INSIGHTS

SYNERGIA FOUNDATION

OCTOBER 2020 | EDITION III | WEEKLY

SECURING CYBERSPACE IN A CHANGING WORLD ORDER

EXPERT INSIGHTS

Robert Morgues

Senior Director US Cyberspace Solarium Commission, Task Force 2

Laura Bate

Senior Director US Cyberspace Solarium Commission, Task Force 3

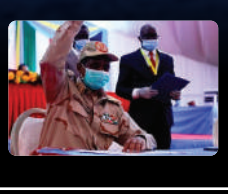
Lt Gen Rajesh Pant

National Cyber Security Coordinator, GOI

MUST READ

- PAKISTANI OPPOSITION – AN EXTREMIST IN THE LEAD

- A SPLINTERED SUDAN SIGNS UP TO BE WHOLE AGAIN



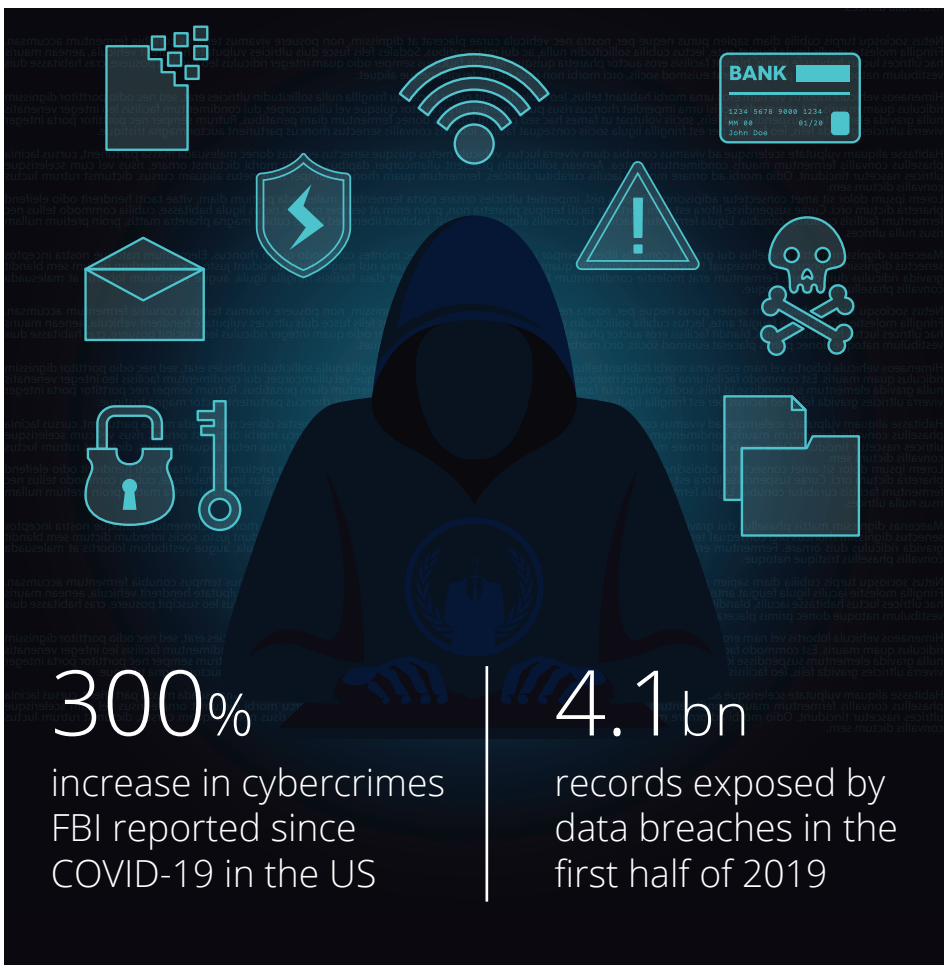
- CAUCASIAN TINDERBOX: ON FIRE AGAIN

INSIGHTS
SYNERGIA FOUNDATION

Girding up to tackle cyberattacks

The U.S. government's Solarium Commission is tasked with evolving strategies against cyber threats and it is drawing up short and long-term plans to mitigate this new-age hazard

Robert Morgues
is the senior director at the U.S. Cyberspace Solarium Commission Task Force 2. The Solarium Commission was created in 2019 with the objective of finding effective strategies against cyberattacks. In the 86th Synergia Virtual Forum, he shared his views on what should be done to make cyberspace more secure.



The U.S. Cyberspace Solarium Commission was born out of the problem of cyberspace attacks, and despite numerous criminal indictments and economic sanctions, the attacks on the United States continued. This showed that deterrents in cyberspace, which is a core tenant of U.S. foreign policy and other security spaces, was failing, through both nation and non-nation state actors. Digital connectivity, which obviously brings with it great benefits, has also created a strategic dilemma.

The bottom line is that the more digital connections people make and the data they exchange, the more are the opportunities for adversaries to destroy lives, said Robert Morgues. The three main points the commission has discerned is: the deterrence isn't working to stop adversaries; public and private partnership is absolutely imperative in crucial areas; and defence and resilience are meaningful differentiators in cyberspace.

COMMISSION FINDINGS

The commission works to answer two questions: what strategic approach will defend the United States against cyberattacks of significant consequences, and what policies and legislation are required to do so. In a series of 80-plus recommendations, many of which have legislative proposals, the strategy of the report is largely layered on cyber deterrence to emphasise national resilience, public-private partnership, the concept of defence as well as international norms, and the need to reform and improve the government structure in the United States to handle cybersecurity.

The short-term goal is to prevent meditated attacks and mitigate the effects of cyberattacks of significant consequence. The long-term target is to create a digital environment that is safe, stable, and promotes continued innovation and economic growth, while protecting personal privacy and ensuring national cybersecurity.

There are three layers to deterrence: one is shaping behaviour, which involves working with allies through aspects like international norms and international cooperation on law enforcement. Second is about denying benefits, securing critical infrastructure networks, collaborating with the private sector, and building a more robust and secure cyber ecosystem as a whole. The third is about imposing costs, which is where one talks about maintaining the capability, capacity and credibility needed to retaliate against actors who target the U.S.

In the report, recommendations are organised around six pillars. The first is that there is the need to reform the U.S. government to function and operate in an era where things move at the speed of cyber. There isn't the capacity or structures in the organisation to address the challenges we face against insiders in cyberspace.

The second one is strengthening norms and non-military tools.

The third is to promote national resilience, which is where one talks about the importance of ensuring continuity of the economy. The

economy is a major pillar of national power and strength in the United States. This also leans into the need to re-shape the cyber ecosystem.

Fourth is to improve the behaviour of online users and make them more aware about secure coding and asking Internet service providers to do more.

The fifth deals with the need to operationalise cybersecurity collaboration with the private sector. Private sector entities have the primary responsibility for defence and security of their networks, and the private sector makes up about 85 per cent of critical infrastructure in the United States, with the remaining either owned by federal government or state municipalities.

The final piece of the puzzle for the commission is to preserve and employ the military instrument of power in cyberspace, as future crises and conflicts will almost certainly contain a cyber component.

Source: UBER

INDUSTRIAL STRATEGY

In one of the initial reports by the commission, there were observations about the need to produce or create an industrial strategy to help secure American high-tech supply chains from malign influence and threats. Right now, the U.S. lacks key industrial capacities for the production of essential technologies, including features like 5G telecommunications equipment. This has forced critical dependency on production in places like China, but also in partners like Japan, South Korea, Taiwan as well as Sweden and Finland. In the commission's view, it undermines American economic competitiveness.

The commission recognised this dependency and lack of strategy and also proposed a five-point plan.

- The need to identify key materials, components, and finished products that are critical to national and economic security.
- The U.S. must ensure minimum viable manufacturing. This doesn't mean the need to produce everything in the U.S. alone, but that one needs to know the capabilities we can trust in a time of crisis.
- To leverage existing efforts to provide greater government support through intelligence and information sharing to help private companies better address supply-chain risks.
- To do more to facilitate the domestic market for finished technologies. If one is going to incubate more manufacturing in the U.S., there needs to be a customer on the other side who is going to buy it.
- The U.S. government must take steps to ensure the competitiveness of U.S. and partner companies in global markets. This is where things like standards come into play, but one observation from the commission is that we would like to talk about a free and fair system of international commerce.

LEADERS AND ATTRIBUTION

On a query by T.M. Veeraraghav, Consulting Editor, Synergia Foundation, on whether there would be a "leader of the pack" -- either a singular entity, or a private enterprise, or a collective of nations -- guiding the way to stability and bringing out an international order, Mr. Morgues said there hasn't always been a singular leader, such as Pax Romana or Pax Britannia. Right now is the period where we might see more multi- or at least bipolarity in the international system. When one talks about international relations, a profit-motive company stepping up to the forefront is very unlikely to be the one that sets the guardrails or tone of the discussion.

To a query on whether there will be a time frame or a mechanism by which one can develop that international trust, since as much as the idea is about national security, it is implementable only when there is a sense of international camaraderie, Mr. Morgues explained that the commission had found that the U.S. government needs to be a more mature

INSIGHTS
SYNERGIA FOUNDATION

partner with the private sector. The Infrastructure Security Agency in the U.S., for example, which is part of the Department of Homeland Security, is a great concept. However, the government doesn't have a good way of reaching out to the company that they know the attack is emanating from, and getting the information they need from it.

One of the major barriers to operational international collaboration on this front is the mutual legal assistance treaty (MLAT) system. We also talk about the need to improve U.S. capacity and the Department of Justice capacity in the cases in the MLAT backlog.

On the intelligence front, Mr. Morgues said the private sector necessarily doesn't need to be driving intelligence collection, but there is the need to recognise that the private sector, both in the U.S. and around the world, is critical to cyber defence.

Finally, for attribution, international cooperation as well as public-private collaboration is lacking. There is no individual in the White House that has the authority as a national cyber director. One of the proposals the commission is working through Congress is to institutionalise a national cyber director position in the White House that gives the private sector and international partners a person they know they can call, and that person has tendrils out into the rest of the administration.

The U.S. Cyberspace Solarium Commission was born out of the problem of cyberspace attacks, and despite numerous criminal indictments and economic sanctions, the attacks on the United States continued

The private sector has a competitive advantage in data gathering, synthesis, and analysis, but there are certain things that the private sector cannot do, in terms of intelligence and authority, which are always going to reside in government. There is a certain value that can be added from the government. Through the commission, they're working for the creation of a joint collaborative analytical environment where we have folks from the private sector and the government coming together and sharing.

EXPERT QUESTION

CRITICAL THREATS TO DEMOCRACIES AND HOW TO COUNTER THEM

M.K. Narayanan was the National Security Adviser of India from 2005 to 2010. Subsequently, he served as Governor of West Bengal from 2010 to 2014. His questions to Robert Morgues at the Synergia Virtual Forum.

M.K. Narayanan: Is it possible to categorise the five critical cyberthreats to democracies across the world, and what would be the minimum protection available to institutions and governments against such threats?

Robert Morgues: The first threat is the power actors, through cyberspace, possess to undermine confidence in democratic institutions.

The second is the threat to operational technologies, and this is where one gets into cyber-physical systems and the potential ability for disruptive cyber actors to not only disrupt in cyberspace, but disrupt in real life. We've seen in Ukraine where the lights have gone out for a long period of time by a cyberattack. We have also heard rumours of other disruptive attacks that cause physical damage, like the ransomware attacks on hospitals that are increasing in number, and at least in Germany, they have directly attributed deaths due to ransomware in hospitals.

The third is a more systemic challenge that the United States and other democracies face, which is the battle over the nature of the global internet itself. We have an idealised version of the internet, based on security, interoperability, resiliency, and reliability. We think about all of these terms and that that's what it needs to embody. The reality is that there are actors around the world that are seeking to undermine that vision for the internet. They want for it to be a more closed system that has less interoperability.

The fourth major threat is the aspect of splintering existing coalitions for alliances in international cooperation. It's a major threat in cyberspace, and I think the more that bad actors are able to drive schisms or wedges between actors in cyberspace, the more that will begin to translate with the real world.

And the final piece, I think, is the threat to individuals, which is certainly a major challenge, and I think through much of the deep and dark web, a lot of harm can come to individuals, but we're also talking about general data protection, that is, the duty of the individual to keep himself safe online. We need to figure out a way to leverage scaled neighbours, like internet service providers and cloud security.

We need international cyber norms

With global collaboration, we can collectively move forward in a multi-stakeholder way, says Laura Bate

Laura Bate
is the senior director at US Cyberspace Solarium Commission Task Force 3. She gave her insights on the findings of the commission, and what should be done to make cyberspace secure

The international processes that have established cybersecurity norms, from the perspective of the commission, are the first layer in a deterrent strategy. While they are not universally effective, the ability to set most international actors on a path that we all agree on and towards responsible state behaviour is a powerful tool, especially when one can contextualise that with other steps in a deterrent process.

The Budapest Convention and several of these different international structure treaties, discussions, and agreements, lay out a structure of norms upon which there can be a general understanding of what responsible state behaviour should look like. However, what is at stake now is the system. Specifically, there's the open-ended working group that is working to rethink how we presently define cybersecurity in broad terms, and to rethink what we're talking about when we talk about cybercrime. Some of these alternatives, while they are cast as being more inclusive groups, inclusive bodies, and inclusive discussions, also serve to renegotiate some of the very foundational principles of what the definitions are.

While currently cybersecurity is defined as defending networks and defending information itself, we're starting to see expansions to that definition to really talk about the spread of information, making it much easier to prohibit sharing information that's unflattering. It then becomes not just about the cybersecurity of the system, the data, the computers, and the networks, but rather controlling the whole of the information space. And the problem is that for mature democracies like India and the United States, there is a need for the free exchange of information. Accordingly, there is a need for international cyber norms that are really built on a definition of cybersecurity that supports this.

MORE THE MERRIER

In terms of what can be done, one of the very first things possible is to collaborate, particularly on joint attribution of attacks, which is already happening in the United States and from like-minded partners. There is information sharing about identifying where the action occurred and knowing where it came from. Being able to say, we as an international community agree, that this took place, and this is where it came from, is really powerful and reinforces the norms that we have established. The more partners there are, it makes it a lot harder to claim that something was simply politicised and it's the U.S. going off.

Other things that can be done is the joint imposition of consequences, and not just limited to sanctions. For example, for two years in a row, with Montenegro, there has been work done to really counter some of the adversary interactions that they're seeing. There are also changes to the International Cy-

INSIGHTS
SYNERGIA FOUNDATION

bercrime Prevention Act that would allow increased international collaboration on botnet takedown, since criminals are exploiting breakdowns in the gaps between nations and breakdowns in coordination between nations. Through collaboration, a lot can be addressed.

The law enforcement cooperation is something that is looked at a lot. The commission dug into part of what's making international cooperation difficult. With the mutual legal assistance treaties (MLAT), the recommendation that was made was to increase the use of administrative subpoenas. There's a particular bureaucratic challenge in the U.S. that inhibits one from processing those MLATS quickly, which is literally that the office that handles it is very small and the steps that they have to go through legally to obtain access to that information is extensive.

More generally, whether it is law enforcement tools, economic tools, diplomatic tools, all of these things serve to reinforce the norms and make a stronger system. This is a manifestation of very similar issues, and are very, very high level. These overlap with a lot of the norm-setting questions discussed previously. Technical standards should be about which technology is best, but there's no way to decouple that from some basic assumptions about the internet, about how information moves across it, and who has access to that information. The new Internet Protocol is a way in which adversary governments are taking these standards as an opportunity to reshape the internet in a way that corresponds to authoritarian understandings of what the internet should look like based on control of information and control of surveillance.

EXPERT OPINION

HOW SAFE ARE THE U.S. ELECTIONS FROM CYBERATTACKS?

Robert Morgues: The overarching point is the need to build societal resilience in the face of disinformation. The government in the U.S. is not going to be the arbiter of truth and nor should it be, which means that in order to help citizens understand truth and fact, there is the need for robust civil society capability. Right now, there are a number of initiatives in the U.S. run out of think tanks and other civil society organisations that aim for this, but they are underresourced, underfunded, and understaffed.

Laura Bate: What is interesting this time around is that directors of organisations that handle cybersecurity and the FBI, among others, came out and said that the elections are safe and secure. What we need to do, however, is to be cognizant of the fact that there are attempts to shape the information space. There are attempts to influence, not the elections themselves, but voters, through the information put out on the internet. That's another interesting question: how does one work with social media providers, with other private sector actors in the U.S. and the population at large to figure out how to protect the information space.

SYSTEMIC PROBLEMS

T.M. Veeraraghav, Consulting Editor at the Synergia Foundation put forward the question of whether, like the Nuclear Deterrence Treaty, there was something that defines what is acceptable and what is not in cyberspace and brings to account countries that may not implement it in the right form. Ms. Laura Bate replied that the one nuance to add is when one thinks about who leads the pack, the reality is that who leads it is less important than who else is participating.

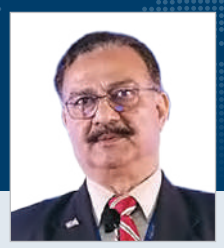
Taking for example standard-setting bodies, it is something that the U.S. cannot do independently of the private sector. A lot of the standards, a lot of the research, and a lot of the technological innovation is coming out of the private sector, and it's coming out of nonprofits, and academia, to mention a few. Each of these actors has a distinct role to play which holds true when we move internationally as well. It's not about who is starting the conversation, but rather how we are all collectively moving forward with it in a multi-stakeholder way.

Ms. Laura Bate also reinforced Lt. Gen. Pant's point, on how the dark web is a manifestation of a lack of cyber deterrence. It is a way that the internet is used to conduct crime, and people are looking at the systemic issues that allow them to address symptoms like the dark web. For example, one of the recommendations that the commission put forward was an increase in the number of assistant legal attachés, since there are only around 10 or 12 in the world as of now. This would help the United States to engage on a bilateral level more directly to address some of these manifestations of cybercrime. On a bilateral level, the commission recommended the significant increase in the size of the State Department's capacity to handle bilateral engagement and international engagement in general on cyber issues, through the creation of a Bureau of Cyberspace Security and Emerging Technology, and generally scaling up that capacity. Those systemic changes could allow for the translation of theory into practice to address symptoms like the dark web.

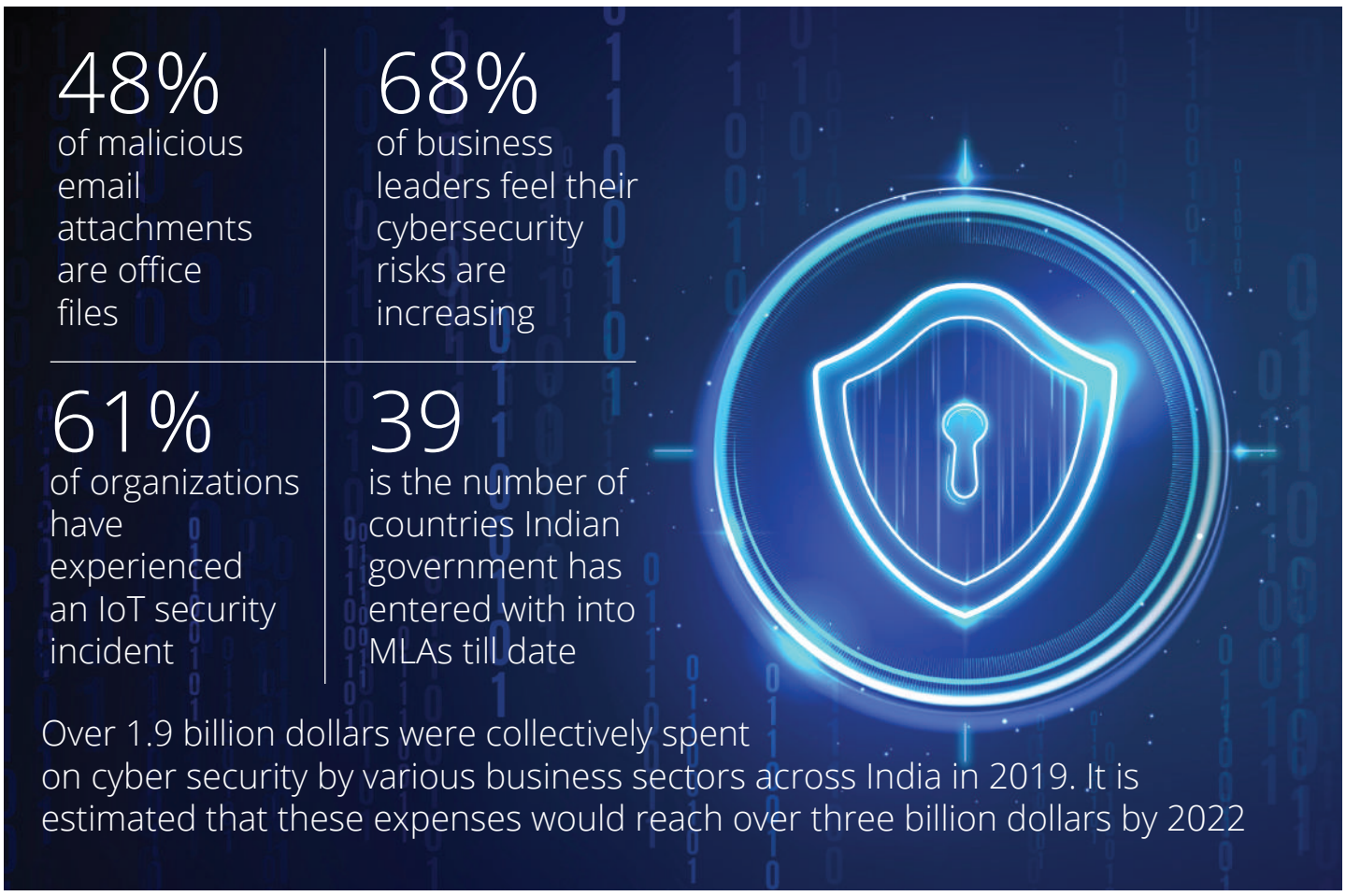
Coming to the question of trust in attribution, Ms. Laura Bate stated that in the past six or eight months, there have been a number of international joint attributions of various attacks. The timeline between when an attack occurs and when it is attributed publicly internationally is distinctly getting shorter and shorter, which is a sign of hope. This shows that not only is the world building trust amongst a group of partners and allies, but there is also something akin to muscle memory being built, where people are getting better at doing it faster.

UN led interventions required

Having set the foundation, it is now time for India to have a new strategy, says Lt. Gen. Pant



Lt. Gen. (Dr.) Rajesh Pant (retd) is India's National Cyber Security Coordinator. He was a panelist on the 86th Synergia Virtual Forum on the Solarium 2020: US Cyber Security In A Changing World Order. The article highlights his views



Cybersecurity is an international team sport. Having said that, the U.S. and India today share a global comprehensive strategic partnership. We have a very active cybersecurity dialogue. The present policy in India is based on a 2013 cybersecurity policy, and India was one of the first few countries to come out with a cybersecurity policy. The vision of that policy was to create a safe and secure cyber ecosystem for individuals, businesses, and governments. Over the last seven years, the creation part is by and large over. The National Critical Information Infrastructure protection centre came out of the policy, along with The National Cyber Coordination Centre for Threat Prediction, and the Indian Cyber Crime Coordination Centre under the Ministry of Home Affairs. The Ministry of External Affairs has also opened a cyber diplomacy division.

It is now time for India to have a new strategy, which was under the works and almost ready until the pandemic hit us. Because of the pandemic, there was the need to step back as we realised that the entire work-from-home environment and the increase in cyberattacks had created a need to review the strategy.

The National Cybersecurity Strategy, which was also announced by the Prime Minister, is going to be released soon. However, there are still a lot of unresolved issues. A whole-nation approach is being followed. The individual, businesses, academia, and the government — each has some responsibility. This is a common but differentiated responsibility (CBDR) approach and we also have the concept of an assured defence posture. The environment in which we are operating is that criminals are taking advantage of the infighting, and the geopolitics. And because of that, the cyberattacks are continuing.

That the cyberattacks are increasing consistently seems to be the lack of international cooperation or attribution of the cyberattacks. On a larger scale, the United States' plan of a clean network connecting the world and furthering diplomatic relations has been met by the Chinese coming out with the GIDS, a global initiative on data security. They've also approached the International Telecommunication Union with a new Internet Protocol, based on which they want to create a new internet, along with a whole new data protection policy.

SKEWED CONTROL

In the 5th United Nations Group of Governmental Experts on Information Security (UNGGE), the talks collapsed because Russia, China, Cuba, and Mexico collectively opposed the biased control of the internet, which will be supported by the Western countries and U.S. lobbyists. The bias of control refers to internet governance, the ICANN, the ETF, and the fact that out of the 13 root servers of the internet, 11 are in the U.S., one is in Europe, and one is in Japan. In the 4th UNGGE, there were some very good principles and norms of good internet behaviour by responsible nations and there were eleven of those principles. In the 6th UNGGE, they are still trying to promote those norms of the internet. Even when it came to International Humanitarian Law (IHL) applying in cyberspace, in the last conference, the Russian contingent said that the IHL is meant for

INSIGHTS
SYNERGIA FOUNDATION

wartime conditions, throwing another spanner in the works.

Overall, the internet is heading towards a very serious condition — call it the splinternet or Balkanisation — for at the international level, there is a lot of concern on how the internet will be shaped in future. In such an environment, the criminals are taking advantage. In the first nine months of 2020, the total loss in cybercrime has been up to $6 trillion. The department that controls the government sector ICT requirements shows that most of the attacks one finds are coming from the U.S. The reason for that is because the last-hop server has been hired from around there. Which is not the case, as we all know?. In order to attribute the attacks, one has to go to the U.S. and ask them for the details. This is usually done through the Mutual Legal Assistance Treaty (MLAT), which takes a very long time.

There are some regional corporations like the Budapest Convention where there is some traction. However, in India, in its stated policy, we believe in a UN-led solution or a multilateral, multi-stakeholder solution.

It is not a single-nation strategy that would help stop cyber crimes. There has to be cooperation among people on an international level. There is a need for a new architecture because of the way everyone is working in a distributed manner, since today everyone or at least most of the people are working from home. The identity and access management has become very important. On security, the endpoint has become very important, so these are new issues which are certainly coming up from the cybersecurity point of view.

UN-LED SOLUTIONS

Regarding the question on whether we need leaders for cyberspace, and if so, would it be a single nation, a collective, or a private entity, there already exists a system like that in the United Nations, which should be used to its fullest potential. Perhaps the UN could have a cyber cell, but the strength of the UN must be exploited to solve the problems. People are speaking of creating an International Court of Cyber Justice, so these structures are already in place, since there is already an International Court of Justice. There's also already an international humanitarian law. It operates in five domains, to which now cyber has to be incorporated. While there is no way a private entity could be the forerunner, a single nation as well is doubtful in today's geopolitics. A UN-led solution is recommended.

The dark and depraved web plays a big role in cyber crime. There is a need to start the conversation around the topic with our strategic partners like the U.S.

As to whether big corporate conglomerates should follow a cyber protocol, I must emphasise that the critical sector is not only the government sector — power is private, water is private, even the transport is private. The private sector is equally important as the critical sector. The innovation, creativity and the speed at which the private sector works cannot be matched. However, there are issues like the dark web that we need to look into. The dark and depraved web plays a big role in cyber crime. There is a need to start the conversation around the topic with our strategic partners like the U.S.

There is a need to move from theory to practice. How does one tackle the problem on the ground, is the question. Until a UN solution comes up, the answer lies in bilateral and regional cooperation. There are also many other things that need discussing, like 5G, IoT and OT. The real threat as a national cybersecurity coordinator, is to the CII, to the protection of the technology in the power systems, nuclear, space, etc. That is where these CADA and industrial control systems come in.

Tobby Simon, Founder and President of the Synergia Foundation, talked about resilience in cybersecurity, based on research done by the foundation that looked at the surface area of cyber or networks in cybersecurity. When looked at from a larger perspective, the maximum surface area for networks was 30 per cent at the time, which meant that more than 60 per cent of the threat lay outside the net. This is where the nation states and countries have to use a lot of intelligence. The best way to go about it would be to prevent attacks from happening altogether instead of allowing it to happen, and then to fix it. The only way to do it is by having actionable intelligence. The normal adversary can never have the same intelligence capability unless it's a nation-state. However, if many nation-states come together and are willing to share intelligence, there could be a model for higher resilience that isn't much too centred on the network, since networks are vulnerable.

ACKNOWLEDGEMENT

RESPONSE FROM PARTICIPANTS

Gen. David H. Petraeus
Partner, KKR and Chairman, KKR Global Institute
It was quite informative and thought-provoking

Lt Gen Arun K Sahni
PVSM,UYSM,SM,VSM
Former General Officer Commanding in Chief, Indian Army
Enjoyed the event. No comments as the speakers conveyed the issues well. Thank you

Meenakshi Gopinath
Founder and Director WISCOMP
I must say I enjoyed the session. Thank you for providing us rich and new insights.

Ravi Bangar, *IFS (1982) Retd. Former Ambassador of India to Colombia & Ecuador and High Commissioner to Cyprus*
The Forum in a short time dwelt on all important factors affecting cybersecurity and possible responses to credible challenges to cybersecurity posed by state and non-state actors. The discussion was very interesting and useful.

Amb Suresh K Goel,
IFS Retd, Director General of Indian Council of Cultural Relations (ICCR), GOI
I was in fact, quite delighted and impressed with the high professional caliber of the discussions and the analysis of the issues. I liked both the presentation of some very complex issues and their honest examination. The Indian presentation was unusually candid, to my surprise and delight.
I am seriously considering how I would be able to contribute to the work of the Foundation and will revert shortly.

Bala Chauhan
New Indian Express
Absolutely brilliant session

An extremist in the lead

The nascent opposition combine aims to topple the military-managed PTI government through mass protests, entrusting a veteran street-smart right-wing cleric to lead the way

MAJ GEN AJAY SAH (RETD)

Geopolitical and strategic anaylst, Synergia Foundation

In the latest episode of the drama of Pakistani politics, a gaggle of political parties came together in an alliance to topple the military-propped government of Prime Minister Imran Khan. Adding a twist to the tale, they chose a fundamentalist and radical cleric, Maulana Fazlur Rehman, chief of the Jamiat Ulema-e Islam (JUI-F), as their point's man to lead the front.

QUESTIONING CLAIMS

In the last week of September, in a conclave attended by 11 Opposition parties, prominent being former Prime Minister Nawaz Sharif's PML-N and Bhutto-Zardari's PPP, the Pakistan Democratic Front (PDF) came into existence to "oust the incumbent government and hold new elections in order to achieve 'real democracy'". The alliance accused the government, among other things, of increasing the political space of the military in all spheres of governance.

For a country which is inured to the all-powerful military acting as the kingmaker, this assertion is reflective of the groundswell against the current government's pliant posturing before the generals, a sentiment that the Opposition wants to exploit.

As the Pakistani Tehreek-e-Insaf (PTI) government led by Mr. Imran Khan celebrated its second year in power — projecting its success in controlling the pandemic, rising stock market, reducing the current account deficit from $20 billion to $3 billion, and its preeminent role in guiding the peace talks in Afghanistan — the Opposition was not as sanguine.

Both the PML-N and the PPP called out the government's performance as an "unmitigated disaster" that has "increased the woes of the masses manifold" resulting in a "massive decline in the GDP". Bilawal Bhutto was especially critical of PTI's report card in foreign policy, calling its handling of Kashmir and the rift with the Saudis as massive foreign policy failures.

MILITARY TARGETED

The PDF has mapped out a six-point strategy to oust the PTI government through "the constitutional and legal" course, by mobilising lawyers, traders, farmers, and the civil society. It will galvanise the masses through huge rallies and marches, the first of which is scheduled on October 10. That the real target is the military was made amply clear by Mr. Sharif when he declared "Our struggle is against those who installed Imran Khan and who manipulate elections to bring an incapable man into power and thus destroy the country."

In all fairness to Mr. Imran Khan, when one looks at the chaotic state of the economy and governance that he inherited — one of the lowest points in Pakistan's existence — he has made significant steps in hauling the country from the mess, especially in the areas of the economy and law and order. There is no denying that Mr. Imran

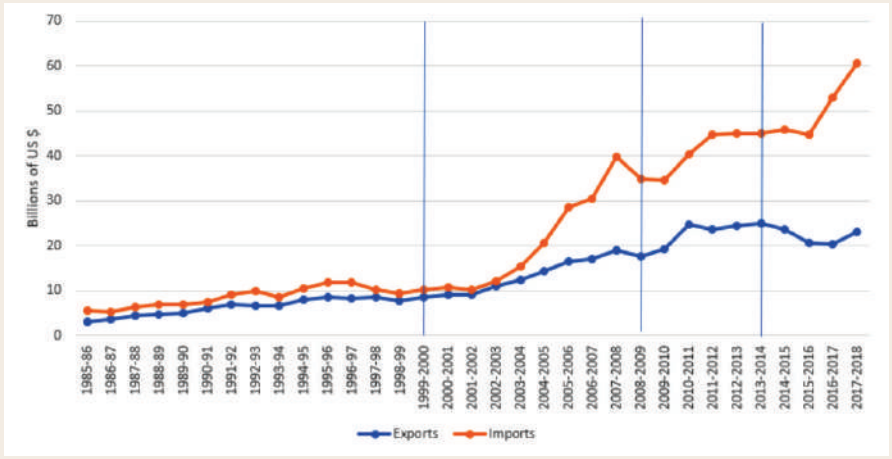
The federal government in 2019 officially revised downward the 5.8% economic growth rate in the last year of the Pakistan Muslim League-Nawaz (PML-N) government's tenure to 5.2%, denying a claim over achieving the highest growth rate in 13 years

GDP growth was less than 3 percent in 2013 compared to 5.8 percent when the PML-N left the government in 2018

In 2017, Pakistan ranked 147 out of 190 countries on the World Bank's 'Ease of Doing Business Index', a metric that measures how conducive regulatory and infrastructure environments are to allowing private enterprise to flourish

INSIGHTS
SYNERGIA FOUNDATION

PAKISTAN TRADE STATISTICS



Khan's handling of the COVID-19 pandemic has been exemplary, a fact supported by the lowering infection rates. Not to forget, many of the alliance's luminaries themselves have in the past sought the backing of the army to further their own political agenda.

An Opposition that has for the last two years remained largely in the background, perhaps daunted by the menacing presence of the military behind the PTI government, is now striving to remain relevant in the political landscape of Pakistan. According to speculations rife in the Pakistani media, the alliance is trying to kickstart a major political movement against the incumbent government before the elections to the Upper House of the Parliament scheduled in March next year.

Both the PML-N and the PPP called out the government's performance as an "unmitigated disaster" that has "increased the woes of the masses manifold" resulting in a "massive decline in the GDP"

As is common in the subcontinent's politics, Mr. Imran Khan was quick to blame the "foreign hand", accusing the PDF of "Indian links". That the government was rattled was indicted by the lodging of a case for seditious activities against all the leaders in the alliance through a private citizen.

MAULANA FAZLUR REHMAN TAKES THE CENTRE STAGE

The choice of Maulana Rehman to lead them to victory was a surprise move. The Maulana heads the right-wing religious JUI-F which has walked the aisle with both secular parties like the PPP and the Awami National Party while retaining its ideological links to the extreme Deobandi sect of Islam.

Fawad Chaudhary, a minister in the PTI government, tweeted, "Sad Day for Pakistan an extremist Mullah considered close to terrorist groups of Afghanistan is selected to lead opposition movement against Government."

However, the reason for the cleric to lead this fledgling movement is not his extremist credentials, but the power he can wield to generate masses on the streets. He is a veteran street-protest campaigner, who had led a sit-in at Islamabad for several weeks in 2019 before the army evicted him.

The Maulana is a protégé of Nawabzada Nasrullah Khan, who led protests against the British and later took on every military dictator. In the 1960s, he led the alliance called the Democratic Action Committee that forced the exit of President Ayub Khan from power. Mr. Rehman has followed in his mentor's footsteps, with a long history of dissent with those ruling Pakistan. Mr. Nasrullah Khan's dream was to appoint him as the Prime Minister of Pakistan one day.

While in private, leaders of both the PML-N and PPP may have their reservations about the Maulana, publicly they have endorsed him for short-term gains. For the future, it is being reported that there is an arrangement for a rotating leadership. This will put to rest any speculation that if at a later date, the PDF is able to convert itself into an electoral alliance and form a government, the Maulana may not be the chosen one to lead it.

The European Foundation of South Asian Studies said in a commentary that if the new alliance is really serious in "loosening the stranglehold of the military establishment", they must "stick together".

RESURGENCE OF TTP

Seen in the background of these developments, there is yet another worry for the embattled PTI government: the resurgence of Tehrik-e-Taliban Pakistan (TTP). Recently, two of its splinter groups, Jamat-ul-Ahrar (JuA) and Hizb-ul-Ahrar (HuA), announced their return to the fold of their parent organisation.

The TTP, proscribed by the U.S. as a terrorist group in exchange for Pakistan's cooperation in facilitating talks with the Taliban, was in disarray for the last couple of years, especially after its top hierarchy was decimated by U.S. drone strikes.

Coming at a time of the Afghan peace talks, this merger is significant as there are approximately 6,500 TTP fighters in Afghanistan. From its sanctuaries in Kunar and Nangarhar provinces in eastern Afghanistan, the TTP can resume sustained military operations. As the Afghan Taliban gains political power, the TTP will always remain a tool in their hands to put pressure on Pakistan to elicit concessions.

Conclusion

As the PTI government slowly recovers from the double whammy of the pandemic and its economic crisis, it had hoped to begin the process of consolidation for the balance of its tenure in political office. The military has been steadfast in its support for Mr. Imran Khan, which has evidently given him strength and the confidence to deal with his myriad challenges. It remains to be seen what direction the street protests take, once launched, and whether they can generate the requisite public momentum to unseat the incumbent government.

INSIGHTS
SYNERGIA FOUNDATION

EDITION III
OCTOBER 2020

A splintered Sudan signs up to be whole again

While the August 31 peace deal with rebel alliances promises closure to years of conflict, long term stability and prosperity demands a deeper political overhaul inclusive of all

SYNERGIA FOUNDATION RESEARCH TEAM

Sudan's Sovereign Council Chief Abdel Fattah al-Burhan, South Sudan's President Salva Kiir, and Sudan's Prime Minister Abdalla Hamdok lift copies of the peace agreement with the country's rebel groups in Juba, South Sudan, August 31.

Sudan's journey as a nation-state has been rife with strife. A thinly populated country, blessed with both the Blue and White Niles enriching its valleys and with rich oil deposits, yet cursed with bitter infighting, famines and poverty.

With the country's worsening economic crisis, the civil war in Darfur, and conflict in South Kordofan and the Blue Nile, rebel groups across the region have shown dissatisfaction with the administration. Ever since President Omar al-Bashir's ousting and subsequent arrest for war crimes in 2019, the country's transitional military-civilian government has attempted to mitigate fragmentation through various peace deals. Finally, on August 31, after a year of negotiations, the government signed a deal with one of the major rebel alliances, the Sudan Revolutionary Front (SRF). If implemented effectively, this peace agreement could end 17 years of violence that has displaced millions and led to over 3,00,000 deaths.

The SRF consists of rebel factions mainly from all three conflict-ridden regions, who believe that the current government is biased towards Arab Khartoum elites and discriminatory against marginalised communities. The peace deal grants the rebels three seats in the government's sovereignty council, five seats in the transitional cabinet, and a quarter of the seats in the transitional parliament. The agreement calls for a permanent ceasefire while integrating the rebel forces with government security forces and supporting domestic refugees.

WILL IT WORK?

Although the peace deal paves the way for optimum representation in Sudan's political bodies and more inclusive society, some rebel groups are yet to agree to the terms as they are awaiting complete civilian rule and right to self-determination. The Sudan People's Liberation Movement-North (SPLM-N) – one of the factions that did not sign the deal – did, however, sign an accord a week later that separates religion from state, thus ending 30 years of Islamic rule in the country. This suggests that the negotiations have attained a significant breakthrough in Sudan's peace process.

The country's history, however, raises scepticism on the effectiveness of the agreement. Prior deals such as the 2006 and 2011 Darfur Peace Agreements also echoed similar terms, by promising power-sharing with the rebels and an end to the humanitarian crises. But they fell through as several rebel factions backed out, and with the government side also reneging on its promises, the fighting resumed. This time, with the support of major alliances, the agreement can become successful since it addresses

INSIGHTS
SYNERGIA FOUNDATION

a root cause of the conflicts i.e. Sudan's Islamic regime that marginalises other religious communities.

However, the challenge lies in implementing the deal. The current government's rehabilitation plan is hinged on the availability of large funds to support Sudan's refugees as well as for development. But due to its ruined economy and extensive war damages, Sudan relies on international assistance which in turn depends on the generosity of western donors, themselves plagued by the pandemic and subsequent economic fallout.

Sudan remains in the U.S. list as a state sponsor of terrorism since 1993, which bars it from aid and even loans from IMF and World Bank. It has the dubious distinction of being one of the first harbourers of Osama Bin Laden, and also providing sanctuary to Hamas that is considered a terrorist organisation by the West.

The U.S. did lift some of its sanctions in 2017 due to Sudan's continued cooperation to address its humanitarian concerns, especially in its willingness to help the ICC to bring Bashir to justice. Sudan's decision to hand over al-Bashir to the International Criminal Court for war crimes and genocide might also suggest its willingness to cooperate and follow international humanitarian norms. In the meantime, al-Bashir has been sentenced to two years in jail for corruption in Khartoum.

WAY FORWARD

The peace deal has been welcomed by several western countries, including the U.S., Norway, and the U.K., in addition to international institutions such as the United Nations and African Union.

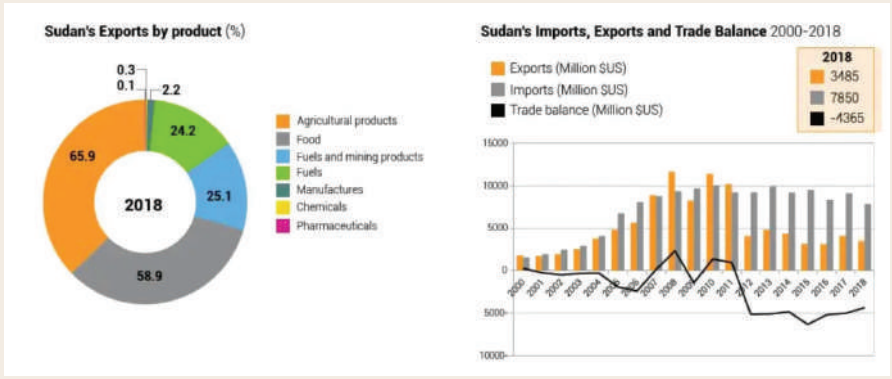
Despite the praise, Sudan still has a long road ahead to restore its economic and political establishments. The current peace process was a result of extensive mediation with the help of third parties such as the East African Intergovernmental Authority on Development (IGAD), African Union, the UAE, and the United Nations. Mediators from South Sudan also played a significant role in the peace process, which was finalised in Juba, the South Sudanese capital. This might bring some repose to the two countries' strained relationship due to territorial disputes (such as over oil-rich Abyei), although this also depends on each country's rebel group allegiances.

Sudan would most likely continue relying on outside parties to mediate with remaining rebel groups and provide compensation to its affected population. It would, therefore, benefit in continued cooperation with international institutions. Sudan can increase cooperation with the U.S. by cutting off ties with Iran and forming diplomatic relations with Israel, which in all probability could end its state-sponsored terrorism status.

In the meantime, the public needs to be empowered to become more active in political affairs, to prevent falling under the control of Islamic militant groups. The present government's reliance on Islamic elites would continue to marginalise non-Arab communities. A complete political restructuring that is inclusive of civilian groups would be necessary.

By moving towards secular governance and sustained international assistance, Sudan can gain the resources necessary to fix its socio-economic and humanitarian situation. But this depends on the effective implementation by a non-corrupt political body. With mass shootings in Darfur reported in as recently as July this year, Sudan still has a long way to go before it attains peace.

FACTFILE



Estimates suggest that oil accounts for between 70% and 90% of Sudan's total exports. The primary importers of Sudanese oil are Japan, China, South Korea, Indonesia, and India

Assessment

The peace deal signed on August 31 is one of the most significant steps taken towards Sudan's transition to democracy. The deal raises hopes to end 17 years of violence in Darfur which has claimed over 300,000 lives and displaced 2.7 million. However, two major factions- Sudan People's Liberation Movement-North and Sudan Liberation Army remain recalcitrant and can continue to cause mayhem.

The military junta was forced by the stark economic situation to accede to the August 17, 2019 deal to allow military-civilian transitional rule which lifted Sudan's African Union membership suspension. This raises hope for the growth of democratic institutions in a country which was run by the Sharia law followed by a military rule.

Sudan will have to do a better job of convincing the western democracies that it has turned a new leaf for good, than merely throwing the deposed dictator Bashir to the wolves now that he had outlived his utility. Recognition of Israel could be one such trump card up its sleeve.

Caucasian tinderbox: It's on fire again

In Nagorno-Karabakh, the escalating hostilities between Armenia and Azerbaijan threaten to spiral out of control, drawing in regional powers like Russia, Turkey and Iran

SYNERGIA FOUNDATION RESEARCH TEAM

The disputed enclave of Nagorno-Karabakh, in the sensitive Southern Caucasus, has captured global headlines after a hiatus of nearly four years. This time around, the fighting has rapidly escalated into a full-blown conventional conflict with unrestricted use of armed drones, airpower, artillery barrages and mechanised forces, which are supported by massed infantry attacks on fortifications.

As casualties continue to mount, the world has watched on helplessly. Azeri strongman Ilham Aliyev has demanded Armenia's complete withdrawal from Nagorno-Karabakh as a precondition for any ceasefire.

As of October 10, Russia has managed to convince both sides to come to a ceasefire agreement, including a prisoner swap, after days of bloodletting. Few, however, expect it to hold, as Azerbaijan with its strong Turkish military backing, seems determined to bring a closure in its favour through military force. As expected, the ceasefire is being constantly violated by both sides on an hourly basis.

SOVIET HANGOVER

Azerbaijan and Armenia were important constituents of the USSR since the 1920s. They gave Stalin a foothold in the Caucasus; a strategic land bridge between the Black and Caspian Seas as well as the meeting point of three empires - Russian, Ottoman and Persian/ Iranian.

The Soviets accorded Nagorno-Karabakh the status of an 'autonomous oblast' within the territory of Azerbaijan, reportedly with an eye to mollify Turkey which had been demanding its inclusion within Azerbaijan. Inhabited by a majority of ethnic Armenians, Nagorno-Karabakh had a history steeped in conflict, with various powers vying for it for influence in the Caucasus. It was also a source of deep-rooted tensions between Christian Armenians and Muslim Azeris, with both sides having staked claim to it, on historical and ethnic grounds.

Once the Soviet iron hand over the Caucasus slackened in the 1980s, this historical

INSIGHTS
SYNERGIA FOUNDATION

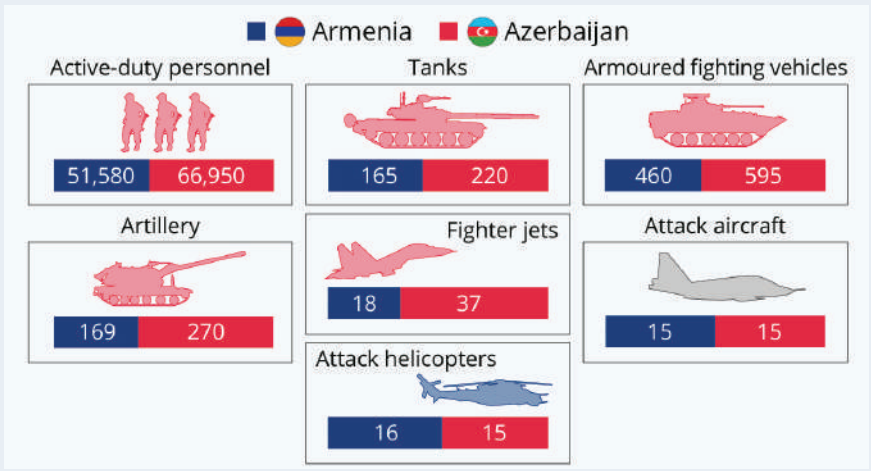
tension resurfaced with renewed vigour. Sensing freedom from the crumbling USSR, Armenia demanded the merger of Nagorno-Karabakh with Armenia. When the Soviet Union refused, protests erupted in Armenia, followed by a full-blown military conflict that led to the occupation of the enclave by Armenians. It is alleged that a large number of Azeris were forcefully driven out of the region, leading to ethnic cleansing.

To make matters worse, these events also coincided with the disintegration of the Soviet Union in 1991. As a result, what had hitherto been an internal Soviet conflict, was transformed into an all-out war between the newly independent states of Armenia and Azerbaijan.

In 1994, an uneasy ceasefire was mediated between the two countries by Russia. Although Nagorno-Karabakh continued to be recognised as part of Azerbaijan, the Armenians had de facto control over the region as well as the adjoining Azerbaijani territory. The 'Minsk Group', headed by Russia, France and the United States, sought to broker a lasting peace agreement under the aegis of the Organization of Security and Cooperation in Europe (OSCE). Unfortunately, this proved to be unsuccessful.

ARMENIA & AZERBAIJAN MILITARY STRENGTH

Estimated military equipment/personnel of Armenia & Azerbaijan in 2020*



*Selected equipment, Russia also stations MIG-29 fighter jets in Gyumri, Armenia.

Source: Statista Research

Over the years, the Nagorno-Karabakh issue has continued to fester, with occasional ceasefire breaches and violence across the border. The last major outbreak of fighting was in 2016. With more than 300 casualties, the fighting had lasted for four-days between Azerbaijani forces and separatist elements of the self-proclaimed 'Republic of Artsakh' backed by Armenia.

THE GREAT GAME IN THE CAUCASUS

It is speculated that the current round of fighting has been provoked by a resurgent Azerbaijan that seeks to regain the territorial losses of the 1990s, having failed to achieve any progress through negotiations. Backed by Turkey and taking advantage of the distraction caused by the COVID-19 pandemic, Azerbaijan is now trying to correct what it calls "a historical injustice".

The escalation is somewhat distinct from the erratic violence of the past, due to a more direct engagement by Turkey in support of Azerbaijan. President Recep Tayyip Erdoğan is seeking to flex his muscles in what has traditionally been a Russian sphere of influence. Apart from reports of Turkey pushing in Syrian foreign fighters from the Al

Armenian forces currently control approximately 9% of Azerbaijan's territory outside the enclave

Nusra Front to fight on behalf of the Azeris, Armenia has also accused the country of supplying F-16 jets and military drone technology to its adversaries. In fact, Armenian Prime Minister Nikol Pashinyan has dubbed Turkey's actions as a 'continuation' of the Armenian genocide, a historical event in which more than a million Christian Armenians were reportedly massacred in Turkey. There have also been unsubstantiated reports of Pakistani fighters being inducted into the fighting.

Turkey's recent politico-military adventures has been in defiance of its NATO allies and this one is no exception. Having dared the NATO first in Syria, followed by Libya and the Eastern Mediterranean, it is playing a pivotal role in this conflict as well.

Nagorno-Karabakh could also prove to be integral in Russia's broader competition with Turkey. The two states are already involved in a proxy conflict in Syria and Libya. If Russia decides to intervene in the Nagorno-Karabakh conflict, another front would be opened in this Russia-Turkey proxy war.

However, Moscow's calculations in the Caucasus are far more complex than meets the eye. It desires peace in the Caucasus land bridge, due to the latter's location in a vital energy corridor. It also has a larger strategic interest in ensuring the continuation of Russian hegemony in the region. Russia desires that the Caucasian states seek its mediation, as opposed to forging alliances with Turkey or Iran. It is for this reason that it supplies Azerbaijan with the bulk of its military equipment, ignoring widespread public support for the Armenian cause as well as a defence pact which it has signed with Armenia.

Iran is also a key stakeholder in the Southern Caucasus. Apprehending the possibility of a larger regional war, it has extended an offer to mediate. By purporting to be neutral, Iran is trying to secure its own domestic stability. After all, it plays host to a significant number of Armenian and Azeri minorities. Upsetting them by taking sides would not bode well for Iran, which is already embattled by economic distress and public discontentment.

The U.S. and France have also called for a ceasefire, while the E.U. has re-activated the Minsk Group. The American response has been reportedly tepid, since the country remains engrossed in its impending elections.

Assessment

The Nagorno-Karabakh conflict is a relic of Stalin's version of 'Divide and Rule' wherein the borders of constituent states were drawn in such a manner, as to leave ethnic minorities in each state. Apart from ensuring sustained Soviet hegemony, it had the advantage of countering Turkey's pan-nationalist tendencies. Like other colonial creations the world over, such legacies will continue to fester and have no 'band-aid' solutions.

In the fresh outbreak of hostilities between Azerbaijan and Armenia, Turkey has adopted a more proactive role. While this poses a challenge for Russia's traditional hegemony in the region, there are strategic and economic factors that could preclude it from directly intervening in the conflict.

To arrive at an enduring peace agreement, the fault lines have to be addressed. For one, there is a direct contradiction between Azerbaijan's assertion of territorial integrity and the Republic of Artsakh's demands for self-determination. Secondly, the conflict represents a tussle over national identity and self-conception between the Armenians and Azeris. Unless these structural causes are addressed, a peace deal between Armenia and Azerbaijan is unlikely to succeed and mediation efforts by outside powers can only put a temporary stop to hostilities.

To access all editions of the Synergia Foundation Key Insights Newsletter, visit:
www.synergiafoundation.org/insights


Major General
AJAY SAH
(Retd.)
Chief Information Officer


Major General
MONI CHANDI
(Retd.)
Chief Strategy Officer


T.M.
VEERARAGHAV
Consulting Editor


SAMBRATHA
SHETTY
Chief Operating Officer

SYNERGIA FOUNDATION
Synergia Foundation is an independent and strategic think tank whose purpose is to augment decision-making at a policy level while enriching individual discourse and public dialogue. With fact based insights,the Synergia Foundation provides impactful solutions that challenge the status quo,turning risks in to opportunities.

SYNERGIA FORUM/VIRTUAL FORUM
The Synergia Forum is a by-invite only session where we invite eminent subject matter experts to discuss the challenges and disruptions that governments, academia and businesses may face today and in the future.

INSIGHTS
Synergia Insights is our weekly print and digital publication. Authored by functional and geostrategic experts, we provide unbiased analyses and assessments of both national and international affairs that affect our lives.

Address
34, Vittal Mallya Road,
Bengaluru, Karnataka 560001,
India
Tel : +91 80 4197 1000
Email : info@synergiagroup.in

@SynergiaFoundation
@SynergiaImpact
www.synergiafoundation.org
www.synergiaconclave.org