KEMENTERIAN SAINS, TEKNOLOGI & INOVASI, MALAYSIA

# [TECHNOLOGY ROADMAP FOR CYBERSPACE SECURITY]

*Prepared for*:

[Ministry of Science, Technology and Innovation]

[15 August 2011]

*Prepared for*:

[Ministry of Science, Technology and Innovation]

*Contributors*:

[MIMOS together with a consortium of 22 organizations representing the academics, government, industry and researchers have formulated the National R&D Roadmap for Self Reliance in Cyber Security Technologies]

KEMENTERIAN SAINS, TEKNOLOGI & INOVASI, MALAYSIA

# Technology Roadmap for Cyberspace Security

## 1. Introduction to Cyberspace Security

Initiatives to strengthen the cyber security research and development efforts would be more effective and efficient with the establishment of a National Cyber Security Technology Roadmap that prioritizes the current and future R&D agendas. It would help to align and integrate all cyber security related R&D programs and initiatives to avoid duplication of efforts and to encourage collaboration where appropriate.

The government especially has played a vital, irreplaceable role in providing support for ICT R&D. The current initiative by Ministry of Science, Technology and Innovation (MOSTI) on the study of the National Information Security Framework has identified R&D one of as the main tenets of National Information Security strategy.

Malaysia’s commitment in using ICT for socio-economic development increases its dependency on the national cyberspace. The cyberspace is highly vulnerable to cyber threats and attacks. The cyberspace encompasses not only the known uses of the Internet such as e-commerce, communication, and Web services but also the less visible systems and connections of the nation’s critical infrastructures such as power grids, air traffic control systems, financial systems, and military and intelligence systems1. The growing dependence of these critical infrastructures on ICT brings about the critical need to protect this infrastructure from destruction and incapacitation.

Securing cyberspace is a national e-sovereignty challenge which needs to be pursued in a comprehensive manner. It must be driven by an integrated R&D framework, focusing on technology that protects our National Information Infrastructure, towards achieving self-reliance. Securing cyberspace is an extraordinarily difficult strategic challenge that requires a coordinated and focused effort from all stakeholders.

A national technology roadmap helps outline research priority areas. The National IT Council (NITC) report on “Securing Malaysia Sovereignty in the Cyber World” has outlined three strategies to enhance our e-sovereignty. They are: self-preservation – the preservation of identity and the sovereignty of the nation state; projection – towards enhancing the use of ICT to promote Malaysian image and worldview towards enhancing Malaysia’s stature and sphere of influence; and protection – enhancing security of National Information Infrastructure (NII).

The critical areas in which new and additional R&D is needed to increase the protection of the national information infrastructure are:

Secure communication: To help protect the confidentiality and integrity of information during transmission and storage

High availability systems: To ensure the continuous and uninterrupted operations of critical ICT systems

Network surveillance, response and recovery: As part of the proactive management of the ICT systems network surveillance is required to trace or detect abnormal activity and to respond to the incident and recover from the incident to prevent system disruption

Trust relationships: Relationships between ICT systems and users to address non-repudiation issues

Secure access: Protects the ICT system from unauthorized entry

System integrity controls: To ensure that a system and its data are not illicitly modified or corrupted by malicious code

Traceback, identification and forensics: To enable an investigation of events and consequent preventive measures to be tightened or introduced

Priority areas are based on the Self-Reliance Framework that identifies the critical technologies that are essential for the operation of the country's Critical Information Infrastructure and the Defence in Depth approach that takes the concept of a security perimeter layer-by-layer to ensure a greater level of security. These are areas deemed critical in times of peace, crisis and war.

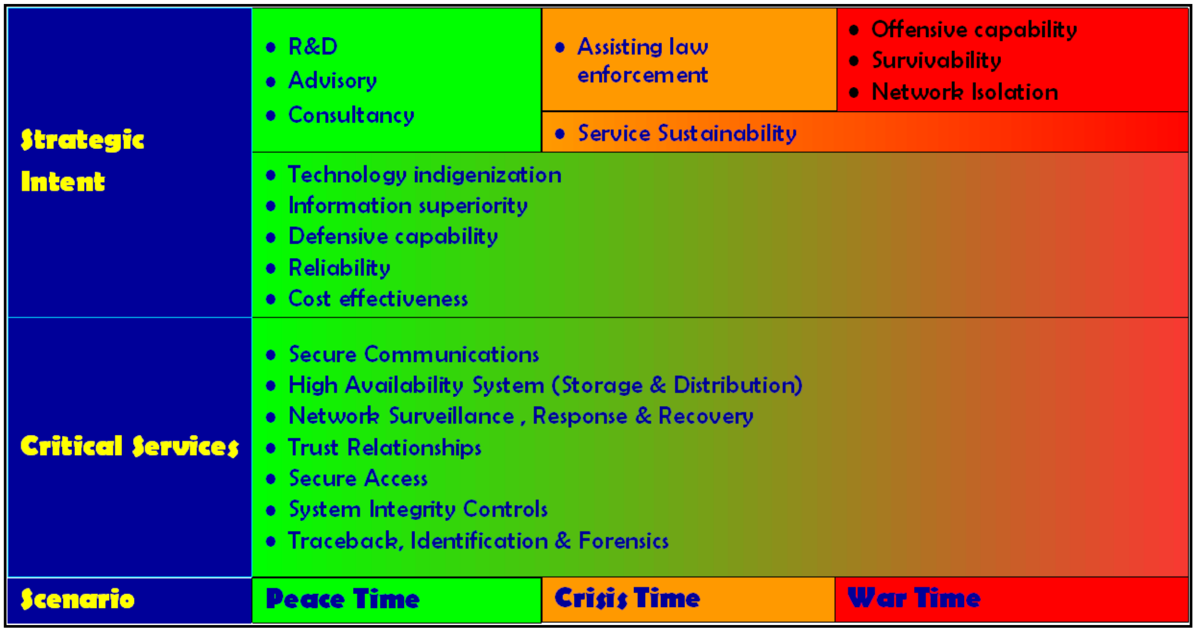
## 2. CyberspaceSecurity Framework

There is a need to adopt an integrated approach to address the concerns on cyber security. This includes the development and implementation of policy frameworks, inculcating a culture of cyber security awareness, prioritization of cyber security technologies, allocation of fund for cyber security programs and establishment of cyber security standards and certifications. There have been some initiatives and efforts undertaken by both public and private sectors in the areas mentioned.

Research and development in key cyber security technologies is important to address the concerns of cyber security issues. Priority areas need to be identified that is based on self-reliance strategy that identifies the critical technologies that are essential for the operation of the Critical Information Infrastructure to continue to function. These are areas deemed critical in time of peace, crisis and war.

Realizing the impact it has on the country, the development and identification of the R&D priority areas is a joint initiative involving all parties in the business of cyber security. This includes all related government agencies, critical organizations that operate the critical information infrastructure, the key industry players and security experts from research institutes and academia.

Establishment of a national R&D framework that outlines cyber security research priority areas is indispensable.  Priority areas will lead to efficient R&D efforts and clear direction towards a secure and self-reliant nation.



| | | | |
|---|---|---|---|
| **Strategic Intent** | • R&D<br>• Advisory<br>• Consultancy | • Assisting law enforcement | • Offensive capability<br>• Survivability<br>• Network Isolation |
| | | • Service Sustainability | |
| | • Technology indigenization<br>• Information superiority<br>• Defensive capability<br>• Reliability<br>• Cost effectiveness | | |
| **Critical Services** | • Secure Communications<br>• High Availability System (Storage & Distribution)<br>• Network Surveillance , Response & Recovery<br>• Trust Relationships<br>• Secure Access<br>• System Integrity Controls<br>• Traceback, Identification & Forensics | | |
| **Scenario** | **Peace Time** | **Crisis Time** | **War Time** |

Figure 1: The Framework

The framework as depicted in Figure 1 is developed to address three main questions that are deemed crucial to the nation's cyber security R&D needs and requirements.

1. What is the cyber security requirement for the protection of the critical information infrastructure?

i. **Cost effectiveness**
Cyber security has always been associated with requiring high investment and expensive budget. Looking at the alarming growth of cyber threats and attacks and the growing number of broadband users, there is a need to ensure the benefits are enjoyed by critical mass This is especially important as more and more cases of Distributed Denial of Service and worms or virus attacks are affecting home-users who have no protection and defense against these cyber attacks. The expansion of operations from manual to more automated processes, especially with the public sector moving into electronic-government environment, requires mass deployment of internet infrastructure reaching critical agencies and inter-linking organisations across the nation. In addition, the current promotion and demand for online-business and banking has increased the need for online safety to protect the financial sector and its users. All of these contribute to the need for more cost-effective cyber security solutions to address mass deployments and to provide benefits to critical mass.

ii. **Technology indigenization**
Intensifying cyber security efforts in R&D is crucial to help improve current and increase new capabilities in the cyber security area. By increasing capabilities in this field through effective technology transfer, knowledge building and support from the government, it helps promote technology development and advancement in this field. With expert skills and a large research community base, shall give the country the ability to produce home-grown critical technologies particularly for defensive and offensive cyber initiatives. This results in the country taking charge and control over critical cyber security technologies towards achieving a more self reliant state.

iii. **Information superiority**
Having the right information at the right time is how one stays ahead of cyber threats. This is true since defending against today and emerging security threats requires proactive measures. Having enough information helps improve warning, response and recovery capabilities. Technology in relation to intrusion and threat detection and prevention, network surveillance and management, honey nets, patch management and early warning systems require handling of large data. Effective handling and analysis of such data, produces valuable information to forecast new attacks, provide for early warning, and prevent escalation of threats. The cyber security R&D aims in these areas, shall enforce effective and improved handling of emergency response and recovery techniques providing for a better mitigation strategy in defense of the growing cyber threats.

iv. **Defensive capability**

"Attack" technologies are getting more sophisticated. The increasing complexity is reaching a level beyond human ability to manage and secure. The virus and worm threats which started in the 90s, has evolved over the years developing into contagion timeframe that soon is close to near-impossible for human intervention to respond. Attacks are getting from moderate to highly severe which means successful exploitation of vulnerability could result in complete compromise of target systems. The time between the disclosure of a vulnerability and the release of an exploit code remained extremely short at 6.4 days as reported in Symantec Internet Security Threat Report for the period of July 1, 2004 to Dec. 31, 2004. Cyber security defense is becoming critical in protecting critical information infrastructure of a country from such threats and attacks from occuring. A cyber security defense needs to formulate layered security to ensure for a greater level of security. A greater control of e-sovereignty will only be attained if the national information security initiatives are developed to safeguard the security of the nation's cyber space.

v. **Reliability.**

The country's critical network infrastructures are highly interconnected and interdependent. Many critical sectors are increasingly relying on this infrastructure to deliver their respective essential services. Disruptions of services in one sector may adversely impact others. It can reach well beyond the vicinity of the initial occurrence and can cause regional and, potentially national disturbances. For example, a disruption in the energy sectors can impede the telecommunications sector and vice versa. Problems can cascade through these interconnected infrastructures, causing unexpected and increasingly serious failures of essential services. As such the protection of the critical information infrastructure is very important to ensure reliability and smooth running of the country's operations. It becomes very critical to provide a reliable infrastructure that minimises disruptions of essential services during the period of cyber attacks.

2. What are the cyber security technologies that provide critical services to ensure protection of the critical information infrastructure?

The identified key cyber security technology areas are:

i. **Secure communication**

This is achieved by encrypting and/or hiding data during transmission and when it is stored on a system. Encryption is the process of transforming ordinary data into a code form so that the information is accessible only to those who are authorized to have access. Five areas have been identified as the priority areas with respect to secure communications: i)conventional steganology - allows the concealment and unconcealment of the information itself, whether encrypted or not, ii)quantum cryptology and quantum steganology – a new, secure communication technology, iii)conventional cryptology - which provides the fundamental security and privacy in the information society and comprises of two complementary fields: cryptography and cryptanalysis, iv)security protocols - range from the basic areas of key agreement and key management, to the complicated protocols such as multi-party computation and digital voting, and v)bio-computing - an interdisciplinary field that draws together molecular biology, chemistry, computer science and mathematics.

ii. **High availability systems**

To ensure continuous and uninterrupted operations of critical ICT systems. These are technologies that provide availability, reliability, and fault tolerance where they are built into design, architecture, and component infrastructure. A framework for High Availability has been identified. In the framework, there are 3 components which are considered as technology priority areas namely Platform, Systems (Application and Data); and Physical/Site. Within each component, 3 phases of similar approach has been proposed as the main principle that defines a set of goals in High Availability research that must be achieved. These are fault to detection, detection to reconfiguration and reconfiguration to full recovery. Each phase has its primary goal and for fault to detection is to mask all fault if possible. For detection to reconfiguration, its goal is to make this stage fast enough so as to minimize service disruption, to preserve reconfiguration accuracy and to maximize the utilization of surviving resources. Lastly the reconfiguration to full recovery, its goal is to provide graceful performance degradation.

iii. **Network surveillance, response and recovery**

As part of proactive management of the ICT system, network surveillance is required to trace or detect abnormal activity and to respond to the incident and recover from the incident to prevent further system disruption. Network surveillance is the process of monitoring networks for malicious activities. There are two different approaches on how to detect intrusion attempt. First and the most common way is by using signatures which uses predefined packet patterns and try to match them with every packets found in the network. The second approach is using anomaly detection techniques which uncover abnormal patterns of behavior. Anything that widely deviates from the normal patterns gets flagged as a possible intrusion. Once a network attack is identified, action to circumvent it will take place.

This is where the response part takes place. This includes active, passive or simulation mechanisms. The last part of proactive management is the recovery. Recovery element in this context basically lies at the protocol level. It involves initiatives to develop an architecture tailored to protocol stack that allows self healing after cyber attacks.

iv. **Trust relationships**

It is a combination of sub categories, which are technology (including algorithms, delivery channel and protection), process (including delivery, soft infrastructure) and social (including human factor, delegation of trust). There are three priority areas that fall into trust relationship, namely Public Key Infrastructure (PKI), Digital Signature and Time Stamping. PKI is a policy for establishing a secure method for exchanging information within an organization, an industry, or a nation. PKI is also an integrated set of services and administrative tools for creating, deploying, and managing public-key-based applications, which includes the cryptographic methods, the use of digital certificates and certificate authorities (CAs), and the system for managing the process. Meanwhile, digital Signature is a block of data attached to a message that serves to "digitally sign" the message; it is transmitted along with the message to a recipient. The purpose of the digital signature is to identify the sender, verify the message has not been altered in transit, and provide support for nonrepudiation. Time stamping is a prerequisite in a public key infrastructure (PKI) for providing proof-of-existence of a message/document at a given time, thereby ensuring non-repudiation. A digital signature is only legally binding if it was made when the user's certificate was still valid, and a time stamp on a signature can prove this.

v. **Secure access**

The Secure Access Security area focuses on providing protection at the level of boundary protection, authorization and authentication. In any event, intrusion is prevented using the physical or protocol characteristic. The issue here is to prohibit any unauthorized access to system, system resources or information of any organization. The focus on three layers of protection is due to the existence of different type of hackers. Each category has its level of tolerance and sophistication thus the existence of three pronged approach to Secure Access protects the ICT system from unauthorized entry.

vi. **System integrity controls**

At the host level, the matter of concern is system integrity. System integrity controls protect the system from improper alteration to any of their components. Attacks on system integrity will disrupt system services or cause the system to run unintended tasks. Threats towards system integrity include direct manipulation by intruders, malicious software presence, unintended/unwanted content, and flawed software. To protect the system from such threats controls are required for integrity assurance, malicious software protection, content filtering and software assurance. Integrity assurance is the study of detecting and correcting unauthorized system environment or file directories alteration. Malicious software protection aims to detect presence of virus, worms, Trojan horses, adware and other malwares, and prevent or correct damages caused by them. In addition, unwanted or unintended contents such as spam and phishing websites can be prevented from entering the system by content filters. Flaws in good software would allow attacks on a system to be successful. Such flaws can be detected and corrected with software assurance measure taken during software development cycle. Besides all that, in the case of a successful attack, system's ability to self-heal would be essential. It would reduce damage and dependency on human intervention for correction. All these control residing at the hosts would protect system integrity.

vii. **Traceback, identification and forensics**
To enable an investigation of events and consequent preventive measures to be tightened or introduced. Computer forensics tools are used to identify, preserve, extract, and document computer-based evidence. They can be used to recover files that have been deleted, encrypted, or damaged. Computer forensics tools are used during the investigation of a computer crime to determine the perpetrator and the methods that were used to conduct the attack. There are two main categories of computer forensics tools: (1) evidence preservation and collection tools, which prevent the accidental or deliberate modification of computer-related evidence, and (2) recovery and analysis tools.

3. When can these cyber security technologies be applied and who are the intended recipients?

The cyber security technology areas are based on Self-Reliance strategy. They are critical services that are essential for the operation of our Critical Information Infrastructure. They embrace the Defense in Depth approach that takes the concept of a security perimeter layer by layer to ensure a greater level of security. These are areas deemed critical in time of peace, crisis and war. The technology areas identified is based on realizing the value cyber security technology brings and the impact it has on our country where it is important to capitalise the potentials and benefits they can offer during all times. Cyber Security technology has limited usage may not produce high security impact to the country due to its limitation of use.

i. **Peace time**

The main stakeholders that shall make use of this technology are:

a. R&D community. It is essential for the community to expand and improve capabilities in the respective areas. Building capabilities provide strength and better control in possessing and maintaining growth in this area.

b. Advisory authority. Such technology should support the security management and operation activities of the advisory authority such as MyCERT and GCERT and other existing CERTs community in the country. Successful mitigation of cyber security risk lies within full awareness and staying ahead of the cyber threats.

c. Consultancy. This is another form of an advisory provision where a certain degree of service level agreement needs to be fulfilled. To spur the growth of the cyber security to become an industry sector, such technology should be the driving factor to the economic growth, employment and business opportunity.

ii. **Crisis time**

The main stakeholders of these technologies are:

a. Law Enforcement agencies. Cyber crime investigation requires support from the right set of cyber security technologies. It should cover preventive, detective and recovery capabilities to support investigatory exercise in time of national crisis.

b. Legislative and regulatory bodies. The laws and regulations are very important firstly to define, categorize and penalize the types of cyber crime and information security-related offences so as to deter future malice and negligence, and secondly, to provide a comprehensive framework that directs the country to a maximum level of compliance in order to meet the security of critical information infrastructure. To perform these functions, it is critical to make available the cyber security technologies as a tool in increasing public trust and confidence in the legal system.

iii. **War time**

The main stakeholders that require support from these technologies during this time are:

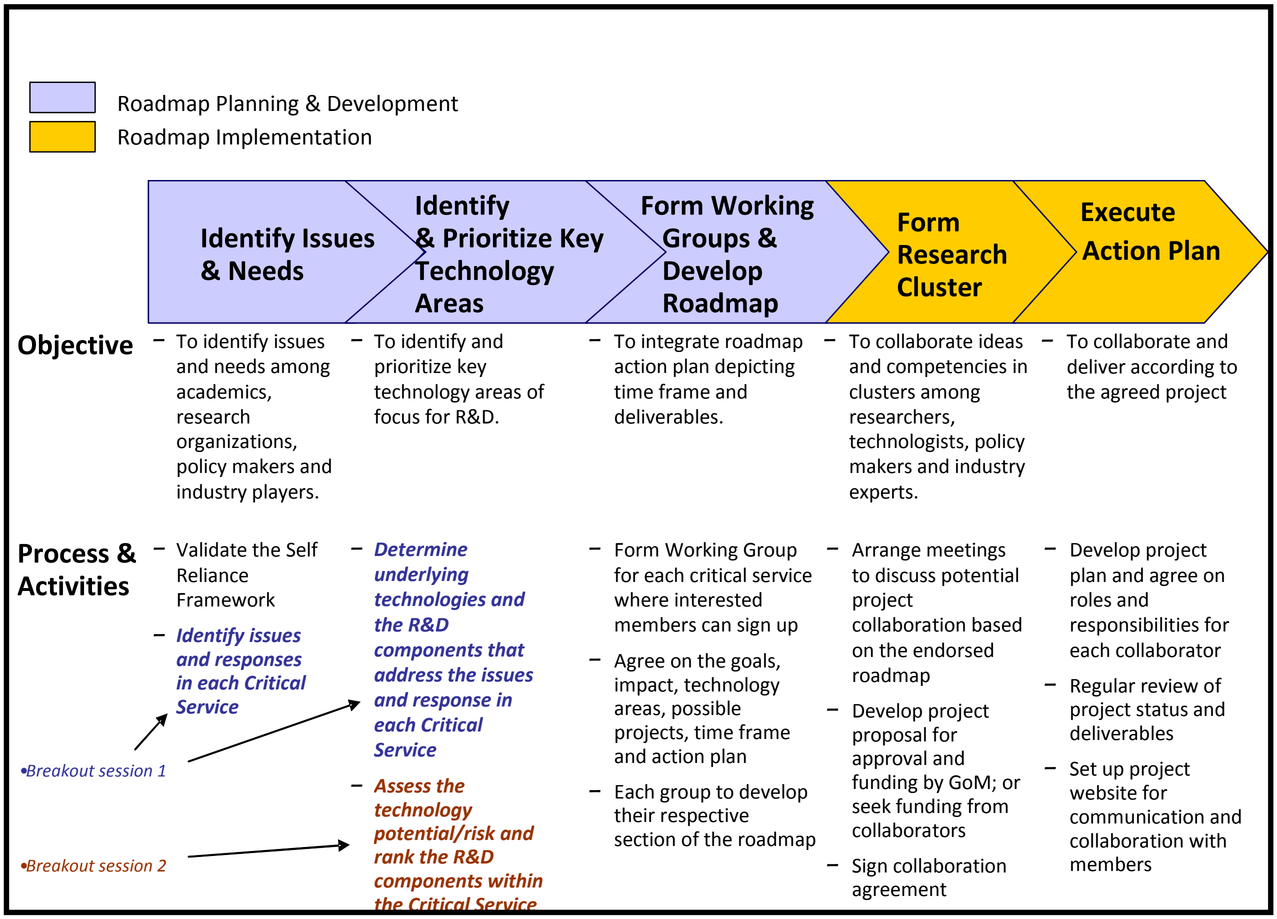
Military and Defense. The role they play in protecting the national security and sovereignty of the country brings about the critical need for such cyber security technologies to support the readiness and combat capability of the national defense and security system. Defensive and offensive capabilities are deemed crucial in providing protection of the country against internal and external threats. This includes maintaining public safety and survivability of the nation when under attack.

## 3. Methodology

This roadmap is developed through a technology roadmapping process. It is a market driven process that brings together key stakeholders (researchers, government, end-users and industry) to identify critical technologies for existing and emerging cyber security needs. It aims towards identifying existing challenges and strengths, prioritising and selecting key technology areas and formulating linkages within the cyber security multi-stakeholders. This section explains the methodology or process to develop this cyber security technology roadmap.

### 3.1 Roadmap Planning and Implementation Process

The roadmapping deliverables are the key technology areas and its prioritisation for the purpose of the protection of the critical infrastructures. This activity of an overall roadmap development process is shown in the following Figure 2.



🟪 Roadmap Planning & Development
🟨 Roadmap Implementation

| | Identify Issues & Needs | Identify & Prioritize Key Technology Areas | Form Working Groups & Develop Roadmap | Form Research Cluster | Execute Action Plan |
|---|---|---|---|---|---|
| **Objective** | – To identify issues and needs among academics, research organizations, policy makers and industry players. | – To identify and prioritize key technology areas of focus for R&D. | – To integrate roadmap action plan depicting time frame and deliverables. | – To collaborate ideas and competencies in clusters among researchers, technologists, policy makers and industry experts. | – To collaborate and deliver according to the agreed project |
| **Process & Activities** | – Validate the Self Reliance Framework<br>– ***Identify issues and responses in each Critical Service*** | – ***Determine underlying technologies and the R&D components that address the issues and response in each Critical Service***<br>– ***Assess the technology potential/risk and rank the R&D components within the Critical Service*** | – Form Working Group for each critical service where interested members can sign up<br>– Agree on the goals, impact, technology areas, possible projects, time frame and action plan<br>– Each group to develop their respective section of the roadmap | – Arrange meetings to discuss potential project collaboration based on the endorsed roadmap<br>– Develop project proposal for approval and funding by GoM; or seek funding from collaborators<br>– Sign collaboration agreement | – Develop project plan and agree on roles and responsibilities for each collaborator<br>– Regular review of project status and deliverables<br>– Set up project website for communication and collaboration with members |

*•Breakout session 1*

*•Breakout session 2*

Figure 2: The Overall Roadmap Development Process

The process is divided into 5 stages:

### i. Issues and Needs Identification

The first stage is the identification of the Issues and Needs related to the protection of the critical infrastructures. A Self-Reliance Framework was developed through brainstorming discussions. From this initiative the seven critical services areas were identified i.e.

- Secure Communications
- High Availability Systems
- Network Surveillance, Response and Recovery
- Trust Relationships
- Secure Access
- System Integrity Controls
- Traceback, Identification and Forensics

The framework was discussed amongst the consortium members and clarifications were made and subsequently the framework was adopted.

### ii. Identify and Prioritize Key Technology Areas

The second stage of the process identified the key technology and R&D areas and rank them based on criticality and need. The key activity in this stage is to identify the technology and R&D areas apart from the itemization of issues and responses to each critical service.

Then assessment is made on the technology potential and R&D risk if a particular technology or R&D area is not developed locally. It is also required to develop a realistic timeline and cost range for the technology and R&D areas. Workgroups are formed to develop the roadmap in the following stage.

### iii. Form Working Groups and Develop Roadmap

The third stage uses the output from the second stage to develop the roadmap for the technology and R&D areas. The main objective is to integrate the action plan depicting the timeframe and deliverables. This is to be done through the formation of workgroups, one for each critical service, from the consortium members as well as including other interested parties who can contribute to the effort.

The workgroups will bring the development of the roadmap to the final level of detail to include clear goals, impact of the technology, identified projects and the timeframe for development and the action or execution plan i.e. how the technologies will be realized in a manner that will lead to a logical set of products or deliverables that will incrementally be used by the critical infrastructure providers as well as to build the self-reliance goals for such technologies. Preliminary project funding disbursement may also be identified to harmonize and coordinate the research spending.

Various modes of product realization will be explored. In some cases a proof of concept is required before further work can be carried out. In some other areas a pilot implementation is necessary. Technologies that can serve as a base and crosses several critical services e.g. the artificial intelligence engines will be identified and blended into the overall technology roadmap as intermediate deliveries.

The above are just some of the foreseen considerations in the development of the roadmap but the final shape and form and detail of the roadmap that will meet the needs of the critical services will be guided and moderated by MIMOS after the workshop.

### iv. Form Research Cluster

Research Clusters will be formed in the fourth stage of the process. This will involve organizations and institutions in both the private and public sectors who have the potential to contribute or whose potential to contribute can be developed with the appropriate support and funding from the government or other sources. Collaboration of ideas and competencies are expected to take place to optimize research cluster focus.

The clusters will be formed through a variety of mechanisms. Where possible collaboration with other established outfits in particular technology areas whether locally and especially overseas will help jumpstart some of the technology initiatives while meeting self-reliance objectives.

The detailed funding strategy and details on disbursement schedule will be developed.

Project proposals will be developed and approval sought for funding and moving to the next stage of product realization. Funding can come from the Government or from collaborators of technology and other interested parties that will fit into the national self-reliance agenda.

### v. Execute Action Plan

The plan developed from the previous stage will be executed in this final stage with the research clusters obtaining the appropriate funding and work towards product realisation.

A detailed project plan with clear indication of roles and responsibilities of the various parties will be finalised. Project control and progress monitoring mechanisms will be instituted. The project plan will work towards actual product realisation for the use of the critical infrastructures.

## 3.2 Programme Matrix

A programme matrix is developed to establish a standard in reporting the R&D programmes under each critical service identified in the technology framework. The following describes the measurement features of the programme matrix.

**R&D Programme**:
reflects the programme name and the features of the programme including underlying technologies that will be researched and developed.

**Potential/Risk**:
reflects the potential of the technology/output produced by the research programmes within the context of e-sovereignty or the risk of not implementing the research program. This will determine the urgency of the proposed research programme.

● Absence of research programme will comprise Malaysia's cyber security independence

◐ Absence of research programme will put Malaysia in a vulnerable state

○ Absence of research programme will have no major impact to Malaysia's e-sovereignty

**Technology Maturity**: reflects the stability of the underlying technology the programme will be implementing. The assessment is based on past and future research direction of the underlying technology globally. This is important to determine the technical risk of implementing the proposed programme.

● Technology has been sufficiently demonstrated

◐ Technology has been preliminary demonstrated

○ Technology has not been demonstrated

**Local Capability**: reflects the strength of local expertise in technology area.

● Strong – our presence is felt at the global arena

◖ Adequate – there are local R&D players recognised by the local R&D communities but not internationally

○ Weak – there may be some local R&D players but they have not been recognised by the local R&D communities

**Estimated Cost**: the estimated cost of implementing the proposed programme.

● More than RM 10 million

◖ Between RM 1 million to 10 million

○ Less than RM 1 million

**Programme Types**: reflects the nature of the R&D for the proposed programme.

**F** Fundamental – experimental or theoretical work without particular application or use in view

**A** Applied – research directed towards a specific practical aim or objective

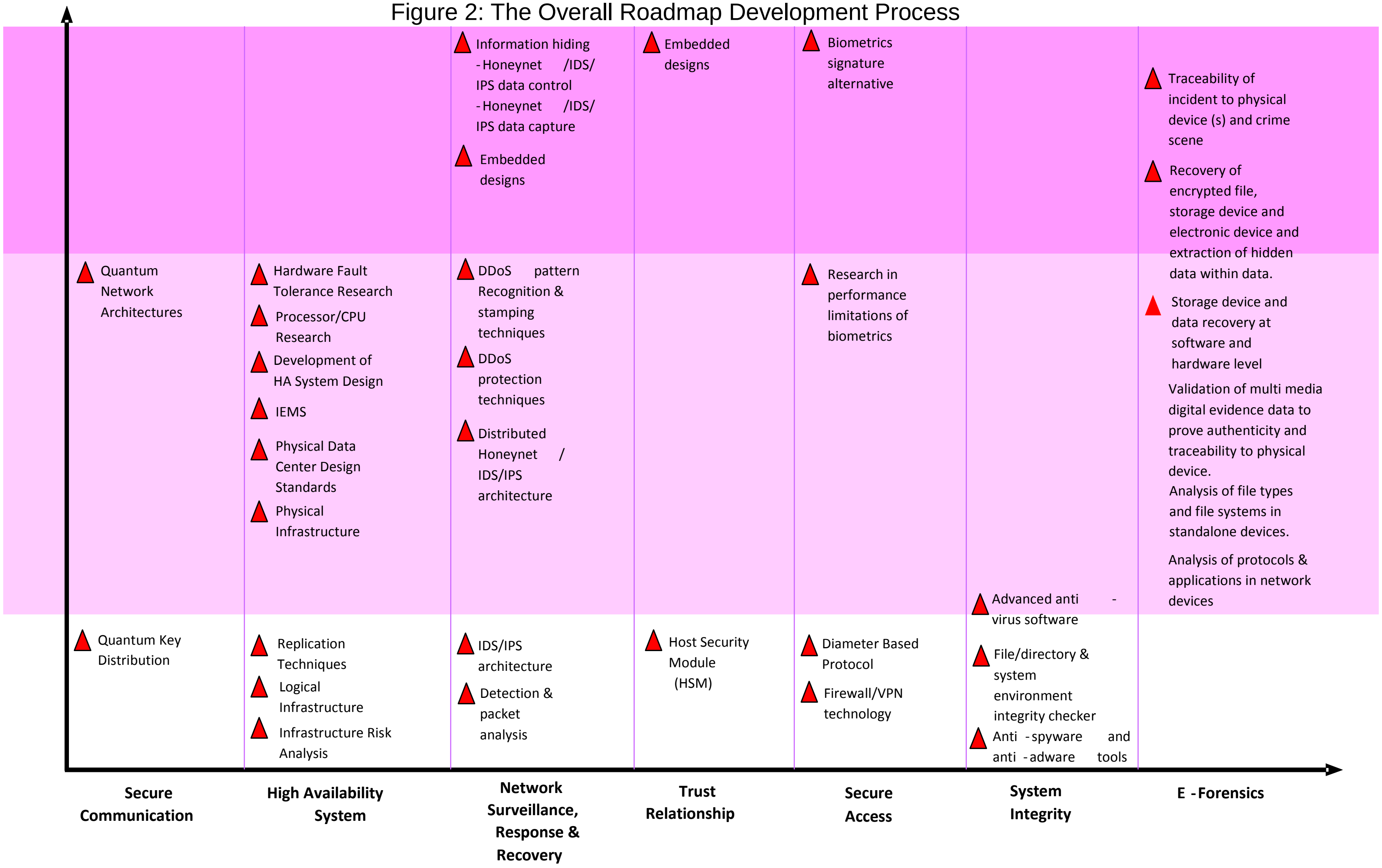
**P** Product Innovation – integrating results from applied research into existing or new products

### 3.3 The High Level Roadmap

The roadmap provides a long-term strategy for attaining a self-reliant state for the country. It maps out a logical prioritised sequence of cyber security R&D programmes to deliver what the short-term to future needs for the protection of critical infrastructure.

It provides a consolidated view as depicted in Figure 3 of all the R&D programmes that possess high value for potential/risk for each of the critical service. Absence of any of these programmes will compromise Malaysia's e-sovereignty. The roadmap serves as a foundation for formulating the national R&D initiatives in collaboration with Government, RI's and industry.

Figure 2: The Overall Roadmap Development Process



| Secure Communication | High Availability System | Network Surveillance, Response & Recovery | Trust Relationship | Secure Access | System Integrity | E-Forensics |
|---|---|---|---|---|---|---|
| | | ▲ Information hiding<br>- Honeynet /IDS/ IPS data control<br>- Honeynet /IDS/ IPS data capture<br>▲ Embedded designs | ▲ Embedded designs | ▲ Biometrics signature alternative | | ▲ Traceability of incident to physical device (s) and crime scene<br>▲ Recovery of encrypted file, storage device and electronic device and extraction of hidden data within data. |
| ▲ Quantum Network Architectures | ▲ Hardware Fault Tolerance Research<br>▲ Processor/CPU Research<br>▲ Development of HA System Design<br>▲ IEMS<br>▲ Physical Data Center Design Standards<br>▲ Physical Infrastructure | ▲ DDoS pattern Recognition & stamping techniques<br>▲ DDoS protection techniques<br>▲ Distributed Honeynet / IDS/IPS architecture | | ▲ Research in performance limitations of biometrics | ▲ Advanced anti - virus software | ▲ Storage device and data recovery at software and hardware level<br>Validation of multi media digital evidence data to prove authenticity and traceability to physical device.<br>Analysis of file types and file systems in standalone devices.<br>Analysis of protocols & applications in network devices |
| ▲ Quantum Key Distribution | ▲ Replication Techniques<br>▲ Logical Infrastructure<br>▲ Infrastructure Risk Analysis | ▲ IDS/IPS architecture<br>▲ Detection & packet analysis | ▲ Host Security Module (HSM) | ▲ Diameter Based Protocol<br>▲ Firewall/VPN technology | ▲ File/directory & system environment integrity checker<br>▲ Anti - spyware and anti - adware tools | |