An Analysis of Cyber Reference Architectures

Dr. Dennis H. McCallam
2691 Technology Drive
Annapolis Junction, Maryland
USA

dennis.mccallam@ngc.com

ABSTRACT

If you asked 5 people what cyber architecture looked like, chances are you would get 5 opinions. Architecture is defined by views, which are visual representations of different perspectives of the architecture [1]. For example, the Department of Defense Architecture Framework [2] has three primary visual representations: operational, system, and technical [1], [3]. Cyber architectures must be dependable and secure against both cyber related attacks and computer generated faults, which are defined as compromised components and computer generated faults that cause natural or accidental component failure [4]. Cyber architectures also need to maintain flexibility and resiliency when actions occur that stress the system design and/or occur due to unexpected situations [5].

The systems engineering process is well defined however the systems security engineering process is not incorporated into the systems engineering process [6], [7]. Cybersecurity architecture and solutions development needs additional rigor being integrated into the systems engineering process as opposed to having solutions that are added on after system development [8]. This also impacts the ability to develop repeatable solutions. The emphasis on rigor is important as it points out the lack of a cyber engineering approach, a view shared by others [8], [9] and [10]. This has relevancy to the study because this research will add to an already thin body of knowledge related to cybersecurity and to further establish cybersecurity as a science [11].

Systems security engineering is a relatively new field that is starting to mature [12]. According to McAllister (2002), systems security engineers "must be educated in and trained to employ a systems engineering process" (p. 3). [8] further corroborates that by pointing out that most security engineers approach security requirements from a checklist mind-set as opposed to having a systems engineering background that helps to more properly approach cybersecurity solutions. This implies a lack of structure and a lack of architecture, and additionally illustrates the gap in approaching security engineering as a systems engineering discipline [12].

1.0 ARCHITECTURE DEFINITIONS AND CYBER SECURITY

Architecture provides structure and definition to things. For example, in the construction of buildings, architecture is important not only from the standpoint of stability and safety, but also in terms of where things such as plumbing, electrical, and air conditioning are placed. The architecture is rendered in a series of blueprints and that provides a visual for the stakeholders in terms of where things exist in relation to each other. The same can be said of visual representations of technology. The visual architectural rendering provides a mechanism to look at how technologies interact, where the touch points exist, and can be used to explore options and reconfigurations. Most importantly, if this is done in conjunction with the requirements, then this visual can provide a means to not only represent the requirements but also a backdrop to examining the completeness of the requirements. Cyber requirements need to be understood, and visuals present an expedient way of addressing that need.

Some architectures and processes result in a disparity of views, such as DoDAF [2], The Open Group Architectural Framework ToGAF) and Zachman [13]. There were two reasons for this. Ref. [15] points out that none of these processes were designed for or provide for information security and all provided for views but the processes utilized resulted in views that are system specific [16]. While these approaches are helpful, they do not address the specifics of cyber security architecture. The goal of this research was to map a representative set of requirements to some specific cyber security views and then examine the results to see if they appeared to be useful in developing a solution.

2.0 REVIEW OF THE ARMOUR REQUIREMENTS AND PRE-ANALYSIS

The research elected to use a very good representative set of cyber defence requirements from the ARMOUR program. Ref. [17] provided the analysis of the Automated Computer Network Defence (ARMOUR) system that satisfied two concerns: first that the information about the system was freely available and second that the system satisfied the "real world" contextual requirement. ARMOUR became the exemplar chosen. As described both the ARMOUR RFI [23] and the analysis of Sawilla and Wiemer, ARMOUR provided a rich area for utilization as an architectural study artefact. The following overall view of ARMOUR is from the ARMOUR RFI – "Defensive actions (e.g. remove a network route, shut down a service, or apply a virtual patch) must be taken either proactively or, at the very least, at a speed capable of mitigating attacks. ARMOUR will demonstrate the capability to proactively deal with vulnerabilities and reactively mitigate ongoing attacks in real-time. ARMOUR will demonstrate the capability to automatically generate optimized courses of action (COA). Proactive COAs will minimize the risk of attacks on the networks while reactive COAs will allow operators to react more quickly to on-going attacks. The focus of the ARMOUR Technology Demonstration Program project is to deliver an integrated and automated demonstration system that will:

- Compute defensive COAs in response to identified cyber security vulnerabilities and attacks;
- Prioritize cyber security defensive COAs to minimize cost and impact to operations;
- Proactively and reactively respond in a semi-automatic (man-in-the-loop) or fully-automatic manner; and
- Compute system security metrics over the entire system to enable comparison of previous and potential cyber security network states."

Some subjectivity was used to begin the analysis of the ARMOUR requirements. In all, there were 331 total requirements from the ARMOUR system. A process to identify groupings of requirements elected to use two classes of requirements and then within each class there were 3 identical subclasses. The overall classes were defined to be those requirements that appeared to be cyber security related and those that did not. The criterion for selection was that the requirement either did or did not call out an explicit security relationship. If the requirement more addressed general systems or design approaches about architecture, then it more became a non-architecture requirement. This defined the two overarching bins for requirements….essentially either one that impacts the security architecture or one that impacts the overall system design and architecture.

Under that those higher classes, there were 3 subclasses. There was the architecture sub-class that defined how the system would be constructed. The second sub-class was for computational requirements. These were recognizable by defining components of a computation. For example, a requirement like "the metric shall be computed from" or "shall be based on" was considered to be a computational requirement. The third sub-class was for performance requirements. These were defined as requirements that are some ways were measureable, such as "the graphs shall be displayed with two axes".

It was also recognized that the sub-classes and how requirements could be allocated would be highly subjective. Some examples are given to illustrate the initial allocations.

3.0 OVERVIEW OF THE ARCHITECTURAL VISUALS

Alignment of architectural views has to consider a few characteristics in order to be useful. Somehow there should be reference and alignment with universally accepted standards. There was alignment in this particular case with NIST 800-53 and by extension the ISO 27000 series. A second characteristic is that any process in performing analysis using these should be consistent across different systems. The implication is that the process remains constant and the view in abstraction remains constant. Most importantly, the views have to convey the cyber architecture to someone (usually a senior stakeholder) who is a non-architect.

Four architectural views were used for the analysis representing different facets of architecture: the SANS Critical Security Controls (CSC), the Fan™, CyCape™ (cyber capabilities view), and the NATO Cyber Defence Capability Framework. These views are relatively independent of the systems they describe and provide a means to compare solutions from different systems [18].

The NATO Cyber Defence Capability Framework [19] shown in Figure 1, was developed by NATO Consultation, Command and Control Agency (NC3A), NATO stakeholders (e.g. NOS and NSRAG) and nations through NATO Research and Technology Organisation (RTO) and with support from IST-096. The overall objective is to provide a hierarchical decomposition of capabilities with the goal of providing a maturity model that would have metrics for evaluation for each capability. This shows that a comprehensive cyber defence capability needs to address a wide range of aspects, ranging from prevention and reaction mechanisms to recovery and interoperability. Cyber defence capability development should benefit from such a framework as it eases the communications and makes it easy to divide effort in order to advance capabilities quickly. It can further serve as a taxonomy and to identify interoperability points.

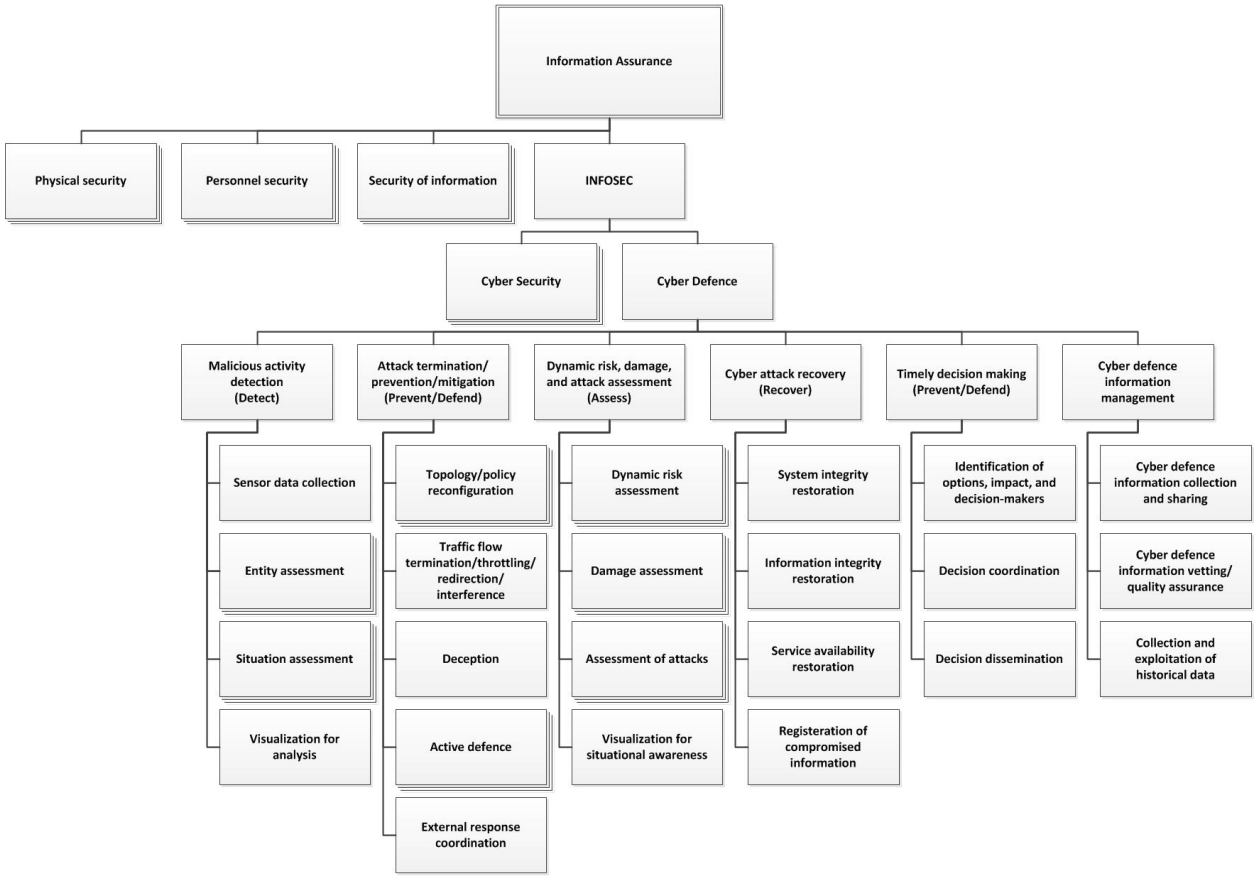

Figure 1: NATO Cyber Defence Framework.

The SANS Critical Security Controls (SANS CSC), shown in figure 2, represents a baseline solution for cybersecurity defence architecture [20]. The guidelines, subsequent security controls and architecture proffered by SANS CSC were designed to combat the most prevalent cyber threat and counter the threat's ability to conduct reconnaissance, exploit common vulnerabilities to gain and maintain access, and proactively defend against attacks. [21] gives a detailed description of the controls and how this set of controls was selected. The SANS controls are recognized as a cyber-defensive measure against the most common forms and tactics and were established to provide the right response to attacks that are or have been successful. As such, the SANS CSC represents an 80% solution to cyber defence. SANS represents basic cyber hygiene approaches. For example, on control number 1, the focus is to know and be able to identify all the devices that are within a security boundary. This is straightforward to accomplish since scanning is a basic tool of every security arsenal, and the scanning results can be used over time to identify all devices and endpoints of the system. Another one of the controls, 18, stresses the need to test and exercise on a periodic basis the incident response capability.

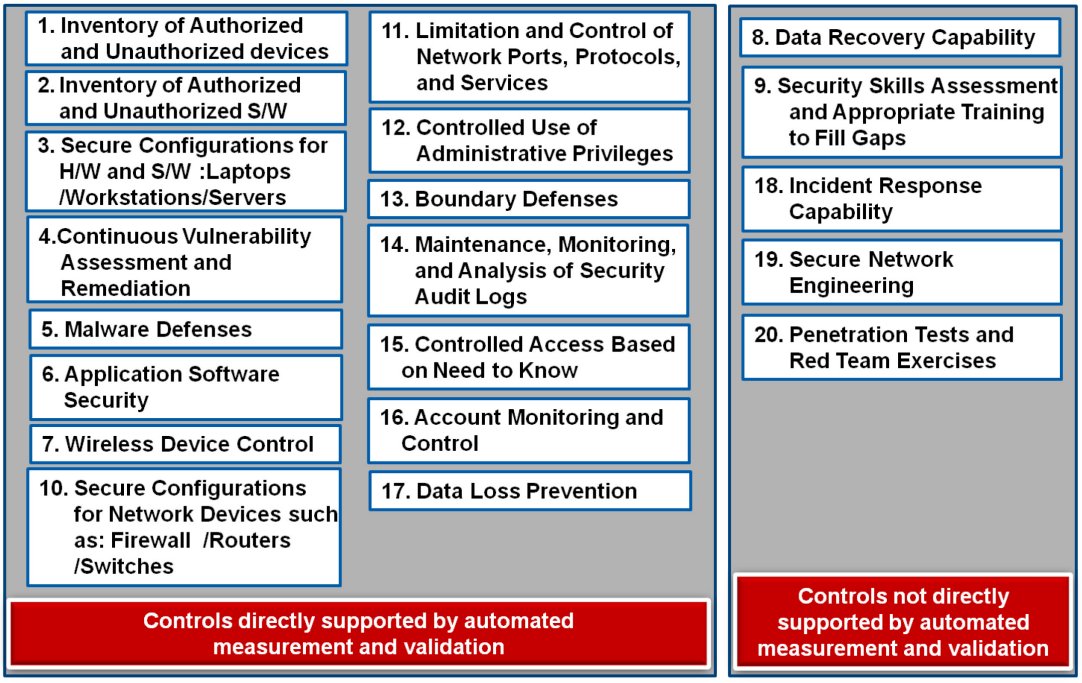

Figure 2: SANS Critical Security Controls.

The central component of this approach to defence is the concept of continuous monitoring. The US Information and Communications Enhancement (ICE) Act of 2009 [22] requires agencies to "monitor, detect, analyse, protect, report, and respond against known vulnerabilities, attacks and exploitations and continuously test and evaluate information security controls and to ensure that they are effectively implemented" [21]. The SANS controls were established as a means of meeting the US ICE Act of 2009 requirements for guidelines on information security policy and information security protections.

The SANS baseline of security measures and controls have been piloted through the State Department and have been validated to correlate against the highest technical and operational threats. There are twenty controls in total, and the visual structure is illustrated in Figure 2. This visual structure allows flexibility in use, since the individual boxes indicating the controls can be coloured in or highlighted as needed for emphasis. For example, one typical use would be in a "stoplight chart" fashion where the colours red / yellow / green are used to indicate (for example) no compliance / some compliance / full compliance to a specific SANS guideline [18].

CyCape™, shown in figure 3, is a Northrop Grumman developed visual representation of cyber capabilities against a flexible analysis concept for: cyber requirements for a system to be built, cyber capabilities an existing system provides, cyber capability gaps against desired cyber capabilities, and the ability to identify cyber capabilities provided elsewhere. CyCape™ provides a lexicon and a process that is useable to perform requirements analysis, capability and gap analysis; a cyber-reference architecture framework that renders into a visual which provides instantaneous representation of the analysis; and as a process it is repeatable.

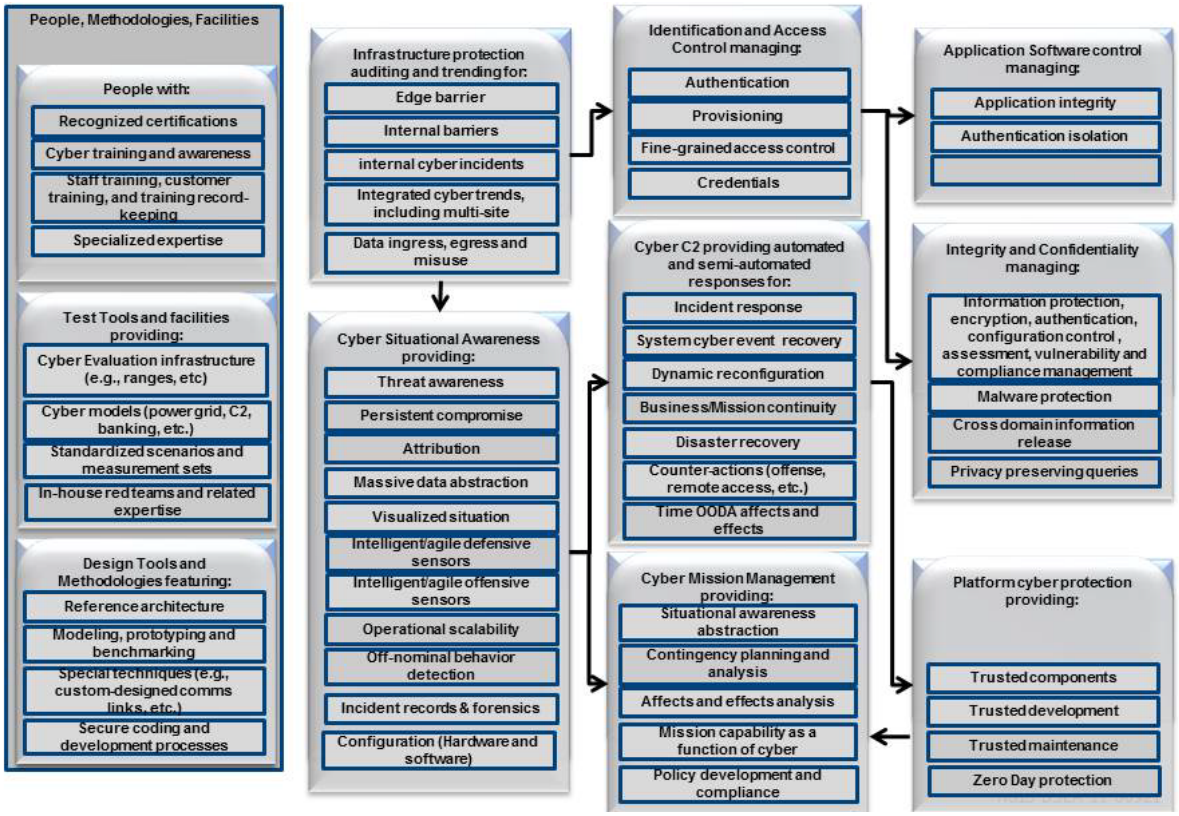

Figure 3: CyCape™ Cyber Capability Framework.

There are 2 basic components of the CyCape™ cyber reference architecture system: the framework that contains the division of capabilities and features being analysed and then the analysis criteria. The analysis criteria have been developed to assess both requirements (for systems/implementations not yet developed) and for fully developed systems (to understand the fidelity of the cyber capabilities and features).

It allows a quick and effective analysis and a subsequent results presentation for evaluating cyber capabilities utilizing a consistent cyber reference architecture view. CyCape™ also provides the capability to analyse both existing systems and requirements for new systems and provide a strength / weakness analysis. The easy to understand visual is straightforward enough for senior stakeholders.

The Fan™ is a Northrop Grumman invention that provides a picture of "what the defence is", illustrates technology placement, and provides a visual understanding of how security "flows" within the network. From an illustrative point of view, the Fan™ is divided into seven primary areas as shown in figure 4.

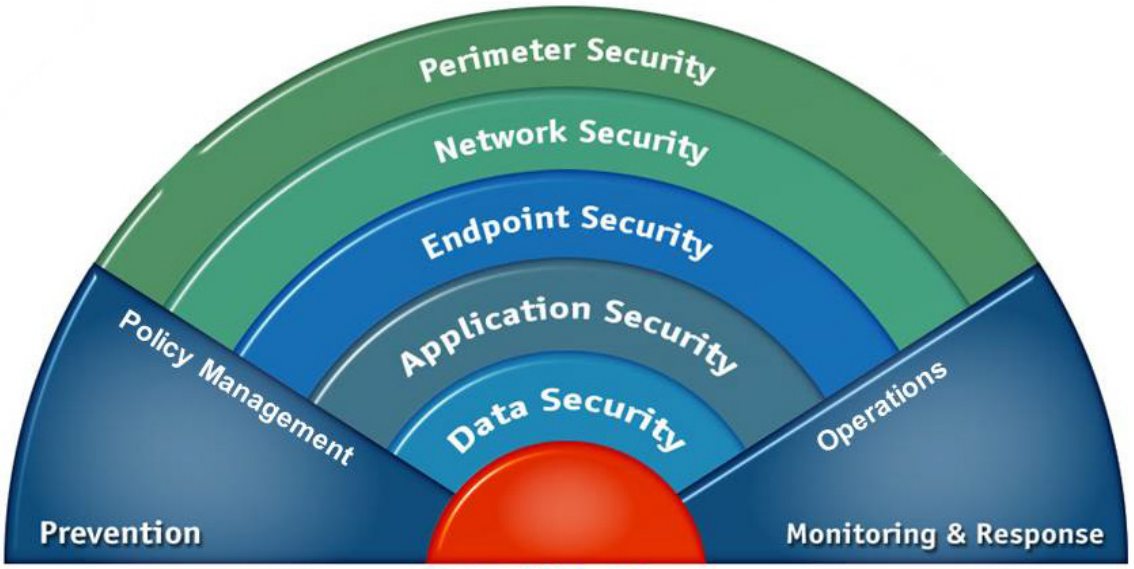

Figure 4: High Level View of the Fan™.

The five sections in the centre represent the 5 primary layers where cyber defence can be applied: the perimeter (the primary interface to the outside world), the network (the layer that partitions the enterprise network into enclaves), endpoints (devices that interface with the enterprise), applications (software packages that reside on devices in the enterprise or on endpoint devices), and data (the information contained in or used within the enterprise). In addition there are 2 other areas: Policy Management and Operations. The Policy Management includes governance processes that take preventive measures ensuring that security implementation and operations are in compliance to the federal regulations, laws, and enterprise security requirements. The Operations area contains tasks for cyber monitoring & response, providing continuous monitoring and management of enterprise cyber security operations in accordance to the security policies. It addresses the understanding of how cyber defensive technologies can be layered across the components of an enterprise and provides an architectural view that can be used to evaluate placement of technologies, vendors that supply those technologies, gaps in defence technologies, and data flow indications. The view or visual representation provides: an understanding what cyber technologies / processes can have maximal benefit, how these technologies/processes can support (or just as importantly inhibit) each other, and where it is best in the architecture to employ these technologies/processes and be able to provide a consistent visualization of the results [18].

The following provides the lexicon for the areas within the subsections of the Fan™ and sets the contexts for the areas chosen as shown in figure 5.

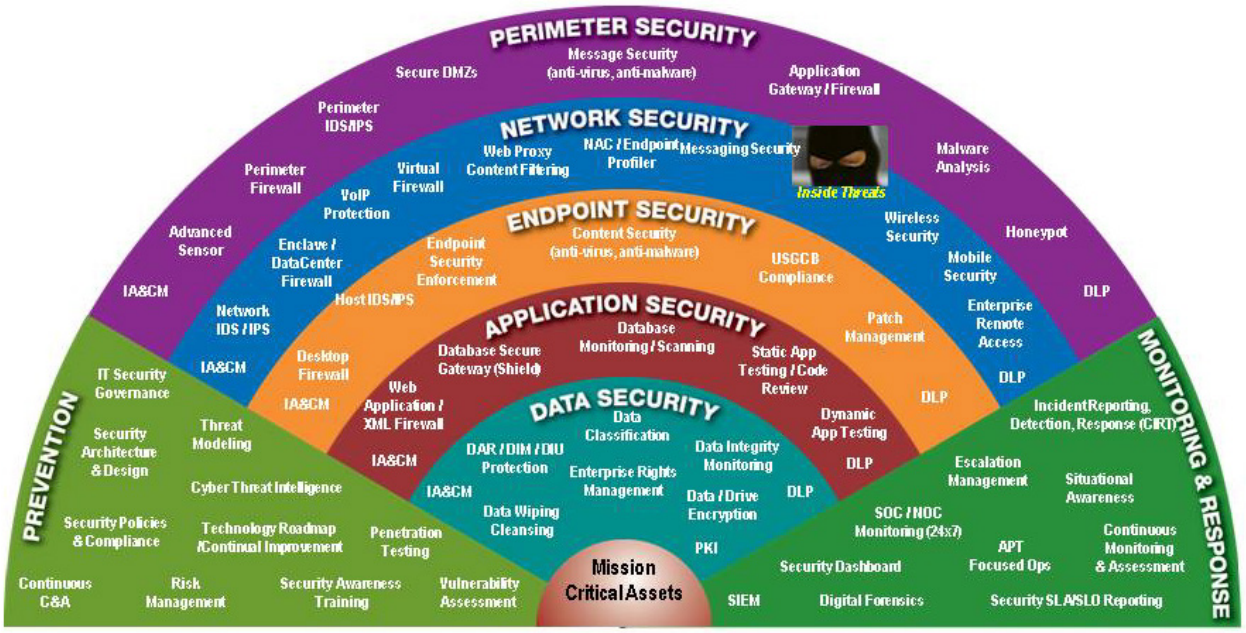

Figure 5: Detailed Level View of the Fan™.

1) PERIMETER SECURITY LAYER. The set of physical & technical security and programmatic policies that provide levels of protection against remote malicious activity; used to and protect the back-end systems from unauthorized access. When properly configured, the perimeter defence security model can prevent, delay, absorb and/or detect attacks, thus reducing the risk to critical back-end systems.

   a) PERIMETER FIREWALL: A device or set of devices on the very edge of the network, designed to permit or deny network transmissions based upon a set of rules. It is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass. The perimeter firewall is usually the very first device encountered when entering an enterprise from Internet.

   b) IDS: Intrusion Detection System. A passive system (does not sit in-line with network traffic, also known as "out-of-band") that monitors the perimeter for malicious activities, analysing traffic by comparing traffic to information in its database that contains patterns, called "signatures," found in known exploits. It usually does not stop the "bad" traffic, just identifies and reports it.

   c) IPS: Intrusion Prevention System. An active (in-band) system that analyses traffic by comparing traffic to signatures (and sometimes behaviour) and then stops traffic identified as malicious from entering the network.

   d) SECURE DMZ: An network enclave (distinctly bounded outside the Enterprise) that sits on the edge of the Enterprise (Demilitarized Zone) exposing external services, such as email, web servers, Honeypots, proxy servers and other public facing devices to a larger Internet. They are located at the perimeter to keep users/guests/malicious intruders that don't have a need to be inside the Enterprise, outside the Enterprise. Also protects the Enterprise from malicious content entering (see Message Security).

   e) APPLICATION SECURITY: Applications that run on publically facing servers inside the DMZ incorporate "application security", that is, the applications have been scanned for vulnerabilities (such as Injection Flaws and Cross-Site Scripting) and have been mitigated. The applications may also

incorporate active file integrity monitoring software to alert if a file/system has experienced an unauthorized change; the file monitoring system may also revert the system back to its last known "good" state.

f) MESSAGE SECURITY: Servers that sit in the DMZ to identify messages with potentially malicious content (either in the message itself, embedded URLs, and/or an attachment) and blocked accordingly.

g) HONEYPOT: A server or group of servers that reside in a DMZ that imitate servers inside the Enterprise to trick malicious intruders. They are used to observe and obtain surreptitious intruders' Tactics, Techniques and Procedures (TTPs).

h) MALWARE ANALYSIS: Servers residing in the DMZ that perform analysis of malware (infected software designed to launch a virus, worm, rootkit or other malicious code); usually coupled with a Message Security Server and in addition to conventional anti-virus products, providing advanced zero-day malware detection capability.

i) ADVANCED SENSOR: Sensors that are specifically designed to address the Advanced Persistent Threat (APT) and many times purposefully built to handle a specific attack signature based on TTP reconnaissance.

j) DLP: Data Loss Prevention or Data Leak Prevention. Refers to systems that identify, monitor, and protect data in use (e.g. endpoint), data in motion (e.g. network), and data at rest (e.g. data) through deep content inspection, contextual security analysis of transaction, and with centralized management framework for known security vulnerabilities. It is specifically designed to observe and stop data from leaving the Enterprise. The perimeter DLP is the last bastion of defence to prevent data from disappearing.

2) NETWORK SECURITY LAYER: The layer that partitions the Enterprise Network into enclaves; an enclave is a distinctly bounded area enclosed within a larger unit. Enclaves incorporate their own individual access controls and protection mechanisms.

a) ENCLAVE FIREWALL: A device that protects the enclave and is designed to permit or deny network transmissions into the enclave based upon a set of rules; it is used to protect the enclave from unauthorized access while permitting legitimate communications to pass.

b) ENTERPRISE IDS/IPS: These are the same devices as described in the Perimeter Security Layer section, however here they are deployed throughout the enterprise and usually in combination with an Enclave Firewall.

c) VoIP PROTECTION: Voice over Internet Protocol (also known as IP Phones) security protection; can include policies, procedures and VoIP switch security (embedded software) to help protect VoIP telephone systems.

d) VIRTUAL NETWORK SECURITY: Policies, procedures, hardware and software that protects a virtual network. A virtual network is a computer network that consists of virtual network links. These links don't consist of physical (wired or wireless) connections between two computing devices; rather they implement methods that incorporate network virtualization. The most common forms are protocol-based virtual networks (VLANs, VPNs and VPLSs) and virtual networks that are based on virtual devices (such as the network connecting virtual machines).

e) WEB PROXY CONTENT FILTERING: A device (usually a dedicated server) that acts as an intermediary for requests from clients seeking resources from external sources, such as the Internet; it is

used to keep users/machines behind it anonymous. Applies access policies to network services or content to block undesired sites and scans outbound content for DLP.

f) NAC: Network Access Control – hardware or software that provides an automated system to discover and enforce access controls for all endpoints regardless of how they are managed or connected to the enterprise network (wired, wireless or VPN access). The NAC system can integrate with the enterprise identity management service to authenticate users, assess endpoint security posture, and make network admission decision based on the findings. Non-compliance endpoint may be denied network access, remediated, and re-assessed for network admission.

g) ENTERPRISE MESSAGE SECURITY: Same as Perimeter Message Security however these devices sit inside the Enterprise. They can be designed to scan inbound/outbound messages to ensure content security.

h) WIRELESS/MOBILE PROTECTION: Policy, procedures, hardware and software design to defend wireless networks from surreptitious actives and intrusion. For example, connectivity to the Enterprise wireless network may only be accomplished using a VPN (encrypted tunnel) connection.

i) ENTERPRISE REMOTE ACCESS: Policy, procedures, hardware and software design to enforce remote access connectivity. This may include desktop/notebook firewalls, anti-virus and other items on remotely connected devices to ensure devices are protected before they connect with the Enterprise. For example, a NAC will confirm if the connected device meets all the policy elements required to connect remotely with the Enterprise.

j) DLP: Data Loss Prevention or Data Leak Prevention. Refers to systems that identify, monitor, and protect Data in Use (e.g. endpoint), Data in Motion (e.g. network), and Data at Rest (e.g. data) through deep content inspection, contextual security analysis of transaction, and with centralized management framework for known security vulnerabilities. It is specifically designed to observe and stop data from leaving the Enterprise. At the Network Layer, multiple DLP solutions may be deployed throughout various enclaves.

3) ENDPOINT SECURITY LAYER: Security protection mechanisms and controls that reside directly on an endpoint device interfacing with the Enterprise.

a) DESKTOP FIREWALL: Firewall software that resides in the desktop/laptop that performs firewall functions at the individual device level.

b) HOST IDS/IPS: Performs IDS/IPS functions within the host. For example, an attached WORD document may have a behaviour that is foreign to how WORD should work; hence the IDS/IPS will stop it from running and report accordingly.

c) CONTENT SECURITY: Keeping the endpoint device up-to-date with the latest anti-virus and anti-malware patches along with any other security software dictated by policy to be present on the endpoint device.

d) ENDPOINT SECURITY ENFORCEMENT: Works in conjunction with Enterprise Remote Access; if the endpoint device is not current with patches, the Enterprise Remote Access system may not allow the endpoint device to connect with the Enterprise. This requires that Content Security must be up to date and correspond with the Enterprise Security Policy.

e) USGCB COMPLIANCE: United States Government Configuration Baseline. If the policy mandates that the system must comply with the USGCB, then the system will not be allowed to connect with the Enterprise until it is in compliance. Additionally, the system must be updated as the baseline is updated.

f) PATCH MANAGEMENT: Confirming that all endpoint devices are current with their respective patches and there is a record of all patches including patch level: When patched and by whom. Patch Management is an essential element of Configuration Management.

g) DLP: Data Loss Prevention or Data Leak Prevention. DLP host software that can identify, monitor, and protect data in use at the endpoint device while stopping data leakage if an unauthorized event should occur. It can stop unauthorized activities, e.g. copying sensitive data files to an external USB storage device.

4) APPLICATION SECURITY LAYER: Security protection mechanisms and controls that are embedded within the applications residing on the Enterprise network, enclaves, and Endpoint devices.

a) STATIC APPLICATION TESTING/CODE REVIEWS: A form of software testing where the software isn't actually used. It checks mainly for the software security weakness that would later result in vulnerabilities in production. CODE REVIEW is the systematic examination (often as peer review) of computer source code. It is intended to find and fix mistakes overlooked in the initial development phase. Reviews are done in various forms such as pair programming, informal walkthroughs, and formal inspections.

b) DYNAMIC APPLICATION TESTING: Refers to the examination of the response from the system to variables that are not constant and change with time. In dynamic testing the software must actually be compiled and run; Actually Dynamic Testing involves working with the software, giving input values and checking if the output is as expected. Web Application Vulnerability Scanning is commonly used for testing web based applications, yielding exact vulnerability locations in the code and instructions on how to mitigate the vulnerabilities.

c) WAF: Web Application Firewall. Unlike the traditional firewall used in the Perimeter and Network layers, the WAF performs deep packet inspection seeking hidden scripts that can exploit application vulnerabilities such as injection and cross site scripting flaws. The WAF rejects any packets incorporating embedded exploit scripts.

d) DATABASE MONITORING/SCANNING: DB Monitoring is for detection of database vulnerability, incorrect or non-compliant settings, and monitoring data integrity.

e) DATABASE SECURE GATEWAY (Shield): Also known as a database Firewall (DBF). Some perform deep packet inspection protecting against injection exploits. They may include real-time monitoring, alerting and blocking, pre-built security policies and audit rules.

5) DATA SECURITY LAYER: The layer of security that protects data in the Enterprise regardless of the data's state, that is, whether it is in motion, at rest or in use.

a) PKI: Leverages all three forms of encryption (symmetric, asymmetric and hash-based) to provide and manage digital certificates, a public key signed with a digital signature. Digital certificates can be server-based (as in SSL Web Sites) or client-based (bound to a person). If the two are used together, they provide mutual authentication and encryption. The standard digital certificate format is X.509.

b) DAR/DIM/DIU PROTECTION: Data at Rest / Data in Motion / Data in Use must always be protected to ensure Confidentiality, Integrity and Availability (CIA). To accomplish this, the data's location must be known at all times regardless of its state (DAR/DIM/DIU), and when applicable, should be encrypted.

c) DATA CLASSIFICATION: Data is categorized by asking the following: What data types are available? Where is the data located? What access levels are implemented? What protection level is implemented

and does it adhere to a specific compliance regulation (or classification in the government world.) Data classification is closely related to the data controls involving the SUBJECT (an active entity on the information systems) and the OBJECT (a passive data file). Widely used Controls are Discretionary Access Control (DAC), Mandatory Access Control (MAC) or Role-Based Access Control (RBAC).

d) ENTERPRISE RIGHTS MANAGEMENT: Also known as Enterprise Digital Rights Management (eDRM) and/or Information Rights management (IRM); technology which protects sensitive information from unauthorized access, alteration or copying. Used extensively in the music and motion picture industry to protect the unauthorized copying of data (songs and movies).

e) FICAM: Federal Identity Credential and Access Management. A Federal Government document that presents a common framework and implementation guidance needed to plan and execute Identity, Credential & Access Management (ICAM) programs.

f) DATA INTEGRITY MONITORING: Also known as "file integrity monitoring". It is software that alerts if data has experienced an unauthorized change; it may also be set up to revert the data file back to its last known "good" state.

g) DATA/DRIVE ENCRYPTION: Encrypting plaintext data (using a cryptographic algorithm) to make it unreadable.

h) DATA WIPING/CLEANSING: The process of destroying the data and many times the media holding the data. Degaussing is a common data wiping method that destroys the integrity of magnetic media (such as tapes or disk drives) by exposing them to a strong magnetic field.

i) DLP: Data Loss Prevention or Data Leak Prevention. Refers to systems that identify, monitor, and protect Data in Use (e.g. endpoint), Data in Motion (e.g. network), and Data at Rest (e.g. data) through deep content inspection, contextual security analysis of transaction, and with centralized management framework for known security vulnerabilities. It is specifically designed to observe and stop data from leaving the Enterprise.

6) MISSION CRITICAL ASSETS: Systems that perform a function essential to maintaining reliable operation and/or data whose compromise would severely impact the mission and/or the organization's ability to function.

7) MONITORING & RESPONSE: Constant observation of the Enterprise with a keen eye, coupled the right tools and processes, to recognize incidents & events, and respond accordingly in a timely manner.

a) SIEM: Security Information & Event Management. Provides real-time analysis of security alerts generated by network hardware and applications; they may consist of software, appliances or managed services, and are also used to log security data and generate reports for compliance purposes.

b) SECURITY DASHBOARD: An executive information system with user-interface delivering security event information that is designed to be easily read (like a car's dashboard).

c) SOC/NOC MONITORING (24/7): Security Operations Center/Network Operations Center operating 24 hours a day, 7 days a week. The SOC/NOC monitors security and network events and its success depends on the quality and expertise of the individuals performing Detection, Protection, Response and Sustainment security best practices.

d) FOCUSED OPS: Surveillance and reconnaissance operations that are focused on a specific target; usually associated with malware analysis and forensics Honeypot/Honeynet to obtain an attacker's Tactics, Techniques and Procedures (TTPs).

e) DIGITAL FORENSICS: Recovering and investigating material found in digital devices usually relating to a digital crime or when DLP occurs. The digital forensic process covers the seizure, forensic imaging (acquisition) and analysis of digital media.

f) ESCALATION MANAGEMENT: The approved policies and procedures to manage an event's response and its associated escalation.

g) INCIDENT REPORTING, DETECTION, RESPONSE (CIRT): Computer Incident Response Team. A well trained team to coordinate and handle computer incidents. Detection includes: Correct Event Detection, Information Gathering & Historical Review, Event Triage, Escalation, and Optimization & Tuning (to improve detection accuracy). Response encompasses: Preliminary Incident Analysis, Incident Containment, Incident Analysis, Incident Eradication & Recovery, Post-Incident Process Improvement / Lessons Learned.

h) CONTINUOUS MONITORING AND ASSESSMENT: The activities that constantly collect security data, monitor security events and alerts, and assess system security state and status in real-time or near real-time. Enterprise management operator may use SCAP compliant tools to automate the processes, with risk scored and displayed on dashboard.

i) SITUATIONAL AWARENESS: The broad understanding of all the elements that comprise the network Enterprise and its security in relationship to time and/or other variables that can alter the current "picture" of the Enterprise environment. It is a "layered" relational view that includes the following separate diagrams: Geographic, Physical, Logical, Device and Persona. These diagrams are then rolled into a single comprehensive view.

j) SECURITY SLA/SLO REPORTING: Reports showing the metrics outlining how well the security monitoring and response is meeting the contractual Service Level Agreement (SLA) / Service Level Objectives (SLO).

8) PREVENTION: Policies, procedures, training, threat modeling, risk assessment, penetration testing and all other inclusive sustainment activities to posture a secure position for the Enterprise.

a) IT SECURITY GOVERNANCE: A governing authority that defines the IT Security policy by law, a security compliance directive or other regulation.

b) SECURITY ARCHITECTURE & DESIGN: The security element added to or layered upon a network Enterprise architecture.

c) THREAT MODELING: Developing threat scenarios to help understand and determine the levels of security controls to deploy. Models include: Attack Tree Models, Qualitative Information Assurance Models, Quantitative Information Assurance Models, Multiple Objective Decision Analysis Models, Multiple Objective Decision Analysis for Information Assurance Model, and the Mission Oriented Risk and Design Analysis Model.

d) CYBER THREAT INTELLIGENCE: Gathering and examining cyber threat data from sensors, organizations and other threat intelligence sources.

e) SECURITY POLICIES & COMPLIANCE: The establishment of security controls approved by senior management to ensure security enforcement. Many security policies are set by pre-established directives and/or regulations that mandate strict government compliance.

f) SECURITY TECHNOLOGY EVALUATION: Testing and evaluating security technologies for conformity and/or proving the security product performs as advertised.

g) CONTINUOUS C&A: Continuous Certification and Accreditation as directed by the Accreditation type. For example, DIACAP mandates that accredited systems must be re-accredited every three years.

h) RISK MANAGEMENT FRAMEWORK: A six step process developed by NIST (National Institute of Standards and Technology) that provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle (SDLC). See NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems."

i) PENETRATION TESTING: A method of evaluating the strength of a computer systems security posture by attacking the system and exploiting found security vulnerabilities.

j) VULNERABILITY ASSESSMENT: The process of identifying, quantifying and prioritizing vulnerabilities found in a system. It does not include attacking the system (as done in a penetration test); rather it only scans the system for vulnerabilities.

k) SECURITY AWARENESS TRAINING: The process of teaching employee's better "cyber consciousness", namely, how to protect data and the importance of security controls. Comprehensive Security Awareness Training includes why security is important, who wants the data, how the data can be stolen and what can be done to thwart data loss DLP at the individual employee level.

4.0 THE VISUALISATIONS OF ARMOUR REQUIREMENTS

A rating scale was developed to use that would colour code the results, facilitating and providing rapid assimilation of the results. Typical stoplight colours: blue, green, yellow and red were used to show differences. Definitions of each colour were used to be able to bin the requirement in terms of defence automation, how the requirement impacted real-time, completeness of toolsets, what the technology readiness level is in terms of current solution availability, how this might relate to a full capability, and in terms of relative fidelity with respect to current state of the practice. There was also a rating that just evaluated of a requirement existed or not. This is useful to identify those areas of cyber defence that were not addressed.

For the SANS viewpoint, the analysis showed no requirements addressing wireless and training. One of these, the wireless, was a good news story since wireless implementations for this type of system were not allowed. Six of the areas showed moderate weaknesses, while the remainder lined up well with SANS recommendations.

The Fan™ was used to show requirements existence and by extension, where the requirements recommended placement in specific layers of the defence. An examination of the results shows differences in what was measured with regards to the SANS analysis. Placing the SANS and Fan view side by side, an overall idea of the architecture and the interfacing is developed.

For this analysis, a similar existence only approach was used in mapping the requirements to CyCape™. Aligning with SANS, the lack of training is shown while in other areas the architectural requirements seem sound and complete. The final view used the NATO framework and that visual was rated in terms of requirement existence and fidelity.

5.0 CONCLUSIONS

Using the visuals, some observations can be made with respect to the overall set of requirements as stated in the ARMOUR documents. At the highest level, ARMOUR presents a fairly complete set of requirements

particularly in the areas where there were requirements. One of the more useful observations is that there were a host of requirements that specified features of the architecture and defined in some cases as *how* the system would be built and what it would structurally look like.

Another observation was that the presentation of the requirements, in functional areas, allowed enumeration and delineation of requirements. With the separation of requirements into the performance and computation areas, a better understanding of any common analysis or analytics can be made.

One basic observation was that the visuals gave instant presentation of requirements areas that were and were not covered and also, to some degree, a cursory view of the fidelity of requirements. And in the areas of wireless and training, it was quickly identified that there were no requirements for any wireless connectivity or operation and none for any form of training.

The final takeaways dealt with the fact that there were four distinct visuals of the same set of requirements and that those visuals taken en masse present a complete view of the suite of requirements. No one view by itself was sufficient, and as multiple views were generated the more complete the analysis and the quicker the understanding of the requirements.

6.0 REFERENCES

[1] Leist, S., & Zellner, G. (2006). Evaluation of current architecture frameworks. *Proceedings of Symposium on Applied Computing*, 1546–1553. Retrieved from http://dl.acm.org/ft_gateway.cfm?id=1141635&type=pdf.

[2] Department of Defense. (2011). *The Department of Defense Architecture Framework Version 2.02*. Retrieved from: http://dodcio.defense.gov/Portals/0/Documents/DODAF/DoDAF_v2-02_web.pdf.

[3] Cano, L., Pritchard, D., & Ellis, D. (2009). The role of systems engineering in security systems design. *43rd Annual 2009 International Carnahan Conference on Security Technology*. doi:10.1109/CCST.2009.5335555.

[4] Jones, R., & Horowitz, B. (2012). A Systems Aware Cyber Security architecture. *Systems Engineering*, *15*(2), 225–240. doi:10.1002/sys.

[5] Veríssimo, P., Bessani, A., Correia, M., Neves, N., & Sousa, P. (2009). Designing modular and redundant cyber architectures for process control: Lessons learned. *In Proceedings of the 42nd Annual Hawaii International Conference on System Sciences*. Retrieved from http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=4755530.

[6] Davis, J. (2004). Information systems security engineering: a critical component of the systems engineering lifecycle. *ACM SIGAda Ada Letters*, 13–17. Retrieved from http://dl.acm.org/citation.cfm?id=1032297.1032300.

[7] Cline, B. (2008). Factors related to the implementation information systems security engineering: a quality perspective. (Unpublished doctoral dissertation). University of Fairfax, Fairfax, Virginia.

[8] Bayuk, J. (2011). Systems Security Engineering. *IEEE Security and Privacy Magazine*, 9(2), 72–74. doi:10.1109/MSP.2011.41.

[9] Bayuk, J., & Horowitz, B. (2011). An architectural systems engineering methodology for addressing cyber security. *Systems Engineering*, *14*(3), 294–304. doi:10.1002/sys.20182.

[10] Fuhrman, T. (2012). The New Old Discipline of Cyber Security Engineering. *2012 International Conference on Security and Management (SAM '12)*. Retrieved from http://elrond.informatik.tu-freiberg.de/papers/WorldComp2012/SAM9773.pdf.

[11] McMorrow, D. (2010). Science of Cyber-Security. *MITRE Corporation Report JSR-10-102*, *7508*(November). Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA534220.

[12] Irvine, C., & Nguyen, T. (2010). Educating the Systems Security Engineer's Apprentice. *Security & Privacy, IEEE*, *8*(4), 58–61.

[13] McAllister, R. (2002). Information systems security engineering the need for education. Workshop for Application of Engineering Principles to System Security Design (WAEPSSD) Proceedings, 1–5.

[14] Sessions, R. (2007). A comparison of the top four enterprise architecture methodologies. Retrieved from http://msdn.microsoft.com/en-us/library/bb466232.aspx.

[15] Jalaliniya, S., & Fakhredin, F. (2011). *Enterprise Architecture & Security Architecture Development*. *Technology*. Lund University. Retrieved from http://www.enterprisearchitecture.ir/downloads/thesis/Thesis_Shahram%26Farzaneh.pdf.

[16] Osvalds, G. (2011, March). Model-Based Systems Engineering (MBSE) Process Using SysML for Architecture Design, Simulation and Visualization. In *NASA Goddard Space Flight Center Systems Engineering Seminar*.

[17] Sawilla, R., & Wiemer, D. (2011, November). Automated computer network defence technology demonstration project (ARMOUR TDP): Concept of operations, architecture, and integration framework. In *Technologies for Homeland Security (HST), 2011 IEEE International Conference on* (pp. 167-172). IEEE.

[18] McCallam, D. (2012, April). *An analysis of cyber reference architectures*. Presented at NATO 2012 Workshop with Industry on Cybersecurity Capabilities, The Hague, Netherlands.

[19] Hallingstad, G. & Dandurand, L. (2011). Cyber Defence Capability Framework, Revision 2, The Hague, Netherlands: NATO Consultation, Command and Control Agency.

[20] Hardy, G. (2012). Reducing Federal Systems Risk with the SANS 20 Critical Controls. *[White paper]*, Retrieved from http://www.sans.org/reading_room/analysts_program/20CriticalControls.pdf.

[21] SANS. (2011). *Twenty Critical Security Controls for Effective Cyber Defense : Consensus Audit Guidelines (CAG)*. Bethesda, Maryland. Retrieved from http://www.sans.org/critical-security-controls/guidelines.php.

[22] S. 921--111th Congress: United States Information and Communications Enhancement Act of 2009. (2009). In GovTrack.us (database of federal legislation). Retrieved November 24, 2012, from http://www.govtrack.us/congress/bills/111/s921.

[23] DRDC. (2010). *Statement of Work for the Automated Computer Network Defence (ARMOUR) Technology Demonstration.* Reference document (Version 0.1). Ottawa, ON, CA.