-Making & Strategy Building

Terrorists breaking UAE ‘LAWS’

National Security in the Age of Pandemic

Saud bin Saqr Al-Qasimi:

Praised the Pivotal Role played by the National Defense College as an Academic Institution

2020:

The Preparation Year for the Next 50 Years

"In the year 2020, we will cooperatively work together from all sectors, society groups, citizens, and residents. Since we are all united, we can make significant changes and we can aim higher in our aspirations".

Mohammed bin Rashid Al Maktoum

Editorial

Major General Staff Pilot
Rashad Mohamed Alsaadi
Commandant of the National
Defense College (NDC)

The United Arab Emirates approaches its Golden Jubilee celebrations of the 50th anniversary of the glorious Union, a vibrant representation of civilization in recent decades, despite the stark challenges and crises facing other countries nowadays from which recovery will be arduous. This might take years, possibly decades, especially in certain Arab countries. Our beloved country, through its wise leadership, bright vision, noble goals, great deeds, and loyal people, has sought to be a unique role model, a source of good and inspiration, and a homeland of tolerance and peace. The United Arab Emirates overcame the challenges of the past and laid down developmental and civilizational foundations for a brilliant future and clear ambitions, which keep pace with the times and aim to achieve a sustainable prosperity and well-being on the basis of our national security and legitimate vision. The best example on this positive humane leadership is the UAE's exemplary model of managing the COVID19- pandemic.

Our armed forces are a national power of great value and play a vital role in maintaining the Union and its sovereignty as well as the nation's achievements and aspirations. The armed forces also work with resolute determination to keep abreast of modern threats and challenges in order to fulfill their role to the maximum, and to strengthen their capabilities to accomplish a range of tasks and duties with the utmost efficiency; thereby ensuring victory and deterrence against all those who try to undermine our achievements, sovereignty, and capabilities. Despite the challenges posed by modern warfare in its various forms, weapons, tools and tactics, our armed forces are at high readiness to deter and confront simultaneous threats, emphasizing a strong and distinctive resolve to play a pivotal role in safeguarding international peace and regional stability.

The military education and the training system pay great attention to all levels and areas of concern, taking advantage of the significant and committed support given by the leadership, with the role of the National Service essential in complementing and strengthening the national capabilities of the state. Our National Defense College continues to move forward to realize its vision, mission, objectives, and to achieve a prominent position locally, regionally, and internationally—all thanks to Allah the Almighty, the support of our wise leadership, and our clear vision and goals. Our college has embarked on plans to achieve international recognition and attract participants from outside the country, as well as continuing to improve its quality program, which focuses on developing the critical thinking skills of the graduates who are fortified with strong will and determination to serve our blessed United Arab Emirates. They also gain advanced strategic knowledge and insights that enable them to realize their aspirations and serve the country with a common perspective and consistent concepts that have a noticeable impact on unifying their scientific capabilities to carry out their duties and innovate, while seizing opportunities to safeguard the country's national security and to face challenges effectively.

Furthermore, the NDC faculty members have a prominent role in linking academic programs to reality and managing the educational process in an interactive approach that corresponds well to the level and experience of our course participants and motivates their learning and research. These NDC success indicators have become clearer year by year as a result of the support received from the NDC Supreme Council and the GHQ UAE Armed Forces, in conjunction with the cooperation of state institutions and officials, as well as the competencies and enthusiasm of all the NDC staff. The graduates from the NDC also represent a national resource, which is of vital importance in the comprehensive national development, as their number increases annually, the bond deepens among them, and their cumulative experience keeps growing. The college continues to give attention to the graduates and encourages them to keep ahead of events and understand the causes, motives and forms of change, maintain discussion and exchange of advice, and apply the knowledge learned in the NDC course regarding strategic security studies and advanced leadership skills.

In this current issue of the NDC Journal, I would like to extend my sincere thanks and appreciation to His Highness Sheikh Saud Bin Saqr Al-Qasimi, Supreme Council Member, the Ruler of Ras Al Khaimah for his distinguished meeting with the participants of the 7th NDC Course. The meeting was marked by a valued transparency, profound thinking, and tolerance in discussing a number of national issues, which enriched the thoughts of the participants. NDC also extends its sincere thanks to His Highness Sheikh Ammar Bin Humeid Alneimi, Crown Prince of the Ajman Emirate for his warm reception of the NDC delegation and for his appreciation of the NDC role in the national qualification of leaders and the level of the NDC learning outcomes in addition to his continuous support to the college and for nominating candidates from Ajman Emirate to the NDC courses.

I would like also to extend my thanks to all those who have enriched this issue with their articles that cover important fields and provide the readers with added cultural value, diverse visions and experiences, and qualitative concepts. I would like to express my due respect and appreciation to the editorial staff for their strenuous efforts to produce the NDC Journal at the required level and in a timely manner.

Finally, indeed, it is my pleasure to congratulate the graduates of the 7th NDC Course, who have worked diligently to acquire knowledge according to the specified standards, achieve outstanding scientific and academic results, and benefit to the utmost from taking the NDC course. They have a burning passion to dedicate their skills to the service of their beloved homeland. They have firm self-confidence and a sincere belief in paying back to their country and its wise leadership when returning to their institutions armed with exceptional skills and highest quality knowledge. I wish all of them great success in achieving the very best possible outcomes for the United Arab Emirates.

Contents

30 FORECASTING THE FUTURE: MAJOR GLOBAL TRENDS

46 A Framework for Interpreting US Foreign Policy in the Gulf

50 Electricity supply security in the UAE

62 Bringing CVE 'Front and Center' in the UAE National Security Lexicon

Cover

National Defense
THE EMIRATES
Strategic Annual Journal / Issued by National Defense College/ Issue 07 – June 2020
The Race to Dominate Space: Should the UAE Join?
Strategic Environment Analysis Is Vital For Decision-Making & Strategy Building
Terrorists breaking UAE 'LAWS'
National Security in the Age of Pandemic
Jamal Al Suwaidi:
The Impact of Exponential Technological Development on Terrorist Operations
Saud bin Saqr Al-Qasimi:
Praised the Pivotal Role played by the National Defense College as an Academic Institution

Saud bin Saqr Al-Qasimi

To achieve its vision, mission, and objectives, the National Defense College has enriched the academic programs of the national defense courses with various activities that enhance the participants' strategic leadership skills and expand their strategic thinking horizons at a deeper level by not just studying academic theories.

National Defense

A Specialized Yearly Journal
on Strategic Affairs
Issued by UAE National Defense College
Established In June 2014

General supervisor
Maj. Gen. Pilot /
Rashad Mohamed Al Saadi

Editor in chief
Staff Brigadier Eng. /
Ahmed Alkhoori

Editorial Manager
Staff Lt. Colonel / Yousef Al Hadad

Sub-Editors
Sameera Naser Basaloom
Jameela Salem Alkaabi

Editorial Board
Lt. Colonel Eng. / Ibrahim Alaly
Lt. Col. Staff Dr. Salim Al Zaabi
Lt. Colonel Ali Al Mazrooei
Dr. Mohammad Bani Yonnes

Translation & Editing
Awni Al Khatib
Muhammad Elsayed
Firasse Beale

Layout & Design
Ali Al Shehhi
Ahmed Mahmoud

Photos Archive
Mohammed Ramadan
Liam Clayton

009714961221 ☎

www.ndc.ac.ae

Don’t Worry

“The UAE people›s safety is a top priority irrespective of any other considerations and indeed it is our responsibility.”

Mohamed bin Zayed Al Nahyan

Editor In Chief

Brigadier General Staff Engineer

Ahmed Al Khoury

Editor in Chief

Following the steps of the bountiful Zayed (may Allah rest his soul in peace) on his blessed journey of building and developing and to complete the UAE›s exclusive and globally admired achievements — both regional and global which have placed the UAE at the heart of global competitiveness. Having achieved a high reputation during the past 50 years, the state›s wise leadership has declared that 2020 is the Year of Preparing for the next 50 years. This preparation will be by implemented a fifty-year future for esight strategy. His Highness Sheikh Mohamed bin Zayed Al Nahyan, Crown Prince of Abu Dhabi and Deputy Supreme Commander of the UAE Armed Forces said,» With the willpower, patriotism, loyalty, and solidarity of our people, the UAE will achieve its goal of becoming one of the best countries in the world by the 2071 centennial anniversary of the UAE foundation.

The UAE has achieved a prominent status internationally and regionally by solid steps towards the desired goals following a clear vision and precise strategic plans that address the requirements of the past fifty -year phase. The future foresight has become an urgent need at the regional and international arenas being associated with challenges and opportunities within a vibrantly changing environment in terms of the political, economic, security, technical, health, and social dimensions. In response to this need, the UAE's wise leadership has declared its regionally and internationally exclusive future foresight strategy for the next phase, «Preparing for the next 50 years». This comprehensive outlook aims to achieve a sustainable quality difference at all levels and in a variety of aspects.

Today's conventional strategic plans have proved to be inflexible and incoherent in terms of addressing the requirements of sustainable future environments. On the other hand, the UAE›s strategy in managing the Covid19- pandemic reflects the high national readiness in handling new developments and challenges following a clear vision and strategic plans praised by the whole world and international organizations.

The new issue of our journal is the outcome of a full year of academic work during which participants of the seventh NDC Course have learned various types of sciences and applications in strategic and security studies. This will prepare them as future strategic leaders and ensure that they can overcome challenges and threats while having foresight strategies for future scenarios using all instruments of power to achieve the national security interests.

The journal includes a plethora of topics that tackle the current and future national security threats and challenges within the international and domestic environments. Articles here delve deep and reflect informative conclusions following common theories and practices in security and strategic studies and implementing the comprehensive instruments of national power as well as issues related to international relations, risk analysis, and strategic leadership.

As an assertion of the importance of the various current and future national-security related issues and topics addressed by the journal , His Highness Sheikh Saud bin Saqr Al-Qasimi, Member of the Supreme Council, Ruler of Ras Al Khaimah received the participants of the 7th NDC Course and had an informative discussion with them on the importance of strategic studies in identifying and analyzing challenges, threats, and opportunities, and developing plans to manage and overcome them to achieve security and stability for the homeland.

Finally, I would like to extend my thanks to all those who contributed to this journal. Thanks also go to the editorial board, hoping that we shall meet again in the coming issues that will be enriched with contributions from the faculty members and experts in the current and future topics, and Allah is the arbiter of success.

Meeting with His Highness

Saud bin Saqr Al-Qasimi: praised the pivotal role played by the National Defense College as an academic institution

To achieve its vision, mission, and objectives, the National Defense College has enriched the academic programs of the national defense courses with various activities that enhance the participants' strategic leadership skills and expand their strategic thinking horizons at a deeper level by not just studying academic theories.

In addition to the conferences and seminars conducted in this course, several visits were organized to meet with policymakers, strategists, and decision-makers within and outside the country, thereby placing the academic material in its strategic context. This is achievable by the direct communication and discussion with strategic leaders and decision-makers to give participants a real-life understanding of the strategic context and its direct impact on decision-makers. Furthermore, such meetings improve participants' academic knowledge and leadership skills in tandem with gaining practical skills.

These visits and meetings also achieve other critical objectives including promoting the role of NDC in preparing strategic leaders and instilling strategic thinking. This comes from recognizing the importance of integrating federal and local institutions in developing policies and strategies. National interests and national security are thereby achieved and promote the synergy of planning and implementation between government institutions in times of peace and crisis.

This year, NDC organized a visit for the participants to meet H.H. Sheikh Saud bin Saqr Al-Qasimi, Ruler of Ras Al Khaimah, Member of the Supreme Council, at his palace. A stimulating dialogue ensued covering strategic issues that highlighted the importance of strategic thought and its role in the progress and stability of states.

H.H. Sheikh Saud praised the pivotal role played by the National Defense College as an academic institution that contributes to highlighting and strengthening the prominent status of the UAE Armed Forces. In particular, he mentioned its leading role in preparing and qualifying strategic military and civilian leaders and developing their capabilities to identify national, regional, and international security challenges. He affirmed the need to fully understand the principles of managing the state›s resources and requirements to protect national interests. This will help build an integrated national environment in strategic planning to achieve the vision and aspirations of the country's wise leadership.

His Highness also expressed his pride in the youth of the UAE and his great confidence in their abilities to carry out the tasks and responsibilities assigned to them with a deep sense of patriotism. This embodies the UAE society›s principles of loyalty to the country and its wise leadership that spares no effort in supporting its people. Young people benefit from educational opportunities to enrich their knowledge as a critical factor in the UAE's development across all areas.

To achieve the vision of the UAE›s wise leadership and the state's aspirations in achieving its sustainable development model and dealing with regional conditions, His Highness Sheikh Saud bin Saqr Al Qasimi urged the participants of the 7th NDC Course to study diligently to make the greatest use of the course and to develop their academic and strategic skills to ensure greater security, stability, and prosperity for the nation.

At the end of the meeting, the participants expressed their thanks to His Highness for receiving them and for his dedicating his valuable time to enriching their intellectual knowledge and deepening their strategic awareness. The participants also expressed their appreciation of his trust in them and stressed their fervor to follow his guidance in supporting the country and dedicating their academic skills and abilities to proudly defend the security of their beloved homeland.

The race to dominate space: should the UAE join?

The UAE recently celebrated sending its first man into space; but the race to get to space and increasingly the race to use space technology as a tool in promoting national interests and security started sixty years ago. This article examines who are the leading actors, what technology is deployed, how this affects national interests and security, how space is increasingly deployed in hybrid warfare, and asks, "What role or strategy should the UAE adopt?"

Shaikh Sultan bin Saeed bin Mohammed Al Nahyan
Participant, UAE NDC

Early space exploration was undertaken in the late 1950s by both the United States and the USSR. The term 'space race' was coined in this context, as each country attempted to outperform the other in terms of achievement. This race was used as a proxy to demonstrate scientific excellence, power and as a 'flagship' for the supremacy of the two respective political systems.

Over the sixty years since man began space exploration, the pace of change has been relentless. Like many areas of technology, the cost of entry fell dramatically, allowing the industry to open up to commercial players and more significantly, allowing other countries to join the US and Russia in space exploration. However, with this opening up come new challenges and improvements in technology that have expanded the possible uses of space for military

and espionage purposes.

A brief overview of the main areas in which space technology is used illustrates the potential for state actors to use the technology: space-based intelligence gathering; surveillance and reconnaissance; command and control of forces worldwide; and jamming, spoofing, energy weapons and cyber space attacks.

What concerns military analysts is the possibility for adversaries or competitors, either directly or through a proxy, to gather intelligence or inflict serious harm. This can happen on a large scale and in a way that is relatively easy to implement, but where detection and identification can be difficult. Space is quickly becoming a key component in hybrid warfare; as noted by Dr. Patrick J. Cullen and Erik Reichborn-Kjennerud in 2017. Hybrid warfare – conducted by state or non-state actors – is typically tailored to remain below obvious detection and response thresholds, and often relies on the speed, volume and ubiquity of digital technology that characterizes the present information age. The integration of space and cyber domain causes security risks that are not restricted to military installations, everyday activities include: weather forecasting, navigation, time stamping of ATM transactions, mobile communication, and theft of personal data.

It is the threat to a nation's military and security infrastructure that most concerns military strategists; examples of which include: disruption to battle field communications, intelligence surveillance, missile warning systems, position navigation and timing; satellite command and control, and space launches. As nations become more sophisticated in their use of space technology, there is a fear that one state could develop and use the capability to launch a weapon, either into space towards another satellite or to attack a ground target.

Actions of this nature could cripple a state's ability to detect an attack, or control and communicate with its force should it need to defend itself. The US Defence Intelligence Agency noted in their report "Challenges to Security in Space" published in January 2019, that early on, the world was alert to the potential threat, and drew up a treaty to limit such actions: the 1967 "Outer Space Treaty" bans the stationing of weapons of mass destruction (WMD) in outer space, prohibits military activities on celestial bodies, and details legally binding rules governing the peaceful exploration and use of space. 109 countries are parties to the treaty, while another 23 have signed but not yet ratified. The treaty, however, does not prohibit the launching of ballistic missiles, which could be armed with WMD warheads. The treaty repeatedly emphasizes that space is to be used for peaceful purposes, leading some analysts to conclude that the treaty could broadly be interpreted as prohibiting all types of weapons systems, not just WMD, in outer space.

There is increasing concern about security in space and the UN is moving towards recognizing the reality of advancement in space technology and the recognition that space is a warfighting domain. NATO already announced it considers space a "warfighting domain" at the NATO Leaders Summit, held in London 3-4 December 2019. Kyle Mizokami believes the landmark announcement cemented the notion that, like the air, land, and sea domains, space is a potential battlefield whose control is vital in a future conflict.

Of particular interest for the UAE is the emergence of Iran as a space actor. In April 2019 the Centre for Strategic and International Studies published "Space Threat Assessment 2019" and noted that although Iran is still growing their space industry, there have been developments in recent years, the authors note: "The U.S. intelligence community has concluded that

Iran's continued work to develop space launch vehicles will shorten the timeline to create a successful ICBM since the two systems use similar technologies;" and "Iran has an extensive record of using electronic forms of attack against space systems, including uplink jamming, downlink jamming, and spoofing." Such capability, from a country that is a clear threat to the GCC region, should be of concern to the UAE.

Without appropriate strategies in place, our national interests are likely to be severely damaged by the type of attack or disruption caused by a foreign aggressor using space technology. Given that countries such as Iran are developing such capability, it is imperative that we continue to be an investor in space technology, develop our human capital and enter into partnerships with leading countries such as the US. By developing such a capability, we are contributing to regional peace – our ability to react is a deterrent to Iran.

The UAE has made significant progress in developing its space industry, most recently demonstrated by being the first Arab country to send a man into the International Space Station (ISS) and the first Arab country to have a sustainable astronaut program. What is most important now is for the country to continue to invest and develop expertise to serve the interests of the state.

There are further benefits associated with investing in space. It creates a favourable and positive image for the country and places us in a select group of nations who have acquired the required technical knowledge and expertise. Furthermore, it boosts national morale, encouraging our youth to explore career options in STEM (Science, Technology, Engineering, Math). It also supports cooperation in space with other space-faring nations, enabling knowledge transfer. Finally, it stimulates demand and creates opportunities for the economy in terms of the supply chain and possible spin-offs from the R&D oriented towards space exploration.

Without appropriate strategies in place, national interests are likely to be severely damaged

References

1. Defense Intelligence Agency "Challenges to Security in Space" January 2019
2. www.dia.mil/Military-Power-Publications
3. https://aerospace.csis.org/aerospace101/counterspace-weapons-101/
4. https://www.gps.gov/governance/agencies/homeland/
5. https://techcrunch.com/2018/12/21/the-gps-wars-have-begun/
6. https://asia.nikkei.com/Business/China-tech/China-s-version-of-GPS-now-has-more-satellites-than-US-original
7. http://theconversation.com/space-may-soon-become-a-war-zone-heres-how-that-would-work-125460
8. https://thespacereview.com/article/574/1
9. https://www.unoosa.org/documents/pdf/spacelaw/treatystatus/AC105_C2_2019_CRP03E.pdf
10. Kyle. Mizokami: https://www.popularmechanics.com/military/a29566355/nato-space-war/
11. https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf
12. https://www.newamerica.org/international-security/reports/twenty-first-century-proxy-warfare/
13. https://www.technologyreview.com/s/613749/satellite-space-wars/
14. https://www.theatlantic.com/international/archive/2012/10/syrias-digital-proxy-war/264309/
15. https://www.csis.org/war-by-proxy

The Impact of Exponential Technological Development on Terrorist Operations

The United Arab Emirates is making great strides toward utilizing ever more sophisticated technology to protect the nation and its resources, as a deterrent to those who seek to undermine its successive achievements. The UAE's success in tailoring smart technologies to bolster national security and combat extremism and terrorism has made it a role model for many countries. However, despite the potential of modern technology to make our lives easier, it has also consistently been misappropriated to support terrorist activities, irrespective of their ideologies and beliefs. First of all, we must acknowledge that terrorists

H.E. Minister Prof. Jamal Sanad Al-Suwaidi
Deputy Chairman of the Board of Trustees of the Emirates Centre for Strategic Studies and Research

have managed to abuse technological progress, to give momentum to their operations. This ranges from propaganda, recruitment, coordination, and funding, to inciting violence, identifying targets, preparing for attacks and communicating with agents on the ground, even at a time where all activities have come under surveillance and control. These activities are most apparent in terrorists' exploitation of virtual spaces on the Internet, such as social media, instant messaging applications and Virtual Private Networks (VPNs). Recent examples show that the Islamic State in Iraq and Syria (Da'esh) has managed to broadcast its operations on social media platforms via high definition cameras connected with drones, while in New Zealand last year a right-wing extremist made a live broadcast on Facebook of his shooting attacks at two mosques in Christchurch. In both of these

examples, technology provided terrorists with global channels to achieve their goals of propaganda and recruitment.

The latest indications suggest terrorists are now expanding their efforts to possess technological capabilities that enable them to deliver cyber-attacks against digital infrastructure. A recent security study concluded that terrorist organizations have been able to acquire malware and other advanced digital systems for launching cyber-attacks. These digital weapons were purchased on the black market or dark web, specifically through the so-called Cybercrime-as-a-Service, which any organization can use to purchase or even lease technology devices to carry out criminal activity. Although there is a consensus among security experts that terrorists are unlikely to have the ability to inflict significant damage to vital infrastructure in the immediate future, smaller-scale attacks, such as the use of Ransomware, have seen service sectors such as healthcare, telecommunications, transport, and energy suffering huge financial losses as well as leaving a psychological impact on individuals and societies.

The dark web is part of the Internet but is not accessible through search engines like Google. To access it, one needs to use special software that hides the user's identity. Indications show that terrorists turned to the dark web to create promotional and financial websites with violent and extremist content. Unlike normal websites, it is very difficult to stop websites on the dark web due to their hidden, generally dispersed and unregulated nature. While countries have intensified their efforts to intercept and suspend terrorist communications, and remove extremist content on the Internet, the dark web remains a challenge that should be taken seriously, especially when it is relatively easy for terrorist organizations to use it beyond government control. It is worth noting that many of these websites on the dark web are simply that discuss various areas of interest that may not necessarily be nefarious in nature. However, because information about these sites remains unknown out of a desire for absolute privacy, these websites may serve extremist movements in promoting their ideologies.

It seems that terrorists' use of technology has also extended to the world of cod-

ed currencies, such as bitcoin. Although they came late to the sector, after other criminals who were attracted by the advantages of digital currencies for the drug trade and money laundering, terrorists have made huge progress in developing fully controlled digital portfolios and exploiting coded currencies in their fundraising campaigns, beyond the reach of conventional financial systems and institutions tracking terrorism. Although individual donations to terrorism via coded currencies remain limited, we should not forget that funding can come from anywhere in the world in this manner and terrorists do not need huge budgets to achieve their goals.

Individual donations to terrorism via coded currencies remain limited

There is yet more progress being made by terrorists in the use of drones as part of their operations. The success of Da'esh in using drones, in which they have become major global consumers of the technology, to carry out airstrikes and surveillance operations marked the emergence of a new threat to infrastructure and society. Similarly, other groups have tried to use drones in their terrorist activities. The most recent use of drones and cruise missiles was by Houthi rebels in Yemen, and groups loyal to Iran in southern Iraq, against oil facilities in the Kingdom of Saudi Arabia in September 2019. The use of these technologies suggests that terrorists intend to innovate and use smarter iterations of them. They endeavour to abuse exponential development in artificial intelligence and use it to automate drones and make them more effective in identifying their targets. It is worth noting that modern versions of these aircraft already have some basic forms of artificial intelligence. However, technology is advancing rapidly, with artificial intelligence research carried out by private companies set to make its way into open markets for future commercial applications. This will make

it difficult to contain or prevent the spread of smart drones and their use by terrorists.

It is difficult to contain or prevent the spread of smart drones and their use by terrorists

Another dangerous aspect of terrorist adaptation of technology is in 3D printing. This will enable the manufacturing of weapons with 3D printers. A member of the Neo-Nazis in Germany attacked a synagogue in October 2019 using a gun, parts of which were produced by a 3D printer using computer models downloaded from the Internet. This is an example of a serious new threat, especially in countries with strict policies on arms possession. With the growing quality and accessibility of 3D printers, it is likely that terrorists' effectiveness in creating their own weapons and ammunition with these technologies will increase in the future.

Technology plays a significant role in supporting terrorists' agendas then, but at the same time, it provides defense solutions as key foundations of national security systems and protection measures. In this context, the United Arab Emirates is adopting machine learning and artificial intelligence to improve its accessibility to digital information, collect electronic evidence, and identify and block extremist content on the Internet. In addition, there is a need to build automated capabilities to track and intercept drones. There is another trend that lies in the transformation towards smart technologies, which promote government practices in combating terror funding. Although technology solutions require huge investments, they have become inevitable for a safer future. In conclusion, it must be stressed that international cooperation in this field is of paramount importance for the United Arab Emirates. When using these different technologies, terrorists know no geography and do not distinguish between nationalities.

Terrorists breaking UAE ‘LAWS’

The danger of non-state actors making use of the availability of drones in terrorist acts to undermine the UAE national security is high. In the past, due to aerial drone system complexity and its high expense of operation, their use was confined to governmental entities in support of executing their services to the people of the UAE. Recently drones have made their way to individuals for use in sports and recreation. These are so widespread that some drones are used in dangerous areas. Dubai International Airport had its share of these drone incidents. There have been incidents where a couple of drones caused the shutdown of the airport; the last one being in September 2019.

Col. Staff Eng. Salem Butti Al Qubaisi
Participant, UAE NDC

The airport had to close its airspace for 15 minutes and divert two international inbound flights to other airports (The National 2019). Now had these drones been armed and under the control of a malevolent person, then the harm would have been much greater.

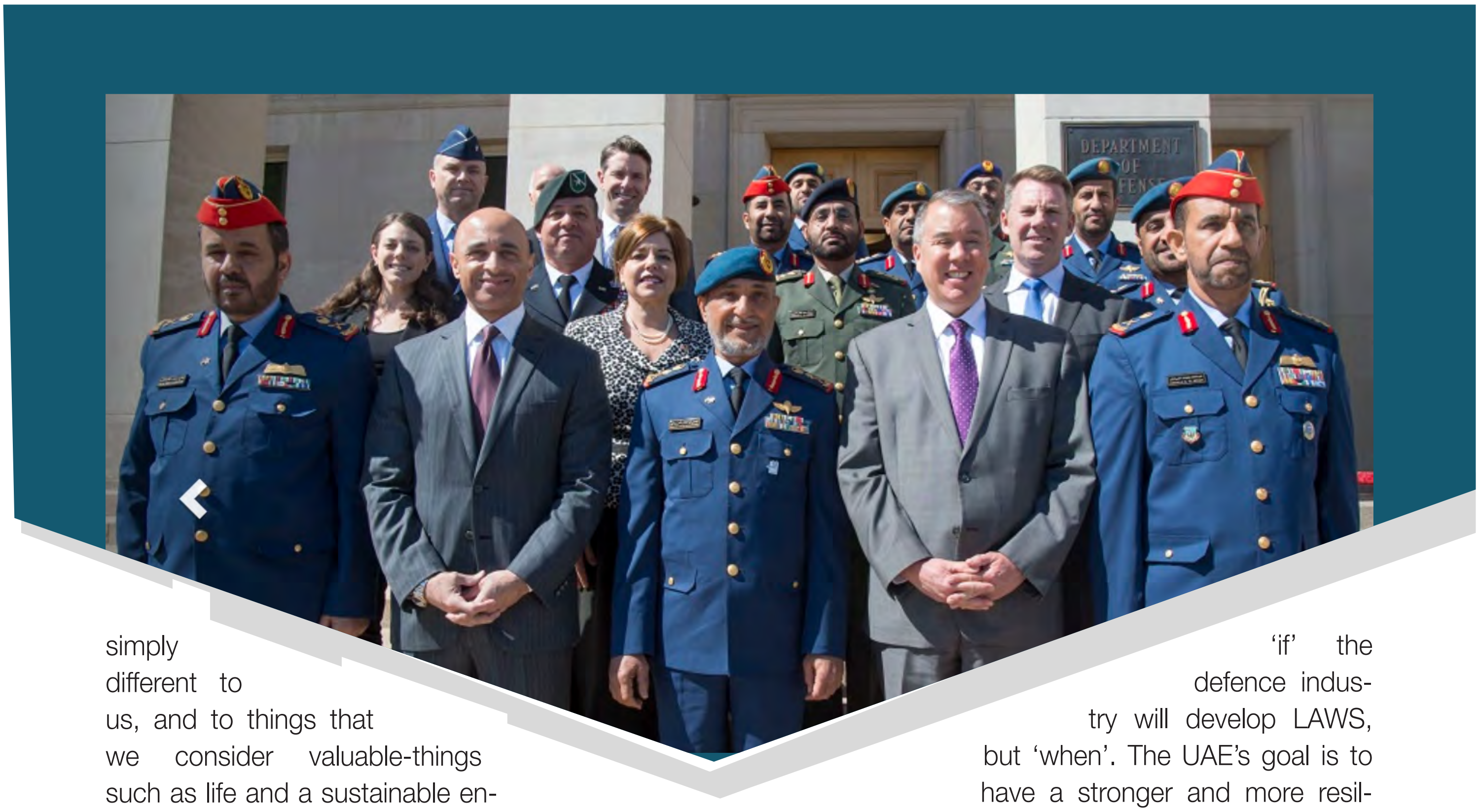
Technological leaps have made aerial drones commercially available to the public with complexity and power that surpasses the ones from the past. The same conceivably might happen using Lethal Autonomous Weapon Systems (LAWS). In simple terms, LAWS are drone systems augmented with Artificial Intelligence that will result in the overly simplified term—’Killer Robots’. Therefore, the consequences of terrorists’ attacks using LAWS could be catastrophic to state security. The surgical precision, high adaptability, and continuous persistence of LAWS makes countering them far

greater of a challenge compared to conventional drones. With the multiple initiatives of the UAE federal government the natural focus of increasing defense companies in the UAE is in the development of products pertaining to LAWS technology. Before it is too late, a policy to constitute a framework for the control of LAWS sensitive technology information in the UAE is direly in need.

The US government definition of Autonomous Weapon Systems is, "A weapon system that, once activated can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation" (UNIDIR 2017). Considering this definition and the products currently produced by the UAE defense industry, one can deduce that some, if not many, fit the definition and the others may easily become so, with the correct technology modifications available. Thus, UN research has concluded that, "With smaller and more efficient systems there lies an ability for such systems to proliferate to individual actors or groups with malicious intent, such as terrorists" (UNIDIR 2017).

Armed drones are widely in use by military all over the world. As reported in 2006, "South Korea announced plans to install Samsung Techwin SGR-A1 sentry robots along the Demilitarized Zone with North Korea. Armed with machine guns, they are capable of fully autonomous tracking and targeting, although human approval is reportedly required before they fire" (Mccormick and Simpson 2014).

What if this human approval was absent? Then the world would be at the mercy of an intelligence that is not bound by ethics or morals as humans. A Cambridge University researcher concluded that, "We risk yielding control over the planet to intelligences that are



simply different to us, and to things that we consider valuable-things such as life and a sustainable environment" (Mccormick and Simpson 2014). This has raised the concern of many intellectuals and subject matter experts which has led to calls for, "A universal framework that governs both [LAWS & drones] technologies – such as an international convention – is the most appropriate approach" (Foster and Haden-Pawlowski 2015).

Focusing on the UAE, the Ministry of Foreign Affairs and the Future have stated in a report titled 100 Trends of the Future that, "New technologies will change warfare and security priorities significantly. It will enable single citizens and amorphous networks to potentially wreak global havoc" (MoCAF 2017). The question that needs attention is "Where are UAE industries heading vis-à-vis LAWS?

The UAE Vision 2021 clearly focuses on innovation and competitiveness and it is foreseen as the main drivers for the UAE economy in the future (MoCAF 2018). This led to the formation of a new Cabinet for Artificial Intelligence Affairs with a specific strategy supported by a dedicated academic organization to spearhead the national program. The UAE Vision resonates in each emirate too, as found in the Abu Dhabi Economic Vision 2030 that states that specifically the defense sector along with others, "Are expected to provide the growth that will be necessary to achieve the Emirate's agenda of economic diversification" (Government of Abu Dhabi 2008).

With the previous strategies in mind, the question becomes not 'if' the defence industry will develop LAWS, but 'when'. The UAE's goal is to have a stronger and more resilient economy based on economic diversification to facilitate the strengthening of other UAE instruments of power.

New technologies will change warfare and security priorities significantly

The earlier mentioned international framework needs time before its conception. While many states have committed to the cause of banning the use of LAWS and are actively participating in a dedicated UN working group, larger states with clear LAWS development programs, are participating to tailor the proceedings of the working group to better suit their respective national interests.

Many states with advanced defense industries have specific frameworks to accomplish the goal of protecting sensitive technology information. This is based on regulations that the state imposes on its defense sector companies. For the US, the International Traffic in Arms (ITAR) is enforced for the purpose of export control framework to stop any US-controlled defense technologies from getting to their adversaries. The leading department on the ITAR program are the Departments of State and Commerce where the concerned directorates, “As a general rule tend toward broad restrictions … due to national security and foreign policy concerns” (US Commitee on Homeland Security and Governmental Affairs 2008). As stated, the general rule is restriction of export of controlled items, rightly so because the national interest is at stake. Similarly, the UAE has an export control regime that involves several government entities. Federal law by decree number 17 of 2019 article 3 restricts any activities pertaining to weapons, ammunition, explosives and military equipment without a permit from the licensing authority (Ministry of Justice 2019). The licensing authority involves the Ministries of Foreign Affairs and International Cooperation, Defense, Economy, Interior and other federal authorities.

Furthermore, the UAE MoD is collaborating with US MoD Defence Technology Security Administration (DTSA) to enhance its controls on defence companies export controls and technology security — as initiated in April 2019 (DTSA Webpage 2020). DTSA’s strategic goal behind this collaboration is embedded in its Strategic Plan where it states the need, “[To] cooperate with U.S. Allies and partners as they build their capability to protect advanced technology and critical information” (DTSA 2013). This collaboration is envisaged to shape the UAE MoD Defence Industry strategy with a clear focus on protecting UAE future ‘LAWS’ from falling into the hands of terrorists.

References

1. DTSA. 2013. DTSA Strategic Plan 2013. Official, Alexandria: Defence Technology Security Administration.
2. DTSA Webpage. 2020. Defence Technology Security Administration. 01 01. Accessed 01 29, 2020. https://www.dtsa.mil/SitePages/default.aspx.
3. Foster, Melisa , and Virgil Haden-Pawlowski. 2015. “Regulation Robocop: The Need for International Governance Innovation in Drone and LAWS Development and Use.” Security and Peace (Nomos Verlagsgesellschaft mbH) 33 (2): 61-66. Accessed 01 05, 2020. https://www.jstor.org/stable/10.2307/26427116.
4. Government of Abu Dhabi. 2008. The Abu Dhabi Economic Vision 2030. Official, Abu Dhabi: Government of Abu Dhabi.
5. Gray, Collin S. 2014. Defence Planning for National Security: Navigation Aids for the Mystery Tour. Carlisle Barracks, PA: United States Army War College Press.
6. Kreig, Andeas, and Jean-Marc Rickli. 2019. Surrogate Warfare: the transformation of war in the twenty-first century. Washington DC: Georgetown University Press.
7. Mccormick, Ty, and Jameson Simpson. 2014. “ANTHROPOLOGY OF AN IDEA: LETHAL AUTONOMY.” Foreign Policy 18-19.
8. Ministry of Justice. 2019. Federal Law by Decree Number 14 Regarding Weapons, Ammunition, Explosives, Military Equipment and Hazardous Materials. Abu Dhabi: Ministry of Justice.
9. MoCAF. 2017. Future Outlook: 100 Global Trends of 2030. Official Document, Dubai: UAE Ministry of Cabinet Affairs and the Future, 108.
10. MoCAF. 2018. UAE Vision 2021. Official Document, Dubai: Ministry of Cabinet Affairs and the Future. Accessed 01 05, 2020. https://www.vision2021.ae/en/.
11. Scharre, Paul. 2018. Army of None: Autonomous Weapons and the Future of War. New York: Norton & Company.
12. The National. 2019. The National. 22 09. Accessed 01 27, 2020. https://www.thenational.ae/uae/transport/two-flights-diverted-as-suspected-drone-spotted-near-dubai-international-airport-1.913502.
13. UAE Government Portal. 2016. UAE Government Portal. 01 01. Accessed 01 29, 2020. https://government.ae/en#/.
14. UNIDIR. 2017. “The Weaponization of Increasingly Autonomous Technologies: Concerns, Characteristics and Definitional Approaches a primer.” The United Nations Institute for Disarmament Research UNIDIR Resources 5.
15. US Commitee on Homeland Security and Governmental Affairs. 2008. Beyond Control: Reforming Export Licensing Agencies for National Security and Economic Interest. Official, Washington DC: US Government Printing Office, 84 - 85.

National Security in the Age of Pandemic

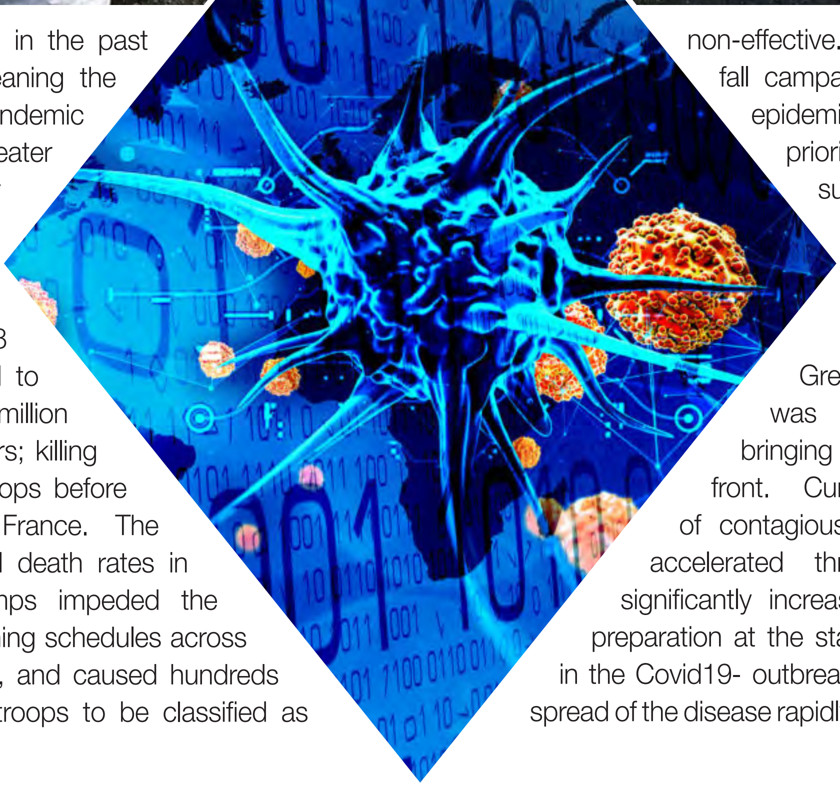
Annually at the National Defense College we poll new participants, as part of our curriculum, on the major threats that they perceive towards the United Arab Emirates. Typical responses include terrorism, oil price shocks, or the malevolent behavior of Iran and its proxies. Rarely does a participant perceive disease as a threat to the safety of UAE citizens and residents, largely due to the excellent in-country health care. The recent outbreak of a novel coronavirus, designated by the World Health Organization as SARS-CoV2- or Covid19-, highlights important national security implications for effectively handling a pandemic crisis. This purpose of this paper is to explore the national security implications of pandemic disease in a highly globalized world and offer policy guidance based on the cases reviewed.

Daniel Baltrusaitis, Ph.D.
Dean of the National Defense College

Pandemic as a National Security Concern

The unexpected influence of plague and disease has been an intermittent security threat over the course of human history. Plague has been known to change the course of wars and governments. Athenian historian Thucydides highlights how plague changed the course of the Second Peloponnesian War. In the early stages of this famous ancient war, a massive plague struck within the walls of Athens while the city was then under siege by Sparta. Over a period of three years most of the population was infected, killing 75,000 to 100,000 people, roughly %25 of the city-state's population. More importantly, the Athenian leader and strategist Pericles died during the plague, which forever changed the strategy of the war. This critical event was instrumental in eventually leading to Athens defeat (Littman, 2009).

Sadly, pandemics such as the plague seen in ancient Athens, are a regular occurrence throughout human history. According to the World Health Organization, three pandemics have emerged per century on average since the 16th century. These pandemics typically occur at 10 to -50year intervals with the most recent flu pandemics in 1957 ,1918, and 1968 (Kilbourne, 2006). Even more sobering is the emergence of new disease, with more than 300 new animal-borne



diseases emerging in the past seventy years, meaning the probability for pandemic is becoming greater (Caballero-Anthony and Balen, 2009). Significantly, the Spanish Flu pandemic of -1918 1919 is estimated to have killed 50 million people in two years; killing almost 30,000 troops before they even got to France. The high infection and death rates in U.S. military camps impeded the induction and training schedules across the United States, and caused hundreds of thousands of troops to be classified as non-effective. Throughout the fall campaigns of 1918, the epidemic made generals prioritize care and support of sick troops over battle with the enemy (Byerly, 2010).

During the Great War the disease was spread by ships bringing troops to the war front. Currently, the spread of contagious disease can be accelerated through air travel, significantly increasing the need for preparation at the state level. As seen in the Covid19- outbreak, the uncontrolled spread of the disease rapidly disrupted hospital

and health care systems while causing devastation to the economy. Although health experts do not consider it feasible to completely halt the spread of a pandemic disease, advanced preparation and planning are necessary to minimize its consequences (WHO, 2005). Just as nations prepare for military conflict to meet the national interest, so too nations should prepare for pandemic disease in the same manner. Similar to the 'whole of government' approach to prosecuting war, defeating 'the flu' becomes the central focus for government in the middle of a pandemic. The security and well-being of the population becomes a national priority (Enemark, 2006).

Pandemic disease has the potential to destabilize governments and cause social unrest. As seen in past pandemics, national populations panic in the face of a fast-spreading, invisible disease, stressing the social contract between the population and its government. During the 2003 SARS outbreak, riots erupted in parts of China on rumors of government plans for forced isolation of SARS patients (Enemark, 2006). Pandemic response, or the lack thereof, stress weak governments by amplifying existing political fault lines. Imposition of quarantines and curfews by security forces are often viewed with suspicion by the public and opposition political leaders. The imposition of restrictive security measures often leads directly to riots and violent clashes with state security forces (Madhav, et. al., 2017)

Responding to a Pandemic

Because of the complexity and unforeseeable probability of a pandemic response, most national plans are incomplete or insufficiently funded. While war or military response fall clearly under a single authority, responsibility for preparing for, and implementing national pandemic response plans is typically spread across multiple agencies which have complementary and in many cases, overlapping roles.

The governance and control of pandemic preparedness and response is a complex issue, with authority fragmented across multiple organizations internationally, regionally, and nationally (Madev, et. al., 2017). Pandemic preparedness requires close coordination across public and private sector actors; much like war planning, successful pandemic planning requires a careful outline of command and control authorities. The World Health Organization emphasizes the importance of clear response authority at the national level, "In order to be able to make clear and timely decisions and to have a uniform policy that is endorsed by all officials, it is essential to know who is in charge of different activities within communicable disease control, and how that might change if a limited outbreak becomes a major emergency" (WHO, 2005).

Unfortunately, pandemic planning is often secondary to traditional security planning pursuits, leaving national plans deficient. The findings of a regional conference on Pandemic Preparedness in Asia indicates that pandemic planning and preparedness in most, if not all, countries remain insufficient to respond to the problem. The response to the recent Covid2019-pandemic shows that national plans are still inadequate. States lack the resolve to stockpile essential medical protective equipment and devices necessary for a pandemic response. Current national plans remain reactive rather than premeditated because pandemics are often seen as a medical rather than a national security concern (Caballero-Anthony and Balen, 2009).

Pandemic Response as a National Security Priority

Studies suggest that a pandemic can have as significant an impact on the health and security of a nation as that of being at war. If a significant portion of the population is sick, essential services will be seriously downgraded, affecting the ability of the government to provide for a functioning society. The current Covid19- outbreak demonstrates how the breakdown of social structures can affect the stability and security of a nation-state.

At the national level, preparing for a pandemic response competes for limited national resources with other national priorities such as national defense or education. Whole of government approaches are necessary to promote cooperation between government agencies as well as the policy, academic, and civil society communities to generate comprehensive and cost-efficient strategies (Caballero-Anthony and Balen, 2009). Given the magnitude and seriousness of the challenge, states should consider pandemic preparation as important as preparation for war.

Preparing for a pandemic response competes for limited national resources with other national priorities

References

1. Byerly, Carol R., "The U.S. Military and the Influenza Pandemic of 1919–1918." Public Health Reports. 125 ;2010(Suppl 91–82 :(3.
2. Caballero-Anthony, Mely, and Balen, Julie, "Introduction – The State of Pandemic Preparedness in Southeast Asia, Challenges and the Way Forward." In Caballero-Anthony, Mely. Pandemic Preparedness in Asia. (2009) S. Rajaratnam School of International Studies: 7-1.
3. Enemark, Christian, "Pandemic Influenza and National Security." Australian Defense Force Journal. July/Aug 32-18:(171) 2006.
4. Holmes, Frederick MD, The Influenza Pandemic and The War. (2019) University of Kansas School of Medicine. Available at http://www.kumc.edu/wwi/medicine/influenza.html.
5. Kilbourne ED, Influenza pandemics of the 20th century. Emerging Infectious Disease. 2006 Jan;:(1)12 14-9.
6. Littman RJ, The plague of Athens: epidemiology and paleopathology. Mount Sinai Journal of Medicine. 2009 Oct; 67-456:(5)76.
7. Madov, Nita, et. al., "Pandemics: Risks, Impacts, and Mitigation." In Jamison DT, Gelband H, Horton S, et al., editors. Disease Control Priorities: Improving Health and Reducing Poverty. 3rd edition. Washington (DC): The International Bank for Reconstruction and Development / The World Bank; 2017 Nov 346-315 :27.
8. World Health Organization. WHO Checklist for Influenza Pandemic Preparedness Planning. 29-1 :2005.

Autonomous Weapons and the Key Ethical Questions: A Few Observations

Over the last three generations, unforeseen and unparalleled advances in engineering and especially in computing, have entirely transformed the lives of most humans and there is no likelihood that the constantly-accelerating speed of technological development will decrease, much less stop. For most of the last fifty years, the speed of computer processors, or their overall processing power, has doubled every two years or so.

Professor Joel Hayward
Faculty, UAE NDC

This has enabled the creation and employment by militaries of weapons that act upon decisions made largely or fully by 'artificial intelligence'; this is, by computers without much or any human decision-making. This article will try to highlight some of the ethical implications of employing autonomous weapons, an issue considered important not only by philosophers and other academics, but also by policy-makers and 'users'.

We should not be surprised that artificial intelligence has entered the military sphere, which has always been profoundly shaped by emerging technologies and which has, during peacetime but especially during wartime, included a ubiquitous demand for constantly more effective weapons. For many decades certain weapons have included an element of autonomy. Land mines, for example, work with an automatic mechanical response

to pressure that involves no human agency. If a vehicle or person places sufficient weight upon the mine, it will explode with no human operator making it do so. But this is very far from the sophisticated and highly legal autonomous weapons now available to the world's militaries – weapons intended for both defense and offense.

No one will contest the moral right of military personnel to protect themselves or civilians by using defensive weapons which will react to enemy stimuli according to pre-programmed commands by an operator who does not play a role in the weapon's operation once the weapon itself detects the imminent threat. Autonomous Gatling guns on a ship, for example, can be pre-programmed to fire against an incoming missile that human operators might be slower to identify and respond to than the speed of the machine's own computer. Likewise, a number of states rely on autonomous missile defensive systems to provide a protective umbrella from neighboring states with threatening missile capabilities. Neither case violates the basic human right to self-defense nor any existing international humanitarian law.

Offensive autonomous weapons, on the other hand, have garnered significant controversy, with greatest concern expressed at the prospect of fully autonomous machines causing the deaths of humans without a human operator making the actual decision to take life [1]. By fully autonomous, one means something different to a drone, which is remote-controlled by an operator even if that operator is thousands of miles away from the weapon. Instead we mean a weapon that has been pre-programmed but which operates self-sufficiently according to its own artificial intelligence. Because such artificial intelligence is essentially pre-programmed algorithms, critics allege that it will be mistake-prone, incapable of nuance, and entirely lacking the human judgment that would make actions accountable to laws and norms; that is, make them 'moral'. Critics further assert that fully autonomous offensive weapons are, without the humane desire of 'in-the-loop' operators to minimize harm to non-combatants, likely to cause non-compliance with human rights and international

humanitarian law [2].

It is a weak argument that autonomous machines will, ipso facto, be less likely than humans to comply with international humanitarian or human rights laws or with the Laws of Armed Conflict. This would require one to believe two unproven assumptions: firstly, that human decision-making on issues pertaining to the identification and non-targeting of non-combatants cannot be replicated by computers, at least in real-time, and secondly, that human warfighters themselves have a proven record of correctly identifying and not targeting or harming non-combatants. How the first assumption could be ever tested and verified through experiment or actual wartime observation has never been stated by critics, and we know from history that the second assumption has already been disproven. Warfighters have frequently been unable to identify non-combatants and ensure that no harm would befall them. Large-scale non-combatant fatalities and maiming remain a persistent feature of warfare. Indeed, we find too many established cases of combatants accidentally killing or wounding non-combatants because of the former's poor judgment or deliberately harming non-combatants because of their innate inhumanity or temporary bloodlust. Advocates of autonomous weapons would argue that their machines cannot experience or operate with anger, hatred or a desire for vengeance.

Al least for the present, the question of whether an autonomous weapon or system can evaluate the proportionality (meaning the appropriateness of scale) of any offensive operation is ethically interesting but a moot point. Proportionality is seldom determined by combatants during military operations. It is established earlier and monitored throughout by senior planners, including lawyers and other civilians, and no one is suggesting that weapons systems, let alone autonomous ones, will themselves assume responsibility for the establishment and maintenance of proportionality.

The question of accountability is also relatively straightforward. According to existing law, states are accountable for the conduct and misconduct of their militaries and the use and misuse of any weapons that they employ. Liability for the misuse or imperfect performance of weapons is not transferable to programmers or manufacturers. It is true that an autonomous weapon might cause an effect that was neither foreseen nor wanted by the state, but that would not absolve the state of responsibility any more than an unforeseen or unintended war crime committed by human warfighters would.

The only meaningful ethical dilemma perhaps relates to whether it is reasonable and moral to leave a decision over the life and death of humans to a machine. The human desire to stay in control of technology and the media-generated 'terminator'-type threat of robots killing people have created a widespread belief that autonomous weapons are not human and are therefore not humane. According to one article which expresses this fear of inhumanity, "Algorithms would create a perfect killing machine, stripped of the empathy, conscience, or emotion that might hold a human soldier back [3]." Yet this ignores the fact that autonomous weapons are purposefully created by humans for specific functions and programmed by them to perform desired specific tasks. They are not created (at least not yet) with the capacity to function outside of, or to choose to reject or modify, their programming. There is little difference between a weapon with an operator within the kill decision and one with no operator so long as the killing itself is conceived and intended as a moral act.

Large-scale non-combatant fatalities and maiming remain a persistent feature of warfare

To offer some concluding remarks, this article has argued that, at least for the time being, there is little of moral concern in the development of autonomous weapons, which, while not having a human operator in the decision-cycle during the performance of their functions, are designed to undertake only tasks programmed into them via complex algorithms that to all intents mimic the human mind. So long as the weapons function as programmed, and they are used for tasks that states conceive and intend to comply with international law, the worst they might do is to rob warfare of some of the glory that human courage and self-sacrifice might seem occasionally to bestow upon it.

References

1. Alex Leveringhaus, Ethics and Autonomous Weapons (Oxford: Palgrave Macmillan, 2016).
2. International Committee of the Red Cross, Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centred Approach (Geneva, 6 June 2019), p. 2.
3. "Fully Autonomous Weapons", Reaching Critical Will, undated, accessed at: http://www.reachingcriticalwill.org/resources/fact-sheets/critical-issues/-7972fully-autonomous-weapons.

FORECASTING THE FUTURE: MAJOR GLOBAL TRENDS

The problem with forecasting the future of world politics is that human nature and behavior are difficult to predict. What is rational, say from Khamenei's or Xi Jinping's or Kim Jong-un's perspective, may seem completely irrational to others. Still, policymakers, economists in particular, always talk about rationality or the rational actor model in policy making. However, historians never do that. Why? Because when historians look back into history, they encounter nothing but sheer foolishness, or complete irrationality in policy making (think of Hitler's attack on the Soviet Union when he had the whole of Europe under his thumb or Japan's attack on Pearl Harbor or Saddam Hussein's invasion of Kuwait).

Professor Mohan Malik, Ph.D.
Faculty, UAE NDC

International Relations textbooks teach us that foreign policy is a cold calculation of costs and benefits. In reality, foreign policy is a mix of "5 Ps": passion (ideology), power, profit, pride and prejudice. Forecasting the future of world politics is difficult because there are too many forces at work at any given time. We need a multi-disciplinary approach. But we all have our blind spots. We are either economists or historians or demographers or scientists and we do not talk to each other. Nonetheless, for long-term planning purposes, policymakers must have some sense of the future from a holistic perspective.

In this context, trend analysis is very popular, even though it is wrong to extrapolate the future from trends. Based on economic trends in 1949, a World Bank study predicted three Asian countries (Burma, India and the Philippines) would be economic powerhouses by 1979. Not Japan or South Korea. Likewise,

a(bc) = (ab)c
a+b = b+a
a(b+c) = ab+ac
= 6xy
(100 ²) a + 100 b + c = 0
10000 a + 100 b - 5000 = 0
$a_n = \frac{1}{2^{n-1}} = \frac{1}{2^{10-1}} = \frac{1}{512}$
y = ax + b
AB + BC =
V = ¼¶r²h
A = ¶r²h
cos (B) = y/x
E = M
f(x) = a

nobody predicted the fall of the Soviet Union. What happened? Well, politics came in the way. The moral of the story is that one cannot separate politics from economics forever. Even China cannot defy the laws of Economics. There may be “Socialism with Chinese characteristics” but there cannot be “Economics or Physics with Chinese characteristics.” In any case, economists cannot foresee the impact of the technologies of the future.

Shocks, Setbacks, and Surprises

International Politics teaches us one thing: rule out nothing, everything is possible. The future is not just a straight line. It is full of crossroads, shocks, setbacks, and surprises. Much like human life, International Politics is also full of ups and downs, disruptions and reverses. The first two decades of the 21st century have been full of shocks and surprises.

In the last 20 years, the world has witnessed two long wars (Iraq and Afghanistan), the explosion of Islamist terrorism, nuclear proliferation in North Korea and Iran, four pandemics (SARS, H1N1, Ebola, and Coronavirus), the energy crisis that saw the price of oil touching $148 per barrel and then crashing to $40 per barrel, a global financial crisis, a tsunami ending in a nuclear disaster, the shale oil revolution, talk of war between China and its neighbors, Donald Trump in the White House, and the impact of Twitter on diplomacy. All these non-linear, tectonic events of the last two decades have permanently changed our world, and given policy makers a whole new perspective on future long-term contingency planning.

Major Global Trends

Against this backdrop and with some caveats, this article identifies key trends that are likely to shape our future:

Power Shifts in the Age of Great Disruptions: The post-World War II order – first bipolar and then unipolar – is history. Multipolarity is emerging. But historically, multipolar systems have been more unstable than bipolar and unipolar ones. During power transitions, rising powers become revisionist. Both China and Russia are busy 'salami slicing' in the East and the West. Iran is doing the same in the Middle East. Not just China, Russia or Iran, even the U.S. under the Trump administration is seen as a dissatisfied power as it moves away from the post-World War II order. A relative decline in American influence has seen the rise of regional hegemons (China, Russia, Saudi Arabia, Turkey, Iran, Brazil, and Australia) working overtime to carve out their separate spheres of influence.

A Fragmented and Polarized World: With competing visions of world order and globalization, and contrasting rule sets in economy, technology, politics, space and cyberspace – a new world order is emerging. As globalization gives way to regionalization of commerce and currency, and economic issues get mired in domestic politics, trade could become a contentious and competitive issue in the future.

The New 'Great Game': Is all about resources, markets, and bases (RMB). We are seeing the return of mercantilism, trade wars, and neo-colonialism. Asian economies are becoming more and more dependent on Middle Eastern energy. Consequently, geopolitical competition from East Africa to East Asia is intensifying as exemplified by the naval base race to acquire forward bases from the Western Pacific to Western Indian Ocean. The growing naval rivalry over small island states in the Pacific and the Indian Oceans bears remarkable resemblance to naval competition to acquire access to markets, resources and bases amongst rising industrializing powers in earlier eras in history. China, for example, is now striving to establish itself as a dominant naval power in the Pacific and as a 'resident power' in the Indian Ocean just as France, Britain and the U.S. did in the 20th century.

The Changing Nature of Conflicts: Oceans, sea-beds, outer space and cyber space are the new arenas of rivalry. The old form of land-grabbing coexists with post-modern cyberwar. Map re-making is not over. A race is on to dominate in new 'strategic frontiers' such as oceans, the North and South Poles, cyberspace and outer space via 'gray

zone' operations, i.e., with little or no use of military force in ways that change regional balances of power and undermine existing trade, financial and military arrangements.

'One World, Two Systems': Tech wars over new disruptive technologies (AI, hypersonic, energy-directed weapons, quantum computing, big data, robotics, drones, IoT) are intensifying with the potential to cause supply chain disruption and a bifurcation of the global economy. Technology concerns involving national security interests are highly sensitive and competitive. A partial economic divorce or 'decoupling' between China and America is already under way. New technologies are the crux of this split. The emergence of two separate digital blocs, driven by security concerns, will have global economic implications.

Clash of Visions and Values: With the march of authoritarianism, religious radicalism, and right-wing populist nationalism, democracy seems to be in retreat. I characterize this coming ideological contest as mainly between Techno-Totalitarianism and Digital Democracies as represented in China's 'Belt and Road Initiative' and the U.S.' 'Free and Open Indo-Pacific'.

No 'multilateral nirvana': Far from being mechanisms for dispute resolution, global and regional organizations have now become the new arenas of shadow-boxing, multilateral maneuvers and machinations to gain relative advantage.

Implications

The next 15 to 20 years in the Indo-Pacific region are fraught with risks – this is where some of the world's most powerful states are forging new alliances, conducting arms races, pursuing mercantilist policies, extracting resources, viewing competitors with growing distrust and engaging in the containment of peer competitors. The security dilemma is worsening as nations – big and small – engage in 'band wagoning'– balancing and hedging games. Consequently, the vast region from East Africa to East Asia and the Polar regions are emerging as major arenas of contestation as countries cooperate, compete, collide, and collude with each other.

Small and middle powers are usually the first to experience geopolitical power shifts as they come under pressure to choose sides. Most strive to play one great power off against the other to their advantage but many fall prey to great power intervention and intrigues. Small and middle powers also tend to be strong supporters of regionalism and international institutions so as to constrain/moderate great power competition and ensure that big powers abide by laws, rules, and norms.

Illuminating the Unseen Elephant: How Complexity Theory Can Help Turn Security Challenges into Opportunities

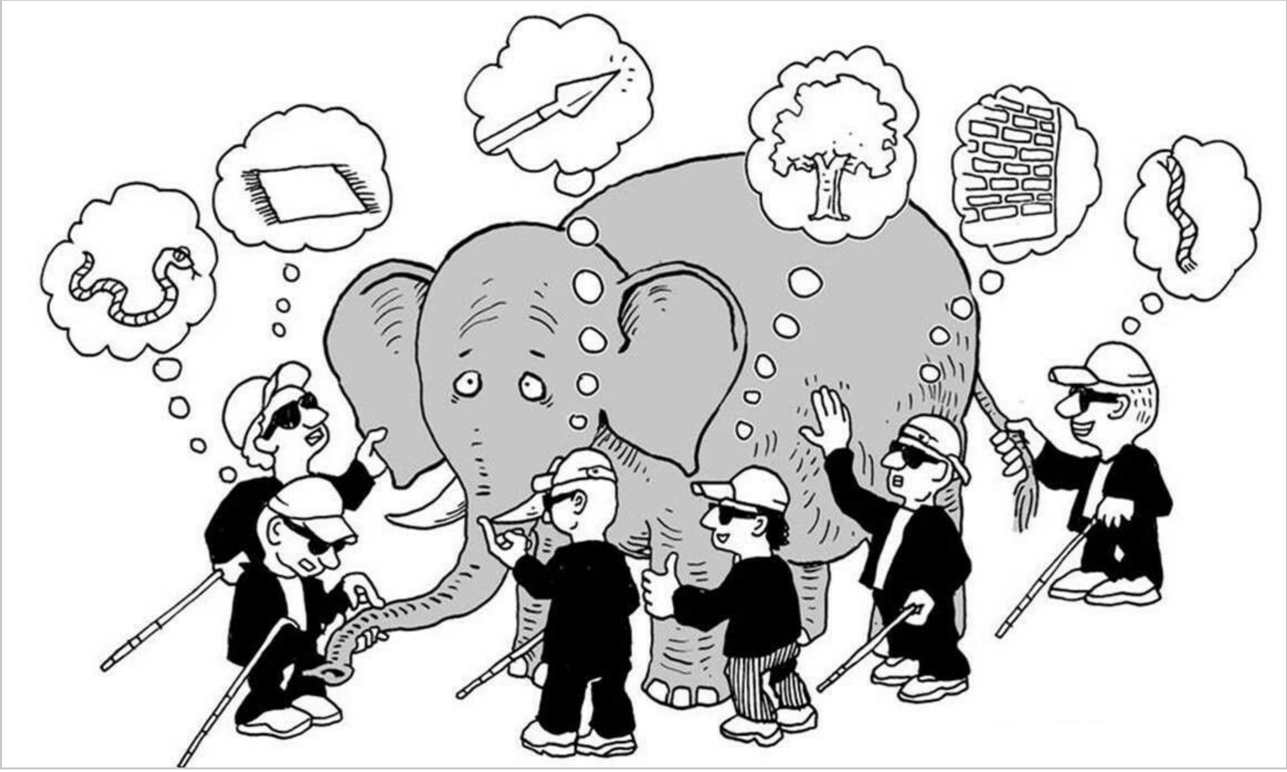
The annexation of Crimea, the rise of far right nationalist parties in Europe, the activities of the Wagner group in the Syrian Civil War and the spread of disinformation and propaganda on social media during the 2016 US Presidential Election, although seemingly unconnected, these four events are part of a concerted effort to increase the influence and geopolitical reach of the Russian Federation. While the connections are widely recognized now they were once shrouded in secrecy.

Patrick Bell, Ph.D.
Faculty, UAE NDC

What the connection between these events reveals is that the larger strategic picture is often unseen — especially by those who are the targets of operations contained within these events. Illuminating the connections between these events is crucial in order to create opportunities for strategic decision makers to proactively address the perennial security dilemmas that impact the security and safety of a state's citizens.

But how can decision makers link seemingly unrelated events? This comes from understanding the dynamic processes through which these events interact. Using complexity theory, decision makers can not only understand, but anticipate the actions of strategic actors — be they friend or foe. The first step in applying complexity theory comes from changing one's perspective regarding the nature of systems.

Systems are all around us — whether the environment, the geopolitical system of nations and states or the people who occupy their territory. Each of these examples is a system in itself — existing and interacting with the other systems. These systems affect and are affected by the world around them. Each actor thinks they understand their system and yet has an incomplete picture.



Just like a set of blind men who are each sensing a different part of an elephant, events and the actors that populate them appear to be unconnected when in reality they are interdependent. Applying complexity theory reframes this perspective, so that they can view this more holistic picture [1].

One change one's perspective by learning the language of complexity. To be sure this language may seem unfamiliar, but once comprehended, it will become clear that complexity is commonplace, even intuitive.

Complexity theory reframes the critical thinking of decision makers

Learning the Language of Complex Systems

To begin with, complexity theory reframes the critical thinking of decision makers in four distinct ways.

1) It refocuses the frame from a focus on the attributes of actors such as how large or small they are, to the actor's actions. More specifically, it focuses on their interactions. These interactions are like many ripples in a pool of water that begin individually but soon encounter other ripples, thus changing the overall pattern as they interact. For example, how will the Russian Federation's use of mercenary forces in Ukraine or Syria impact other groups in Crimea or Western Europe?

2) It also refocuses the frame from individual effects to effects that cannot be attributed to any single actor. These are referred to as second or third order effects. For example, how will Russian support of Bashar Al Assad impact support of right wing nationalists across Europe?

3) It refocuses the frame from a focus on behavior at one point in time, to effects over time which impact the equilibrium or balance that exists within the systems themselves.

These behaviors both positively or negatively impact the course of systems and are referred to as feedback loops. For example, how did using covert active measures such as disinformation and propaganda on social media stoke racial tensions and lead to less voter participation among African Americans in the 2016 US presidential election?

4) Each of these processes; interaction, order effects and feedback loops, are referred to in complexity theory as system dynamics. When taken together, these dynamics reframe decision making from one focused on analysis of individual parts to synthesis at a more holistic level and allow strategic decision makers to see larger patterns. Such patterns impact the function or purpose of the system itself. What becomes apparent at this more systemic level is that the whole is more than the sum of its parts.

From Language to Behavior

Once one becomes familiar with the language of complexity one can start to understand the behavior of systems. Using complexity theory, strategic decision makers can identify the systems they are in and the processes that impact their progress toward obtaining their strategic objectives.

Among the most important behaviors is adaptation. Systems, and the actors that populate them are not static but dynamic entities. Actors, be they states, non-states or even in some cases individuals, respond to their environment by changing their strategies in response to other actors. They learn over time and respond differently to the same stimulus. Identifying these adaptive behaviors is crucial when responding to challenges, especially at the strategic level. This process has been studied in various contexts including that of strategic studies. An example of this process is that of the tactical interaction cycle described first in the work of Douglas McAdam [2]. How Al Qai'da or ISIS changed its behavior in response to US and coalition efforts to disrupt or destroy their networks is an example of adaptation.

Another important behavior is that of self-organization. Self-organization occurs as systems become more complex over time through as their interactions increase. This pattern can be seen in various contexts including collections of states, non-states or individuals. When this behavior cannot be traced to a single factor, this behavior is denoted as emergent. Identifying the processes through which self-organization or even emergence occur is crucial to predicting the development of the system. The development of the Euromaidan protests in Ukraine in 2013-2014 and the umbrella protests in Hong Kong in 2019 are examples of self-organization and emergent behavior.

A third type of behavior is what systems theorist Donella Meadow's refers to as "system traps [3]" . System traps refers to behaviors that are inherent in the structure of a system which lead the system to display disequilibrium. Of the three main "archetypes" of traps, the one most familiar to security studies is escalation — otherwise known as the security dilemma. The international proliferation of weapons of mass destruction is an example of escalation.

Finally, among the most important behaviors in a system is that of information flow. How, and just as importantly what, information flows within the system is critical to determining the behavior of the system. Beyond being the lifeblood of any strategy, information has changed in three important ways. Understanding these changes is crucial to determining the behavior of contemporary systems.

First, the volume of information has increased by orders of magnitude with global IP traffic increasing from 100 GB per day in 1992 to a forecasted 157,000 GB per second in 2022 [4].

Second, the velocity with which this information is being communicated has increased with millions of messages communicated each minute [5].

Third, the variety of sources has increased with 80 % of the data being communicated in an unstructured format by 2025 [6].

When combined with new technologies such as social media, the impact of information flows on system behavior is among the most important system dynamics. The use of social and traditional media by organizations such as Al Jazeera in Qatar or the Internet Research Agency in the Russian Federation are only two examples of how information flow can impact system behavior.

From Behavior to Action

By beginning to understand system behavior one can design strategies that turn contemporary challenges into opportunities. More specifically, applying complexity theory can alert those at the strategic level to be aware of the second and even third order effects that result from the interactions of events that do not seem to be connected when observed from the operational or tactical level. By understanding the system dynamics inherent in all systems, decision makers can more effectively integrate their critical thinking and confront the challenges of contemporary security dilemmas such as climate change, hybrid warfare, lethal autonomous weapons, pandemic diseases and the proliferation of weapons of mass destruction. In other words, by applying complexity theory decision makers will be able to see not just the elephant's tail or trunk, but the whole elephant.

References

1. Adapted from description found in Meadows, D. (2006) "Thinking in Systems" A Primer"
2. This cycle describes a pattern in which opposing sides learn from each other's tactics. Employing "negative inducements" to disrupt the power imbalance experienced by insurgent groups when confronting more powerful opponents. For more information on this process see McAdam (1983) "Tactical Innovation and the Pace of Insurgency", American Review of Sociology Vol. 48 (December).
3. For more information on system traps see Meadows (2008) Edited by Wright, D. Thinking in Systems: A Primer, Earthscan, International Institute for Environment and Development, London
4. For more information on this see the Cisco white paper on Global internet protocal (IP) traffic. Accessed at https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc532256789
5. For more information on this see https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/
6. Data for analysis is structured in two categories, structured and unstructured. For more information on this see https://solutionsreview.com/data-management/80-percent-of-your-data-will-be-unstructured-in-five-years/ and https://www.datamation.com/big-data/structured-vs-unstructured-data.html

Understanding Iran's 'Grey Zone' Strategy

Attacks on oil tankers near the UAE's shores, as well as audacious drone strikes against Saudi oil installations have highlighted the increased intensity of asymmetric operations in the region. These events serve as a clear reminder of Iran's favored 'modus operandi' for waging conflict against its regional adversaries; namely, operating in a 'grey-zone' area where lines between the state of war and peace are deliberately blurred. Tehran has grown quite proficient in leveraging the advantages of 'grey zone' operations to its favor.

Amb. Grigol Mgaloblishvili
Faculty, UAE NDC

A quick look at Tehran's current approach to subvert its adversaries makes it clear that, "Iran typically operates below the threshold of conventional warfare, using a blend of military and paramilitary tools, including proxy forces, missiles, cyber tools, maritime forces and information operations to shape and coerce regional actors to its advantage[1]."- This highly sophisticated approach enables Tehran to minimize the risks of conventional military confrontation and to operate with relative impunity by conducting its subversive operations just below the threshold of an open conflict.

Since Iran has emerged as the region's foremost practitioner of 'grey zone' operations, it is imperative for the regional countries in general, and the UAE in particular, to understand Tehran's strategic approach[2]. This article thus will examine how Iran attempts to leverage advantages of a 'grey zone' strategy

in order to expand its regional influence. Given the significant implications that Iran's 'way of war' poses on regional security, the paper will focus on answering the following questions that are highly relevant for further considerations, "What are the underlying factors that shape Tehran's preference for a 'grey zone' strategy?" "What is the strength of Iran's strategic approach?" And "What are Tehran's 'grey zone' strategy's vulnerabilities"?

Iran's preference for 'grey zone' strategies are clearly dictated by its relatively inferior military and economic capabilities to confront its traditional adversaries in a direct manner, such as the United States and its regional allies. Hence, in recent decades Tehran has grown adept at leveraging the advantages of asymmetric warfare by developing the capabilities that enable it to employ indirect means for its subversive actions. As such, Tehran has developed a force structure and indirect war-fighting tactics that allow it to avoid escalating conflict to the point of conventional warfare[3] . In this respect, the central tenets of Iranian force structure consist of: a guerrilla naval force capable of disrupting oil exports from the Gulf region; an arsenal of missiles and drones capable of conducting long-range precision strikes; well-developed proxy forces capable of conducting conventional and unconventional operations throughout the region and offensive cyber capabilities[4] . The blend of these capabilities has enabled Tehran to overcome its military and economic weaknesses and skillfully exploit its adversaries' vulnerabilities.

Other than reducing its weaknesses, Tehran's preference for 'grey zone' strategies also reflects its traumatic experience of the costly military conflict with Iraq during the 1980s. It has been argued

that, “No single event has defined Iran’s revolutionary ideology, politics, perspectives on society and security more than the Iran-Iraq War[5].” There are at least two reasons why this conflict still matters for understanding the rationale of Tehran’s decision-making process. First, the legacy of this lengthy military conflict facilitated the formation of a strategic culture that centers on aversion to full-scale conventional combat, even after the three decades that have passed since the conflict ended. Second, Iran’s adherence to ‘grey zone’ strategies were heavily influenced by the perceived success of its asymmetric forces, namely the Islamic Revolutionary Guard Corps (IRGC), during the war, and afterwards[6]. Hence, two important factors that explain Iran’s adherence to asymmetric warfare are its relative weaknesses against militarily and economically stronger adversaries, as well as the legacy of the Iran-Iraq War.

These factors led to formation of a strategic culture that centers on investing and developing non-attributable instruments of statecraft. Whether it is networks of proxy groups, offensive cyber capabilities or arsenals of drones, it enables Tehran to undermine adversaries by disguising or denying the extent of its military engagement; and where necessary, running a campaign of plausible deniability. Iran’s agility in using non-attributable tools in a highly effective manner has played an important role in spreading Tehran’s influence in the region with minimum costs and risks of re-engaging in a full-scale conflict. In other words, this strategic approach has enabled Tehran, “To subvert and destroy states without direct, overt and large-scale military intervention[7]” and with relative impunity. Thus, the main strength of Tehran’s ‘grey zone’ strategy lies in its ability to create ambiguity and to obscure the lines between the state of war and peace by employing effectively the non-attributable instruments of statecraft.

Alongside the noticeable gains, however, the pursuit of a ‘grey zone’ strategy has incurred significant costs and, in multiple instances, has backfired on Iranian interests. Its naval provocations as well as its support to proxy forces have significantly damaged its international reputation and have deepened its regional isolation. By undermining the regional stability and supporting malign actors, “Iran has perpetuated its image as an outlier in the international community[8].” This image permitted its adversaries

to consolidate international support for imposing financial sanctions on Iran with relative ease. Moreover, Tehran's aggressive stance towards its neighbors has created unlikely avenues of dialogue and cooperation among those regional actors that have historical rivalries with each other – notably Israel and the Arabian Gulf states[9]. The common denominator these regional actors share is an interest in curbing the spread of Iranian influence in the region. In short, Tehran's 'grey zone' strategy, alongside apparent gains, has also led to unintended consequences that have shattered its international reputation and weakened its regional standing. Despite all this pushback, it seems likely that Iran will continue its 'grey zone' activities in order to expand its regional influence. The gains of operating in a 'grey zone', from Tehran's perspective, significantly eclipse the negative consequences of its strategic approach. Thus, understanding Iran's 'grey zone' strategy acquires particular importance as its relevance is unlikely to recede in the coming months and years.

References

1. Dalton G. Melissa. "How Iran's hybrid war tactics help and hurt it", Bulletin of the Atomic Scientists, 2017, Vol. 73. NO 5, 312-315
2. Eisenstadt, Michael. "Operating in the 'Grey Zone': Countering Iran's Asymmetric 'Way of War' ", 2020
3. Dalton G. Melissa. "How Iran's hybrid war tactics help and hurt it", Bulletin of the Atomic Scientists, 2017, Vol. 73. NO 5, 312-315
4. Eisenstadt, Michael. "Operating in the 'Grey Zone': Countering Iran's Asymmetric 'Way of War'", 2020
5. Behnam Ben Taleblu, "The Iran-Iraq War: It Still Haunts the Middle East to This Day", The National Interests, May 15, 2019
6. Eisenstadt, Michael. "Operating in the 'Grey Zone': Countering Iran's Asymmetric 'Way of War'", 2020
7. Galeotti, M.E. 'Gerasimov Doctrine' and Russian Non-linear War, 2014.
8. Dalton G. Melissa. "How Iran's hybrid war tactics help and hurt it", Bulletin of the Atomic Scientists, 2017, Vol. 73. NO 5, 312-315
9. Dalton G. Melissa. "How Iran's hybrid war tactics help and hurt it", Bulletin of the Atomic Scientists, 2017, Vol. 73. NO 5, 312-315.

Strategic Environment Analysis Is Vital For Decision-Making & Strategy Building

Few leaders in the private or the public sector would deny the importance of developing an effective strategy, but how many really know where to start? In fact, the essential starting point for effective strategy and decision-making is a robust analysis of the strategic environment. This article explains why strategic environment analysis is vital for decision making and strategy building. To develop a clear and implementable strategy that supports national interests, it is important that a robust analysis is undertaken and competent decisions are made.

Mona Al Shamsi
Participant, UAE NDC

One of the most respected writers on statecraft and strategy development is Terry L. Deibel who provided a logical process to follow (Deibel, 2007). It begins with assessing the environment, followed by analysis of threats, challenges and opportunities, and finally, the development of a course of action to address them. Similarly, Zuzana Papulova and Andrea Gazoya (Papulova & Gazoya, 2016) provide a model for decision-making, which emphasizes input, or information gathering; transformation, or analysis of the problem; and output, or a decision. Both models recognize that the starting point and foundation for good decisions and strategy is gathering information, or assessing the environment.

This article will now consider this essential stage, which provides the foundation upon which all good strategies are built.

In their paper “The role of Strategic Analysis in Strategic Decision Making”, Papulova and Gazoya propose a model (Papulova & Gazoya, 2016):

In it, they show that decisions are the considered output of a process that involves the analysis of information, transforming input. This is an important point, a good strategy is based on good decisions, which are based on gathering a broad range of information from a variety of sources that is transformed to become useful. This is broadly supportive of the approach outline in the NDC strategy which uses the terms assess, analysis and plan.

The starting point and

Input	Transformation	Output
PERCEPTION	**UNDERSTANDING**	**CONSIDERATION**
Information Gathering	**Analysis of Problem**	**Decision**

foundation for a good strategy is, as Papulova shows, the INPUT, the information gathering. This review now considers this important aspect, gathering information; this is an essential stage in strategy development and provides the foundation upon which all good strategies are built.

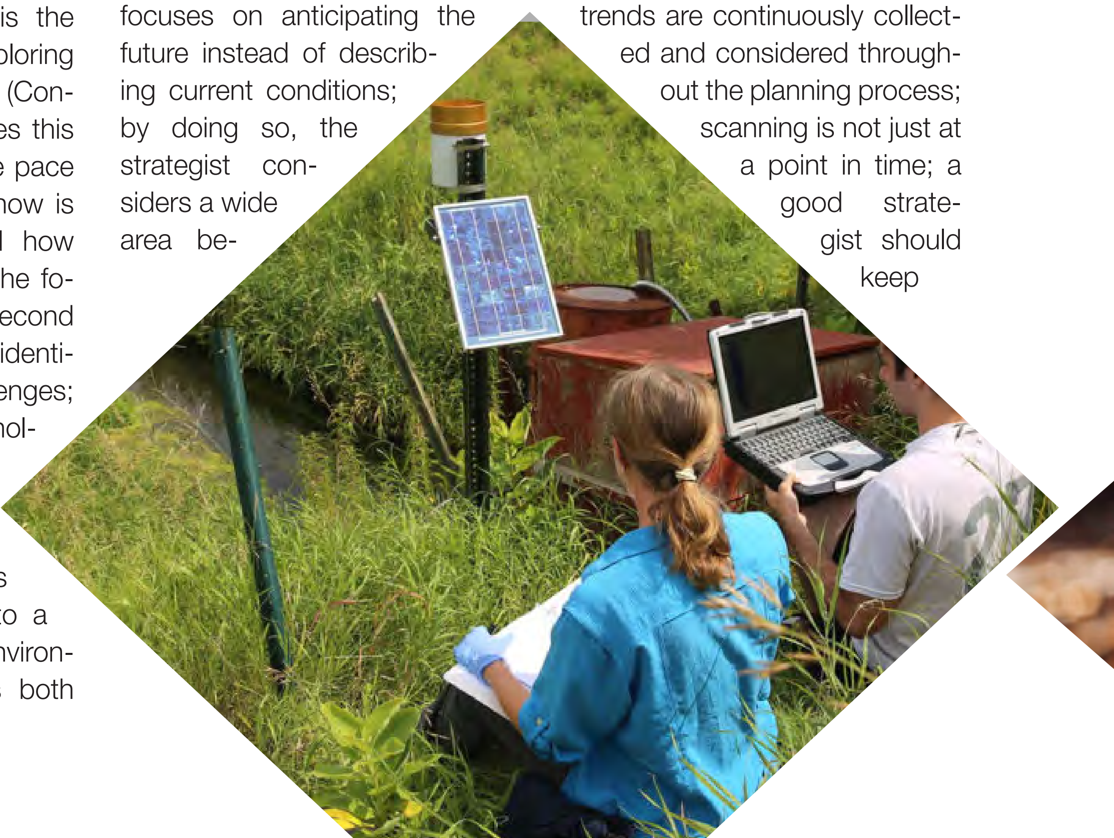
The process to gather information is commonly referred to as "scanning". Fairbanks and Buchko (Fairbanks & Buchko) set out a case to use a structured tool, Maree Conway (Conway, 2013) has also considered this subject, and Éverton Luís Pellizzaro de Lorenzi Cancellier et al, considered "the relation between the scanning of environmental information, strategic behaviour and performance" (Pellizzaro de Lorenzia Cncellier, Blageski, & Rosseto, 2014). They defined scanning as "a manner through which managers acquire relevant information about what happens outside the company so that future courses of action are taken"

What then, is scanning? Referring to Conway once again: "Environmental scanning is the art of systematically exploring the external environment" (Conway, 2013). Conway argues this is to better understand the pace of change. For example, how is technology changing and how will these changes affect the focus for the strategy? The second purpose of scanning is to identify opportunities and challenges; continuing with the technology example, strategists would need to consider how the use of Autonomous Weapons Systems might be incorporated into a revised military strategy. Environmental scanning explores both

new, strange and weird ideas, as well as persistent challenges and trends today. It is about recognising that the future will not be like the past, and that we therefore need to spend some time understanding the trends and likely influencers on the future of our organisations. High quality scanning is the core of effective futures work.

Drumm McNaughton (Mc Naughton, 2018) suggests four reasons why environmental scanning needs to be front and centre in developing a strategic plan:

- Environmental scanning focuses on anticipating the future instead of describing current conditions; by doing so, the strategist considers a wide area beyond just what is happening today.
- Environmental scanning has a wider scope than traditional data collection; consider everything – such as social, economic, political and technical indicators.
- Environmental scanning allows for participants to analyze the interactions of events and trends; therefor allowing extrapolation
- Environmental scanning is a critical and ongoing part of the planning process in which information on external events and trends are continuously collected and considered throughout the planning process; scanning is not just at a point in time; a good strategist should keep



scanning and reconfirm his understanding

What is interesting is that the McNaughton article is referring to the education sector, and yet the points made are as equally relevant to a strategist working on statecraft. The Deibel model describes developing a strategy in similar terms.

The takeaway is that although much of strategic analysis is based on principles outlined originally by military strategists such as Sun Tzu and Clausewitz, political practitioners such as Machiavelli or codified in methodologies around developing strategies for statecraft by exponents such as Deibel, in today's world, strategy development in any industry or sector should be based on a solid foundation supported by a robust scanning process.

The importance of scanning (environmental analysis) is, therefore, clear and its need as the foundation for analysis is demonstrated in Papulova's three stage process, one that ends with the consideration process of taking decisions; nobody can predict exactly what will happen in the future but more reliable decisions and hence more reliable strategies are developed on the back of thorough and well researched scans of the environment. Moreover, as McNaughton (Mc Naughton, 2018) notes, scanning is not a one-off process, it is part of an on-going and iterative process that recognises the world is a dynamic and changing place. Military strategists understand the need for having a clear and well-thought through strategy, and the basis for strategic planning is primarily based on the writings of military strategists. But the principles, and particularly the need to have a foundation based on environmental scanning are appropriate and applicable for any sector and any industry.

References

1. Conway, M. (2013). Environmental Scanning: What it is and how to do it. Retrieved January 2020 ,1, from Thinking Futures: http://thinkingfutures.net
2. Deibel, T. (2007). Foreign Affairs Strategy: Logic for American Statecraft. Cambridge University Press.
3. Fairbanks, s., & Buchko, A. (n.d.). The Strategic Environmental Scan Tool: Performanced Based Stategy. Retrieved January ,1 2020, from DOI.org: . https://doi.org/-795-78743-1-978/10.1108 120181008
4. Mc Naughton, D. (2018, May 3). Strategic Planning and Environmental Planning. Retrieved January 2020 ,1, from The Change Leader .com: https://thechangeleader.com/strategic-planning-and-environmental-scanning/
5. Papulova, Z., & Gazoya, A. (2016, December). Role of Strategic Analysis in Strategic Decision Making. Procedia Economics and Finance No 579-571 ,39 ,39.
6. Pellizzaro de Lorenzia Cncellier, E. L., Blageski, E. J., & Rosseto, C. R. (2014). Environmental Scanning Strategic Behaviour and Performance in Small Companies. JISTEM Inf Syst Management volume 3.

A Framework for Interpreting US Foreign Policy in the Gulf

Many people in the Gulf find it difficult to interpret U.S. foreign policy and to forecast how it might react to significant events in the region, for example the May and June 2019 sabotage attacks on four shipping vessels off of the UAE coast, the September 2019 attacks on Saudi Aramco oil facilities, or the attack that killed Iranian general Qassim Soleimani in Baghdad in January 2020. People speculate what interests drive U.S. policies and responses, with many different answers and theories. A framework for interpreting U.S. foreign policy in the Gulf would help observers to better understand the dynamics involved in shaping U.S. responses to events in the region.

Sterling Jensen, Ph.D.
Faculty, UAE NDC

This framework is built on two main pillars: first, a correct understanding of U.S. interests in the Gulf and how they compare with other U.S. interests in the world; and second, a correct understanding of how U.S. foreign policy is formulated, resourced and executed. This looks at the separation of powers within the U.S. government between Congress, the White House and public opinion. Without correctly understanding these two pillars, it will be difficult for observers to assess and forecast U.S. responses to significant events in the Gulf.

US Strategic Interests

Like any state, the U.S.'s national interests are largely related to its security, economy and values. The U.S.'s main interests in the Middle East are preventing the spread of terrorism, stopping WMD proliferation, allowing freedom of navigation, the free flow of energy

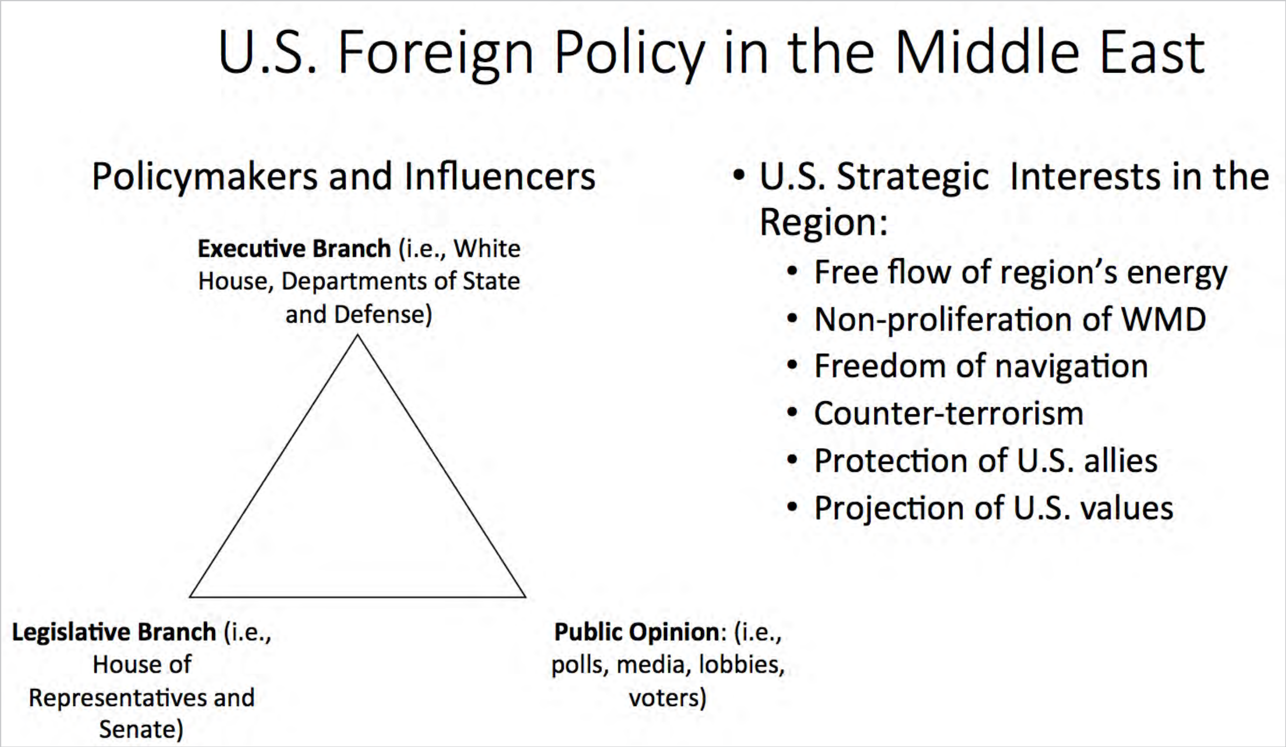
(oil and gas), promoting U.S. values and protecting U.S. allies. U.S. foreign policy is shaped by threats, challenges and opportunities to those interests. However, many in the region are confused as to which of these interests is driving U.S. foreign policy and how they are prioritized in any given event. For example, the U.S. might prioritize one threat to a Middle Eastern ally more than another. Priorities of U.S. interests are shaped by public opinion, lawmakers and assessments made by the White House, which is discussed later.

In addition to identifying U.S. interests in the region, it is important to compare these interest with US interests elsewhere. For example, the 2017 U.S. National Security Strategy declares that great power rivalry (Russia and China), rather than terrorism, will shape U.S. security strategy in the future. More emphasis on great power rivalries could lessen the urgency of U.S. interests in the Middle East. Additionally, the shale oil revolution has helped the U.S. become the world's largest producer of oil, which means it is less dependent on Middle Eastern oil. So while the Middle East might remain an important region to secure U.S. interests, the changing environment might make it less important than regions such as Asia or Europe. This leads on to how U.S. foreign policy is formulated and resourced.

Congress, the White House and Public Opinion

Many outsiders underestimate the impact of the U.S. system of checks and balances on how U.S. foreign policy is formulated, resourced and executed. The U.S. government is divided into three separate powers: legislative, executive and judicial. The most important branches for formulating, resourcing and implementing foreign policy are the legislative and executive branches.

The legislative branch (the House of Representatives and Senate, or Congress) makes laws, oversees the spending of the government budget, has the power of the purse and declares war. It is the only federal government body that can raise funds through taxes, and the President must have any government budget approved by Congress. The Senate must also ratify any treaty the government makes with a foreign country. So if the legislative branch, which is elected to office in two



U.S. Foreign Policy in the Middle East

Policymakers and Influencers

Executive Branch (i.e., White House, Departments of State and Defense)

Legislative Branch (i.e., House of Representatives and Senate)

Public Opinion: (i.e., polls, media, lobbies, voters)

- U.S. Strategic Interests in the Region:
  - Free flow of region's energy
  - Non-proliferation of WMD
  - Freedom of navigation
  - Counter-terrorism
  - Protection of U.S. allies
  - Projection of U.S. values

(House of Representatives) and six (Senate)-year cycles, does not agree with a President's foreign agenda, they can limit the President's ability to resource and execute a foreign policy. A recent example of this was seen with U.S. policy in Yemen. Many Congressional members, both Republicans and Democrats, disapproved of the President's policy on Yemen. They therefore passed a bill to withdraw support for the Saudi-led Coalition. While President Trump's administration vetoed the bill, the Congressional action limited the government's ability to support Saudi-led efforts to stabilize Yemen.

The executive branch (the White House) enforces the laws and has the authority to formulate and execute foreign policy. The President,

who is the head of the executive branch and is elected every four years, is also the Commander in Chief of the Armed Forces. However, the President is not authorized to declare war on a foreign country. This is the authority of the Congress. The President is authorized to defend the country by using the armed forces and conducting foreign policy abroad. Foreign policy is limited, though, when the President and Congress have different views on how to address a national security problem. For example, the January 2020 killing of Iranian general Qassim Soleimani was authorized by the White House without formal Congressional approval or notification. If this action were to lead to the U.S. going to war with Iran, Congress would have to pay for the war effort, which Congress might believe taxpayers would not be willing to support. Therefore, in response to the Soleimani killing, Congress passed a resolution to limit the President's ability to take military action against Iran and potentially other countries, without first notifying Congress. This interdependency between the legislative and executive branches was designed to encourage compromise and prevent one branch from becoming too dominant.

Lastly, public opinion shapes how the legislative and executive branches prioritize U.S. foreign policies. As politicians are elected in two, four and six year terms, they are continually assessing public opinion in order to get re-elected. For example, policies on some issues such as Iran, Israel and terrorism are largely shaped by public opinion. While many U.S. interests are not determined by public opinion, such as some alliances with Arab Gulf countries, they can be impacted by public opinion, for example preventing the sale of U.S. ports to DP World in 2006 or support for the so-called 'Arab Spring' in 2011. Public opinion is shaped by freedom of the press, so the media also plays an indirect role in shaping U.S. foreign policy.

Assessing and forecasting U.S. foreign policy is complex and highly nuanced. It is also difficult for many U.S. citizens unfamiliar with the political system to understand the workings of foreign policy. However, U.S. foreign policy is largely transparent, especially given the U.S. laws on freedom of speech and of the press. Those who understand how to correctly assess and analyze US strategic interests, with a detailed understanding of the nexus between Congress, the White House and public opinion, will find it less difficult to interpret and will better forecast how US policy will respond to a given event in the region.

Electricity supply security in the UAE

Since the formation of the UAE on 2nd December 1971, the national economy has grown enormously. By just looking to the gross domestic product (GDP) numbers for the past forty years, we will see that it has increased from USD 75.1 billion in 1980; to USD 130.1 billion in 1990, USD 258.1 billion in 2000, USD 466.6 billion in 2010 and reached USD 686.6 billion in 2017 which means the growth rate of GDP is around %100 every ten years. This fast growth in economy and population has resulted in a continuous growth in electricity demand as well.

Ali Awadh Al Menhali
Participant, UAE NDC

The primary driver of this demand has been the high consumption of electricity and the rapid urbanization and industrialization in the UAE. The electricity demand increased from 69,914 GWh in 2007 to 131,031 GWh in 2017 (Federal Competitiveness and Statistics Authority (FCSA) 2018). This means that the average annual growth in electricity consumption is around 8% which is very high compared to the average global rate of around 3.5% (Global Energy Statistical Yearbook 2019). The constantly increasing electricity demand is putting more and more pressure on the electricity supply system in the UAE in order to provide prosperity and stability. Moreover, the government in recent decades has been attending to the growing demand by building new generation plants based on hydrocarbon sources. This has increased the amount of carbon dioxide emissions significantly. The emissions increased from 69.1 million tons in 2013 to 77.8 million tons in 2017 (bayanat 2020), which makes UAE one of the world's

top countries in carbon dioxide emissions per capita (Knoema World data atlas 2018).

The UAE current generation strategy is based on building huge centralized generation plants in relatively small areas such as the Taweelah generation compound and the Barakah nuclear plants. This means that all these locations are considered as very sensitive locations from the security point of view. An adversarial neighboring country such as Iran can target these locations with its drones or ballistic missiles, similar to what happened in Biqayq and Khurais oil plants in Saudi Arabia. If this occurred, it would severely disrupt UAE electricity supplies.

Although the government has drawn up a short-term plan (UAE government vision 2021) which includes generating 27% of the electricity demand from clean energy sources and reduce its per capita greenhouse gas emissions (carbon dioxide) (UAE Goverment 2020), the execution of this vision is proceeding very slowly (where the electricity generated from clean sources reached only 0.35% as of 2018). The government has also developed a long-term strategic plan (UAE Energy Strategy 2050) which targets an energy mix that combines nuclear, renewable and clean coal in order to reach

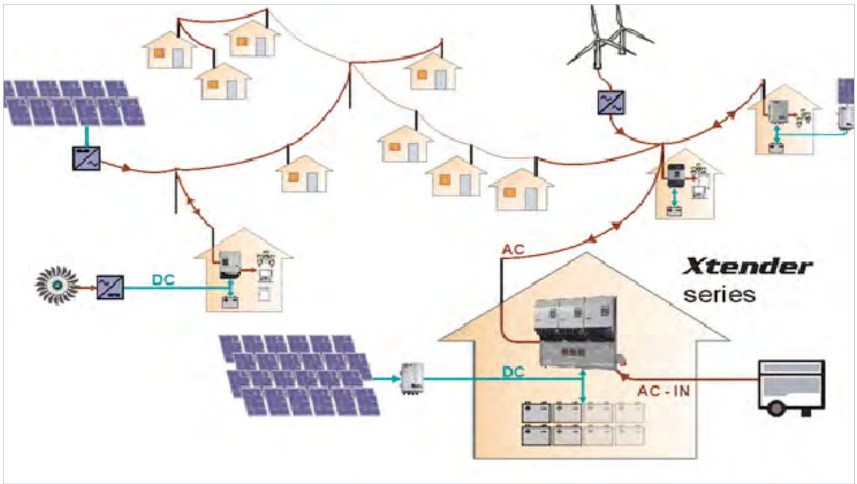
50% of the country's demand generated from clean sources by investing around AED 600 billion and reduce the carbon footprint of power generation by 70% thus saving AED 700 billion. Although this long-term strategy looks promising, it does not address the issues from the security point of view and also it still puts a heavy financial burden on the government..

In my opinion, the government should consider the concept of distributed generation as a response to the current policy issues. Distributed generation is an approach which employs small-scale generation points that can be implemented on multiple levels; a household level, a neighborhood level, or a small city level. The idea of distributed generation is to build small-scale, renewable power generation plants in the neighborhoods where the generation plants can be connected directly to the distribution network thus eliminating the transmission network from the model.

Overall distributed generation brings a lot of advantages to the energy field. For instance, it reduces the government investment since the cost is borne directly by the consumer (considering it is applied at the household level). Moreover, a distributed generation system may use renewable sources of energy or non-renewable sources. It can work while being connected to the current grid and it also can work as a stand-alone system. Also, it will drastically decrease the cost of supplying power to the consumers from the government due to elimination of transmission element in the network. Moreover, it opens the power generation market for small scale investors (i.e. SMEs). Furthermore, it dilutes the bank of targets for any adversaries and it increases the network resilience towards technical failures. As well, it will speed up the government response to the ever-growing demand. Finally, it decouples water generation from the power generation which allows for implementing separate and more efficient solutions on the water generation front. It is worth mentioning here that distributed generation was implemented in the UAE before on a small scale by using hydrocarbon power plants, but those plants were decommissioned and the UAE currently does not have distributed generation stations.

Bringing distributed power generation to the UAE requires addressing a unique problem for the region – fresh water. Current power generation models via gas combined cycle allow for the production of fresh water as a by-product from waste heat recovery. This is done by sea water multi-flushing using the waste heat from the steam turbines. That is why all power generation facilities are located near sea shorelines. Most of the UAE's fresh water needs are addressed by power generation. A good example is the emirate of Abu Dhabi which produced 100% of its fresh water needs by desalination using power generation plants in 2017 (Federal Competitiveness and Statistics Authority (FCSA) 2018). Any proposed policy that undertakes distributed power generation as the sought target has to address the water problem. Moreover, while integration of distributed generation into distribution systems has many advantages, however, our current traditional power systems are not designed to incorporate the power generation sources directly into the distribution network. Accordingly, such integration has to be carefully studied to understand its impact and come up with solutions ahead of time in order to maintain the power network running smoothly.

In light of all the above, I propose to consider covering all the UAE's electricity demand by develop-



ing fully distributed generation plants that employ renewable energy and non-renewable energy at the neighborhood level. The government can allow the neighborhood residents to establish co-operatives that invest, operate and manage power generation in their neighborhoods. Power generation can be done via renewable resources. Internal distribution within the neighborhoods can be managed by the same cooperatives/SMEs; while distribution in between neighborhoods (transmission) can be managed by a central body comprising a council representing the involved cooperatives/SMEs. Accounting for the export/import of electricity or water across neighborhoods can be managed by the private sector. Cooperatives/SMEs will generate revenue from internal consumers (including members) and from exporting excess electrical power to the nearby neighborhoods. The market model followed should be as free as possible to allow competition among neighborhoods. The government role will be only of regulatory nature. The value of such an idea can be increased by employing certain types of renewable energy such as waste-to-energy to generate the needed power which will add more value by reducing or eliminating the waste produced by the neighborhoods.

Overall, this blended approach brings all the aforementioned benefits of distributed generation but limits the role of the government and its influence on the power generation framework. It is known that one of the disadvantages of renewable energy is its instability due to continuous climatic changes. Accordingly, it is very important to highlight that the proposed model in this option is to adopt distributed generation plants which use a mixture of hydrocarbons, clean coal, nuclear and renewables in order to achieve a highly stable and reliable system. Although the proposed solution is to use a mixture of energy sources, renewable sources should be dominant in this option in order to achieve the government goals of higher usage of clean energy, decreasing carbon dioxide emissions to the least and to decrease the dependency on the natural gas to generate electricity.

The government needs to look at this mixed energy sources concept and thoroughly study the possibility of applying it to resolve current policy issues. In my opinion, the fully distributed model provides the optimal compromise between viability, efficiency, government burden and security. Still, transforming the current model of a fully centralized system to the proposed model requires a multi-decade transformation plan whereby old centralized production assets are either phased out or privatized to cooperatives/SMEs. It is my firm belief that a fully distributed model represents the essence of the future that is driven by data analysis and artificial intelligence.

In conclusion, it is in the UAE's national interest to ensure the stability, security and prosperity of the people in UAE by ensuring uninterrupted, sustainable and affordable electricity supplies which will guarantee sustainable and continuous growth for the economy.

References

1. 2020. bayanat . http://data.bayanat.ae/en_GB/dataset?groups=energy&organization=ministry-of-energy-industry.
2. 2018. Federal Competitiveness and Statistics Authority (FCSA). Accessed 2018. https://fcsa.gov.ae/ar-ae/Pages/Statistics/Statistics.
3. 2019. Global Energy Statistical Yearbook . https://yearbook.enerdata.net/electricity/electricity-domestic-consumption-data.html.
4. 2018. Knoema World data atlas. https://knoema.com/atlas/ranks/CO2-emissions-per-capita.
5. 2020. UAE Goverment https://www.government.ae/en/information-and-services/environment-and-energy/environment-and-government-agenda/environment-in-vision-2021.

The Covid-19 Outbreak and Implications for National Security Decision-Making

For every country, the current coronavirus outbreak (the virus causing Covid-19, also known as SARS-CoV-2 or 2019-nCoV) is one of those unique moments when senior decision makers wrestle to devise policy responses as they are confronted with a myriad of challenges. These pressing challenges include incomplete data, lack of knowledge, time constraints, scarce financial, material and human resources, conflicting priorities, bureaucratic red tape, and intense pressure from public opinion, media and political contenders as noted by Dempsey (2017).

Yacouba Gnegne, Ph.D.
Faculty, UAE NDC

This begs the question as to how were some countries more successful in preventing the Covid-19 coronavirus from exacting its toll, while others found it nigh impossible to reduce the odds of the Covid-19 pandemic spinning out of control?

Sadly, Covid-19 coronavirus is a 'gray rhino', in that it was an unsurprisingly likely but neglected disaster. It happened despite warnings from several intelligence agencies, risk experts, and global figures such as Bill Gates, in recent years and even in January and February 2020. Deeply rooted cultural biases, lack of constructive deliberations and the 'tyranny of the present', have trapped policymakers in the dilemma of making right decisions.

While it can be argued that no one could have foreseen the outbreak and extent of the pan-

demic for this very year, the stark reality is that we did know it could happen almost every year, especially since the 2014 Ebola outbreak. As a matter of fact, in recent years the United Arab Emirates (UAE) National Defense College has been training national civilian and military future leaders on responding to epidemic crisis scenarios.

Furthermore, Covid-19 coronavirus has been in the process of evolving in China since late December 2019, if not before. The World Health Organization (WHO) issued its first situation report on 21 January 2020. Therefore, it is no surprise when Micah Zenko wrote in Foreign Policy that the coronavirus is the worst intelligence failure in U.S. history, more glaring than any previous disastrous strategic surprises, including Pearl Harbor, the Iranian revolution of 1979, or even 9/11.

Indeed, for any analyst of national security decision making, this is a frustrating outcome. An extensive literature exists which examines past failures and successes to protect national security, especially in the United States. It seems that lessons from past investigations and case studies have not been learned.

Every country, each situation is unique and there is no 'one-size fits all' response to national security problems. At the same time, a number of pragmatic, practical and reproducible features should have allowed every country to act on a level playing field in decision-making.

First, policymakers should adopt the long

and large view as standard, which is particularly challenging in democracies where electoral calendars tilt in favor of the short term. All past, present and emerging issues, their causes, impacts and implications, have to be analyzed and tackled in real or quasi-real time. As such, it is important to listen to every voice, including when they question long-held world views or assumptions. As Michael Dempsey noted, issues are usually more carefully thought out and the best decisions made with inputs from all relevant agencies and departments, as well as subject matter experts, and not just the traditional security-focused staff members. Many governments were blind to the pandemic risk and the few who prepared for this hazard generally put in place botched measures. While the majority of problems allow some lapse of time before anything is implemented, others demand a quick response. At any time, significant signals should be detected and dealt with as appropriate. South Korea started producing testing kits for Covid-19 coronavirus immediately after the first patient was reported in China.

It is important to listen to every voice, including when they question long-held world views or assumptions

Best decisions are made with inputs from all relevant agencies and subject matter experts

Second, in relation to the long and large view, governments need to systematically identify and account for policy lags and political and operational externalities of every day's decisions and any failures to confront problems. Some of this process may grow silently and take decades to erupt. An important implication here is the need to carefully assess risks. When a risk is irreversible, leaders should follow the principle of precaution and avoid it by any means. A plague can bring a prosperous nation to its knees or precipitate redistribution of power. The principle of proportionality is also relevant. As it happens, countries ought to balance their re-

sponse to the spread of coronavirus, accounting for various national priorities and future generations. In effect, the Covid-19 pandemic has proven to be a real test for both principles.

Third, governments should work more on the final stage of the decision-making cycle: implementation and review. Most decisions vanish in the implementation phase. The role of the national security team is particularly important in coordinating and overseeing the work of operational agencies on national security and foreign policy issues. A modern-day and well-functioning national security architecture is one that effectively runs the interagency process for analyzing threats, challenges and opportunities, crafting options, and then takes its recommendations, repeatedly if necessary, to the head of the Executive Branch. In this regard, a country such as the UAE is a model of high policy integrity and effectiveness in national security decision-making, as proven by the Covid-19 pandemic. The authorities kept calm and assured the public of the availability of substantial strategic reserves of food and medicine.

The 2014 Ebola outbreak in West Africa was indeed a wake-up call. Ebola was confined to three West African countries (Guinea, Liberia and Sierra Leone) essentially because its symptoms were not silent and the virus did not spread through the air. We may face grimmer times if the next pandemic is very communicable and deadly. Now everyone must see that the interconnected and nuclear-deterred world needs to prepare for the next catastrophic war which is not a military confrontation involving strategic bombers or ballistic missiles. The time has come to develop ‘germ gaming scenarios’ and get ready for the next biological battle, whether it is a natural hazard or bio-weaponization by rogue actors. With a ‘white swan’ in the form of a demographic time bomb already set in motion by high fertility rates in Africa, Middle East, and Central and Southern Asia, the ‘doomsday clock’ is already ticking.

References

1. Dempsey, Michael P., 2017. A Guide to Better National Security Decision-Making. War on the Rocks. December 4, 2017
2. World Health Organization (WHO), 2020. Novel Coronavirus (2019-nCoV) Situation Report – 1. 21 January 2020
3. Zenko, Micah, 2020. The Coronavirus Is the Worst Intelligence Failure in U.S. History. Foreign Policy, March 25, 2020.

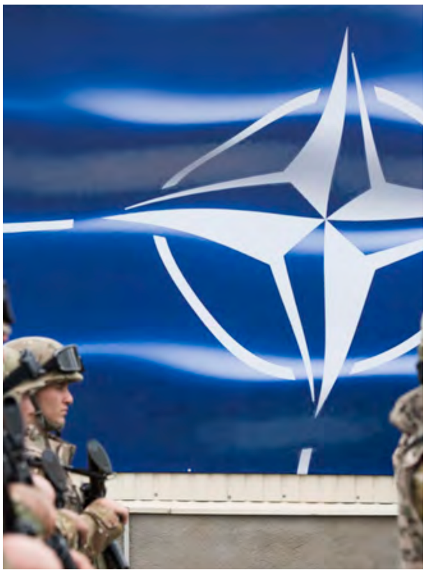
The Evolution of Collective Self Defense

Insights from a UAE partner: NATO

Following the carnage of World War II, the creation of the United Nations (UN) aimed to put an end to inter-state violence through a system of collective security. If there were any threats to international peace, breaches of the peace or acts of aggression, the UN Security Council would decide on what measures to take to restore international peace and security. There was one proviso, however. Under Article 51 of the UN Charter, states could defend themselves against armed attack and they could band together to do so in defensive military alliances (collective self defense). Perhaps the best-known example is the European and North American alliance with which the UAE enjoys a formal partnership: the North Atlantic Treaty Organization (NATO) established in 1949. Article 5 of its founding treaty provides for the collective defense of its member states in accordance with the UN Charter.

Brooke A. Smith-Windsor, Ph.D.
Faculty, UAE NDC

NATO was established principally to defend Western Europe from the menace of armed invasion or nuclear attack by the Soviet Union during the Cold War. Conventional and nuclear deterrence prevailed in preventing either eventuality. Nevertheless, on September 11, 2001, one of NATO's member states did suffer a violent attack. The perpetrator, however, was not a state and the means employed were far from conventional. The terrorist attacks on the United States by Islamist extremists hijacking commercial airliners were not foreseen when the UN and NATO were established in the 1940s. So what was the Alliance to do? It is here where we witness a significant evolution in NATO's interpretation of collective self defense. On September 12, 2001, NATO member states for the first time in the alliance's history invoked Arti-



cle 5. Edgar Buckley, NATO's Assistant Secretary General for Defence Planning and Operations from 1999 to 2003, recalls that alongside viewing the use of the aircraft as missiles, the scale of the attack (amount of physical harm inflicted) and its external direction (from Afghanistan) were the determining factors. The result was the deployment of NATO Airborne Warning and Control System (AWACS) aircraft to help safeguard US airspace and the launch of Operation Active Endeavour in the Mediterranean Sea. The latter aimed to demonstrate alliance solidarity in the fight against terrorism and to help deter and disrupt sea-borne terrorist activity. Although technically not an Article 5 operation, NATO's contribution to the US-led war on terror in Afghanistan – International Security Assistance Force (ISAF) – followed soon after. In this way, 2001 was a milestone in NATOs' understanding of its Article 5—henceforth to encompass defence against non-state actors inflicting significant physical harm on alliance territory orchestrated from abroad.

The reinterpretation continued. In 2014, defense against cyber-attacks was formally associated with Article 5 and this approach evolved, in 2018, to include hybrid-attacks as well. The European Center for Countering Hybrid Threats established in Finland (a NATO partner nation) in 2017, describes hybrid threats as, "Coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities, through a wide range of means (political, economic, military, civil, and information)." Both state and non-state actors may be involved exploiting "thresholds of detection and attribution as well as the border between war and peace." For NATO, such threats came into stark relief in a European context with Russia's 2014 annexation of Crimea and alleged disinformation campaigns and malicious cyber activities in the sovereignty and election processes of established and aspir-

IN MEMORY OF THOSE WHO HAVE FALLEN IN NATO OPERATIONS
A LA MEMOIRE DE CEUX QUI SONT TOMBES LORS D'OPERATIONS DE L'OTAN

Hybrid CoE

ant NATO member states.

What does hybrid defense mean in practice? First, NATO is clear that the primary responsibility for responding to hybrid threats or attacks rests with the targeted member state. Second, capacity building for hybrid defense is provided to individual member states on request. The development of NATO Counter-Hybrid Support Teams may be seen in response to the first phase of hybrid activity when, "the adversary is constantly monitoring the situation, exercising reasonably subtle means of influencing whilst gradually improving its assets." Third, reminiscent of its approach to cyber threats, the Alliance is deliberately ambiguous about the point on the escalation ladder where Article 5 would be invoked in response to hybrid activity. There is no official NATO definition of "hybrid-attack" in the public domain. This approach may be interpreted as a deliberate policy of deterrence—to instill in an adversary uncertainty as to the threshold for NATO retaliation. That said, using the previously cited 9/11 response as a guide, it is fair to speculate that NATO would invoke Article 5 only in the event of significant physical destruction or large-scale human causalities on the territory of one of its member states. Reaching that threshold may, in fact, be quicker in the face of hybrid action compared to a limited cyber-attack. Why? Because it is the combination of the aforementioned elements of power employed by an adversary in a hybrid campaign that makes them particularly potent. As with NATO's 9/11 response, external direction of the hybrid-attack also would likely be a pivotal consideration. Furthermore, compared to an isolated cyber-attack, the attribution challenge (identifying the responsible parties) may prove slightly easier given the number of measures employed by the hybrid attacker. Why? Because in the second phase of a hybrid campaign, an adversary launches a more serious operation, "whereby the effect of measures becomes stronger, means more violent and plausible deniability decreases." Lastly, whether preparing for collective defense or deterrence vis-à-vis a hybrid threat, a civilian-military, so-called "comprehensive approach" is recognized as being essential. "Highly networked challenges require highly networked responses" is as a popular NATO mantra in this context. It should come as no surprise, therefore, that in Europe a 2018 joint declaration between NATO (a military alliance) and the European Union (a socio-economic bloc) identified countering hybrid threats as a key shared priority.

In conclusion, NATO's interpretation of collective self defense now provides for responses to terrorist attacks perpetrated from abroad, as well as cyber and hybrid attacks. Since 9/11, there has been little choice given the changed nature of a state's international adversaries as well as the domains and means of operation open to both state and non-state actors. As a NATO partner, the UAE is well placed to reflect on the rationale behind this evolution in developing its own interpretation of self defense under Article 51 of the UN Charter and, should it one day materialize, a collective defense alliance among the Gulf states.

References

1. 1-Edgar Buckley, "Invoking Article 5," NATO Review, 1 June 2006, accessed 12 March 2020, https://www.nato.int/docu/review/articles/2006/06/01/invoking-article-5/index.html.
2. Hybrid COE, "Hybrid Threats," accessed 12 March 2020, https://www.hybridcoe.fi/hybrid-threats/
3. North Atlantic Treaty Organization, "NATO – EU Relations", Factsheet, accessed 12 March 2020, chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-nato-eu-en.pdf
4. North Atlantic Treaty Organization, Brussels Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels, 11-12 July 2018, accessed 12 March 2020, https://www.nato.int/cps/en/natohq/official_texts_156624.htm.
5. North Atlantic Treaty Organization, "Operation Active Endeavour," last updated 27 October 2017, accessed 12 March 2020, https://www.nato.int/cps/en/natohq/topics_7932.htm.
6. North Atlantic Treaty Organization, Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8-9 July 2016, accessed 12 March 2020, https://www.nato.int/cps/en/natohq/official_texts_133169.htm.
7. North Atlantic Treaty Organization, Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, United Kingdom, 4-5 September 2014, accessed 12 March 2020, https://www.nato.int/cps/en/natohq/official_texts_112964.htm.
8. North Atlantic Treaty Organization, The North Atlantic Treaty, 1949, accessed 12 March 2020, https://www.nato.int/cps/en/natolive/official_texts_17120.htm.
9. United Nations. Charter of the United Nations, 1945, accessed 12 March 2020, https://www.un.org/en/charter-united-nations/index.html.

Bringing CVE 'Front and Center' in the UAE National Security Lexicon

Since the end of the Cold War, the conceptual boundaries of security have undergone a dramatic change and broadened to include a new range of issues and actors. While traditional notions of security are statist and involve the application of military force and securing the nation against external threats, non-traditional security problems are trans-national in scope and coequally affect either threats to states and citizens by non-state actors and/or threats to livelihood and wellbeing. In the policy sphere, this 'conceptual broadening' of security has resulted in a shift, not only in how national security bureaucracies understand and respond to security problems, but in the sorts of the issues that are labeled 'national security problems' in the first place.

Joshua Snider, Ph.D.
Faculty, UAE NDC

Amidst the myriad of emerging security threats faced by national security managers, the challenge posed by religiously motivated extremism is particularly insidious. In states all over the world (and within every religious tradition), some individuals and groups use sectarian language and imagery to alter the ideological moorings of the modern nation-state. Religio-political extremism manifests in several contexts. In some cases, leaders of states instrumentalize religio-political forces to achieve certain ends. In contrast, in other cases, religio-political actors strive to unseat or radically alter the political formation of states, through a mix of violent and non-violent means. In Muslim-majority states, the religio-political extremism associated with Islamist movements has proven to be a potent force and existential challenger to notions of modern nationalism and citizenship. Over the past twenty years, the rise of movements such as Al Qaeda and ISIL and the ongoing trends of Jihadi conflict volunteerism demonstrate the ongoing appeal of extremist ideology and the need for states to incorporate specific counter-violent extremism (CVE) policy into state national security planning. In essence, we see that the struggle against Islamist-inspired religio-political extremism is a prototypical non-traditional security problem to the extent that it, i) does not respect borders, ii) does not involve 'securing the state' from external state actors and iii) strategies to combat extremism rarely involve the application of military power alone. While military force can be used to combat extremism (usually in conflict or post-conflict settings), CVE policy is more often than not conducted quietly, via a mix of intelligence gathering, information sharing, community policing, pastoral care and social work.

This article elucidates the UAE's approach to CVE, highlighting how it has leveraged the 'threat' and 'challenge' posed by religio-political extremism into an 'opportunity,' successfully integrating CVE agendas into its national security strategy – both domestically and internationally. To unpack this theme, we will explore the UAE's unique context for extremism, the evolution of its CVE policy, and the distinct domestic and international contours of its CVE agenda. All of this will be offered in attempt to show how religio-political extremism functions as a non-traditional security problem and how state responses to this problem via CVE policy can have the dual effect of stemming the tide of extremist sentiments while also demonstrating UAE leadership on the global stage.

Definitions/Scope of Activity

There is a need to disambiguate two core concepts; first CVE and the sorts of activities that fall within its purview, and then some discussion on the UAE-specific context of the threat of religio-political extremism and how this is understood in a UAE setting.

Countering violent extremism or 'CVE' is a broad categorical descriptor that denotes a range of state and non-state responses to activism emanating from violent and non-violent religio-political identity movements. While states have been responding to terror and insurgency groups and for generations, the rise of what David Rapoport calls terror's "4th wave" represents

something of a game-changer and necessitates the development of a more sophisticated basket of responses. In this sense, 'CVE responses' tend to be comprehensive and more attuned to root cause dynamics associated with religio-political activism and the complex socio-cultural dynamics which see people adopt the idiom of violent activism. CVE program designs vary, but the core aim is to identify and interrupt an individual's radicalization to violence at an early stage. It does this by de-emphasizing kinetic responses and addressing longer-term ‹push factors,› such as material dispossession/economic vulnerability, indoctrination, radicalization and/or violent transformation.

As a category of religio-political identity politics, Islamism is a descriptive term that can be used to identify movements in different parts of the world. Irrespective of the supposed universality of the Islamist ideology, both the origin and growth of movements on one hand and threat perception on the other hand, tend to be local. The UAE's concern with Islamist-inspired religio-political extremism is centered on local iterations of the Muslim Brotherhood, historically the Jam'iat al-Islah movement, which operated openly and quasi-legally for thirty years from the 1970s through the mid2000-s. Unlike the challenge posed by Brotherhood-inspired Islamist groups in other GCC states, Jam'iat al-Islah remained non-violent and focussed its attention on religious and education institutions, most notably the latter. Jam'iat al-Islah activism posed numerous problems. Domestically, there were concerns that Ikhwan narratives might erode national cohesion, challenge loyalty to the leadership, and strip away the UAE›s culture of hospitality, tolerance, and understanding. Internationally, there were concerns that the distinctly trans-national nature of Jam'iat al-Islah ideology, combined with its connection to the broader Brotherhood paradigm and its tangential relationship to Jihadist movements in the Levant, posed its own set of security concerns. Similar to other religio-political extremist movements, the blurred lines between rhetorical/intellectual activism and modalities of support lead directly to violence or indirectly via material support for persons who advocate the use of violence at home or abroad. Suppression activities began in the early2000-s and escalated following the Arab Spring. By all accounts, the group›s activities and public presence have been curtailed.

CVE and the National Security Agenda

While the UAE's initial interest in CVE came from a desire to stem the tide of Ikhwan narratives, the momentum in CVE policy continued long after Islah's influence was quashed. Rather than being articulated through a particular policy, law, or single implementing agency, it is more helpful to see the UAE›s CVE policy as one that happens informally at multiple levels of government across various agencies. That said, the evolution of the UAE's CVE's agenda and its incorporation into the UAE national

security policy occurred as a re of several reforms. These incl i) key legislative changes, ii) creation of new institutions, iii) broad inclusion of modera and CVE discourses in natic security policymaking at fore and domestic levels and iv) ac UAE participation and sponsors of CVE-related ‹track 2› initiative

Between 2004 and 20 key changes in the legisla sphere served the dual func of formalizing a national posi on acceptable and unaccepta modalities of religio-political activism while simultaneously codifying core national values concerning tolerance and peaceful coexistence. Federal Decree # 1 'Combating Terror Crimes' was enacted in 2004 and provides necessary guidance on what constitutes terror activity, and Federal Decree # 7 enacted in 2014 clarifies Federal Decree # 1 by designating terror organizations. Significantly, this legislation criminalized membership or affiliations with many religio-political movements, including a range of groups affiliated with the Muslim Brotherhood, both in the UAE and abroad. Also, an anti-discrimination law was issued in July 2015 following a decree by UAE President His Highness Sheikh Khalifa bin Zayed Al Nayhan, which criminalizes any act of discrimination based on religion, caste, doctrine, race, color or ethnic origin.

In addition to legislative reform, one of the main innovations to emerge from the CVE agenda was the creation of dedicated CVE-related institutions and repurposing existing institutions in the service of CVE agendas. Amongst these, Hedayah and Sawab Centers, and to some extent, the General Authority of Islamic Affairs and Endowments (al-Awqaf) are all noteworthy and have distinguished the UAE as a center of excellence in the fight against religio-political extremism. These 'CVE institutions' serve distinct purposes, and all reflect a core understanding that one of the best ways the UAE could participate in the global CVE conversation was to help build capacity via knowledge transfer. Hedayah was established in 2012 and is a think tank and research

center that works on global 'best practices' in areas related to CVE generally with a focus on issues outside the UAE. Sawab was established in 2015 and is a digital communications hub designed to degrade Islamist extremists and particularly Daesh/ ISIL propaganda. The center is a joint venture between the UAE and the USA under the framework of the Global Coalition to Counter Daesh (GCCD). Finally, the General Authority of Islamic Affairs and Endowments (al-Awqaf)) plays an important, if not entirely appreciated role in the direction and implementation of CVE activities at both international and domestic levels. While not a ‹CVE institution› in the traditional sense, it is instrumental in the fight against religio-political extremism at the local level. To the extent that it mediates sectarian disengagement (deradicalization) and prevention activities, it also directs overseas developed assistance to Muslim causes, which by default, makes it a CVE capacity-building organization.

The final area of innovation in the UAE›s overall CVE agenda is the emergence of what might be called ‹CVE diplomacy› or the deliberate inclusion of CVE in various strategic and diplomatic initiatives. Here we see a direct and unambiguous link between CVE and the UAE›s external national security interests. In 2015, the UAE led the UN Security Council›s Contact Group on Countering Extremism with participation in other 'track 1' efforts including, i) the Global Counter-Terrorism Forum (GCTF), ii) The Global Coalition to Counter Daesh (GCCD) and iii) the Islamic Military Alliance to Fight Terrorism (IMAFT).

The UAE›s participation in 'track 2' CVE-related initiatives includes the Muslim Council of Elders and the Marrakesh Declaration, devoted to the protection of religious minorities in Muslim-majority countries. In addition to participating in coalitions and international forums, another emerging facet of the UAE›s CVE diplomacy is the bilateral capacity building and the extent to which CVE is becoming a focal point of development assistance. Some of the UAE›s most stalwart allies in the Muslim world face a very serious challenge from religio-political actors and require support, and for optics' reasons, would prefer to reduce dependence on Western donors in the delivery and funding of CVE programming.

Moving Ahead

Religio-political extremism is clearly one of the leading security challenges of our age, and there is a critical need for states to incorporate CVE agendas into national security strategies. Security practitioners and scholars must transcend outdated ‹statist› Cold War mentalities and appreciate the importance of non-traditional security threats, ostensibly delinked from concepts of state sovereignty, borders, and/or traditional warfighting. The struggle against religio-political extremism is one such emerging security threat, and it must be taken seriously. This article has shown how the UAE perceives the threat posed by religio-political extremism, how it responded and how it elevated this response into a broader agenda to strengthen existing partnership, build institutions and boost its own presence on the international stage. In moving forward, the UAE might further leverage this success of its CVE agenda and think about ways of linking CVE capacity-building agendas to the provision of much-needed development assistance across Africa, South and Southeast Asia.

References

1. Caballero-Anthony, M. (ed.). 2016. An Introduction to Non-Traditional Security Studies – A Transnational Approach. Sage Publications, London.
2. There is a vast scholarship addressing definitions and typologies of Islamist movements in different parts of the world. See, for example, Musallam, A., 2010. From Secularism To Jihad: Sayyid Qutb And The Foundations Of Radical Islamism. Westport: Praeger.
3. Wilson Center. 2020. U.N. Warns Of ISIS Resurgence. [online] Available at: <https://www.wilsoncenter.org/article/un-warns-isis-resurgence> [Accessed 1 April 2020].
4. Rapoport, D., 2002. The Four Waves of Rebel Terror and September 11. Anthropoetics: the journal of generative anthropology, [online] 2)8). Available at: <http://wrldrels.org/wp-content/uploads/02/2016/Rapoport-Four-Waves-of-Terror.pdf> [Accessed 1 April 2020].
5. Koehler, D., 2017. Understanding Deradicalization: Methods, Tools And Programs For Countering Violent Extremism. Abingdon: Routledge, pp.9-1.
6. US Department of State, 2019. Breaking Pathways To Violent Radicalization: A Review Of Countering Violent Extremism Intervention Programs. Washington DC: US Department of State - Bureau of Conflict and Stabilization Operations.
7. Wiktorowicz, Q., 2003. Islamic Activism: A Social Movement Theory Approach. Bloomington: Indiana University Press, pp.34-1.
8. Freer, C., 2018. Rentier Islamism: The Influence Of The Muslim Brotherhood In Gulf Monarchies. New York: Oxford University Press, pp.139-129.
9. Kruse, M., 2016. Countering Violent Extremism Strategies in the Muslim World. The ANNALS of the American Academy of Political and Social Science, 1)668), pp.209-198.
10. Hedayah, the international center of excellence for countering violent extremism. 2020. [online] Available at: <https://www.hedayahcenter.org> [Accessed 31 March 2020].
11. Kruse, M., 2016. Countering Violent Extremism Strategies in the Muslim World. The ANNALS of the American Academy of Political and Social Science, 1)668), pp.209-198.

US ‘Energy Independence’ and America’s Role in the Gulf

Since the 1980s, the United States has committed significant military resources to maintain stability in the Gulf region. This commitment has stemmed in large part from a desire to ensure the free flow of oil through the Strait of Hormuz, which has long been essential to the vitality of the global economy. Over the past decade, however, US domestic oil production has increased significantly, ending a prolonged decline that began in 1970.

Nikolas Gardner, Ph.D.
Faculty, UAE NDC

While in 2008 the United States produced approximately 6.8 million barrels of oil per day (bpd), by 2018 this figure had more than doubled to 15.3 million, making it the leading producer of oil and natural gas liquids in the world (BP Statistical Review of World Energy, 2019, 16.) On several occasions in 2018 and 2019 weekly exports of American oil and other energy products exceeded imports (Husari, 2019).

This has led to claims that the US has attained “energy independence”. As US dependence on foreign oil has decreased, American military and political leaders have questioned the necessity of maintaining a significant military presence in the Middle East. In 2019 General Paul J. Selva, then Vice Chairman of the Joint Chiefs of Staff, asserted that the US was, “Not wholly dependent on the movement of Saudi, Kuwaiti, Qatari, and Emirati oil in and out of the Gulf to sustain our economy”

US oil imports have diminished as American domestic production has increased

(Husari, 2019). President Donald Trump went further, claiming that, “We are independent, and we do not need Middle East oil” (Egan, 2020).

Not surprisingly, US oil imports have diminished as American domestic production has increased. But is it really the case that the United States is no longer dependent on foreign oil? A closer examination of the global oil market reveals this assumption to be incorrect, for several reasons. First, the United States still uses more oil and petroleum products than it produces, by a significant margin. While American oil production exceeded 15 million bpd in 2018, the US consumed more than 20 million bpd (US Department of Transportation). Not only does America use more oil than it produces, it also imports more oil than it exports. This is due to a ‘mismatch’ between the grades of oil produced domestically and those required by American refineries. Oil extracted from shale formations, which accounts for the vast majority of the increase in American production, consists primarily of light, sweet crude. However, many American refineries are configured to process heavier crudes, which must be imported (Levine et.al., 2014, 5). Thus, in 2019, the United States imported nearly 6.8 million bpd to meet this demand. While the majority of this imported oil came from Canada, Mexico and elsewhere in the western hemisphere, the US continued to import approx-

imately one million bpd from the Gulf (EIA, 2020).

Even if it no longer imported foreign oil, the United States would remain subject to fluctuations in the global price of the commodity. Different types of crude sell at different prices, depending on factors such as grade and transportation costs. But in general terms, the price of oil is determined by global supply and demand (Levine et.al., 2014, 6). As a result, war and political upheaval thousands of miles from the United States can drive up the prices American consumers pay for gasoline and other petroleum products. The US government is not well equipped to respond to rapid changes in the price of oil. In OPEC member states as well as other large producers such as Russia and Mexico, national oil companies (NOCs) control most oil reserves and production. These states can increase or decrease production relatively quickly in order to influence oil prices, particularly if they have large reserves as do Russia and Saudi Arabia. In comparison, the US government has little influence over the private companies that produce oil in the United States. While higher prices may provide an incentive to increase production, the extent to which individual companies will do so depends on their own capacity and calculations about profitability. Thus, the US government remains dependent on Gulf oil producers to compensate for global supply shortages that drive up domestic oil and gasoline prices. In 2018, for example, President Trump asked Saudi Arabia to increase its production to replace oil removed from the global market by sanctions against Iran (Egan, 2020).

While its consumers continue to feel the negative effects of shortfalls in global oil production, American oil companies are vulnerable to supply gluts. In comparison to NOCs in other large oil producers such as Saudi Arabia and Russia, shale oil companies in the US face relatively high production costs. Oil can be pumped from existing Saudi and Russian fields for less than USD 5 per barrel, but American shale producers break even only at USD 35-45 per barrel. Moreover, unlike their state-owned competitors, private companies face more immediate pressure to repay outstanding debt and provide positive returns for their investors. Thus, when oil prices fall below USD 30 per barrel, as they have in early 2020, these companies must curtail production in order to cut expenses, or worse, go out of business entirely (Daiss, 2020). If these low prices persist, shale production will decline, once again increasing US dependence on foreign oil. As has been the case with high oil prices, addressing low prices before they threaten American shale production will require negotiation with OPEC producers, particularly Saudi Arabia.

Thus, it is misleading to claim that the United States has attained anything resembling energy independence. Not only do US refineries remain dependent on the import of grades of crude oil unavailable domestically, but US consumers remain exposed to higher global oil prices while producers are exceed-

ingly vulnerable to lower prices. Ensuring stability in the Middle East, and particularly the Gulf, therefore remains very much in America's national interest. While American dependence on oil from the Gulf region has diminished in recent years, the Middle East still accounts for a third of global oil production, and more than 20% of the world's oil supply transits through the Strait of Hormuz (EIA, 2019). Ensuring the uninterrupted flow of this oil, and maintaining strong relations with GCC oil producers, are essential to the US economy and the American shale oil industry. We should therefore be skeptical of predictions of an imminent American departure from the Gulf region and the consequent emergence of a security vacuum to be filled by other great powers. Crises in the Middle East will never be the only concern of American leaders responding to domestic issues and security threats elsewhere. Other powers, particularly China and India, may take an increasing interest in safeguarding regional stability. Nevertheless, continued American dependence on oil from the Gulf will mean that the United States will preserve a significant presence in the region for the foreseeable future.

References

1. BP Statistical Review of World Energy, 2019.
2. Daiss, Tim. "Who will Cave first in Saudi-Russia Oil Price War?" Asia Times. 18 March 2020. https://asiatimes.com/2020/03/who-will-cave-first-in-saudi-russia-oil-price-war/ (accessed 20 March 2020).
3. Egan, Matt. "Trump Says American Doesn't Need Middle East Oil. It's Not That Simple." CNN Business. 8 January 2020. https://edition.cnn.com/2020/01/08/business/oil-middle-east-trump-iran/index.html (accessed 24 March 2020).
4. Husari, Ruba. "Shale Oil and the Illusion of US Energy Independence". Middle East Institute. 15 July 2019. https://www.mei.edu/publications/shale-oil-and-illusion-us-energy-independence (accessed 25 March 2020).
5. Levine, Steven et. al.. "Understanding Crude Oil and Product Markets". American Petroleum Institute. 2014. https://www.api.org/oil-and-natural-gas/energy-primers/crude-oil-and-product-markets (accessed 22 March 2020).
6. US Department of Transportation, "Overview of U.S. Petroleum Production, Imports, Exports, and Consumption." 2019. https://www.bts.gov/content/overview-us-petroleum-production-imports-exports-and-consumption-million-barrels-day (accessed 25 March 2020).
7. US Energy Information Administration (EIA), "The Strait of Hormuz Is The World›s Most Important Oil Transit Chokepoint." 20 June 2019. https://www.eia.gov/todayinenergy/detail.php?id=39932 (accessed 24 March 2020).
8. US Energy Information Administration (EIA). "How Much Petroleum Does the United States Import and Export?" 3 March 2020. https://www.eia.gov/tools/faqs/faq.php?id=727&t=6 (accessed 24 March 2020).

تخريج دورة الدفـاع الوطنـي السابعة 2020 / 2019
الأربعاء 2020 / 6 / 17