International Journal of Education, Modern Management, Applied Science & Social Science (IJEMMASSS)
ISSN : 2581-9925, Impact Factor: 7.150, Volume 06, No. 02(II), April - June, 2024, pp. 27-37

CYBERSECURITY VISION FOR INDIAN BORDER AREA SECURITY

C J Jagadeesha*

ABSTRACT

The India's present Borderman needs three recipes (a) tech-savy, (b) continuum learning and (c) brave enough to enter conflict zones technologically. The cyber security of the existing physical infrastructure in the borders needs to be augmented. The critical infrastructure within the borders and in the conflict zones needs a continuous surveillance. The surveillance has to come from small satellites, geo-spatial technologies with AI, drones (UAVs), Wi-fi and a set of minimum counter measure infrastructure in all the entities be it private, public, government, NGO, the enterprises set up for serving welfare functions in the border areas. It needs investment, awareness of cybersecurity, training/capacity building of interdisciplinary graduates / whatever type of certification needed for country's security. The think tanks from present BORDERMAN has to make ways for emerging border cybersecurity men by bringing awareness, training for efficient security along the border areas of the country. The homeland security needs to be enhanced to match the world wide technology trend especially at the time of disasters. The digital skills should be imparted with cyber security in view. Department of Homeland security should bring harmonisation of cyber incident reporting and management of cyberthreats. In this, institutes like Borderman when enlarged in numbers to help in national security along borders, can help bring awareness in cyber security by providing assistance to frame policies and regulations. Also, educating masses (online or offline periodically) in the simplest cybersecurity modules like (a) password management,(b) privacy settings,(c) protection against social-engineering cyberthreats, (d) backing up data. The advanced training is already in place with universities like NFSU. The first and foremost is to have countermeasure infrastructure in place near our health centres, welfare departmental data centres (large housing complexes, oil, energy, water supply, forests and industries like mineral, cement, pharmaceuticals, and others), satellite ground stations (their number increases due to private sector participation) and transportation sectors. The curriculum is already developed and people are getting training in drone operations for agriculture, health services, revenue survey etc. This should be extended to include cybersecurity of drones, drone formations flying with appropriate PNT services either from satellites or land based.

Keywords: *Baseline Cybersecurity, Border Security Areas, Geospatial Technologies.*

Introduction

The cybersecurity talent gap hampers India's competitiveness and growth, which heavily depend on the development and uptake of strategic digital technologies (e.g. artificial intelligence, 5G and cloud). A skilled cybersecurity workforce is needed, to keep India cybersecure, in order for the India to remain in a position to deliver key advanced technologies in a global setting. Cybersecurity is not only part of citizens, businesses, and member States' security. It is also a necessity to ensure the India's political stability, the stability of its democracies and the prosperity of our society, neighbour hood relations, and businesses. Threat actors increase their capabilities and novel, hybrid and emerging threats, such as the use of bots and techniques based on artificial intelligence, are emerging. Ransomware threat actors are routinely inflicting considerable damage, both financially and reputationally, to entities.

* Adjunct Professor, Karunya Institute of Technology and Sciences, Coimbatore & Former Scientist ISRO-NRSC-RRSC, Bangalore, Karnataka, India.

Elections and Cybersecurity

Elections across the globe have become a frequent target of cyberattacks in the last few decades. Cyber threat activity targeting elections has increased worldwide. These cyberattacks are often combined with information operations and other hybrid threats. Along the border areas and a little inside are the Critical Infrastructure to be protected. In digital India we are expecting smart water electric, banking, finance, telecommunications, emergency services and transportation system/enterprise grids as critical infrastructure. The term critical infrastructure refers to assets of physical and logical systems that are essential to the minimum operations of the economy and government. The levels of the government, private and even individuals are becoming networked in a global-centric way. The individuals and private enterprises are calling service centres halfway around the world to assist them with their networking difficulties. The CIP- critical infrastructure practitioners need to understand the contexts (economic, environmental, cultural and political) to maintain, operate, predict and analyse problems in the operations and maintenance.

In the electoral context the following cybersecurity threats need to be taken into account: (a) ransomware and wiperware attacks, (b) distributed denial of service attacks, (c) social engineering and phishing attacks, (d) website defacement, (e) supply-chain attacks, (f) cybersecurity attacks facilitating the creation and spread of manipulated information. The attack surface - assets and processes at stake throughout the electoral cycle are as mentioned here: (a) set-up period (1. registration of eligible politician and party,2.registration of voters) ; (b) campaign period (campaigning by politicians and parties) ; (c) Voting period (1.voting,2.vote counting, transmission and tabulation,3.results, publication and display); Post-Vote (1.auditing of the process, 2.lessons learned). The range of election technologies adopted for electoral process around the world including India are the following (completely or partly): (a) internet voting system, (b) election information system, (c) electoral results web page, (d) voters register. Election technologies are part of a broad range of e-government applications based on public and private sector (energy, telecom,banking) systems.The following needs to be understood by electoral officers and voters in elections for a democracy: (a) Hybrid threats and foreign information manipulation and interference (FIMI), (b) Mapping cyberattacks to election phases,(c) Social media networks and disinformation, (d)The benefits and technology risks of using AI (artificial intelligence),(e) Election organization and possible threats,(f) Relevant legal and policy documents .

The critical infrastructure protection (and relevant practices) aspects involve concepts of understanding and defining (a) capacity and emergence of networks (translations of informatics systems into physical infrastructure), (b) thinking beyond national response frameworks, (c) NRF and public private partnerships, (d) critical information protection and critical infrastructure assurance domains, (e) emergency preparedness and readiness for (i) hazardous materials (explosives, gases, flammable liquids/solids, radioactive materials, oxidizers, toxic material, and WMD weapons of mass destruction (ii) the range of evolving threats, including the following- problems in the transportation sector, invasive species (damaging agriculture, water supply etc), counetrfeit goods (particularly in the high- tech sectors), climate change- related issues (drainage and drought), cyber-related and telecommunications (in terms of converged technology).The guideline classifications are to be broken down into three definitive areas. First, awareness-level guidelines, second is performance-level guidelines, third is planning and management level guidelines (Robert Radvanovsky and Allan McDougall, 2013) The general threat mitigation procedures involve the risk assessment and management methods using, MEI-Minimum Essential Infrastructure, SVA Security Vulnerability Assessment, VAF Vulnerability Assessment Framework.

In India there exist already some institutes / organizations / forums / forces assigned to these emergency preparedness, monitoring, management and mitigation. For health hazards we have public health departments. For Oil and Gas hazards we have ONGC. Chemical gas hazards is it the government or private organizations? Do we have enough preparations for Security and then cybersecurity? The department of Homeland Security has to give guidelines specifying each category of guidelines, risk assessment methodologies, countermeasures to be adopted, threat analysis and incident management methods. This will help bridge the collaboration and cooperation among sates and institutes across India. It should tie up with policies , regulations, standards to all related departments like public health, climate change and disaster management, enterprises owning hazardous materials, agriculture and communications etc.

Countermeasure Infrastructure

Risk analysis is the basis for appropriate and economical countermeasures. Risk calculation matrix makes use of likelihood/probability summary matrix, vulnerability matrix, and consequences matrix. As per department of homeland security in USA, which follows ISO31000 risk formula,

Risk = Likelihood x Consequences

Likelihood (probability) assumes a threat actor that is both interested and capable and has the logical resources and adequate proximity to the target, which has exploitable vulnerabilities. The nexus of these two variables results in likelihood. In fact, Likelihood is the composite of (a) a particular type of threat actor's potential interest in a target, (b) the vulnerabilities that threat actor could exploit on that target, (c) the potential for a desired outcome (economic, subversive, or violent criminals) or the potential for achieving the desired consequences (for terrorist)

This is just a simple glimpse of likelihood of a terrorist threat actor (class I toV), and criminal threat actor (transnational criminal organizations, organized crime, sophisticated economic criminals, unsophisticated economic criminals, information technology criminals, non terrorist violent criminals, subversives, petty criminals) categories. This information needs to be evaluated (to get from major crime and minor offences statistics) to find out economic crime asset target value, non-terrorism violent crime asset target value, petty crime asset target value estimates.

There are many security consultants and contractors who will design card readers and cameras into an architectural space without any risk analysis or security policies, based solely on their experience of what previous clients for similar companies have wanted. The questions that security policies answer (just a few out of many) : (a) where should access control technology go and where should guards be placed in lieu of card readers?, (b) when are guards better than card readers, (c) where should cameras be used and what should they view and not be allowed to see?,(d) where are alarms needed and where are they likely to be a problem?,(e) how could crime prevention through environmental design be used to reduce the need for both security manpower and technology?, (f) what type of security credential is necessary, (g) How should high-tech, low-tech, and no-tech security solutions be mixed to achieve an appropriate balance between best results and best economy? , (h) how much attention should be paid to perimeter detection?, (i) should cameras be used in interior places and where?, (j) how can we achieve effectiveness, and still control costs?, and the list goes on and on. Policies answer all these questions. Security policies are not likely to be effective without a risk analysis. And without security policies, security countermeasures will almost not certainly not be effective.

All security countermeasures have 3 main goals: (a) Potential threat actors should be identified and denied access wherever possible,(b) Except for legitimate approved , controlled and monitored materials, the countermeasures have to deny access to the facility of weapons, explosives, and dangerous chemicals,(c) they have to make the environment suitable for appropriate behaviour and unsuitable for and inappropriate for criminal or terrorist behaviour and also to mitigate the actions of both hazards and threats.

Baseline Security Program is different from Budgeting/Special purpose Security Programs (CRS, 2007)

Baseline Security Program (BSP)

The BSP is the heart of the countermeasures. It is designed to cater to day-t-day operations. It allows for the identification of unwanted exceptions so that they can be handled . The highly unusual conditions (terrorism) are not handled by BSP.

The following 3 elements are basic to BSP:

- Design an environment that encourages appropriate behaviour and discourages inappropriate criminal or terroristic behaviour
- Detect, assess, and respond to exceptions
- The program design is to mitigate any potential harm from hazards and threats

In general, the specific countermeasures should include (a) terrorism and major crimes difference program, (b) emergency preparedness program, (c) disaster preparedness program

The basic selection of countermeasures utilize high-tech elements, low-tech elements and No-tech elements.

High-tech elements are (i) access control systems, (ii) detection systems, (iii) CCTV systems, (iv) two-way voice communication systems, (v) consoles and management offices, (vi) security archiving technologies and schemes, (vii) security system infrastructures. High-tech elements of the system can also be a force multiplier when correctly designed. Thar means, a well designed security video system can support video surveillance, video guard tours (many more tours of the facility each hour than a walking guard can perform), and video pursuit (following a subject through the building). Access control systems are capable of saving many tens of thousands of dollars annually in guard costs. ***Low-tech elements*** may include (i) locks, (ii) barriers, (iii) lighting, (iv) signage, (v) crime prevention through environmental design elements etc. Low-tech elements can be designed to provide an environment that reduces the possibility of criminal behaviour and encourages appropriate behaviour. ***No-tech elements*** may include (i) authorities and responsibilities, (ii) reference to charter for security unit, (iii) statement from the president/chairman/CEO etc. That means No-tech elements majorly include human beings for (a) security posts, (b) patrols, (c) responses, (d) security awareness program, (e) news letters, e-mails, (f) security investigation program, (g) security intelligence program, (h) emergency services liasion program etc. They also have access control objectives but with very minimal technology elements.

For Ex: *Access control systems* may include (a) card technologies, (b) magnetic stripe cards, (c) Weigand wire cards, (d) proximity cards and key fobs, (e) active cards, (f) radio-frequency access devices, (g) barcode cards, (h) contactless smart cards, (i) transportation worker identification credential cards (maritime), (j) magnetic stripe card readers, (k) long-range card readers, (l) barcode readers, (m) keypad readers,(n) scramble keypad readers, (o) niometric reader technologies, (p) photo ID systems etc.

For Ex: *CCTV systems* may include (a) visible light cameras, (b) PTZ video cameras, (c) pinhole video cameras, (d) day/night imagers, (e) analog cameras, (f) digital cameras, (g) digital -fish eye PTZ cameras, (g) thermal imaging cameras, (i) video analytics software etc.

For Ex. *Low-tech systems,* Locks: (a) electrified morise locks, (b) electrified panic hardware, (c) magnetic locks, (d) delayed egress hardware coupled locks, (e) high security electric locks, (f) drop-bolt locks, (g) electrified cylinder locks, (h) lock power-fire alarm etc.

The present day digital transformation needs many more devices to be understood cursorily by BORDERMEN. Incidentally BORDERMEN is a new institute / organization or a type of Cybersecurity skills academy which has started in New Delhi recently (Inspira Research Association 2024).

In essence the capacity building of Bordermen should start from suitable risk analysis methods and end up in choosing countermeasures at an affordable level. Appropriate national policies, standards, regulations and practice should be strategically built for each State in India. The appropriate certification programs be it three months, six months or one year should be designed for Bordermen. All Agniveers can be trained in these certification programs after their tenure in defence.

Cross-border Security Operations Centres will have to procure, countermeasures infrastructure and cyberthreat detection tools and services together with the Department of Homeland security designated centre for cybersecurity competence.

Geospatial Technologies in Border Security Programs

Geospatial technologies has the following: Spatial images-2D- of object/ phenomena from satellites, aerial height or Drones operations height/platform. It uses remote sensing technologies using MSS-Hyperspectral, Microwave/radar/sonar, Lidar and Lasers. The communication and navigation technology satellites use GPS (global positioning system)/ GNSS or from aerial heights too for PNT (position, Navigation and Timing technologies). The GIS (geographic information systems) is capable of mixing geospatial image databases with attributes data obtained from land surveys from field departments. The 3D technologies (photogrammetry measurements) from mobiles, drones and satellites need to be understood to know details of disaster scenes of a forest, ecosystem destruction and technological disasters like railway accidents, airoplane accidents or even road junction accidents. The data of these are in the form of pixels (picture elements) or points represented in some computer compatible formats and amenable for image processing, analysis and interpretation using mathematics / statistics.

Common GIS Tasks for Disaster Planning and Preparation Activities are for Evacuation Route Planning, Evacuation Zone Planning, Scenario Modelling for Answering What-If question s (table top exercises-FEMA), Spatial Statistics and Hot Spot Mapping (Heat Mapping Vs Hotspot Mapping), Public outreach and Citizen Participation. This GIS is used for virtualise a hot sopt surface using IDW technique and allow one to calculate hotspots via incremental spatial autocorrelation (ISA) and Hot spot analysis.

The national geospatial data model as in USA is depicted in Fig.1.Geospatial data model (GDM) is a comprehensive framework for organizing features of interest to the homeland security community. The primary purpose of GDM is to provide a means for sharing of geospatial information obtained in real time / even in not-real time, the sharing between organizations and agencies whose primary responsibility is to plan for, and respond to natural disasters and hostile events. The GIS person and IT support persons should develop good relations to solve the regular system updates problems (for operating systems), virus protection and other activities to keep computing infrastructure running (Brian Tomaszewski,2000).

The various data themes that are pictured in GDL model (Fig.1) expand into several sub themes. India has all the capabilities to develop a GDL like this. The listing of geospatial databases available in India here is appropriate.

- Government of India CWC https://indiawris.gov.in/wris/#/
- Government of India https://www.india.gov.in/
- Government of India, Ministry of Jalshakti, http://jalshakti-dowr.gov.in/
- Government of India, Ministry of Water Resources, http://nhp.mowr.gov.in/
- Government of India, Central Water Commission, http://www.cwc.gov.in/
- Government of India, Central Ground Water Board, http://cgwb.gov.in/
- Government of India, ISRO-NRSC, https://www.nrsc.gov.in/
- Government of India http://ffs.india-water.gov.in/
- Government of India https://bhuvan.nrsc.gov.in/home/index.php
- Government of India https://www.mosdac.gov.in/
- Government of India, ISRO-SAC, https://vedas.sac.gov.in/vcms/en/

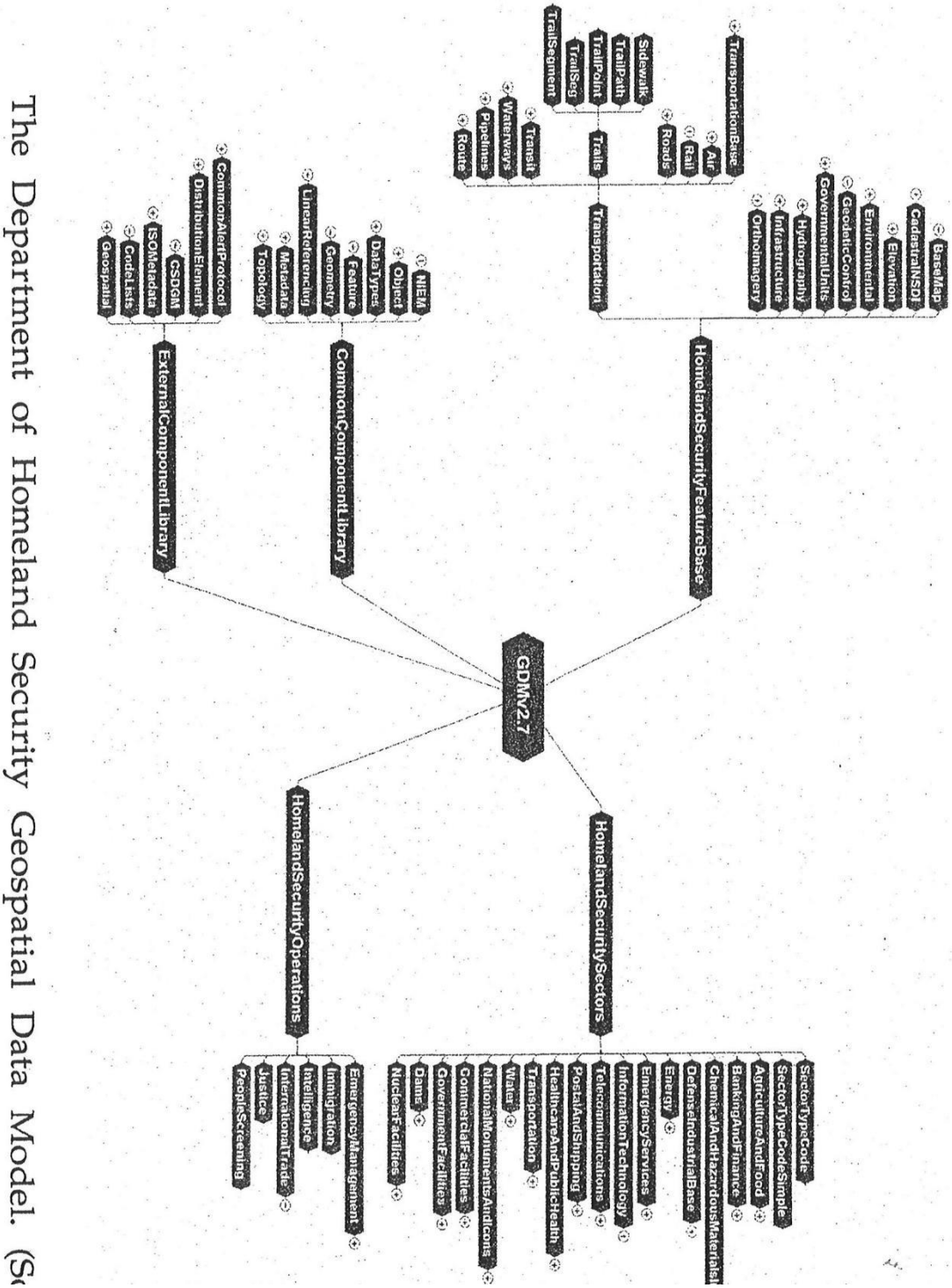
Added to this there are websites which are having worldwide information and having specialized attributes / themes added to data taken from India in a collaborative mode. The geospatial knowledge infrastructure is expanding gallopingly, as more and more small satellites constellations are adding spatial data into world geospatial databases including India. See Fig.2 for knowing more about how Geospatial Knowledge Infrastructure is trending towards Digital India / World with sustainability goals in mind.

Information Security vs. Cybersecurity

The primary difference between information security vs. cybersecurity is the role of technology. Cybersecurity involves the safety of computer systems and everything contained within them, which includes digital data. In contrast, information security refers to the safety of information in all its forms, whether it's stored on a computer system or not. As a concept- information is closely related to notions of constraint , communication, control, data, form, instruction, knowledge, meaning, mental stimulus, pattern, perception and representation.

Whereas information security refers to the safety of information contained within or on any medium, cybersecurity is solely concerned with the safety of technology. If you think of information security as an umbrella category, you'll find cybersecurity nestled within it as a subcategory. Yet, cybersecurity encompasses more than just the safety of data. Although it's true that hackers, often attempt to gain unauthorized access to a network for the sake of exploiting sensitive data for financial gain, some may disrupt a computer network for other reasons, such as to commit a political attack or act of terrorism. It's the job of cybersecurity professionals to prevent all types of cyberattacks, and to investigate them when they do occur (Naikodi C, Venkappanavara B 2023), (Gupta S, Gupta G 2023).

Fig.1: Department of Homeland Security GSD Model (USA)



Source: Brian Tomaszewski 2021 p250

The Department of Homeland Security Geospatial Data Model. (S

Fig. 2: Geospatial Knowledge Infrastructure Components

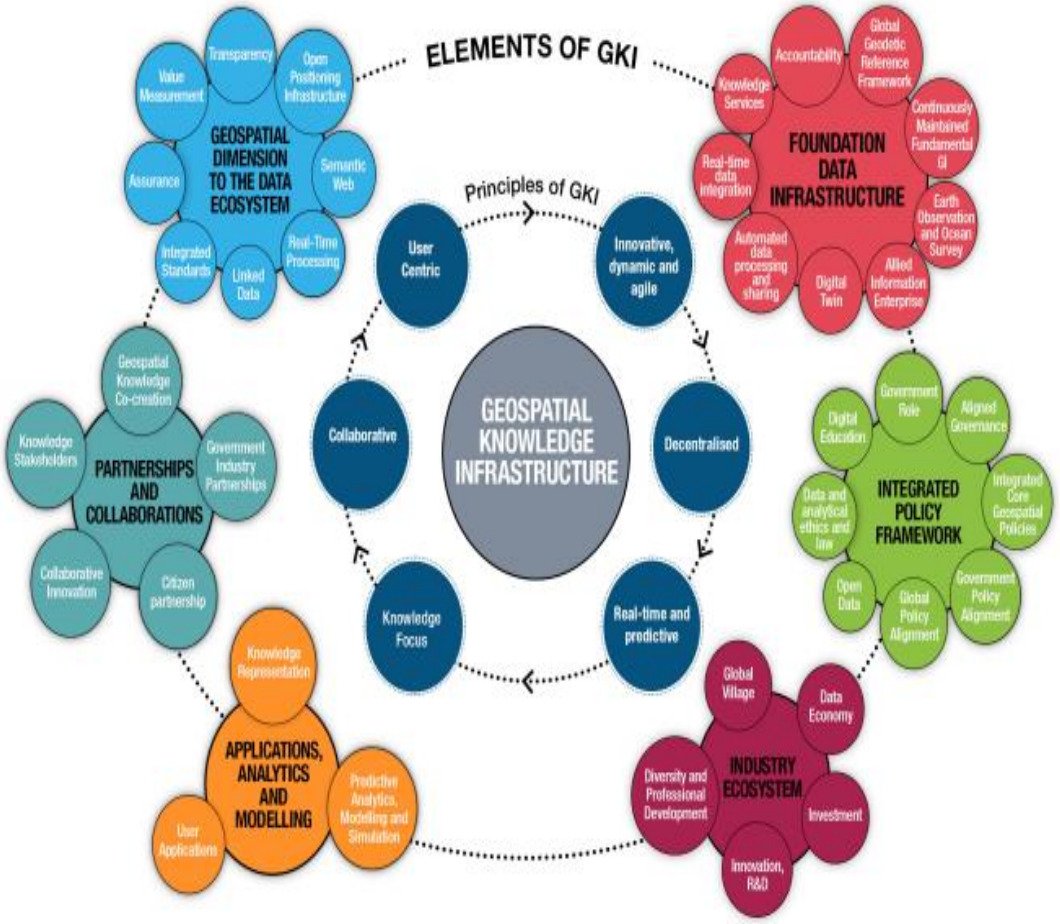


Figure 3: Elements and Components of Geospatial Knowledge Infrastructure

Source: Geo Spatial Media, World

Cybersecurity Framework

Cybersecurity framework consists of three important elements (a) Cores, (b) Tiers, (c) Profile. Framework Core -is a set of desired cybersecurity activities and outcomes organized into Categories and aligned to Informative References. The Framework Core is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language. The Core consists of three parts: Functions, Categories, and Subcategories. The Core includes five high level *functions*: Identify, Protect, Detect, Respond, and Recover.

- **Identity:** Refers to what processes and assets need protection
- **Protection:** What safeguards are available to protection
- **Detect:** What techniques can identify incidents of threats
- **Respond:** What techniques can contain (reduce) impacts of incidents
- **Recover:** What techniques can restore capabilities

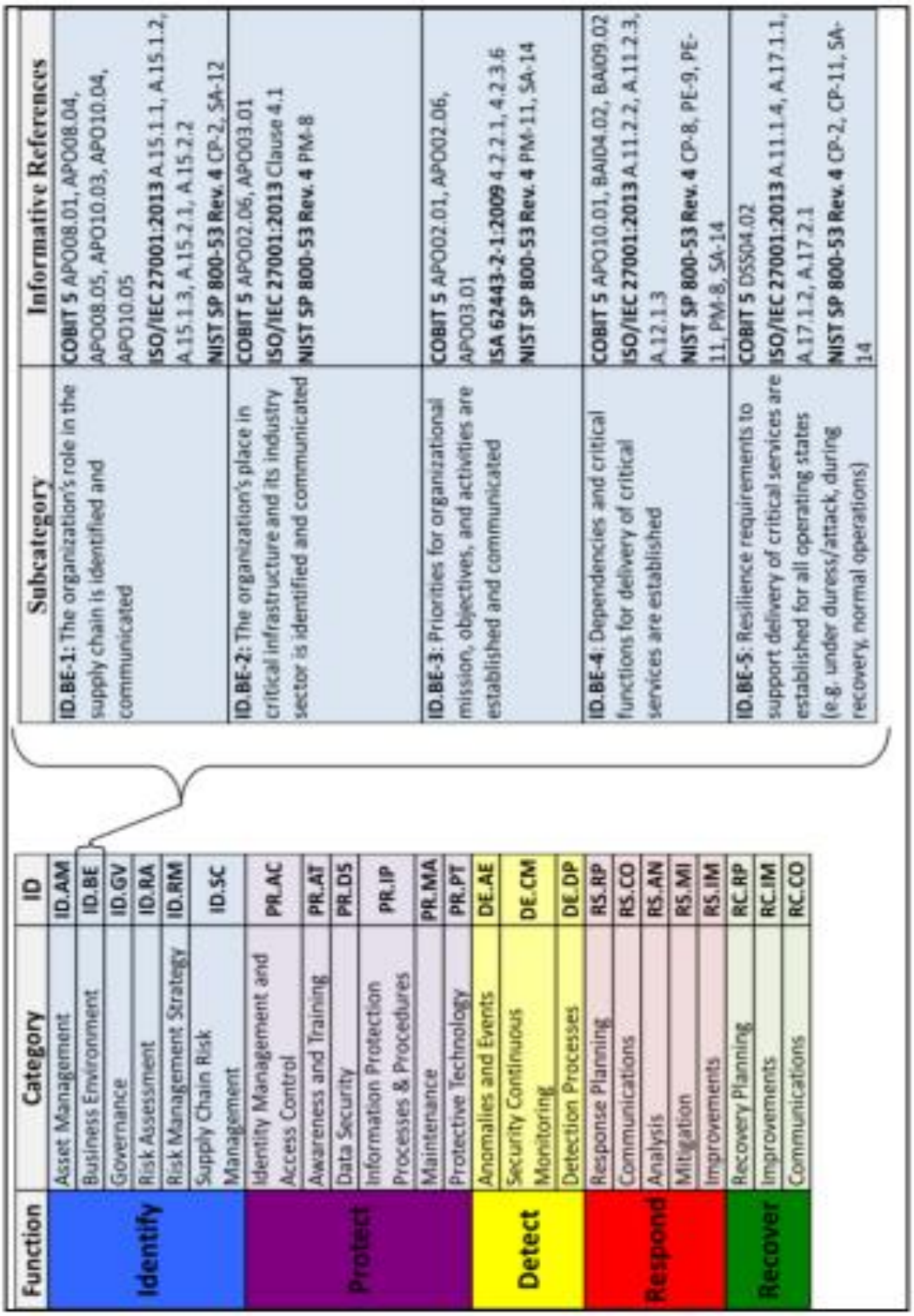
These 5 functions are not only applicable to cybersecurity risk management, but also to *risk management at large*. The next level down is the 23 Categories that are split across the five Functions. Figure 3 as an image below depicts the Framework Core's Functions and Categories.

Fig. 3: Cybersecurity Framework's Functions and Categories

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Source: NIST USA 2018

Fig.4: Cybersecurity Framework's Categories, Sub-categories Informative References



Source : NIST USA-2018

The five Subcategories pictured from the Business Environment Category (ID.BE) provide an example of the outcome focused statements that are found throughout the core. The column to the right, Informative References support the Core by providing broad references that are more technical than the Framework itself. Organizations may wish to use some, none, or all of these references to inform the activities to undertake to achieve the outcome described in the Subcategory. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the Framework. The Tiers range from Partial (Tier 1), Risk informed (Tier2), Repeatable (Tier3) and Adaptive (Tier 4) and describe an increasing degree of rigor, and how well integrated cybersecurity risk decisions are into broader risk decisions, and the degree to which the organization shares and receives cybersecurity info from external parties.

Tiers do not necessarily represent maturity levels. Organizations should determine the desired Tier, ensuring that the selected level meets organizational goals, reduces cybersecurity risk to levels acceptable to the organization, and is feasible to implement, fiscally and otherwise. For more information regarding the Informative References, see the Informative References Learning Module. As the Cyber Security Framework is Developed for USA (NIST 2018).There is a need to orient it (cybersecurity framework) for Indian conditions as informative references/knowledge are available in various departments like Indian Meteorological Department (climate), Central Water Commission(floods), Meity (communication networks), Earthquakes (NDRF and PWDs and educational institutes), National/State Disaster Management Institute and Agency(ies), Information Technology , Smart City agencies, etc.

Immediate Attention to Practical Cybersecurity in Borders through Borderman or Bordermen

India should aim for technological industrial base by having collaboration with neighbouring countries and also stimulate training, attracting, and retaining cyber talents for cyber defence. India should seek cross-border cyber threat detection platforms, each bringing together relevant public entities from several states across India, as well as private entities. Cybersecurity skills academy (like BORDERMAN) should start educating people in citizens belonging to border areas about cybersecurity. They can start doing these by having each month a Cybersecurity day in the border citizen's common premises. Most important elements to teach are (a) backing up data, (b) privacy, (c) password management, (d) protect against social engineering.

- **Sharing tips A:** "Backups are important because they allow the restoring of files and data that are lost or stolen. Back up those files or data which you have in your computer that you would hate to lose. There are many devices that store files. A USB pen drive or an external hard disk are great, they are relatively cheap and they have plenty of space to store. Consider using an online storage service for storing files free of charge for a limited amount of space , say up to 15GB".
- **Sharing Tips B:** "It is important to value and protect our online privacy. If one constantly shares everything online, it is easier for cyber criminals to profile you and find patterns. As a rule of thumb, one should assume that anyone might read what is posted online. If every Monday and Friday you take a selfie while you run on the gym's treadmill, for some people this means that you are fit, whereas for malicious actors, it means you are not at home. A great moment to break into your home and steal everything! Determine firmly whether what you posted online last year is really valid now. Before you start using a social networking site, a game or an online platform, one should make sure to carefully check the privacy settings. Moreover, do not add people if you do not know them! They might be just curious people chilling online, but it might be someone who is looking to cause harm to you. When you have time, it is a good idea to take a look at the permissions granted to an app (such as access to your contacts, calendar etc.) and read their privacy policies. Then (a) Use private browsing and multiple web browsers, (b) Use multiple (and possibly private) search engines, (c) Surf on websites with "https", (d) Turn off Wi-Fi, Bluetooth and GPS, if they are not being used".
- **Sharing Tips C:** " Passwords are important to keep personal information safe or to access an online service. Test your password strength with the following tool created by the Luxembourg Safer Internet Centre: https://pwdtest.bee-secure.lu/?lang=en. Choose 3 words, say, chilly, heatwave, season. Have a combinations of these as "heat wave season chilly" Make few letters as capital "heatwa Veseas OnchilLy" or Heatwave Season Chilly" it will take a computer several thousand years to guess such password. To complicate this add a number at the end of three words .Still better is use special character of your choice as ! oe# or& etc. To remember

passwords: write them down and put them in a safe place ;Don't tell a personal password to anyone ; Use different passwords for different accounts ; If you change your password, change it entirely.avoid entering passwords when these public Wi-Fi connections are used and, more generally, on computers that are not your own."

- **Sharing Tips D:** "Social engineering techniques are frequently used by online criminals to trick victims into trusting them, and then obtain information they need to fully perpetrate their crimes. How (silly and ssophisticated) social engineering works.

  Watch the following videos.

  - https://www.youtube.com/watch?v=UzvPP6_LRHc
  - https://www.youtube.com/watch?v=lc7scxvKQOo

One for silly and other for sophisticated social engineering. Never send confidential information to anyone, be careful when you share personal data. Be critical and vigilant. Checkout the context and person/service interacting with you. Be extremely cautious of what you share online and aware of social network aggregator software and sometimes they are used to gather as much information as possible about a person, before sending a carefully planned social engineered attack".

Conclusions

The following conclusions may be drawn:

- The global security, cyber security and border security should go hand in hand
- The simplest cybersecurity measures like back ups, password formation, social engineering should have a wide awareness in all sections of the society, at least in order areas
- Baseline cyber security with countermeasure infrastructure should be encouraged with full measure of capacity building (preferably in local languages) with the help of Cyber Skill academies and a connection to NFSU-National Forensics Science University and Geospatial institutes nearby should be established for urgent necessities
- The critical infrastructure cybersecurity teams should be ready to fight the emergencies.

References

1. Robert Radvanovsky and Allan McDougall, (2013) Critical Infrastructure -third edition- Homeland Security and Emergency Preparedness, CRC press Taylor and Francis Group © 2013
2. CRS2007.CRS Report for Congress. (2007) The Department of Homeland Security's Risk assessment methodology: Evolution, issues, and options for Congress, February2, Congressional Research Service Prepared for members and committees of Congress USA. Order Code RL33858.
3. IRA-(2024) The announcement brochure of INSPIRA organised International Conference on "Multi-disciplinary Research, Security, Cooperation, Artificial Intelligence & Environmental Sustainability" conducted during May24-25, 2024 in a Hybridmode.
4. Brian Tomaszewski, (2000) Geographic Information System (GIS) for Disaster Management, Second Edition, Routledge Publishers, Newyork and London.
5. Naikodi Chandrakantha-Venkappanavara Basavaraja (2023) Cyber Security (Skill Enhancement Course-Kannada &English Version), Davanagere Publishers
6. Gupta Sarika, Gupta Gaurav (2023) Information Security and Cyber Laws; AICTE approved text book-Khanna Publishers 2013-reprint 2023
7. NIST-USA-https://www.nist.gov/cyberframework/online-learning/informative-references.

❖◆❖