National Maritime Foundation

www.maritimeindia.org

Physical Protection of India's Critical Maritime Infrastructure: Part 1

Author: Vice Admiral Pradeep Chauhan
AVSM & Bar, VSM, IN (Retd)

Date: 28 November 2019

It is a well-established fact that the physical protection of critical infrastructure can prevent the commission of high-impact terrorist attacks. Consequently, it is quite distressing, and more than little perplexing, to note that while there is a reasonable body of Indian literature covering the protection of critical information-infrastructure, and while organisational structures such as the Delhi-based National Critical *Information* Infrastructure Protection Centre (NCIIPC) have been put in place to coordinate the protection of **information**-infrastructure, there is very little Indian writing that addresses the physical protection of critical infrastructure. This void is even larger when it comes to the physical protection of critical ***maritime*** infrastructure. All this is in sharp contrast to the large body of literature on this subject that abounds in the West — including Europe and the USA.

This is the first of a series of articles intended to address this lack. The series seeks to provide 'baseline-inputs' to the lay reader and specialist alike, in respect of the physical protection of India's critical *maritime* infrastructure.

The protection of critical infrastructure has become a subject of the most intense concern, thanks to rise of the malevolent non-State actor (as also its fraternal twin, the State-sponsored non-State actor). The malevolent actions of these entities are frequently and collectively subsumed in a single word — 'terrorism'.

An internationally accepted definition of 'terrorism' and, consequently, that of a 'terrorist' continues to elude us, largely because of the persistence with which the cliché that "one man's terrorist is another man's freedom-fighter" is trotted out. This cliché can easily be shown to be riddled with flaws, but for the purposes of this article, it might be sufficient to note that, as Mr Ronald Reagan, the former President of the United States of America pointed out on 31 May, 1986, *"Freedom fighters do not need to terrorize a population into submission."*[1]

[1] Ronal Reagan. Radio Address to the Nation on Terrorism, May 31, 1986, Presidential Library and Museum; available at url: https://www.reaganlibrary.gov/research/speeches/53186a, accessed on 01 Nov 19

In the wake of horrific terrorist attacks visited upon the United States of America on 11 September 2001 — an event that has embedded itself into the global lexicon simply as "9/11" — the United Nations Security Council (UNSC) has been wrestling with issues relating to the protection of critical national infrastructure such as communications, emergency services, energy, dams, finance, food, public services, industry, health, transport, gas, public communications, radio and television, information technology, commercial facilities, chemical and nuclear sectors, and water.[2] In seeking the protection of such critical infrastructure, the more significant of the resolutions passed by the UNSC include the following:

- Paragraph 2 (b) of Security Council Resolution 1373 (2001).[3] This resolution calls on all Member States to "take necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information".

- Security Council Resolution 1566 (2004).[4] This resolution calls on States to prevent criminal acts, including against civilians, committed with the purpose of provoking a state of terror in the general public or in a group of persons, intimidating a population, or compelling a Government or an international to do commit, or abstain from committing any act.

- Security Council Resolution 2341 (2017).[5] This resolution, inter alia, invites member States to consider possible preventive measures in the developing national strategies and policies.

And yet, there are a number of complications in any attempt to arrive at a uniform or common understanding of how all these resolutions might best be implemented. To begin with, each sovereign nations-state determines for itself what constitutes its critical infrastructure. This, in and of itself, is a challenge of no small proportions and there are a number of problems in the determination of which assets should be considered 'critical'.

---

[2] United Nations Security Council Report. "Physical Protection of Critical Infrastructure against Terrorist Attacks", March 2017 p.2; available at url: https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-March-2017-Final.pdf, accessed 08 Nov 19.

[3] United Nations Security Council, Counter Terrorism Committee, Resolution 1373 (2001); available at url: https://www.un.org/sc/ctc/resources/databases/recommended-international-practices-codes-and-standards/united-nations-security-council-resolution-1373-2001/, accessed on 10 Nov 19

[4] United Nations and the Rule of Law, Counter Terrorism Committee, "Security Council Resolution 1566 (2004) on Threats to International Peace and Security caused by Terrorist Acts"; available at url: https://www.un.org/ruleoflaw/blog/document/security-council-resolution-1566-2004-on-threats-to-international-peace-and-security-caused-by-terrorist-acts/, accessed on 10 Nov 19

[5] United Nations and the Rule of Law, Counter Terrorism Committee, "Security Council Resolution 1566 (2004) on Threats to International Peace and Security caused by Terrorist Acts"; available at url: https://www.un.org/sc/ctc/news/document/s-res2341-2017-protection-critical-infrastructure/, accessed on 10 Nov 19

- First, because of the myriad interconnections, networks, nodes, links and interdependencies that exist between sectors — most of which are both facilitated and complicated by cyber pathways — it is often difficult to prioritise one infrastructural element over another.

- Secondly, which segment of infrastructure is — or should be — considered 'critical' is quite likely to change over time. Although this lack of permanence is acknowledged and recognised, bureaucracies, and even practitioners — such as the police or the defence forces — are, more often than not, unwilling to accept the huge political risk of removing items from a 'critical list',[6] even though this can — and often does — result in a waste of precious resources.

- Thirdly, priorities accorded within a 'critical list' of infrastructure are political in nature and mirror popular fears without necessarily or accurately reflecting prevailing risks or probabilities. For instance, control-systems in respect of traffic lights on city-roads might well be included along with roads in critical urban infrastructure even though the roads themselves may well continue to be functional despite the fact that the traffic lights have gone out.[7] Such ambiguities adversely impact the development of security-measures.

- Fourthly, an increasingly large quantum of what might intuitively be considered to be critical infrastructure is owned by the private sector. It is estimated that in the case of western democracies, more than 80 per cent of the critical infrastructure is owned and operated by the private sector.[8] As a consequence, the State itself may no longer be able to ensure comprehensive security of critical infrastructure and could well become almost entirely dependent on the private sector for this purpose.[9]

- Finally, many States increasingly depend on infrastructure and assets that are partially or completely located outside their jurisdiction and over which they have little or no control.[10]

It is obvious that determining which infrastructure-assets are 'critical' requires careful judgement and detailed calculation, and, in addition, calls for an extremely well-defined

---

[6] United Nations Security Council (UNSC) Counter Terrorism Committee Executive Directive (CTED) March 2017. "Physical Protection of Critical Infrastructure against Terrorist attacks"; available at url: https://www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-March-2017-Final.pdf, accessed on 10 Nov 19

[7] *Ibid*, p. 2

[8] Balaji Srimoolanathan. "Adopting a holistic approach to Protecting Critical Infrastructure"; Janes 360, 18 June 2014; available at url: http://www.janes.com/article/39495/adopting-a-holistic-approach-toprotecting-critical-infrastructure-es14e3, accessed on 10 Nov 19

[9] *Op Cit* (See Supra Note 6)

[10] Dave Clemente. "Cyber Security and Global Interdependence: What is Critical?" Chatham House. February 2013; available at url: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf, accessed on 10 Nov 19

public/private partnership for the creation and implementation of a policy on the protection (both physical and informational) of this critical infrastructure. In seeking to integrate these considerations into national and international security frameworks, nation-states must carefully factor the relationship between the public and private sector on the one hand, and, the importance of a particular area of critical infrastructure, on the other. This is a daunting task and one that requires the continuous engagement of all participants concerned.[11]

As in much of the world, in India, too, the subject of the protection of critical infrastructure has been receiving a great deal of attention. This is hardly surprising given that India has been subjected on a continual basis to the horrors of State-sponsored terrorism from across its western border ever since the late Prime Minister of Pakistan, Zulfikar Ali Bhutto, in the wake of his country's resounding defeat to Indian Arms in 1971, laid down the doctrine of 'bleeding India through a thousand cuts'. Pakistan's Inter-Service Intelligence (ISI) has assiduously explicated this doctrine over the half-a-century or so that has since elapsed.

India's Critical Sectors.

India defines *Critical Sectors* as those *that are critical to the nation and whose incapacity or destruction will have a debilitating impact on national security, economy, public health or safety.*[12] In 2015 the **National Critical *Information* Infrastructure Protection Centre** (NCIIPC) presented a list of twelve critical sectors. It needs to be noted that this is the list of information-infrastructure. There could well be critical infrastructure that lies outside the limits of information-infrastructure. That said, the identified sectors are:[13]

1. Energy
2. Transportation
3. Banking & Finance
4. Telecommunication
5. Defence
6. Space
7. Law enforcement, security & intelligence
8. Sensitive Government organisations
9. Public Health
10. Water supply
11. Critical manufacturing
12. E-Governance

---

[11] *Ibid* (See Supra Note 10)

[12] National Critical Information Infrastructure Protection Centre (NCIIPC) Workshop, 2015; available at url: http://workshop.nkn.in/2015/sources/speakers/sessions/NKN_NCIIPC.pdf, accessed on 10 Nov 19

[13] *Ibid* (See Supra Note 12)

Of this dozen, six — 'energy', 'transportation', 'telecommunication', 'defence', 'space' and, 'law-enforcement, security and intelligence' — are especially relevant to the maritime domain. However, even a relatively cursory examination of issues and processes relevant to the physical protection of each of these sectors is a formidable task that will need far more elastic a word-length limit than that permitted for this piece of writing. And yet, there is no gainsaying that such an examination is necessary.

Consequently, each of the subsequent articles in this series will present the reader with an overview pertinent to the physical protection of a specified sector of critical infrastructure that is relevant to India's maritime domain.

****

The author, Vice Admiral Pradeep Chauhan (Retd), Indian Navy, is the Director General, National Maritime Foundation (NMF), New Delhi. He may be contacted at directorgeneral.nmfindia@gmail.com

This article was previously published in the "South Asia Defence & Strategic Review" (DEFSTRAT) magazine (May-June 2019 Volume 13, Issue 2) and is reproduced with permission of the editor, DEFSTRAT. DEFSTRAT is a Media Partner of the National Maritime Foundation.