Scholarly Research Journal for Humanity Science & English Language,
Online ISSN 2348-3083, SJ IMPACT FACTOR 2017: 5.068, www.srjis.com
PEER REVIEWED JOURNAL, OCT-NOV 2018, VOL- 6/30

TOP FIVE THREATS TO NATIONAL SECURITY IN THE ASIAN REGION

H. K. Pandey[1], Ph. D. & Col Shantonu Roy[2]

Introduction

1. Defense technologists are most successful when they hone in on specific problems. The Pentagon's research agencies and their contractors were asked in 2003 to come up with ways to foil roadside bombs in Iraq and Afghanistan, and although they did not defeat the threat entirely, they did produce a number of useful detectors, jammers and other counter-explosive systems. More recently, military researchers received marching orders to help tackle the so-called "anti-access area-denial" threats, which is Pentagon-speak for enemy weapons that could be used to shoot down U.S. fighters and attack Navy ships.

2. The next wave of national security threats, however, might be more than the technology community can handle. They are complex, multidimensional problems against which no degree of technical superiority in stealth, fifth-generation air warfare or night-vision is likely to suffice.

The Threats

3. The latest intelligence forecasts point to five big challenges to the global security and also to our national security in the coming decades.

4. **Biological Weapons.** The White House published in 2009 a National Strategy for Countering Biological Threats with an underlying theme that biological weapons eventually will be used in a terrorist attack. To prevent deadly viruses from being turned into mass-casualty weapons, officials say, one of the most difficult challenges is obtaining timely and accurate insight on potential attacks. The Defense Threat Reduction Agency has a team of researchers working these problems. But they worry that the pace of research is too slow to keep up with would-be terrorists.

5. **Nukes.** Large stockpiles of nuclear weapons are tempting targets for nation-states or groups set on attacking the world. Black-market trade in sensitive nuclear materials is a particular concern for security agencies. "The prospect that al-Qaida or another terrorist organization might acquire a nuclear device represents an immediate and extreme threat to global security," says an administration report. No high-tech sensors exist to help break up

black markets, detect and intercept nuclear materials in transit and there are no financial tools to disrupt this dangerous trade. A much-hyped effort to detect radioactive materials at various ports has been plagued by technical hiccups. Analysts believe that although a full-up nuclear weapon would be nearly impossible for an al-Qaida like group to build, a more likely scenario would be a low-yield "dirty bomb" that could be made with just a few grams of radioactive material.

6. **Cyber-Attacks.** The drumbeats of cyber warfare have been sounding for years. Network intrusions are widely viewed as one of the most serious potential national security, public safety and economic challenges. Technology, in this case, becomes a double-edge sword. "The very technologies that empower us to lead and create also empower individual criminal hackers, organized criminal groups, terrorist networks and other advanced nations to disrupt the critical infrastructure that is vital to our economy, commerce, public safety, and military". The cybersecurity marketplace is flooded with products that promise quick fixes but it is becoming clear that the increasing persistence and sophistication of attacks will require solutions beyond the traditional.

7. **Climate Change.** The national security ramifications of climate change are severe, according to various analysts. While the topic of climate change has been hugely politicized, analysts casts the issue as a serious security crisis. "In the 21st century, we recognize that climate change can impact national security — ranging from rising sea levels, to severe droughts, to the melting of the polar caps, to more frequent and devastating natural disasters that raise demand for humanitarian assistance and disaster relief," as brought out by analysts . The administration projects that the change wrought by a warming planet will lead to new conflicts over refugees and resources and catastrophic natural disasters, all of which would require increased military support and resources. The scientific community, in this area, cannot agree on what it will take to reverse this trend. There is agreement, though, that there is no silver bullet.

8. **Transnational Crime.** Defense and law-enforcement agencies see transnational criminal networks as national security challenges. These groups cause instability and subvert government institutions through corruption, the administration says. "Transnational criminal organizations have accumulated unprecedented wealth and power through the drug trade, arms smuggling, human trafficking, and other illicit activities. … They extend their reach by forming alliances with terrorist organizations, government officials, and some state security

services." Even the sophisticated surveillance technology is not nearly enough to counter this threat.

9. **Bio-Threats.** The public health community's dream is to make the arrival and spread of communicable diseases as easy to predict and track as the weather.Just as a meteorologist spots the seeds of a hurricane off the African coast, and begins to plot its possible path as it makes its way toward the Caribbean, a global bio-surveillance network would allow officials to detect a bio-weapon or the emergence of a deadly flu virus in China and track it as it spreads throughout the world. Measures could then be taken to quickly develop and distribute vaccines.

10. **Nuclear Weapons**. Still at the top of the list of the most terrifying threats to the world are nuclear weapons. The nations have spent an almost incalculable amount of money over the past six decades to find them, monitor them, and destroy the means by which they are delivered. Open source information suggests there is still a lot of work to be done. Research into hitting an intercontinental ballistic missile bearing a nuclear warhead with another missile began 50 years ago. Yet today, this can still only be accomplished under the most controlled circumstances with questions remaining on whether decoys could easily defeat the "hitting a bullet with a bullet" scenario. President Reagan's dead-end effort to shoot down missiles from space, better known as Star Wars, came to naught. The Airborne Laser program, which envisioned destroying missiles on the launch pad by using directed energy shot from an aircraft, also came to a halt. The mutually assured destruction doctrine offset these defensive shortcomings. But as many analysts have noted, non-state actors such as terrorist groups, if they were to get their hands on a nuke, don't play by those rules. More recently, the Department of Homeland Security abandoned a program to develop Advanced Spectroscopic Portals that could detect a smuggled warhead inside a shipping container. The congressional mandate to scan every container entering the United States means that this effort will continue, although on a smaller scale. Less overt is the detection problem. Who has nukes? And where are they? The answer is: underground. North Korea's nuclear weapons program is hidden deep in its mountains, as are Iran's alleged efforts.

11. Defense Intelligence Agency in their annual threat assessment say underground facilities that may hide missiles and weapons of mass destruction are "spreading."Finding, assessing, mapping and ultimately destroying a hard and deep buried target — HDBT in military lingo — has become an increasingly difficult challenge for the military and spy communities, . The

two communities have placed a great deal of emphasis on tackling this problem during the last decade, he wrote. Most of it has been carried out with little attention. Despite the low profile, the military has been taking the problem seriously. An effort to destroy an underground complex may require repeated bombings by massive ordnance penetrator. These can only be carried by bombers, and only one at a time. We obviously need weapons that can penetrate through certain depths, through certain hardness. But whether they can even build them to attain certain levels of destruction, I just don't know … I'm not even sure the people in the Defense Department know. They are guessing, trying to figure it out using various models." Then comes the difficult question of battlefield damage assessment. Some things could be determined from outside, such as whether a bombing campaign collapsed an entrance. But since there may be an incomplete picture of what was inside a deeply buried bunker in the first place, it would be hard to know if a strike was successful. Intelligence community over the past decade have been taking this problem seriously. It has become more prominent and more important in recent years.

12. However, The Comprehensive Nuclear Test Ban Treaty, signed by most countries, has yet to be ratified. But it has helped create a robust global network that can monitor clandestine underground nuclear weapon detonations. A National Academies report released in 2000 spelled out the shortcomings signees would have in attempting to detect tests. On a typical day, the Earth experiences hundreds of earthquakes and large mine blasts. The seismic clutter make it difficult to detect underground nuclear explosions, said Paul Richards, a Colombia University emeritus professor of geophysics and seismology at a Center for Science, Technology and Security Policy briefing on Capitol Hill. A follow-up report released this year showed remarkable progress over the last decade. Hundreds of seismic and air-sniffing sensors have been placed all over the world, and countries have done a better job of sharing their legacy seismic sensor data with those who monitor the treaty. The radioactive particles released by the Fukushima Daiichi Nuclear Plant accident last year were detected all over the globe and as far as South America, said Robert Werzi, who maintains the Comprehensive Test Ban Treaty Organization's 80 radionuclide air monitors. If a sensor detects a manmade radioactive particle, analysts can then determine how many days old it is, backtrack the weather patterns, and pinpoint its origins, he said. Officials believe the network of seismic sensors is good enough to detect 90 percent of any clandestine attempt to test a nuclear weapon that is over 1 kiloton. The lower the yield is on a test, the less effective it

is. It is necessary to consider how well nuclear tests can be carried out evasively. There is a need for a continuing research-and-development program to improve the network of sensors, he added. The goal of the monitoring effort is to drive ever downwards the yield of anything that might go undetected or identified.

The Future of Cyber-Wars

13. A day in the not too distant future when attacks on computer networks cross the line from theft and disruption to "destruction."And this chaos will not all take place in the digital world of ones and zeroes. Reference is to remote adversaries taking down infrastructure such as power grids, dams, transportation systems and other sectors that use computer-based industrial controls. The last decade has seen mostly exploitation by adversaries, or the theft of money and intellectual property. Next came distributed denial of service attacks when hackers overwhelm networks and disrupt operations of businesses or other organizations. Other than intercontinental ballistic missiles and acts of terrorism, an adversary seeking to reach out and harm the world has only one other option: destructive cyber-attacks. How to thwart such attacks is the problem the world is facing. Most of the Internet's infrastructure through which malware is delivered is in the private sector's hands. So too are the banking, energy, transportation and other institutions that are vulnerable to the attacks. During the past year, there have been innumerable attacks on core critical infrastructures in the transportation, energy, and communication industries ."And that is only the tip of the iceberg. Despite having poured countless amounts of money into cybersecurity at all levels, there is still a lot to be learned about the threat, said one analyst.

14. "Why do we have a cyberwar community? Because we haven't mastered cyber. The main problem is that computers were originally seen as something to be "tinkered" with. "We've built the most important infrastructure on things that were made to be toys. Being toys, computer systems from the start have gaps and vulnerabilities needing to be patched."Every cyber-attack is a reflection of some vulnerability in the system and it's not enough to defend the nation from attacks, offensive capabilities are required. Over the next few years, the hackers will become more sophisticated. This doesn't necessarily mean that the technologies are becoming more advanced — even the most sophisticated threats often use known vulnerabilities and malware — but the adversaries have become more effective. A shortage of network security experts continues to be a problem in both government and the private sector. With cybersecurity, government and industry need to work together from the

beginning during the procurement process. This, is one way to reduce costs and achieve better cybersecurity. "It's not just about acquiring pure cybersystems anymore; it's about acquiring UAV's, radars, ships, etc, where cyber needs to be embedded to ensure mission success. Government and industry need to consider cyber in almost everything they do.

Climate Change

15. While politicians debate the legitimacy of climate science, the Defense Department has recognized it has a practical, hard-security interest in tackling issues like its energy footprint. There's no tree-hugging, sandal-wearing, granola eating aspects to the military's approach. The water-food-energy nexus of issues caused by climate change is going to be a rising challenge for the national security strategy reflects that. These technologies are increasingly particularized and specialized. We need to make sure that all of our eyes in the sky are not only looking at North Korea, for instance, but gathering a wealth of data from many areas. We need an inclusive data network to which many different observation technologies contribute. The chronic results of climate change are more challenging. Funneling resources to combat a problem that might not manifest for decades is a hard sell, especially with constrained budgets. But phenomena associated with climate change like persistent drought, violent flooding and agricultural disruption are real and immediate concerns for many of the nations the United States partners with around the world. The effects are also causing the most disruption in some of the world's most politically unstable regions — Southern Asia, Sub-Saharan Africa, South America and India is not far from this calamity. "To the extent that climate change is an issue for our partners … it is going to become an issue for us," . "The military is also aware that … climate impacts could be accelerants of instability in the countries where we have political interests or strategic concerns."

16. There are opportunities also associated with a warming planet. Some effects like the melting polar ice caps are regrettable ecologically but potentially a windfall for global commerce. A receding Arctic icecap could mean the Northwest and Northeast passages and Russia's Northern Sea Route could remain open longer in summer. Eventually they could remain navigable to commercial shipping year-round. The National Snow and Ice Data Center of the USA in September announced that the polar ice cap shrank over the summer months to the smallest area in the 33 years that records have been kept — just 1.5 million square miles at its nadir. "As the ice recedes, there are increases in commercial and other

human activity. It also opens new sources of oil and gas and tourist opportunities in new waters." The implications of the sudden availability of natural resources and shipping lanes through the Arctic have drawn much attention from nations spanning the globe. The obvious players — the eight-member Arctic Council, which includes the United States, Canada, Denmark, Finland, Norway, Russia, Sweden and Iceland — are concerned about border security where a sea of ice once did the work for them. Other nations as far away as India and China are trying to gain admission to the council to advocate for their interests in shipping through an open Arctic, which could lessen by a third the time and cost of trans-oceanic shipping.

17. It is another instance where the military, by addressing a practical challenge to national security, can have a positive ecological impact, like the Navy being a champion of biofuels. Navy officials view renewable energy as a means of bringing down the cost of operations. The Marines care less about curbing global warming than they do about keeping fuel and water convoys off vulnerable roads. But the net result of sustainable resource programs is a significant reduction in the military's carbon footprint. In the Arctic, however, the world is woefully unprepared for the challenge.

Transnational Crime/Terror

18. Well before the May killing of Osama bin Laden at the hands of U.S. Navy SEALs, the terrorist organization he headed had become a dispersed, loosely linked network of international terror and criminal groups. Add to that the existing transnational trafficking in narcotics, weapons and people, and the recipe yields a complicated problem for the military and law enforcement agencies at home and abroad. Countering those threats is made all the more difficult given that the military can't take its eye off state-level actors to fight non-state, non-standard actors. Events like the Arab Spring have created power vacuums and ungoverned lands where criminals and terrorist groups are able to operate with impunity. While much of the U.S. military's attention has been on the Middle East, anti-U.S. terror groups and al-Qaida sympathizers have spread elsewhere. Today, the arc of instability, from West to East Africa to Pakistan to Bangladesh has any number of al-Qaida copycat sympathizers, Arnaud de Borchgrave, senior adviser and director of the Transnational Threats Project at the Center for Strategic and International Studies, wrote in January. Illegal trade is "increasingly converging with ideologically-motivated networks, fostering a new generation of hybrid threats," according to information. Mali and Libya were two examples given by

Reid of places where those two forces are converging. A coup last year in Mali left the country's inhospitable north largely ungoverned. "Bandits and kidnappers" have since set up shop. Al-Qaida in the Islamic Maghreb has reared its head in Mali, operating without constraint in the arid north, some of the most inhospitable terrain on earth.

19. "Al-Qaida branched into there a few years ago and showed mixed results with proselytizing their ideology," Reid said. "They have not posed a transnational threat per se to attack the United States, but they are of growing concern to our interests in the region especially the South Eastern Hemisphere and India." The group draws its origins from desert bandits and smugglers taking advantage of a power vacuum to advance their and al-Qaida's interests. The instability in Libya has afforded them an opportunity to spread their beliefs there also. They gain a significant amount of resources from kidnapping for ransom — tens of millions of dollars go into their treasure chests. For al-Qaida, kidnapping to fund terrorist activities is a relatively new brand of criminality. These are small-scale crimes with regional implications for which military intervention is not well suited. They call instead for foreign military engagement by special operations forces, which have been overstretched this last decade, and for which no respite is in sight. The situation calls, as many others do, for technologies that are force multipliers, like intelligence, surveillance and reconnaissance platforms that are easily deployed and operated by militaries short on resources. Technologies like unmanned aerial vehicles and persistent border surveillance can enhance that absorption.

20. But it is "not as simple as providing a piece of kit and waving goodbye," ? "How do we allow a small nation to have the advantage of these capabilities? These technologies will have to be scalable." Simply handing over or lending the large and complicated unmanned aerial vehicles and surveillance systems won't do. Once criminal activity is detected, the host nation must be have the will and training to curtail it. That will require a steady presence of SOF personnel in remote parts of the world. Distributed operations of that nature and scope call for a secure communications network the world doesn't currently have.

21. The transnational threat also hits close to the US and also India. The United States is the world's primary market for illicit drugs. They flow over the nation's land and maritime borders by the ton and government agencies catch only about a third of what's smuggled, Gen. Douglas Fraser, then the commander of U.S. Southern Command, told defense reporters in March. An estimated 1,200 to 1,500 metric tons of illegal drugs are produced in South and

Central America each year. Of that, about 60 percent eventually makes it to the United States. Here again, intelligence, surveillance and reconnaissance technologies can help. But eyes in the sky can only spy, and in South America are often hampered by rain forests.

22. In countries like Colombia and Honduras, criminals hide beneath a triple-canopy rain forest through which current sensors cannot penetrate. "That's really a effort right now. ... We have not gotten to a penetrative capability yet." Our neighbours are no les , sheltering criminals and boistering crime without boundaries which need to be curbed as they are also fuelling the fire of religionalism .

23. UAVs, however, cannot interdict drugs or smugglers once they are found. The Coast Guard and Navy need more ships for that task, or other weapon systems that both spot and stop illegal drug and gun trafficking, he said. But technology is not always the silver bullet. Just as in North Africa, countering transnational threats in South America is accomplished by using some technologies like maritime radar but is best done through direct cooperation with regional allies and old-fashioned word-of-mouth intelligence gathering, he said.

Conclusion

24. Synergy is essential to deal with India's complex internal security operations. Post 26/11, there appears to be a conscious effort to ensure better networking of agencies involved in these operations. Strategically, India cannot afford to be perceived to be buckling down under internal security or externally induced terrorist pressures. That would be disastrous. Neither can it afford to depend on other nations to take care of its internal security problems. Hard decisions, based on hard analysis of options in the current trend of internal security activities, have to be taken. We need a comprehensive centre-state strategy to deal with different insurgencies and communal terrorism. It should include broad-based domains of national and state policies including accelerated economic development and social justice, security and media policies. Most importantly, it should address dedicated and effective governance through good administration, prompt and fair judiciary and a law and order machinery that inspires public confidence.

References

Democratic Process, Foreign Policy and Human Rights in South Asia by Joseph Benjamin

Terrorism in Southeast Asia by Bruce Vaughn , Emma Chanlett-Avery , Thomas Lum , Mark Manyin , Larry Niksch

Inter-State Conflicts and Contentious Issues in South Asia Challenges and Prospects for SAARC by Emanual Nahar

Handbook of Terrorism in the Asia-Pacific by Dr Rohan Gunaratna

Human Insecurities in Southeast Asia (Asia in Transition) by Paul J Carnegie, Victor T King , Zawawi Ibrahim

Angels, Mobsters and Narco–Terrorists: The Rising Menace of Global Criminal Empires by Antonio Nicaso