KONRAD ADENAUER STIFTUNG

ACADEMIC PEACE ORCHESTRA MIDDLE EAST

POLICY FORUM

ON CBRN CHALLENGES/TERRORISM & DISARMAMENT/ NON-PROLIFERATION IN THE MIDDLE EAST/GULF

ACADEMIC PEACE ORCHESTRA MIDDLE EAST

No. 6 • JUNE 2019

The European Union's Centres of Excellence Initiative on CBRN Risk Mitigation

Innovative Approaches for the Disruptive Security Environment

Nasser Bin Nasser

This POLICY FORUM sets forth some of the most disruptive changes witnessed over the past decade, and assesses their impact on the security environment. It goes on to emphasize the need for security governance approaches and frameworks that are flexible and adaptive to changing security landscapes. In doing so, the POLICY FORUM exemplifies the European Union's (EU) pursuit of such a framework to effectively address these changes, in the form of the EU Centres of Excellence Initiative on Chemical, Biological, Radiological, and Nuclear (CBRN) Risk Mitigation.

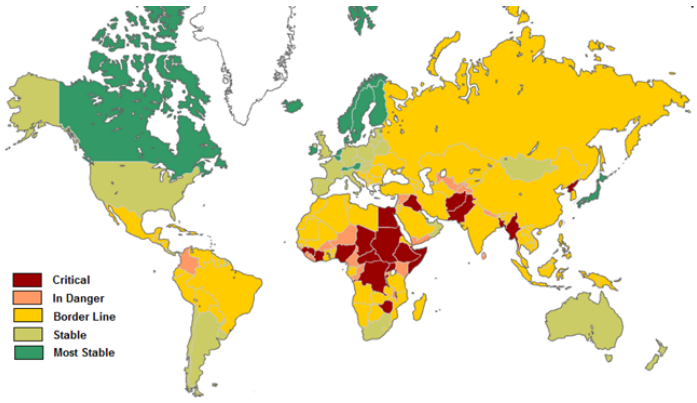
Background and Central Argument

The global security landscape has been greatly influenced by a number of transformative changes during the past decade. New globalizing factors such as the Information and Communications Technology (ICT) Revolution and new domains of warfare such as cyber and biotechnology have challenged traditional security governance. The Middle East is not immune to these changes, but is further challenged by its own unique security conditions following the onset of the Arab Spring and the unprecedented growth of non-state actors. This POLICY FORUM argues for the need to continually develop new operational models for security governance in the face of the new security environment, and highlights the importance of the response of the European Union Chemical, Biological, Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU CBRN CoE).

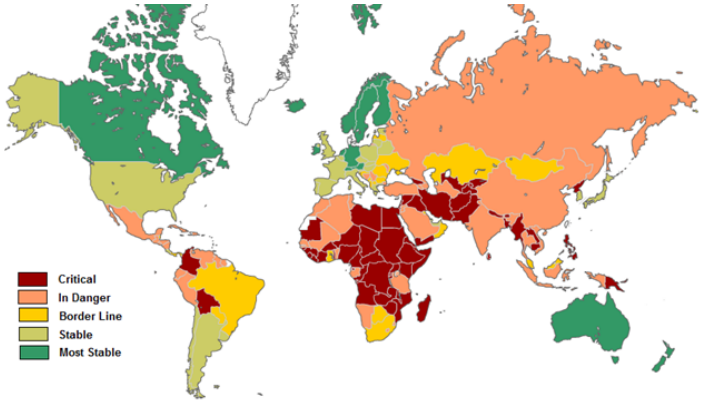
The Changing Security Environment

The Arab Spring uprisings, with a few exceptions, largely failed to achieve their intended promise of peace, justice, and democracy in the Middle East. A predominant view is that the ensuing chaos had a negative impact on regional security because it led to the weakening of states and the growth of ungoverned spaces or security vacuums. While these ungoverned spaces are not literally ungoverned, they are usually ruled by authorities other than the formal state, and can be characterized by either the absence of a formal state, or by limited or anomalous government control. Though ungoverned spaces are not necessarily failed or failing states, reference to the *Fragile States Index (FSI)*[1] can give some indication of the growth of these areas in the period prior to and following the Arab Spring. Notwithstanding criticisms that have been levied against the methodology used for the development and compilation of the *FSI*, the *Index* remains one of the only and most comprehensive tools to gauge the underlying relationship between security and ungoverned spaces. The adapted map used from the *Index* shows a stark contrast of the growth of failing states during the period 2007 to 2015, bearing in mind that a key characteristic of failing states is the presence of ungoverned spaces within their borders.

Map No. 1: Adapted Fragile States Index 2007



Map No. 2: Fragile States Index 2014



1 The *Failed States Index* produced by the Fund for Peace was officially changed to the *Fragile States Index* in 2014. The categories 'ranking states' as well as some of the methodology used to compile the ranking were reportedly also changed. These two maps are adapted from the Fund for Peace *Fragile States Index* to show consistent terminology of categorization and should not be considered the production of the Fund for Peace.

Ungoverned spaces are problematic for security governance for a number of reasons including the following:

First, ungoverned spaces challenge traditional security concepts. Regional security today is no longer contingent upon the long-held belief of balance of power between states. The risk of a war between states, in which states pose threats to each other, has been supplanted with the risk associated with war within states, with weak and fragile states increasingly becoming a core determinant of regional security.

Second, ungoverned spaces are the perfect breeding ground for non-state actors; these can either be terrorist or criminal organizations, given the ever more blurring lines between both. The so-called 'War on Terror' and the subsequent reduction of financing available to terrorist organizations has pushed them to increasingly depend on crime to fund their activities. Both groups of non-state actors ultimately capitalize on and benefit from each other's experiences, structures, and networks. In consequence, they utilize similar schemes to generate funds and establish control (kidnapping, extortion, racketeering, obstruction of justice, targeted assassinations), and operate on intersecting network structures, such as illicit trafficking. Reports indicate that the global black market is valued at $10 trillion, making it the world's fastest growing economy and a clearly attractive source of funding for non-state actors (Neuwirth, October 7, 2011). The RAND Corporation estimates that the so-called Islamic State of Iraq and Syria accrued approximately $6 billion during its reign in both countries, making it the richest non-state actor in history (Clarke, September 7, 2018).

Third, ungoverned spaces create new vulnerabilities in the form of refugees flowing across borders and internally displaced communities. These vulnerabilities add to the security and economic burdens of host and transit countries. According to United Nations Refugee Agency (UNHCR, June 19, 2018), there are about 25 million refugees worldwide, 57 percent of whom have come from just three countries (Syria 6.3 million, South Sudan 2.4 million, and Afghanistan 2.6 million). Incidentally, the top source countries for refugees are also classified as "most critical" in the *Fragile States Index*.

Regional and global networks of terrorists and criminals came to occupy the many ungoverned spaces created by weakened states, effectively eroding borders and de-territorializing states and posing new challenges to security governance. These impacts were further compounded due to the role of other globalizing forces, namely the ICT Revolution and the Fourth Industrial Revolution.

The ICT Revolution has allowed non-state actors to better organize and coordinate dispersed activities and tasks. Similar to the large numbers of private corporations that have embraced ICT to operate more efficiently and with greater flexibility, non-state actors have also harnessed the power of ICT to enable new operational doctrines and forms of organization. And just as companies in the private sector are forming alliance networks to provide complex services to customers, so too are terrorist groups 'disaggregating' from hierarchical bureaucracies and moving to flatter, more de-centralized, and often changing webs of groups united by common objectives. Consider for a moment the following figures that highlight the changed scope and complexity of information which can be shared today, compared to over a few decades ago, as well as the speed in the adoption of new platforms that enable this:

- It took 75 years for 50 million people to adopt and get access to the telephone, whereas it took Facebook two years and YouTube 10 months (Interactive Schools, February 8, 2018).
- As of the third quarter of 2018, Facebook had 2.27 billion monthly active users, compared to 100 million users in 2008 and one billion users in 2012 (Statistica).
- In 2017 it was estimated that YouTube users uploaded around 400 hours of content every minute (Bergman, February 28, 2017).

While the ICT Revolution largely refers to the ongoing digital revolution, the Fourth Industrial Revolution more accurately describes the transformative potential of new technologies and their fusion that are transforming the nature of conflict and international security. This can include fields such as artificial intelligence, robotics, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, and quantum computing. These technologies have created new domains of conflict such as the virtual and biological ones and have also transformed the military instrument, including 3-D printed weapons and autonomous weapons that use artificial intelligence. Most significantly, however, is that these technologies have obscured many of the generally discernable distinctions between war and peace, military and civilian, physical and virtual, and violence and non-violence (Schwab, January 14, 2016).

In short, while these developments have a tremendous opportunity to positively impact global security through their legitimate use, at the same time, they are giving advantage to non-state actors as well. Because the landscape is favoring and strengthening network forms of organization, this has led to an erosion of the knowledge advantage previously, and to an extent exclusively, maintained by security organizations – in turn, this has reduced the cost structure of information previously deemed to be accessible only by them.

According to the European Commission's Adviser to the Directorate-General for International Cooperation and Development on Security and Nuclear Safety, "[e]xpanding global trade and interconnected data networks also increases the opportunities for state and non-state actors to acquire dual-use equipment and technology. These threats and trends are exacerbated by rapidly-changing technologies (e.g., additive manufacturing, powerful computer-aided design applications and cyber-attack tools) and greater diffusion of dual-use knowledge that may provide proliferators easier access to WMD [weapons of mass destruction] capabilities. Moreover, increased intangible technology transfers, such as the transmission of software and technology by electronic data, including brokering and transit, pose new challenges for verification and control". (Van der Meer, May, 2018)

The changed security landscape as a result of these disruptions necessitates new approaches and tools for security governance. While it is unlikely that there will ever be an alternative for traditional top-down security governance, there is an increasing need for new operational models to supplement, yet not altogether replace, existing models. The former Director of Security Policy at the European Union refers to this as a horizontal governance mechanism that brings together broader communities of policy-makers, users and scientists to assess their potential contribution to collective safety and security (Jenny, November 9, 2017). For instance, given that developments in artificial intelligence, biotechnology, and 3-D printing are no longer being driven by states, state actors need to work with these communities of users to assess, regulate and manage the potential misuses of these technologies in a way that they would not have had to two decades ago.

The European Union's Centres of Excellence Initiative – a New Operational Model for Security Governance

The EU CBRN CoE, which was launched in 2010, promotes this new operational model and framework for security governance. To begin with, the Initiative places the onus on partner countries to better define their needs so that they can be met by tailor-made projects designed and funded by the European Union. This challenges the traditional model of donor assistance where donors either typically identify these needs on behalf of partner countries or, from a more pessimistic perspective, pursue opportunities to meet their own needs. The EU's bottom-up approach is especially novel for three reasons:

Whole-of-government approach: In order to identify their needs, partner countries are required to establish National CBRN Teams that oversee the development of national needs assessment processes and national CBRN plans. As a result, partner countries are inadvertently promoting and legislating the whole-of-government approach rightly believed by the EU as being necessary to effectively address relevant risks. An innovative approach such as this addresses a key challenge across regions like the Middle East where there is an overreliance and an overdependence on security organizations for anything deemed to be security-related, including CBRN risks. By forming National CBRN Teams, non-security organizations such as Ministries of Health and Agriculture, for instance, are forced to become partners and play their respective roles, which are critical in the area of managing biological risks. Likewise, non-governmental organizations such as universities and think tanks can also be members of National CBRN Teams and provide much needed insights from unique perspectives.

Knock-on effects: The requirement to conduct needs assessment processes and other similar mechanisms also builds functional long-term capabilities required for security governance. This includes (but is not limited to) capacities such as gap analyses, proposal writing, and monitoring and evaluation. The EU and other international partners recognize that the development of such capacities can help overcome key obstacles related to administrative shortcomings. In the Middle East, as is the case in other parts of the world, many of the administrative and organizational capacities needed to support enhanced CBRN are less developed when compared to the technical subject matter expertise that is often already present. This can be problematic in more ways than one, because not only does it restrict a country's ability to effectively utilize and benefit from this local source of expertise, but it can negatively distort the perception of a country's capacity to address these risks as well.

Regional cooperation: In order to foster much needed regional security cooperation, the Initiative establishes Secretariats to liaise with partner countries and organize regional roundtable meetings that identify common needs across partner countries. Considering that the EU prioritizes project funding for proposals that have a strong regional dimension, partner countries are encouraged to consider how to best address threats cooperatively. They also regularly utilize the Regional Secretariats as an apolitical space where seemingly sensitive discussions can be held and best practices can be exchanged. This is an effective way to overcome the common perception of a lack of security cooperation across the region, which is critical given that these are cross-border threats that cannot be addressed through national solutions alone.

Governments and donors such as the EU are rarely the first actors to evoke a sense of innovation, and security governance is certainly not a field that comes to mind when considering disruption. Yet the Centres of Excellence Initiative is a good example of how even a large sprawling bureaucracy such as the EU can challenge a traditional security governance model in progressive ways. Through the Initiative, the EU was able to achieve three goals:

1. Establish a network-based approach within countries and across regions to address CBRN risks and match the network-based approach of non-state actors.
2. Broaden the network of security actors within states to tap into capabilities that would otherwise not be utilized.
3. Allow users to define the growth and trajectory of the Initiative to match their needs.

In this sense, the Initiative has outgrown its initial form and adapted to the needs of the users. While the EU continues to offer funding for capacity building activities and provide organizational guidance as a whole, the Initiative may look different from its original version and across the various regions and Secretariats where it operates. Owing to the recognition that the Initiative could run the risk of becoming outdated and irrelevant, the European Union has, in fact, encouraged this fluidity. At the time of the EU CBRN CoE's establishment, the changing security landscape necessitated an innovative approach — as new security threats facing the world today continue to emerge, so too should the methods required to address these threats continue to evolve. In this context, the EU CBRN CoE effectively demonstrates how a flexible governance approach can best be adapted toward this end, in an attempt to remain ahead of the curve.

Conclusion and Key Lesson

Given the rapidly and ever changing security environment, it is vital to consider the role of disruption and innovation in the support of security governance. Political considerations aside, a major reason why non-state actors are able to pose the threat that they do is because they are better disruptors than security institutions. This means that security institutions need to play catch-up during every cycle of conflict. It is vital for security institutions to increasingly think as disruptors when facing such adversaries or in failing to do so, to at least create spaces and opportunities for actors from outside government to do this for them through collaborative partnerships. A key lesson of innovators is to always question existing business models, take nothing for granted, and regularly consider new ways in which sectors, processes, and services can be transformed. It is increasingly clear to many that governments can no longer do this alone. ■

References

- *Bergman, Sirena, February 28, 2017*: We Spend A Billion Hours A Day On YouTube, More Than Netflix And Facebook Video Combined, *Forbes Magazine*. Online available at https://www.forbes.com/sites/sirenabergman/2017/02/28/we-spend-a-billion-hours-a-day-on-youtube-more-than-netflix-and-facebook-video-combined/#37bb61595ebd.
- *Clarke, Colin P., September 7, 2018: An Overview of Current Trends in Terrorism and Illicit Finance. Lessons from the Islamic State in Iraq and Syria and Other Emerging Threats.* Testimony presented before the Committee on Financial Services, Subcommittee on Terrorism and Illicit Finance, United States House of Representatives. Online available at https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT498/RAND_CT498.pdf.
- *Fund for Peace, Fragile States Index*: Online available at https://fundforpeace.org.
- *Interactive Schools, February 8, 2018*: 50 Million Users: How long Does It Take Tech To Reach This Milestone? Online available at http://blog.interactiveschools.com/blog/50-million-users-how-long-does-it-take-tech-to-reach-this-milestone.
- *Jenny, Joëlle, November 9, 2017*: Security Risks Reduction through CBRNE Science, Education and Human Factors. World Science Forum 2017, Jordan, Moderator comments (transcript).
- *Neuwirth, Robert, October 28, 2011*: The Shadow Superpower, *Foreign Policy*. Online available at https://foreignpolicy.com/2011/10/28/the-shadow-superpower/.
- *Schwab, Klaus, January 14, 2016*: The Fourth Industrial Revolution: what it means, how to respond. Available at https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.
- *Statistica*: Number of Facebook users worldwide 2008-2018, Number of monthly active Facebook users worldwide as of 3rd quarter 2018 (in millions). Online available at https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.
- *UNHCR/United Nations Refugee Agency, June 19, 2018*: *Figures at a Glance. Statistical Yearbooks.* Online available at https://www.unhcr.org/figures-at-a-glance.html.
- *Van der Meer, Adriaan, May 2018: Promoting a Scientist's Duty of Care 4.0*, Vienna Center for Disarmament and Non-Proliferation. Available at https://vcdnp.org/wp-content/uploads/2018/05/Van-Der-Meer-Adriaan_Scientists-Duty-of-Care-4.0_May-2018.pdf.

The Author

Nasser Bin Nasser *is the Managing Director of the Middle East Scientific Institute for Security (MESIS) and the Head of the Middle East Regional Secretariat of the European Union's Centres of Excellence Initiative on Chemical, Biological, Radiological and Nuclear Risk Mitigation.*

The Editor of the Entire Blue Policy Forum *Series*

Dr. Bernd W. Kubbig*, Coordinator of the* Academic Peace Orchestra Middle East (APOME) – *see http://www.academicpeaceorchestra.com.*