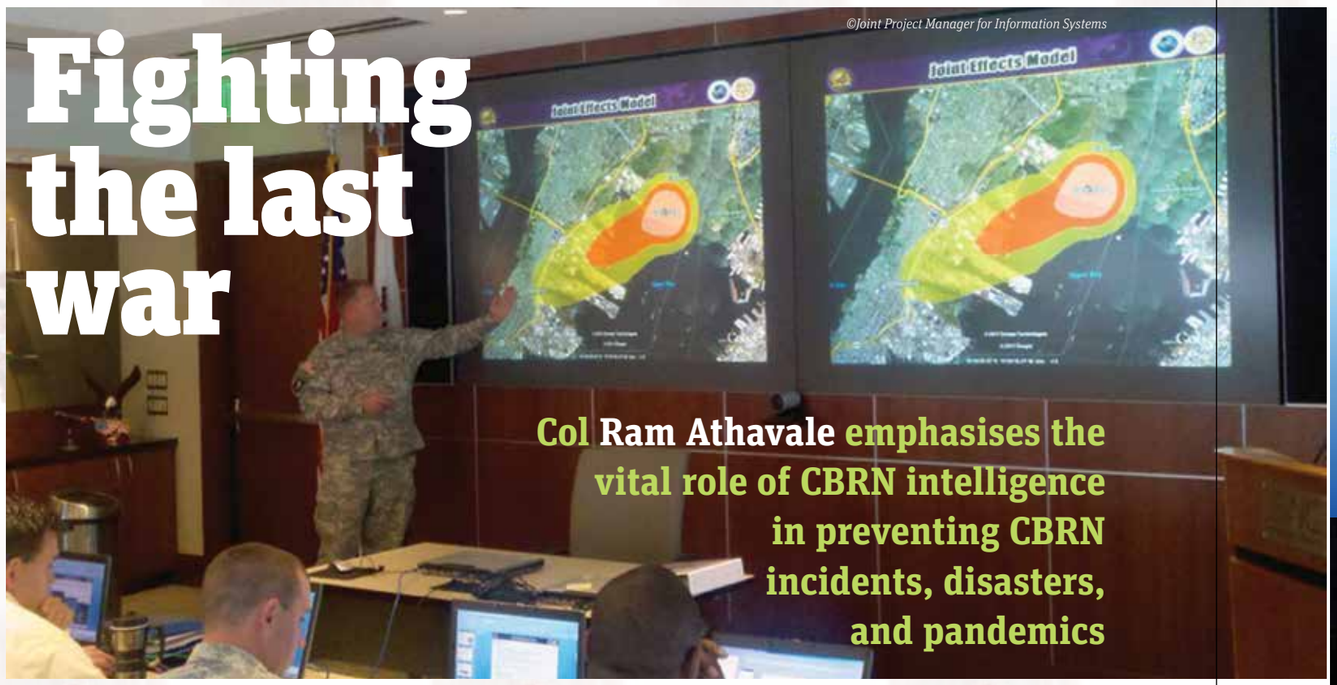
Fighting the last war



©Joint Project Manager for Information Systems

Col Ram Athavale emphasises the vital role of CBRN intelligence in preventing CBRN incidents, disasters, and pandemics

The Covid-19 pandemic has exposed the need for the international community to come together to take preventive measures. This can only be done effectively if we acquire and apply adequate and timely intelligence on these and other CBRN threats

Covid-19: where it all began

The Covid-19 crisis began in Wuhan, China in November 2019. On 31 December, the World Health Organization (WHO) stated that a mysterious pneumonia was sickening and killing dozens in China.

It was only on 30 January that the WHO declared the disease a "public health emergency of international concern" – a designation reserved for extraordinary events that threaten to spread internationally. It took two months from the onset for the world to recognise Covid-19 as a global pandemic. By that time there were scores of cases worldwide and increasing by the hour.

Nearly all nations failed to understand the likelihood of the outbreak in China becoming a pandemic. The gross lack of intelligence on the virus and its anticipated spread, disregard for expert advice, apathetic actions on lessons learnt from earlier similar incidents and exercises/simulations – such as the Clade X pandemic simulation exercise by the US – were compounded by the near negligible understanding of proactive actions.

This led to an epidemic becoming a pandemic. By 21 November more than 1,377,790 Covid-19 deaths had been recorded worldwide. By mid-January 2021, the number totalled 2 million.

SEC Technologies' Falcon 4G Chemical Stand-off Detector is based on LiDAR.

©SEC Technologies

The Beirut explosion

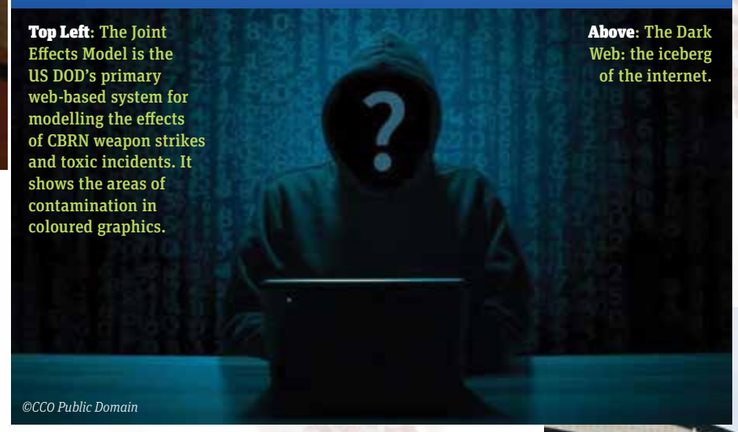
On 4 August 2020, two massive explosions ripped apart much of the Lebanese capital, Beirut. Reports state that nearly 2,750 tonnes of ammonium nitrate stored in warehouses at the port blew up and that several port warehouses were clandestine Hezbollah weapons caches. The unsafe conditions and growing vulnerability were known but no cognisance was apparently taken of the impending threat. Following the explosions, news emerged of tons of toxic chemicals being stored at other ports and dry ports, as well as well-known precedent of AN explosions at ports.

Such vulnerabilities caused by slack control on toxic substances also pose a danger from terrorist groups inclined to use CBRN material to cause disruption, chaos and casualties. Smuggling of CBRN material, deals brokered on the 'dark web,' thefts from laboratories and industries, supply chain interdictions and clandestine research and manufacture of CBRN agents have been on the intelligence radar for several decades. Despite agencies being aware of these threats, incidents still occur.

Sadly, we react rather than preempt. Do we have no advance input? Why didn't we see it coming? Do we not monitor such developments in our neighbourhood or anywhere in the world? Do we not have a system of intelligence gathering and analysis on CBR incidents? Are we not geared to sequentially initiate actions and capabilities to meet the challenges of such incidents? Are we not aware of such toxic threats in our midst?

If we are, why is no action being taken to correct the system? And if we are not, we need to seriously review our strategy and our reporting system.

©Wikimedia Commons



©CCO Public Domain

Top Left: The Joint Effects Model is the US DOD's primary web-based system for modelling the effects of CBRN weapon strikes and toxic incidents. It shows the areas of contamination in coloured graphics.

Above: The Dark Web: the iceberg of the internet.

Above: The dark web is a bottomless pit for shady deals.

Right: Chinese medics in the city of Huanggang, Hubei on 20 March 2020.

National strategy

A nation needs a strong comprehensive national CBRN strategy and a National CBRN Plan to lay down the actions, capabilities and capacities required to meet such challenges. Such a plan would spell out the tasks of various agencies and entities which gain CBRN intelligence.

Had this been put in place, we would not have been caught napping with inadequate testing facilities, ventilators, PPE and masks at the onset of the pandemic. Even hospitals, healthcare facilities and administrative machinery were found to be totally unprepared for the pandemic.

CBRN intelligence

If intelligence is not planned, it can lead to grave national security concerns. There ➤

©Walter Grassroot/Wikipedia

is an emergent need to understand these implications from such threats. CBRN security needs to be factored into our intelligence mechanism.

Intelligence is a deliberate painstaking process and needs highly trained personnel supported by state-of-the-art technologies. CBRN intelligence (like terrorism intelligence) needs careful and synergetic actions by domestic and external intelligence agencies.

CBRN threats are of global nature and their impact transcends borders. Intelligence agencies and related support entities need to understand CBRN hazards and develop structures within their organisations to analyse inputs pointing towards CBRN threats.

In essence, a CBRN section is a must for all intelligence and homeland security agencies. There are many CBRN stakeholders and this spectrum needs to be understood by the specialists. Such special intelligence agents need CBRN training to understand the nuances of CBRN threats and their likely manifestation.

Ease of best analysis and threat assessment depends on effective sharing of CBRN intelligence among the agencies. The US Government's H.R. 2200 (114th): CBRN Intelligence and Information Sharing Act (2015) and other protocols will also help to avoid false corroboration of input.

There are many potent disciplines for intelligence gathering like human intelligence (HUMINT), signals intelligence (SIGINT), imagery intelligence (IMINT), measurement and signatures intelligence (MASINT), and open source intelligence (OSINT).

The internet is a potent source of CBRN intelligence. Clandestine deals, illegal trading in toxic materials and deals leading to CBRN trails are all important inputs that can be gleaned from the illicit dark web. Analysts need to be trained to identify and track such CBRN trails.

Intelligence technologies

Real-time detection and identification of agents, stand-off detection, remote sensing, use of drones and unmanned ground vehicles (UGVs) are among the technologies to enhance surveillance and early warning. Newer technologies must be utilised for early detection and prevention of CBRN incidents. CBRN risk and vulnerability mapping and adequate preventive measures must be adopted.

Based on risk clusters, agencies need to game plan and simulate adverse contingencies and accident/sabotage scenarios. Lessons from such exercises and simulations should be studied carefully and shared on a need-to-know basis with concerned stakeholders and the intelligence community. This will enable early detection of threats and application of optimal preventive measures.

INTELLIGENCE CONTRIBUTORS

Domestic

- Healthcare, hospitals and clinics
- Local police stations
- Fire brigades
- Pathology laboratories
- Municipal authorities, civic workers and sanitation workers
- Pharmacists and medical stores
- Meteorological and pollution control
- Industrial safety and security agencies
- NGOs and social support groups
- Logistic hubs, warehouses, storage yards and trans-shipment points
- Cargo handlers at ports, airports and railway junctions

International

- Embassies and High Commissions
- Trade bodies, World Custom Organisation
- Businesses abroad
- NGOs and social support groups
- Local news media
- International monitoring agencies, CDC, WHO
- International Intelligence and policing bodies, INTERPOL, Europol

SPECTRUM OF CBRN INTELLIGENCE

Proliferation/smuggling

- Illicit shipping and transportation
- Cross border smuggling – coordinated interdictions
- Covert meetings and collaborations
- Clandestine deals and trade on the web or dark web

Emerging threats

- Illicit capability development for CBRN agents – technology, dual-use acquisitions
- Training for CBRN incidents
- Covert laboratory activities
- Reports of unnatural disease incidence
- Intelligence of planned attacks or releases/transportation of CBRN material

Early warning of actual CBRN release

- Industrial accidents/sabotage
- Logistic accidents/sabotage – warehouse, handling, air, sea or land transportation
- Laboratory/research accidents/sabotage
- Terror related explosions or releases

A Joint EDA/European Space Agency (ESA) Autonomous Drone Services Quad Copter RPAS in CBRNe Operation (AUDROS)

©ESA

Col Ram Athavale, PhD is a former Key Adviser to the Government of India (MoD and MHA) on CBRN Security and has been a Key CBRN Expert for the EU CBRN Risk Mitigation Centres of Excellence initiative in Eastern and Central Africa. The author of **Toxic Portents on CBRN Incident Management in India**, *he is currently a freelance CBRN Security and Risk Mitigation Consultant based at Pune, India.*