

ROYAL HOLLOWAY

MSc PROJECT

R. Osman Tekes
Student Number: 100682179

Supervisor: John Austen

A Common Architecture for Cyber Offences and Assaults - (Organized Advanced Multi-Vector Persistent Attack):

Cyber War Cyber Intelligence, Espionage, and Subversion Cyber Crime

SEPTEMBER 2011

Submitted as part of the requirements for the award of the MSc in Information Security at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature

Date

ACKNOWLEDGEMENTS

I would like to thank John Austen, my Project Supervisor, for his invaluable encouragement and guidance in helping me to achieve better results in the MSc in general and in completing this project.

Table of Contents

ABSTRACT	6
1. INTRODUCTION.....	8
1.1. OBJECTIVES	9
1.2. THE MOTIVATION	10
1.3. METHODOLOGY OVERVIEW	10
1.4. OVERVIEW OF THE CHAPTERS	13
2. THE BACKGROUND AND CONTINUUMS.....	14
2.1. THE HUMANISTIC VIEW	15
2.2. THE HISTORICAL AND ANTHROPOLOGICAL PERSPECTIVE:	16
2.3. THE TWO CONTINUUMS	16
2.3.1 CONTINUUM ONE: THE SCALE OF ESCALATION - INTENSITY OF COERCION	16
2.3.2 CONTINUUM TWO: THE SCALE OF LEGITIMACY.....	18
3. ANALYSIS: STRATEGIC SCOPE - CONTEXTUAL VIEW – ROW 1 OF ZACHMAN’S FRAMEWORK	19
3.1. USA.....	19
3.1.1 U.S. CYBER STRATEGY:.....	19
3.1.2 US CYBER COMMAND.....	23
3.1.3 NSA.....	25
3.1.4 AN EVALUATION OF ALIGNMENTS, MISALIGNMENTS, GAPS, AND CONFLICTS	26
3.2. CHINA	27
3.3. RUSSIA	28
3.4. STRATEGIC SCOPE: THE MAIN POINTS.....	31
4. ANALYSIS: ENTERPRISE MODEL CONCEPTUAL VIEW – ROW 2 OF ZACHMAN’S FRAMEWORK	33
4.1. CYBER WAR.....	34
4.1.1 FIRST CUT DATA MODEL	34
4.1.2 FIRST CUT PROCESS MODEL	35
4.2. CYBER INTELLIGENCE, ESPIONAGE AND SUBVERSION	38
4.2.1 THE OBJECTIVES OF INTELLIGENCE, ESPIONAGE AND SUBVERSION OPERATIONS	39
4.2.2 FIRST CUT DATA MODEL	39
4.2.3 FIRST CUT PROCESS MODEL	41
4.3. CYBER CRIME	42
4.3.1 THE OBJECTIVES OF CYBER CRIME ORGANIZATIONS.....	42
4.3.2 FIRST CUT DATA MODEL	43
4.3.3 FIRST CUT PROCESS MODEL	45
4.4. CONCEPTUAL ANALYSIS: THE MAIN POINTS -SUMMARY	46
5. SYNTHESIS: ENTERPRISE MODEL CONCEPTUAL VIEW – ROW 2 OF ZACHMAN’S FRAMEWORK	47
5.1. WHY: (OFFENCE TYPES) (OBJECTIVES) X (OFFENCE TYPES) (OBJECTIVES) MATRIX – SAMPLE.....	47
5.2. WHAT: (OFFENCE TYPES) (OBJECTIVES) X (ENTITY TYPES) MATRIX – SAMPLE	50
5.3. HOW: (OFFENCE TYPES) (OBJECTIVES) X (PROCESS MATRIX) – SAMPLE	52
6. CONCLUSION	54
6.1. THE PURPOSE OF THIS PROJECT.....	54
6.2. THE MAIN FINDINGS	54
6.3. THE MAIN RESULTS	55
6.3.1 RESULTS FROM THE SYNTHESIS MATRICES.....	55
6.3.2 THE MOTIVATIONS: THE WHY MATRIX - WHAT IS THE DEGREE OF SIMILARITY AMONG THE OBJECTIVES?	56
6.3.3 THE ORGANIZATIONAL CONCEPTS AND DATA: THE WHAT MATRIX - WHAT IS THE DEGREE OF ALIGNMENT AND SUPPORT PROVIDED BY THE ENTITY TYPES?	57
6.3.4 THE ORGANIZATIONAL PROCESS AND VALUE CHAIN: THE HOW MATRIX - WHAT IS THE DEGREE OF ALIGNMENT AND SUPPORT PROVIDED BY THE PROCESSES?.....	58

6.3.5	SUMMARY OF MAIN RESULTS FROM THE SYNTHESIS MATRICES	60
6.3.6	ADDITIONAL OBSERVATIONS AND CONCLUSIONS	60
6.3.6.1	Who.....	60
6.3.6.2	When.....	60
6.3.6.3	Where.....	61
6.3.6.4	Additional Observations for Cyber War and Active Defence	61
6.4.	THE PROJECT OBJECTIVES AND THE PROJECT RESULTS	62
6.5.	CONTRIBUTION TO KNOWLEDGE	64
6.6.	THE FUTURE OF THE CYBER WAR; CYBER INTELLIGENCE, ESPIONAGE AND SUBVERSION; AND CYBER CRIME.....	65
CONCLUDING REMARKS:.....		66
REFERENCES		67
APPENDICES		92
1.	AN OVERVIEW OF ENTERPRISE ARCHITECTURE APPROACH AND ZACHMAN'S FRAMEWORK	92
2.	SOME POLITICAL THOUGHTS ON INJUSTICE, USE OF VIOLENCE, AND SUBVERSION OF DEMOCRACY .	102
3.	THE CRIME OF AGGRESSION: UN CHARTER	104
5.	CONTINUUM ONE: THE SCALE OF ESCALATION - INTENSITY OF COERCION	106
6.	UNITED STATES STRATEGIC COMMAND (STRATCOM)	107
7.	USCYBERCOM HIGH LEVEL MISSION STATEMENT AND ORGANIZATIONAL STRUCTURE	108
8.	SOME EXAMPLES OF SKILLS SOUGHT IN CYBER WARRIORS.....	110
9.	THE THREE GAPS IN KNOWLEDGE OF CHINA AND "LEAP FROG" WEAPONS	112
10.	THE RUSSIAN INVASION OF GEORGIA	113
11.	RUSSIAN ATTEMPTS TO UPGRADE NUCLEAR CAPABILITIES	115
12.	ANALYSIS OF STRATEGIC WARNING: INDICATION INTELLIGENCE.....	116
13.	FIRST CUT DATA MODEL CYBER WAR – COMPLETE	117
14.	ENTITY TYPES OF FIRST CUT CONCEPTUAL DATA MODEL.....	123
15.	FIRST CUT PROCESS MODEL CYBER WAR – COMPLETE.....	124
17.	FORMER NSA & CIA DIRECTOR SUGGESTS EMPLOYING MERCENARIES FOR CYBERWARFARE	128
18.	GLADIO ORGANIZATIONAL STRUCTURE	130
19.	SOME EXAMPLES OF SIMPLE ATTACK TECHNIQUES	131
20.	CYBERWARFARE MARKET 2008-2018.....	131
21.	KEY COMPANIES IN CYBERWARFARE AND CYBERSECURITY [130]	133
21.	SPYMASTER SEES ISRAEL AS WORLD CYBERWAR LEADER [131].....	133
22.	TREADSTONE CYBER COUNTER INTELLIGENCE DOCTRINE [108]	135
23.	INDUSTRIAL ESPIONAGE NOTABLE CASES [144].....	136
1.	<i>"France and the United States</i>	<i>136</i>
2.	<i>Volkswagen.....</i>	<i>136</i>
3.	<i>Hilton and Starwood.....</i>	<i>136</i>
4.	<i>GhostNet</i>	<i>136</i>
5.	<i>Google and Operation Aurora</i>	<i>136</i>
6.	<i>CyberSitter and 'Green Dam'.....</i>	<i>137</i>
7.	<i>USA v. Lan Lee, et al.....</i>	<i>137</i>
8.	<i>Dongxiao Yue and 'Chordiant Software, Inc'.....</i>	<i>137</i>
9.	<i>Stuxnet Worm</i>	<i>137</i>
10.	<i>Operation Payback.....</i>	<i>137</i>
11.	<i>Chengdu J-20 stealth fighter jet.....</i>	<i>138</i>
24.	THE HUMANISTIC VIEW:.....	139
25.	THE CRIME OF AGGRESSION: THE ANALYSIS	140
26.	THE ANTHROPOLOGICAL PERSPECTIVE FROM FRIEDRICH ENGELS	141
27.	CYBER ATTACKS COULD BE CLASSIFIED AS ACTS OF WAR CAUSED CONCERN.....	142
28.	THE DOD'S STRATEGY IS FOUNDED ON FIVE PILLARS	142
29.	U.S. CYBER COMMAND, A NEW MILITARY UNIT	142
30.	CHINESE AND RUSSIAN RESPONSE.....	142
31.	MISTRUST ABOUT THE MOTIVES OF THE UNITED STATES	143
32.	PERCEIVED HYPOCRISY OF U.S.	143
33.	THE INTERNATIONAL POLICY ON THE INTERNET SHOULD BE A MATTER FOR THE WHOLE WORLD	143
34.	CULTURES OF THE ARMY, NAVY AND AIR FORCE ARE INCOMPATIBLE WITH THAT OF CYBER WARFARE	144
35.	PRC MAY BE A GLOBAL POWER ECONOMICALLY BUT ITS MILITARY LACKS FORCE PROJECTION.....	144

36. REVOLUTION IN MILITARY AFFAIRS.....	144
37. CHINESE MILITARY STRATEGISTS VIEW THE WORLD AS A PLACE BASICALLY HOSTILE TO BEIJING'S NATIONAL INTERESTS	145
38. US AND CHINA FACE VAST DIVIDE ON CYBER ISSUES	145
39. UNDERSTANDING OF OFFENSIVE OPERATIONS	145
40. THE HIGH-VALUE INTELLECTUAL PROPERTY THEFT	146
41. RUSSIA SEES GREATER EURO-ATLANTIC THREATS MOVING FARTHER EAST	146
42. CYBERWARFARE BY RUSSIAN STATE	146
43. OVERVIEW OF THE APPROACH: ANALYSIS.....	147
44. KNOWN CYBER CRIMINAL ORGANIZATIONS	149
Cybercrime organizational structures and modus operandi	149
<i>Top 10 posts in cybercriminal operations Cybercrime organizations often run like corporations, staffed by experts in specific jobs</i>	150
Cyber-crime organizations: a specialist classification	150
45. OVERVIEW OF THE APPROACH: SYNTHESIS	151
46. THE MOST INTERESTING QUESTIONS ABOUT FUTURE DEVELOPMENTS IN CYBERSPACE ARE:.....	152

Abstract

The purpose of this project:

The major motivation behind this project is to create a reference blueprint for the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime. The purpose of the blueprint is to contribute to the security of the citizens of smaller, free and independent states and to enhance cyber deterrence capabilities of such states such as Latvia, Lithuania, Georgia, Ukraine, and Moldavia. This project is only a very humble beginning. I hope to build on this foundation in future. The intermediate goals are to:

- Establish a foundation to build capabilities in Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime fighting.
- Explore the possibility of using software engineering models as an aid to represent knowledge.
- Provide training about the subject matter.

The main findings:

It is demonstrated with the sample models, that a very high level blueprint of the foundation for enterprise architecture is established. The data modelling, process modelling, and matrix analysis are effective tools to analyse and represent knowledge about the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime.

As one would observe from the sample data, process, and matrix models, there are significant similarities and overlaps among the three subject areas. These models, anecdotal evidence, and materials researched, indicate a critical need to integrate the capabilities of law enforcement, secret services, and military with clearly defined responsibilities. Common integrated enterprise architecture for the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime is invaluable in building cyber capabilities and training programs.

It is difficult to differentiate between crime and espionage or military attack. It is also difficult to differentiate between cyber espionage attacks or cyber-on physical destructive attacks. To complicate things further, a multi-vector persistent attack could start as cyber crime, turn into cyber espionage and lay the groundwork for a catastrophic cyber attack.

Over multiple phases of an attack, a simple cyber incident event could be transferred from being the responsibility of law enforcement, to the secret services or to the military for active defence. This near real time seamless transfer is critical in cyber space. These capabilities require a common integrated enterprise architecture.

The answer to the question of how to build an effective Cyber Warfare capability is answered at a very high level.

- Align the bulk of the offensive and defensive capabilities with the Cyber Intelligence, Espionage, and Sabotage organization.

- Deploy operational offensive and defensive capabilities with the dimensions of the armed forces.
- Assign the initial detections, impact assessment, and attribution to the law enforcement for civilian and non-military infrastructure.
- Establish an integrated common architecture and platform for cyber defence and cyber offence systems, tools, procedures and techniques.
- Ensure that ‘near-real-time incidents’ data could be seamlessly shared and jointly analysed, similar to “target-centric-intelligence”.

1. Introduction

It is useful to clarify what some terminology means and why, in this report.

Cyber War

This terminology is not used consistently and it is usually not clear what is meant by Cyber War or Cyber Warfare.

As defined in UN Charter [27, 28] or as in Article 8 of the International Criminal Court [29, 30], war or warfare requires two or more states to fight each other.

Since the nature of cyberspace allows use of proxies and non-state Actors, it is more convenient for aggressor states to hide behind plausible deniability, even though the attack is planned, orchestrated, and supported within the borders of the aggressor state.

According to this criterion, most of the cyber attacks would not be considered to be an act of war or state of warfare because there was no declared war and it was not possible to conclusively attribute the aggression to a state.

Cyber Intelligence

Cyber Intelligence is collecting, relating, analysing, and reporting information about a topic, an organization or a person, from sources available on the internet and other open sources.

Cyber Espionage

Cyber Espionage is the act of stealing secrets or confidential material when the receiver of the information has no legal rights to that information. Cyber Espionage is usually conducted by states and sometimes by companies under “Competitive Intelligence”.

Cyber Crime

Cyber Crime is defined by national laws and international conventions as any illegal cyber activity or unlawful computer network action. Cyber Crime usually involves territories of multiple states in order to obfuscate the origin of the criminals. Cyber Crime may include cyber espionage conducted on behalf of companies, organizations, or states.

Cyber Attack

Cyber Attack is an act of Cyber Offence or Assault such as Cyber Crime, Cyber Espionage, Cyber Subversion, and Cyber War.

Cyber Offence

Cyber Offence terminology is chosen because of its all inclusive meaning. Usually in the beginning we do not know whether a detected cyber anomaly is an attempt at an unlawful act, espionage, or an all out cyber warfare assault.

If it is a crime, it is a law enforcement offence, which the law enforcement organizations will deal with. If it is an attempt at espionage, then the appropriate counter-espionage organization would deal with it. If it is an act of war, then it is a military offence, in the sense of a military aggression or assault. Then appropriate military responses would be initiated.

Cyber Assault

Cyber Assault is defined as any cyber criminal act, Cyber Espionage activity, Cyber Subversion or military cyber operation.

A Classification of Cyber Assaults based on outcome and objectives: as **categorized by General Michal Hyden [106]**

- Exploitation of Cyber Assets: activities like cyber crime, cyber espionage, etc. are considered exploitation. These activities may not even leave any trace. [106]
- Create an effect - Cyber-on-Cyber: Intended impact on cyber assets and cyber infrastructure e.g. disrupting the cyber infrastructure or subverting the cyber infrastructure [106]
- Destruction of Physical assets – Cyber-on-physical assets: e.g. stuxnet attack on Iranian centrifuges [106]

Cyber Offences and Assaults

The concept of “Cyber Offences and Assaults” groups and consolidates the subject matters of Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime under one category. I have chosen this concept to analyse, understand, and model all three topics together. As we will see, there is substantial conceptual similarity and synergy between them.

Further information on real life assessment of past attacks and future trends is in Appendix 20. Cyberwarfare Market 2008-2018. [130]

1.1. Objectives

The objectives of the project are to:

- Establish a foundation to develop a Cyber War, Cyber Espionage, Cyber Counter Insurgency Course(s).
- Explore the possibility of using software engineering models as an aid to teaching Information Security Related Subjects.
- Examine the subject matter from a new perspective.

- Apply knowledge and experience in enterprise architecture, data modelling, and process modelling to the topic.

1.2. The motivation

I chose this project topic because cyber conflict, or Cyber War and Cyber Espionage and Cyber Insurgency is a very exciting, fascinating, intriguing, and vital area of study.

The reason I chose this project scope, project perspective, and scope objectives was because I have more than 20 years of Information Systems Strategic Planning (ISSP) or enterprise architecture, Data Modelling, Process Modelling, and software / information engineering experience. I have analysed complex organizational, strategic alignment, and competitive advantage problems.

If I could, I would like to contribute to the cyber security of citizens of smaller, free and independent states, and enhance their cyber deterrence capabilities (e.g. Latvia, Lithuania, Georgia, Ukraine and Moldavia)

1.3. Methodology Overview

During IBM years, when John Zachman¹ was working with different clients from different industries, he observed distinct patterns when organizations were tackling complex and large projects e.g., designing and building aeroplanes, ships and complex information systems.

John Zachman recognized that independent of the industry or the organization, people would use levels of abstraction to architect analyse, design, and build. These levels of abstractions, contextual, conceptual, logical, and physical are represented as rows of Zachman's Framework.

He also observed during these endeavours that people tackle a distinct set of problems which could be summarized, such as: Why are we doing this? What is this? How will this work? When should it happen? Who is responsible? Where should this be? Out of these questions, John Zachman created the columns: Why, What, How, When, Who, and Where.

He then observed that during these large and complex projects, the deliverables match to the cells of a matrix with the rows and columns described above. Usually these deliverables are considered as artifacts, which defines and constitutes the whole.

¹ John A. Zachman (born December 16, 1934) is an American business and IT consultant,[1] early pioneer of enterprise architecture, Chief Executive Officer of Zachman International, and originator of the Zachman Framework. John Zachman is one of the founding developers of IBM's Business Systems Planning (BSP),[6] and worked on their Executive team planning techniques (Intensive Planning). In 1987 he originated the Zachman Framework a standard for classifying the descriptive representations (models) that comprise enterprise architecture. http://en.wikipedia.org/wiki/John_Zachman

The enterprise architecture [1,2,3,4,5,6,7,8,9,10] methodology is a way to analyse and investigate how an organization may operate. Since the criminal, military, law enforcement and secret service establishments are organizations too, their missions or objectives, data requirements, processes, organizational structures and skill requirements, locations, operational sequences and cycles could be architected, designed, and analysed using the enterprise architecture approach.

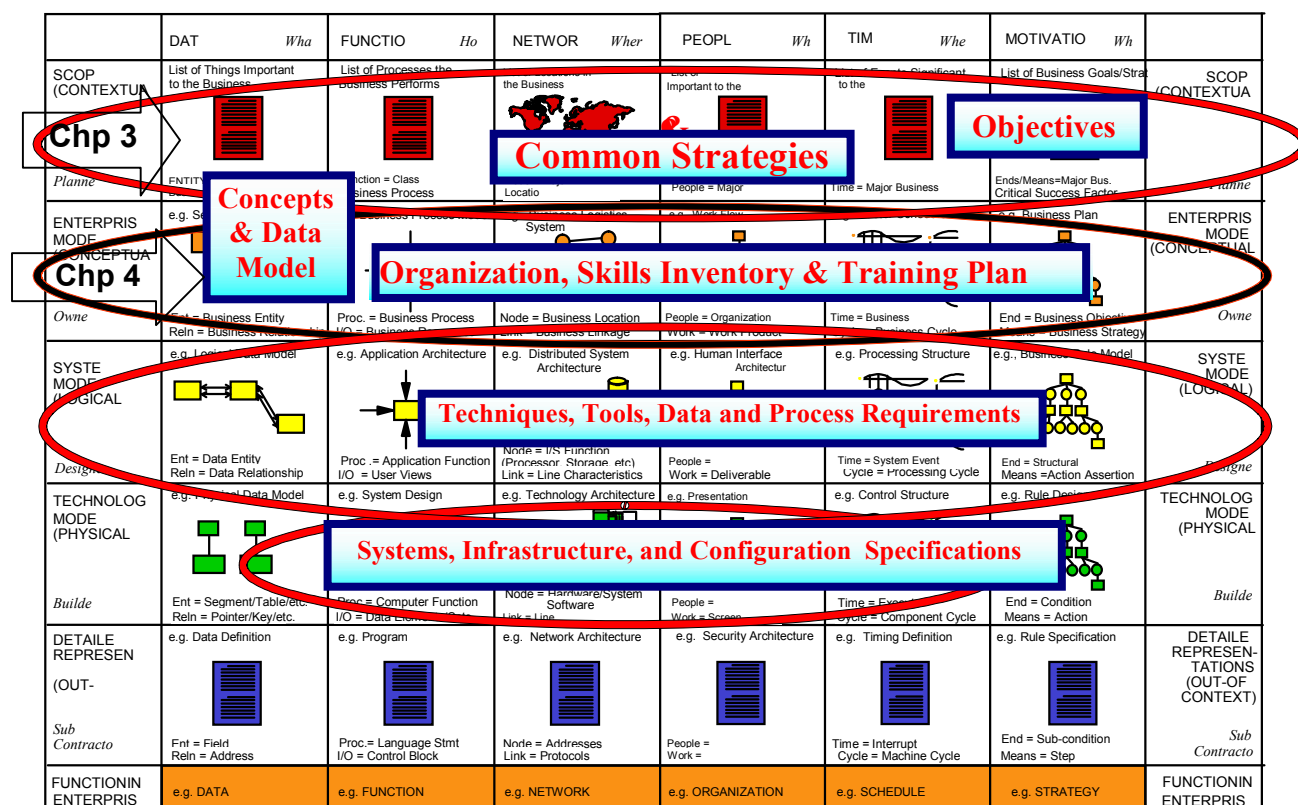
At row 1 – Contextual Level: The aim is to investigate and document artifacts as defined by different columns of rows of the Architectural Framework. The main purpose of this approach is to extract and understand organizational objectives and direction and make sure everything else in the lower levels of abstraction aligns and supports the organizational objectives and direction.

At lower level, rows of Zachman's Framework [11, 12, 13, 14] data models [15, 16, 17] are used to capture organizational data requirements and Data Flow Diagrams [18, 19] are used to capture organizational processes.

Through various matrices, relationships between artifacts (the cells of the framework) are analysed. They are then clustered according to rules, and a logical build sequence is established. The logical build sequence defines how various dimensions of the enterprise architecture and specific requirements should be packaged without any constraints. Next, the logical build sequence is modified to take into account the constraints reflecting the organizational and environmental reality. Out of this work, a series of projects are proposed to support organizational objectives and direction.

All of the above activities are usually conducted during workshops, modelling sessions, and facilitated discussions (brain storming, root-cause-analysis). Since no such opportunity was available at this time, published material will be used instead and gaps will be filled with assumptions. Moreover, since due to the enormous size of the scope and time limitations, the Swiss - cheese technique will be used. From time to time, certain gaps will be left or certain analysis will be skipped for future investigation beyond this project. All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

For a quick overview of the techniques, you may like to consult Appendix 1. A simplistic view of enterprise architecture approach.

ENTERPRISE ARCHITECTURE - A FRAMEWORK^T

John A. Zachman, Zachman International (810) 231-

The above diagram indicates how the Zachman's Framework and normal enterprise architecture Methodology will be modified.

On Row 1 Scope (Contextual), the objectives and strategies of the major players (USA, Russia, and China) will be investigated and analysed. This investigation and analysis is in Chapter 3.

The aim of row 1 is to understand what the distinct objectives are for the major players. What strategies are they using to achieve their objectives? How do they allocate resources, organize resources, and direct them toward their aims? How are they aligning their strategic resources? What responsibilities are they assigning to whom? How have they perpetrated offences or attacked in the past (modus operandi)?

On Row 2 of Zachman's Framework Enterprise Model (Conceptual) the goal is to understand what the important concepts, high level processes, and high level organizational structure, responsibilities, and skills requirements are. These map to the columns, What, How, Who of Row 2.

Since it is not possible to conduct in-depth research within the limitations of an MSc, a more detailed and complex analysis and modelling is out of the project's scope.

A similar approach may also be used a when collecting and analysing intelligence, and during surveillance and reconnaissance activities to map a target organization and its IT Infrastructure Architecture. [138 pages 17 and 18, 37,]

1.4. Overview of the Chapters

Chapter 1 provides an overview of the background, terminology, objectives, motivation, methodology of the project.

In Chapter 2 we review the background from the perspectives of beliefs, values, ethics, law, and the current pragmatic perspective. The cyber offences and assaults are some of the pieces of a big jigsaw puzzle in which the cyber pieces fit. In order to understand the cyber pieces, one has to understand the environment and the context which these pieces are plugged into. Chapter 2 provides this bigger picture or frame in which the cyber pieces do fit.

Chapter 3 provides a very high level investigation of the objectives and strategies of the major players in cyberspace.

When we move one level down in abstraction to the enterprise level of Zachman's Framework, we start to develop an understanding of that industry or type of operations. This high level of understanding of concepts and processes is covered in chapter 4. Only simplified subset models are in the chapter 4. The more detailed models are in Appendices 13, 14, and 15.

In Chapter 5 I will synthesize all of my previous work, to show similarities and the overlap between cyber warfare, cyber espionage, and cyber crime. We will see that the same set of techniques, tools, tactics, skill set and infrastructure is used in Cyber War, Espionage, and Cyber Crime.

2. The Background and Continuums

We reviewed the background from the perspectives of beliefs, values, ethics, law, and the current pragmatic point of view. The cyber offences and assaults are some of the pieces of a big jigsaw puzzle in which the cyber pieces fit. In order to understand the cyber pieces, one has to understand the environment and the context in which these pieces are plugged in. This chapter provides this big picture perspective.

Over the last sixty years, the pendulum of acceptable behaviour for western powers has swung quite dramatically. Once, they were striving to conduct themselves according to international law and the principles of justice. They were respectful of the sovereignty of other states, and defending human rights with altruistic deeds.

Now these are complex and shadowy areas, difficult to analyse and document precisely and completely. For our purposes, that is not necessary. We looked at the sample events and operations in the past to bring the reality of things to focus. These are real events, real people, and real lives. The big picture paints a very grim history. The question is then, what role the cyber operations play in this big picture. The rest of this paper will explore these questions using an enterprise architecture methodology.

The actions of states to a degree, are a reflection of national values, beliefs, cultural heritage, and legal frameworks of nations. These are the seeds and the foundations of the political systems, social systems, organizational systems and organizational DNA, which also govern cyber space.

In summary, cyber warfare, cyber intelligence, cyber espionage, cyber subversion, and cyber crime are the products of national identity and culture. They also represent some of the pieces of a much bigger puzzle of world reality. This reality is somewhat similar to trying to keep a level of stability and at least a minimal level of peace that all parties can live with. This is not being achieved over the multiple decades.

From a very simplistic perspective nothing has changed, the only difference is we have faster and more effective tools to do the same things. We need at least a high level understanding of what these offences and assaults are, whether they are cyber or not. What do we mean by subversion, covert operation, misinformation, and propaganda war, etc.? Who did what to whom in the past? Some of the answers to those questions are provided in the references and appendices for this section.

Another important point is if these things were known to the public, how the public would react. Is a more transparent ‘secret service organization model’ a viable option for democracies? Given the capabilities and activities of the hactivist groups, would this be a possibility over the next decades? The References [25, 31, 32, 32a, 33, 35, 43, 65, 68, 70, 71, 72, 78, 79, 80, 81, 83, 84, 88, 89, 90, 91, 92, 93, 94, 95, 102, 103, 105, 111, 113, 114, 116, 117, 118, 119, 120, 127, 128, 129, 140, 141, 144, 146, 156, and 157] and Appendices 1, 2, 3, 4, 5, 10, 18, and 23 provide a very short and brief snapshot of what is currently being practised.

The point of this chapter is “.. while the technology is new. The crimes we are exposed are not so new; “ [139 page ix]

2.1. The Humanistic View

The more detailed background for the humanistic view is in Appendix 24.

Here is another echo on the futility of war and how wasteful it is. About 15 to 20 years before Dwight D. Eisenhower, another General and President, Mustafa Kemal Ataturk, echoed the same ideas and feelings when he established the Turkish Republic after fighting a long war of independence against occupying European powers after World War I (WW1).

“Yurtta Barış, Dünyada Barış (Peace at home, peace in the world.)”

Quoted in many sources including H. Melzig, Ataturk’s political Testament.

What is moral or ethical perspective, what is the legality of the aggressions? What are the pragmatic benefits of all these investments in human lives, human suffering, and intellectual effort? What is the return on investment for all those things we have sacrificed for aggressive activities?

In summary:

1. There is no absolute security anywhere in the real world; why there should be in cyberspace
2. There seems to be no technical or military solution
3. The alternative is to reduce the tensions and injustices in the world, and as a result it is most likely that the number of offences and assaults will decrease

A more detailed overview of the crime of aggression is in Appendix 25. The Crime of Aggression: The Analysis.

In short, states or organizations are left to their own means to defend themselves. The question is then, how many resources for passive defences should be allocated and how much for the active defences – counter attack capabilities- . We will examine these questions later on.

In conclusion, the only viable alternative left is for a state or an organization to stand-up and defend itself. We will examine the use of cyber-minute-man or armed-citizens as possible cyber warriors to defend their or any victim’s cyber borders. [146]

2.2. The Historical and Anthropological perspective:

The historical perspective:

“.... Security is not new. It is one of our most basic needs along food and shelter. We are all concerned with protection of our lives and our property and assets. We wish to preserve our way of life in the future. “

Professor Richard Walton CB [22]

Over millenniums for most animals and humans, protection of the young, water supply, food supply, shelter, and later on other valuables have been important. This is also true for cyber assets and cyber property. Thus, the cyber valuables need protection and there should be consequences for the offenders. Additional discussion is in Appendix 26. The Anthropological Perspective from Friedrich Engels.

If one has cyber assets or valuables, they require protection. If there are valuables in cyberspace, some would like to plunder and unlawfully take advantage of them. Since the probability of detection and prosecution are very low, the cyberspace produces an ideal opportunity for crime. [22, 23]

2.3. The Two Continuums

We could consider two continuums. One continuum is the scale of escalating intensity of a conflict, which represents alternative coercion techniques available to bring to bear on competitors. The second continuum is about the scale of the relative legality of cyber attack, similar to different shades of grey, but not pure black or white.

The policy makers may choose from the first continuum, determining how much coercion to use and how far to escalate a conflict. They may also choose from the second continuum according to the importance they place on the legitimacy of their actions.

2.3.1 Continuum One: The Scale of Escalation - Intensity of Coercion

States use coercion in order to impose their will over the other states, organizations, groups, or people. There are different levels of coercion a policy maker may employ.

In deciding among the alternative coercion options, in resolving the political differences, both domestically and internationally, legitimacy may or may not be a factor. The policy makers may employ these alternatives sometimes within the constraints of legitimacy, and sometimes without any constraints of legitimacy. The ones in control of political power decide the escalation path and the combinations of which means to apply and when.

Now we can add cyber war and cybercrime as another battlefield dimension among the traditional ones as a means of coercion. As listed in Appendix 5 there are a series of means to intensify levels of coercion. Some of these means are covert (clandestine subversive operations with deniability) and some of them overt. The complete list of “Force Intensity Alternatives” is provided in Appendix 5. Continuum One: The Scale of Escalation - Intensity of Coercion.

There are many threats to representative democracies from internal and external quarters. Foreign secret services attack democracies, first subverting their defensive organizations such as domestic secret services, domestic intelligence services, police, and military. The typical clandestine techniques the foreign secret services may use in subverting domestic defensive organizations are: Deceit, Forger, Bribery, Blackmail, Sexual favours, Murder [25], [84, 85], [93, 94] [111]

One forewarned is one forearmed.

Another one of the covert attacks to a democracy is clandestine misinformation and propaganda war, based on fabricated misinformation and taking control of media via secret operations using subversive techniques such as those mentioned above. Cyber media, with its semi-anonymity cover and speed of distribution is the easiest choice to use relative to the traditional media.

Use of engineered pictures, stories, email distribution, blogs, and social media sites have been just some of the many ways to perpetrate these kinds of attacks. Usually there are no consequences to the attackers. In most of the jurisdiction there is no state or NGOs to defend against misinformation or propaganda attacks. We will revisit the role of the armed citizen (Minuteman) and their role in exposing these kinds of attacks.

At times, with increasing strength and frequency, democracies are subverted by internal gangs, such as: extremely active ruthless special interest groups, lobbyists, professional lobbying firms, religious pressure groups, very well organized and vocal minority interest groups. More often external forces subvert democracies using agents of influence; secret campaign contributions, professional lobbyist, bribing prime ministers [88, 89], secretly taking control of intelligence services, secret services, police, and military. (Gladio) [78, 79, 80, 81, 84, 117, 118, 119, 120]

In this game of deceit and treason, cyber options fit very nicely since cyber options provide deniability to states, and leave behind almost no real or forensic evidence. Thus, cyber subversion and cybercrime are the preferred weapons of choice for covert attacks.

Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime will require cyber weapons or crimeware research & development.

Furthermore, Cyber Offence and Assault require systems and procedures to manage a complex undertaking such as command and control systems, deployment systems, etc. in addition to the cyber weapons. In chapters 3 and 4 we will review such concepts and processes at a very simple conceptual level.

2.3.2 Continuum Two: The Scale of Legitimacy

“... differentiation between Cyber Crime, Cyber Warfare, and Cyber Terror (insurgency), can be misleading one – in reality, Cyber Terror (insurgency) is often Cyber Warfare utilizing Cyber Crime.” [72 – page 5]

Determining what the crime is and when it is a crime is not easy in general, but it is much more challenging in the cyber dimension. As we have seen in the previous sections, legality of wars is in dispute [28, 29], at least in most of the cases. It has become very subjective over the decades. The answers are different from one culture to another and from one territory to another, plus the answers are different over time too.

The difference between war and crime appears to have become blurred over the last 60 years. From one perspective what is considered “war”, from another perspective looks like “crime”.

Based on the above arguments, at this point it is possible to assert that the difference between cyberwar and cybercrime is not that significant. Later we will also argue that the technologies used to develop cyber weapons are not that different from crimeware.

Might Is Right [31, 32]

Nevertheless, for the rest of this paper the “Might is Right” principle would be accepted as the current reality. [32] Various other indicators of this reality are;

Some claim that during the Nuremberg trials after WWII, while the Nazis were prosecuted for genocide, France was conducting genocide in Algeria [33] without any condemnation – also in Maroc. [34]

Trumped up charges have always been very popular with some governments. In recent years, the most popular ones in Russia were tax evasion; in some other countries rape charges [35, 36]; in another country falsely accusing active duty admirals and generals with coup planning and keeping them indefinitely in custody without any credible evidence. Some still follow the principle of ‘reward the guilty and punish the innocent’.

These are the oppressive tactics of the state to intimidate the opposition. One of the latest additions to the classical arsenal is publishing intimate videos of critical members of the opposition on the internet. These are examples of cyber subversion. It is real and it is changing course of history. [90, 91, 92, 111]

Even though the UN Charter prohibits aggression by the armed forces of a state, interestingly enough it does not cover proxy wars, mercenaries of giant multinationals and paramilitary operations supported by states. Of course, cyber offences and cyber assaults are not covered either.

Now as it is the era of “infectious greed”, the more powerful states act according to “*might is right*” and “*end justify means*” public policy principles. For some, the outcome of this change brought to us a series of recessions, depressions for some economies, a climate of fear and hate, and a consequently, a constant state of deadly conflicts to others.

3. Analysis: Strategic Scope - Contextual View – Row 1 of Zachman's Framework

In Appendix 1 an overview of enterprise architecture and the Zachman's framework is provided.

In this chapter, we will examine the contextual view of Cyber Offences and Assaults. During this contextual level overview we will cover a wide area without going into the details. If we were covering a company, the level of detail would be appropriate for a CEO and in direct reports. It would focus on how a company generates value and serves its customers. It would include the business concepts and objectives for the specific business model of that company.

The specific aim is to understand and analyse cyber strategies, cyber objectives, and the high-level organizational structures of three major players; USA, China, and Russia. In addition to the big three, there are other capable cyber warrior states. Further information on this is provided in Appendix 21. Spymaster sees Israel as a world cyber war leader. [131]

In the chapters following this one, we will examine some of the relevant details and more complex relationship at lower levels of abstraction. If we had more time and space, we should have evaluated Horizontal and Vertical Alignments. This analysis could be conducted for one organization or for multiple organizations.

3.1. USA

3.1.1 U.S. Cyber Strategy:

In this section we would like to understand the “WHY” and “WHO” columns of the first row for the USA. In other words, what is the motivation for USA to establish a cyber force? Who is responsible and for what at the organizational and agency level?

A published comment about US Active Defence Strategy is in Appendix 27. Cyber Attacks could be classified as acts of war caused concern.

Due to difficulties attributing a cyber attack and since there is no direct involvement of a state in almost all of the cyber attacks we have observed, retaliating based on a un-attributable cyber attack is faulty logic at best.

This could become another very dangerous precedent for the US to establish. Some critics see that using a cyber attack to justify a retaliatory attack is a very transparent excuse. The murky cyber attribution evidence makes it very easy to go to war on a whim. The idea of lowering a threshold to go to war is not a good policy, cyber or not.

“But many cyber security experts say the policy statement is merely the latest step in a strategy that President Barack Obama began developing two years ago. And, they say, it might act as a deterrent to would-be U.S. enemies. ...” [36]

“Our assessment is that cyber attacks will be a significant component of any future conflict.” [37]

It is not clear how the US could deter other nuclear states like Russia or China without going nuclear. It could be suicidal for the USA to go into another war in Asia. [96] Thus, cyber attacks with plausible deniability for US may give enough leverage to coerce other states, without deploying boots on Asian soil or anywhere else, especially if the adversary has valuable cyber infrastructure and assets such as China or Russia.

The foundation of US Department of Defense (DOD) cyber strategy is in Appendix 28. The DOD's strategy is founded on five pillars.

There are some flaws with the five pillars. Cyberspace is not like any other domain as it is not that simple. Cyber Space is dispersed over the territories of many sovereign states. It is in every military domain, every weapon system every C4ISR² is built from cyber elements, every military logistic management system has cyber elements, etc. Almost all military domains use cyber operations in addition to their kinetic or hard fighting capabilities.

Cyber war fighting requires an additional set of skills and a different attitude than a traditional soldier or sailor may have. The cost structure, deployment, and logistic aspects of cyber war is quite different from other military dimensions. Moreover, cyber dimension intrudes into the territories of other states, some of which could be not even remotely related to the conflicts at hand.

Also regarding the first pillar, most of the time there are non-state actors and individuals in front of the state, giving the state a cover of plausible deniability. Attribution of a cyber attack to a state is not clear-cut and in many ways may not even be possible.

Defences may help against less capable, non-multi-vector, and non-persistent attackers, but defences may be futile or a waste of resources against persistent, multi-vector, and capable attackers.

Through various employment and work visa practices, the US has decimated its programmer workforce over the last 25 years. As another example of Infectious Greed is outsourcing software development outside of the USA and bringing in foreign programmers who would work at very depressed rates or salaries in the U.S., effectively destroying American Programmers. On the other hand, now USA needs more American Programmers to develop effective and efficient cyber war capabilities. [97, 98] A very interesting discussion on US strategic option is provided in Appendix 17 Former NSA & CIA Director Suggests Employing Mercenaries For Cyberwarfare. [106]

² Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance

The analysis of the material in Appendix 29. U.S. Cyber Command, a new military unit, is based on open source documents identified during this analysis. The referenced material indicates cooperation on defensive measures, but there was no indication of any cooperation or integration of detection, qualification, or attribution of attacks against the U.S..

One may think it is critical for the Department of Homeland Security (DHS) and the Military to decide how to detect and qualify attacks and define a threshold between crime and war. In other words, when a cyber attack stops being a criminal activity, that is when the DHS's law enforcement responsibility ends. When and where this is warranted and an initiation of a military counter attack is required, and the situation becomes a Cyber Military Conflict, and therefore becomes a military responsibility.

Also, under the DHS umbrella, there are multiple organizations with different mandates and security missions, such as Customs and Border Protection, Federal Emergency Management Agency, Immigration and Customs Enforcement, Transportation Security Administration, U.S. Citizenship and Immigration Services, U.S. Coast Guard, U.S. Secret Service, Office of Inspector General, (most likely this is an incomplete list). Moreover, there are other federal organizations such as the FBI, and Nuclear Energy Security Administration, etc. It is not clear from the available material how these organizations will coordinate their activities and integrate their detection, qualification, and attribution systems.

The following is the analysis of the material in Appendix 30. Chinese and Russian Response.

There are at least two alternative approaches for the U.S., one being "protect the cyber valuables" and the other being "shoot the hostage."

U.S. technology firms have developed distinct monopolistic position over the internet, e.g. Google, Yahoo, CISCO, MicroSoft, etc. To further exploit its dominant technical and commercial position, protecting these interests seems to be a current priority for the U.S.

The other perspective places more emphasis on protecting US critical infrastructure from cyber attack. A major successful attack on critical infrastructure could have catastrophic consequences. In addition, some attribute these vulnerabilities in critical infrastructure to monopolistic software products such as Microsoft windows, Office etc. They assert that if Microsoft products are removed, at least from government critical infrastructure, the U.S. vulnerabilities to cyber attacks could be reduced significantly.

The choice for the U.S. is therefore between commercial interests and the safety of its citizens. The safety of the citizens is currently being compromised due to vulnerabilities introduced by current US software vendors. This is making the critical infrastructure vulnerable to cyber offences and assaults. For some it is a very simple decision. One may argue that the primary reason of the existence of the state is to protect its citizens.

Further analysis based on the material is in Appendix 31. Mistrust about the motives of the United States. This is a really good strategic option for US. It is definitely cheaper, relative to boots on distant countries or predator attacks or cruise missile attacks. It is not much different from what OPEC did in the 70's using oil as a weapon.

Review of the points made in Appendix 32. The perceived hypocrisy of U.S. is below.

Not only the Wikileaks incident, during the very beginning of Iraq invasion, when people questioned the existence of Weapons of Mass destruction (WMD) in Iraq and the motives for the invasion they were brutally hassled and silenced, the White House also disclosed the identity of an active CIA field agent in order to silence and punish her questioning and critical husband. Fox News savagely attacked the Americans with different views; they were being accused of being unpatriotic, they reminded some the McCarthy years.

The analysis continues with the points made in Appendix 33. The international policy on the Internet should be a matter for the whole world.

One interpretation of this statement: we are the big three, let's carve the pie into three pieces and leave the crumbs to the others, not much different then from how the US and Soviets shared Europe after the WWII, the only difference is China being added to the table.

The question is then, if the cyberspace is to be divided three ways with different rules, what would be the implications. One simple answer could be business as usual, based on Mutually Assured Destruction (MAD), exactly like the way it is with nuclear arms. The U.S. will continue with its dominance outside the sphere of Russia and China. Russia will use cyber attacks in its sphere of its influence. China and the U.S. will play a dangerous game of escalation and de-escalation based on Chinese cyber espionage attacks on the US and other western countries; and for example U.S. Spy Plane intrusions into Chinese territory.

The above observation highlights the importance of not viewing cyber offences and assaults in isolation. As in the above example, cyber espionage is part of a bigger espionage game than just cyber.

“The Voice of Russia quoted an analyst who suggested that

Russia is afraid that the U.S. might use [cybersecurity] cooperation to damage its national security. “

“So, while Russian and Chinese press felt the strategy “reveals the traditional American approach: we compose the tune and the rest of the world can dance to it” (in the words of Ananyan Artyom at Voice of Russia)...” [38]

Obviously, both Russia and China resent US technological and military superiority, which still constrains Russian and Chinese aggressions to a degree. The question is what will be the importance of cyber weapons when the US starts to decommission some of its carrier groups due to economic difficulties. Could the US use cyber warfare to maintain an advantageous balance of power or would the US require other friendly mid-powers to step up their game e.g. EU Cyber Command, EU Nuclear command, fully integrated EU Military, more capable Indian military (with deployed carrier task forces in multiple oceans).

The point of the questions above is to again assert the fact that the cyberspace is part of a bigger picture. One has to consider overall implications and synergy created by

cyberspace in the larger context. One even may go further to claim cyber strategy should not be a strategy but a subset of an overall national strategy.

3.1.2 US Cyber Command

“United States Cyber Command (USCYBERCOM) is an armed forces sub-unified command subordinate to the United States Strategic Command.” [40]

US CYBERCOM is a subunit of US STRATCOM. Let us briefly look at what the responsibilities of US STRATCOM are.

United States Strategic Command (STRATCOM):

“It is charged with, information operations - *Department of Defense Information Operations* -(such as [information warfare](#)), global [command and control](#), intelligence, surveillance, and reconnaissance ([C⁴ISR](#)), ...” [45]

Based on the above responsibility statement, the STRATCOM is responsible for cyber war operations and their global coordination, in addition to global intelligence, surveillance, and reconnaissance. The terminology “Information operations” is used to mean different things. For example, in reference to the attack on the Serbian Air Defence Systems, it has been used to mean Computer-Network Attack. Serbian Air Defence monitors were blinded with the use of malware. This is similar to an application level attack. In another context, Information Warfare meant propaganda, misinformation to influence the public opinion or coerce the opposition to take a course of action.

One can only speculate that the CIA may have similar mandates and capabilities. It is not clear how objectives, planning and operations are coordinated. There was at least one publicized cyber operation where the actions of these two organizations were in direct conflict. [43] This could be the tip of the iceberg. In reality, it is most likely that multiple organizations and agencies could be conducting conflicting cyber operations without being aware of what the other agencies and organizations are doing.

Mission statement:

‘....., to ensure U.S. freedom of action in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations,’
[45]

There are a few implications of the above mission statement. Since cyber space is global and intrudes into the jurisdiction 140 plus states, the statement “*U.S. Freedom of Action in space and cyberspace*” is claiming control over cyber assets of 140 plus countries. Moreover, the U.S. claims it has the right to do what ever the U.S. wishes within the jurisdiction of those 140 plus states. Fundamentally, this mission objective disregards the sovereignty of the 140 plus states. It is a very dangerous precedent. The implication is that adversaries may take the same liberties with our cyber assets including ones controlling our critical infrastructures, some of which happens to be nuclear power generators.

The other point is integrated kinetic (hard or traditional weapons) and non-kinetic (soft weapons) responses to a cyber attack. This means the total war effort would have integrated objectives, plans, and actions. Given the number of military commands, law enforcement organizations, and secret services that are involved, responding to a cyber attack with a coordinated justifiable counterattack may not be as easy as it sounds. Most likely, the attacker will leave no evidence; there will be no smoking gun, and nothing to directly attribute an attack to a state.

Another point is “*in support of U.S. Joint Force Commander Operations*”. This statement seems likely to exclude the active defence of critical infrastructure when U.S. is under significant cyber attack, even though a counter attack using active cyber operations is warranted.

Further supporting details of US Strategic Command are in Appendix 6. United States Strategic Command (STRATCOM) and Cyber Command in Appendix 7. USCYBERCOM High Level Mission Statement and Organizational Structure.

Given the contents of Appendices 6 and 7, at least on the surface, there is a mismatch or gap between strategy and the assigned responsibilities. Both cyber strategy statements and statements of the policy makers declare that the US may counter attack when a cyber attack reaches a threshold. But, in the above statements it is not even mentioned how detection, qualification, and attribution will be achieved and by whom. In order to implement this policy objective one has to integrate operational procedures and systems of those agencies to hand over to other agencies the relevant data about the state of a progressing cyber attack. This requires a handover in computer-time or near-real-time for cyber operations or counter attacks to be executed.

USCYBERCOM High Level Organizational Structure “Service components:

As it could be deduced from the overview of the cyber warfare roles of military domains in Appendix 7. USCYBERCOM High Level Mission Statement and Organizational Structure. [39]

In the real world, coordination and integration is quite complex, since each military domain has established cyber war capability. It is not clear how their objectives, planning, operations, techniques, tactics, tools and systems would be integrated. In addition, how accountability and an audit trail of weapon deployments would be established. Answers to these questions have not so far been found during this research in the public domain. [39]

“On 23 June 2009, the Secretary of Defense directed the Commander of U.S. Strategic Command (USSTRATCOM) to establish USCYBERCOM. In May 2010, [General Keith Alexander](#) outlined his views in a report for the [United States House Committee on Armed Services](#) subcommittee: ^{[13][14][15][16][17]} “[39]

"My own view is that the only way to counteract both criminal and espionage activity online is to be proactive. If the U.S. is taking a formal approach to this, then that has to be a good thing. The Chinese are viewed as the source of a great many attacks on western infrastructure and just recently, the U.S. electrical grid. If that is determined to be an organized attack, I would want to go and take down

the source of those attacks. The only problem is that the Internet, by its very nature, has no borders and if the U.S. takes on the mantle of the world's police; that might not go down so well.” [39]

The above statement summarized both the problem and solution to a degree. But this point does not currently appear on the publicly available official documents yet. This could be with the addition of cyber militias a better solution to cyber threats and attacks from non-state actors, more information could be found in Appendix 7 and [39, 42].

Conti and Surdu reason: "Adding an efficient and effective cyber branch alongside the Army, Navy and Air Force would provide our nation with the capability to defend our technological infrastructure and conduct offensive operations. Perhaps more important, the existence of this capability would serve as a strong deterrent for our nation's enemies." [42]

Since a cyber force has multiple roles, it could be organized with strong central capabilities for detection, qualification, attribution, counter attack, support of joint operations, training, R&D, etc. However there is also a need for cyber operations components to be embedded and dispersed in all military dimensions, similar to the current cyber units in the air force, navy, marines, and army. The terrain, environment, and domain knowledge of their dimensions are required and there is no point trying to duplicate this knowledge.

“In response to concerns about the military's right to respond to cyber attacks, GEN Alexander stated "The U.S. must fire back against cyber attacks swiftly and strongly and should act to counter or disable a threat even when the identity of the attacker is unknown" prior to his confirmation hearings before the United States Congress. This came in response to incidents such as a 2008 operation to take down a government run extremist honeypot in Saudi Arabia. "Elite U.S. military computer specialists, over the objections of the CIA, mounted a cyberattack that dismantled the online forum".” [43]

These are examples of organizational conflicts and since there are no common objectives, plans, and management systems to coordinate their activities it is wasteful and dangerous. Maybe it is one of the first examples of cyber friendly fire. [106]

3.1.3 NSA

The following is copied from the NSA site on August 02, 2011. Earlier in March – April 2011 time frame, the NSA website had a Cyber Mission statement stating “**Domination of Global Cyber Space**’ as their objective. That web page is no longer available. Most likely, the mission has not changed much, neither has the NSA’s capabilities.

“The **National Security Agency/Central Security Service** (NSA/CSS) is a [cryptologic intelligence](#) agency of the [United States Department of Defense](#) responsible for the collection and analysis of foreign communications and foreign [signals intelligence](#), as well as protecting [U.S. government](#) communications and [information systems](#),^[1] which involves [cryptanalysis](#) and [cryptography](#).” [53]

“NSA/CSS Mission, Vision, Values

The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.” [100]

“Our Vision

Global Cryptologic Dominance through Responsive Presence and Network Advantage.” [100]

“Our Values

We will protect national security interests by adhering to the highest standards of behaviour” [100]

One would think NSA’s Information Assurance mission could be a defensive mission to defend cyber assets of the US and its allies, but ‘*Enables Computer Network Operations*’ is a little bit cryptic. It is unclear whom and how the NSA will enable. One can assume NSA will enable the Cyber Command, and other dimensions of military, or DHS. Enabling could be through training, technology transfer, or providing infrastructure, or in other ways. One could assert that given the history and capabilities of the NSA, most likely, it has the most advanced capabilities in place to detect a cyber attack on US assets and trace a cyber attack to the attackers. One would assume the NSA is more than capable of conducting offensive Computer Network Operations. [107]

One view has been expressed by General Michal V. Hyden. “DHS is a storefront and the NSA is the backroom operations”. NSA would do the heavy lifting. This approach sounds like a logical approach, but first this is not what has been stated in US Cyber Strategy and the second point is that it has not defined how the integration of the storefront (DHS) and NSA is achieved at the day to day or millisecond to millisecond level. [106]

It would make more sense to define (independent of current organizational structures) what would be required for the U.S. or any other state to do in cyber space -e.g., in what and how columns of Zachman’s Framework-, and assign those responsibilities specific components (the Who column of Zachman’s Framework) based on the capabilities of the organizations and agencies.

3.1.4 An Evaluation of Alignments, Misalignments, Gaps, and Conflicts

US Priorities:

There seems to be conflicting US priorities: one is protecting US Commercial interests of technology companies and their monopolistic advantage. The other is protecting US lives and US critical infrastructure. At best the choice is up in the air, or favouring the commercial interests of companies relative to US lives and critical infrastructure.

The argument presented in Appendix 34. Cultures of the Army, Navy and Air Force are incompatible with that of cyber warfare and this sounds like flawed logic. If one

considers the tasks and operations involved in a warship or submarine, they are highly technical, computer, and network based. These tasks require use of very complex computer systems and computer networks and their maintenance. These tasks involve range from simultaneous detection of multiple targets to weapons deployment, electronic countermeasures, electronic warfare, and navigation. The same is true for both aeroplanes and helicopters, for example an AWACS plane [104] may have on board communication and computer equipment which would make a lot of high tech research centres envious. All of these military assets require highly technical people to maintain and operate. Some of these technical skills are quite relevant to cyber war, furthermore they are required critical skills.

3.2. China

If the analysis in Appendix 35. PRC may be a global power economically but its military lacks force projection is true Then obviously, China feels vulnerable to US military superiority and will be seeking ways to level the playing field. Then, the main Chinese cyberspace objective is to deter aggression from US.

Based on Appendix 36. Revolution in Military Affairs; according to a Chinese assessment of their own strength and weaknesses and their assessment of US strength and weaknesses they are making strategic choices. Their strategic choice is to apply their strategic strength to their strategic weaknesses for better protection. Their obvious strength is people power, specifically very well trained engineers and scientists particularly in computer science and software engineering. Just a simple review of how Chinese universities rank in the world and how that has improved over the years has been a very good indicator. While the U.S. has decimated its programmer workforce, China has increased the quantity and the quality of their software engineers and technical specialists.

In Appendix 37. Chinese military strategists view the world as a place basically hostile to Beijing's national interests. This review sums up how China sees the world and the US. They feel threatened and under attack. This is because they have suffered over the millenniums and during the last century under Imperial Japanese occupation.

They recognize the superior military might of the US. They see cyber warfare and tactics as a force equalizer. What is not clear beyond effective cyber espionage attributed to them is how effective they would be at attacking US satellites, C4ISR, and other military targets. Interestingly enough they have not considered US critical infrastructure as targets in any open source material I was able to find. It is hard to know whether it is intentional omission or whether they are really not considering it due to fear of nuclear retaliation from the U.S. It seems like both the Chinese and the US prefer a regional war than an all out global total war.

As expressed in Appendix 38. US and China face vast divides on cyber issues. This is a very different strategy than what has been expressed in the previous Chinese strategy statements. Attacking US civilian infrastructure oddly enough is not mentioned. The target examples were US military capabilities and the Chinese aiming to render them ineffective. Either, in the above statement “cyber infrastructure” means military cyber

infrastructure or a change in strategic targeting. This distinction is very important. Most likely, any attack on civilian infrastructure and its impact and potential civilian casualties would bring any conflict to different level of intensity

The Chinese approach described in Appendix 39. Understanding of offensive operations is also a typical Russian approach, taking advantage of plausible deniability of a cyber attack. It looks like the US is following the same pattern with most of the malware purveyor websites in the world happening to be located in USA, even though some of them are owned by the Russian organized crime networks, which would give US an excellent cover. This is like killing two birds with one stone. Attack someone using Russian Organized Crime infrastructure, enjoy the plausible deniability, and blame the Russians for the attack.

In light of Appendix 40. The high-value intellectual property theft, relative to US advanced spying technologies -such as satellites, spy planes, drones, submarines, spy ships like USS Pueblo- Russian and Chinese capabilities are very limited. It is most likely that the Russians and Chinese are trying to make up for their deficiencies in advanced spying technologies via Cyber Espionage.

"Until the United States gets serious about which concessions that are attractive to our adversaries it is willing and able to make, American talk of a cyber-arms agreement is empty," Goldsmith wrote recently." [59]

Another dimension of Cyber Warfare is the business dimension. The Cyber Defence market is obviously getting bigger and it is exciting times for the cyber security experts, consultants, and the cyber defence contractors. Time and space permitting we may go further into this in the conclusion.

The Chinese Cyber Warfare Investment thought to be 55 million dollars and number of people allocated thought to be more than ten thousand. [139 page 129 and 130] In Appendix 9, you will find more supporting and background information about the details of what we have discussed so far.

Again, the significance of this section is to explore and display how cyber space strategies are interwoven with national strategies. It is not reasonable to study cyber space strategies without understanding strategic perceptions, strategic objectives, and the national strategies.

3.3. Russia

"Since the 1991 Soviet collapse, Russian military planners have relied increasingly on the country's huge nuclear deterrent as the capabilities of its conventional forces have deteriorated. Efforts to develop a new military doctrine in recent years have coincided with plans for a radical modernisation of Russia's armed forces." [63]

Due to economic decline, the Soviet Armed Forces have become a shadow of what they were. The morale of the Soviet military also collapsed after defeat in Afghanistan and use of drugs has become problematic. Russian borders are mostly safe from any conventional

aggression and the other superpowers were checked by large Soviet era nuclear arsenal. During that period, cyber war was not a consideration. As Russian organized crime invented the crimeware and ways to make illegitimate money from the internet, due to close links and cooperation between security forces and organized crime, Russian policy makers realized the potential strategic and tactical values of crimeware, cyber crime infrastructure, and cyber crime skills.

The following analysis is based on Appendix 41. Russia sees greater Euro-Atlantic threats moving further east. I am not sure whether Russia sees an emerging threat from the west or not. It is probably more an emotional response as they are not willing to give up influence over what they feel is their own back yard or real estate. This is not any different to how the US sees the South, Central, North Americas, and the Caribbean. One can assert that neither the US nor EU is in any position to threaten Russian security using conventional weapons, nor that Russia is in any position to threaten the EU or US using conventional weapons. Some may argue that placing the patriot anti-missile batteries in Poland is nothing more than a political posturing attempt by the US and a cheap way of trying to appear strong and important in Eastern Europe, contrary to the reality. It looks like the US and EU has completely abandoned Georgia, the Caucasus States, and Central Asia (Turkic States) to the Russian sphere of influence and exploitation.

Given all of the above, the question is What is the value of cyber warfare to Russia?. First, when Russian sensitivities are offended, they use cyber attacks to communicate their displeasure. The second is they have used cyber attacks to destroy C4ISR capabilities of Georgia during the war. This is most likely not that Georgia could have defeated the Russian Army, but from the Russian perspective to shorten the war, to reduce casualties, and to hide the weakness of their army and equipment.

If NATO and the EU had provided enough training and equipment to the Georgians, Georgia could have easily repulsed the Russian attack and protected its territorial integrity. NATO and EU choose not to do this. Both will pay dearly for these choices over the coming decades. The detailed analysis of how Russia used cyber attack is provided in Appendix 10. The Russian invasion of Georgia.

The most likely interpretation of recent Russian weapon systems development indicates that Russia is attempting to upgrade its nuclear weapons and delivery platforms (submarines, missiles, and fighter planes). There is no indication of any investment into cyber warfare. It is not obvious that Cyber War R&D is a priority for Russians. It looks like they are happy to use what Russian organized crime provides. They may feel they have adequately trained cyber warriors ready to be enlisted clandestinely as required. The supporting details are in Appendix 11 Russian attempts to upgrade nuclear capabilities.

It seems that Russia is conducting cyber attacks in five different areas:

1. Internal cyber war against political opposition to the government
2. Exerting Russian cyber power to the states Russia considers within the Russian sphere of influence
3. In support of conventional aggression (hard attack, kinetic attack)
4. Allowing organized crime to continue
5. Engaging misinformation warfare against almost all others

The following analysis is based on [Appendix 42 Cyberwarfare by Russian](#) and other references provided about the Russian Secret Service and their Cyber Crime Operations.

To sum up Russian Cyber war practice:

The targets:

Depending on political developments, Russian targeting priorities do change. When Russian actions are analysed, a group of targets become obvious. The Russian targets are Internal Opposition to the government, sovereign states which Russia considers its own backyard, Baltic States, Eastern Europe, the Caucasus, Georgia and the Turkic Asian states.

How:

Typical Russian cyber attack approaches includes non-state actors, youth organizations, volunteers from a well-trained technical population, and the use of Russian Organized Crime infrastructure distributed across the globe.

Types of Attacks:

It looks like the policy makers decide on the appropriate response and specific assets to target. So far, the techniques used are disfiguring web sites, DOS, DDOS, and misinformation and propaganda [102, 103] and the attack on C4ISR in the case of Georgia.

“Disinformation [68]

US journalist [Pete Earley](#) described his interviews with former senior [Russian intelligence](#) officer [Sergei Tretyakov](#) who defected in the [United States](#) in 2000. According to him, Sergei would send an officer to a branch of [New York Public Library](#) where he could get access to the Internet without anyone knowing his identity. The officer would post the propaganda on various websites and send it in emails to US publications and broadcasters. Some propaganda would be disguised as educational or scientific reports. ... The studies had been generated at the [Center](#) by Russian experts. The reports would be 99% accurate but would always contain a kernel of disinformation that favored Russian foreign policy. ... "Our goal was to cause dissension and unrest inside the US and anti-American feelings abroad"[3] Tretyakov did not specify the targeted web sites, but made clear they selected the sites which are most convenient for distributing the specific disinformation. “[68, 69]

One may argue that since the Soviets or Russia never had a deep and well-established free press, a state of different levels of misinformation is business as usual for them. Over the decades, they must have developed organizations and skill sets to misinform their citizens and rest of the world. Naturally, they have carried on these practices and skills into cyber space. [105]

It is increasingly becoming more and more difficult to determine the credibility of news or information or to verify the original source over the internet. Since misinforming does

not appear to be a crime or something being eagerly prosecuted, this practice is ongoing all over the globe.

I believe, since misinformation subverts democracies, it requires special attention. It should be recognized as a serious cyber attack and cyber crime. There is a need for more NGOs to track misinformation. There is a need to link the perpetrators to state actors and at least to put them on a 'shame list'.

High-level statistics about Russian Warfare Investment are budgeted to be 127 million dollars and the number of people allocated to be more than seven thousand three hundred. [139 page 129 and 130]

3.4. Strategic Scope: The Main Points

Why: Motivation

China and Russia have articulated their cyber strategies and objectives and their actions seem to match them. On the other hand, it is not very clear what the US cyber strategy is and it looks very much in doubt that it matches the actions of many organizations and agencies with similar responsibilities. One of the clearest indicators of overall US defence strategy is in a warning from Secretary Gates. [96 - Never Fight a Land War in Asia]

Cyber offence and assault capabilities as a force equalizer:

In addition to the Chinese, Israelis also see the cyber offences and assaults as something that would give them an asymmetric advantage against a more powerful adversary. "Cyberspace grants small countries and individuals a power that was heretofore the preserve of great states," Yadlin said." [131]

Who: The Actors and Organization

In China and to a lesser extent in Russia; there is a clear and open debate among professionals about their strategic situations. They discuss how to take advantage of cyber options. The Chinese and Russian governments appear to be following the recommendations of their qualified professionals. In the U.S., there are excellent professional documents and discussions and demonstrated capabilities of some of the military dimensions and government organizations, but it looks like the politicians are calling the shots. The choices the policy makers articulate seem as if they are not closely aligned with the recommendations of the qualified professionals.

Also, in the cases of China and Russia there is indication of unity of command and clear command and control structure. There are indications to suggest they have centrally and clearly defined non-overlapping responsibilities.

Currently in the case of the US, a clear-cut definition of responsibilities and unity of command is not obvious. Based on the available open source documents, there are quite a few US organizations and agencies in the cyber defence, cyber war, cyber espionage, and

cyber crime space. Among many issues, how these organizations and agencies would cooperate, how they would transfer cases and intelligence, and how they would act in unison have not have been defined. It looks like a cohesive U.S. cyber strategy integrating all the organizations and agencies of the US government is yet to be defined. [60] [106]

It seems likely that currently NATO does not consider a cyber attack to be a reason to invoke Article 5, requiring the common NATO response of all member states. For some people, this is a very unfortunate choice. [106]

4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework

States had used traditional or hard or kinetic weapons, relevant tactics, and techniques in order to execute their attacks, but over the last decades, a set of new choices has been devised. These new choices are cyber weapons or crimeware, or soft weapons. The soft weapons open up unusual opportunities and threats. Simply, the soft weapons are the use of computer networks, computers, and malicious software for covert, sometimes semi overt attacks, and espionage.

We will examine the organizational concepts and organizational processes required for the use of these cyber weapons. The cyber weapons take advantage of vulnerabilities of computer networks and computers. Organizations deploy the destructive software as a weapon against these vulnerabilities. This course of action is available to states, state controlled non-state actors, independent groups, and common people. The cyber weapons or crimeware potentially could be as destructive as weapons of mass destruction with plausible deniability.

Knowledge about Cyber Offences and Assaults is obtained from second and third hand sources from news, articles, government websites, academic papers, and books, the lectures, lecture notes, course references, especially computer crime, digital forensics, and penetration testing; all the references are provided in the reference section; but specifically [72, 99, 100, 101, 102, 103, 105, 106, 107, 108, 110, 113, 114, 115, and 116] and [139, 140, 164, 165, 166, 167, 168]. This knowledge is used in creating these first cut models. [15, 16, 17]

That knowledge is cast into the first cut data model, first cut process model, and a set of matrices. These sets of interrelated deliverables are the ones prescribed by the second row of Zachman's Framework. Similar investigations of Cyber War; Cyber Intelligence, Espionage, and Subversion; and Cyber Crime are conducted.

The overview of the approach used for this chapter is in [Appendix 43. Overview of the Approach: Analysis.](#)

The following models are for illustrating how these technique and enterprise architecture approaches could be used in analysing the use of cyber weapons. These models, diagrams and matrices are sample simplified models. They are not detailed enough to be complete conclusive evidence for the conclusions drawn in Chapter 6. Neither space nor time allocated for the MSc allowed that level of detail. That is why the Swiss cheese technique is used to provide sample techniques to demonstrate the overall approach.

4.1. Cyber War

The real life example:

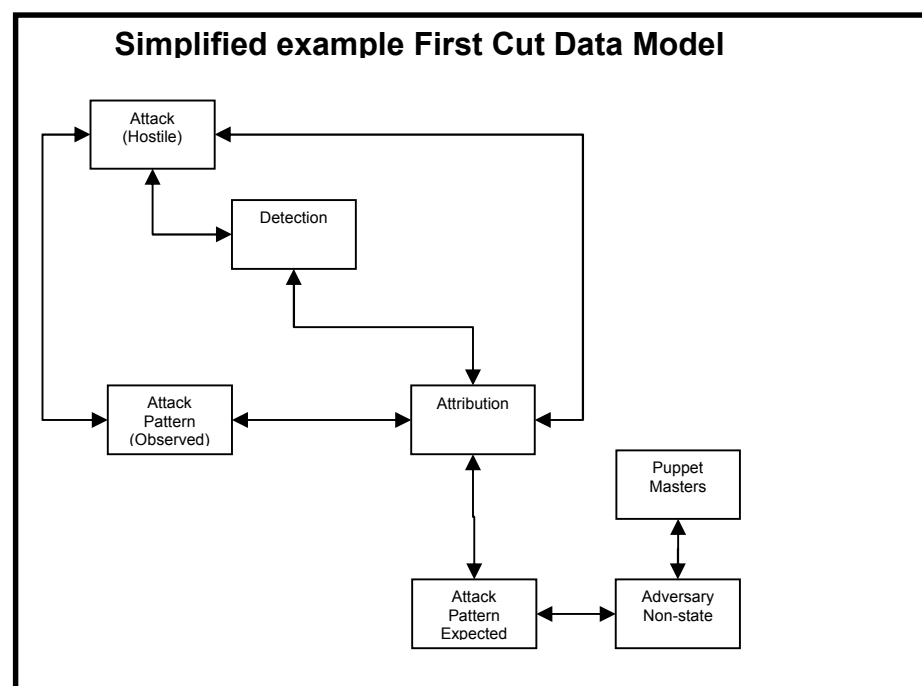
Some of the contents of the models are based on the unofficially unsubstantiated accounts of NATO and the US attack on Serbia. According to [72] the US and NATO have used Information Operations to deceive the Serbian Air Defences System, making sure that US and NATO planes would not appear on their tracking monitors. This would be considered cyber war, even though military documents refer to it as an “Information Operation” or “Computer Network Operation”. Categorized by General Michal Hyden as Cyber on Cyber attack “to create effects”. [106]

4.1.1 First Cut Data Model

A First cut data model is created to identify important concepts and relationships among these concepts. Usually the terminology of a topic would identify important concepts in that topic. In order to manage and operate in that context one must understand these concepts.

Appendix 13 First Cut Data Model Cyber Warfare– complete has a comprehensive example of a complete first-cut-data-model. In this model, the concepts used in Cyber Conflict have been identified and the high-level relationships among them are indicated with lines.

The following is a simplified subset of the data model in Appendix 13 First Cut Data Model Cyber War –complete.



The following narrative aims to explain the basic concepts of a very simplified model of cyber war. The model is not intended to be complete or conclusive. The models are just to demonstrate the technique.

Overview of some of the Entity Types:

This data model shows 7 entity types. When one or more of the discovered anomalies or events meet a certain criteria, an instance of the **Detection** entity type is created. An instance of **Detection** indicates there is some evidence captured and requires further analysis and attribution. The **Attribution** entity type is a container for rules and knowledge used for attributing or disqualifying a detected anomaly as either an Attack or false positive. The **Attack** indicates the concept of a hostile attack. After detection and analysis of an anomaly or event, an instance of the **Attack** entity type may be created as a permanent record of an attack. The **Attack Pattern Expected** is a knowledge base of pre-recorded, attributed attacks used by an Adversary. These are some of the possible interpretations of the entity types. The data contents e.g. percentage of match of patterns, certainty of attribution, etc. could be data elements of entity type **Attribution**.

Overview of the some of the Relationships:

The Relationship between **Attack** and **Attack Pattern** indicates the sequence of events and anomalies of an Attack that has been captured using a specific template and structure. The Relationship between the **Attack** and **Detection** indicates that before an instance of **Attack** created there was an instance of **Detection**, where the initial anomalies and events are captured. Later on, as more data is collected and more investigations take place the **Attack Pattern – observed** would form a more complete picture.

The relationships from **Attribution** to **Attack Pattern – expected**, **Attack Pattern – observed**, and **Attack** indicates using what rules and facts the **Attack** is attributed. These are some possible interpretations of the relationships.

All the models, matrix analysis, and explanations are my interpretation of the materials I have researched.

4.1.2 First Cut Process Model

A very simplified first cut process model is created to understand and describe the conceptual organizational processes independent of organizational structure, specific technology, or systems. [18, 19].

An overview of the techniques used in this section is provided in Appendix 43. Overview of the Approach: Enterprise Model Conceptual View – Row 2 of Zachman’s Framework.

In Appendix 15 First Cut Process Model Cyber War – complete, the major processes have been identified and the data flows of those processes are shown in addition to the data stores.

We could define our context (environment or surrounding) by identifying the external events and external actors (external entities) being interacted with.

In our scope, the major external Events, which may trigger the process within the scope are:

- Attack Detection
- Support Request (Strategic, Tactical, or Operational)
- Changes in the status of Strategic Indicators
- Intelligence
- Surveillance
- Recognisance
- R&D
- Emerging technologies

Note: This is not an exhaustive list, just a sample.

The major External Actors, which may be interacted with are:

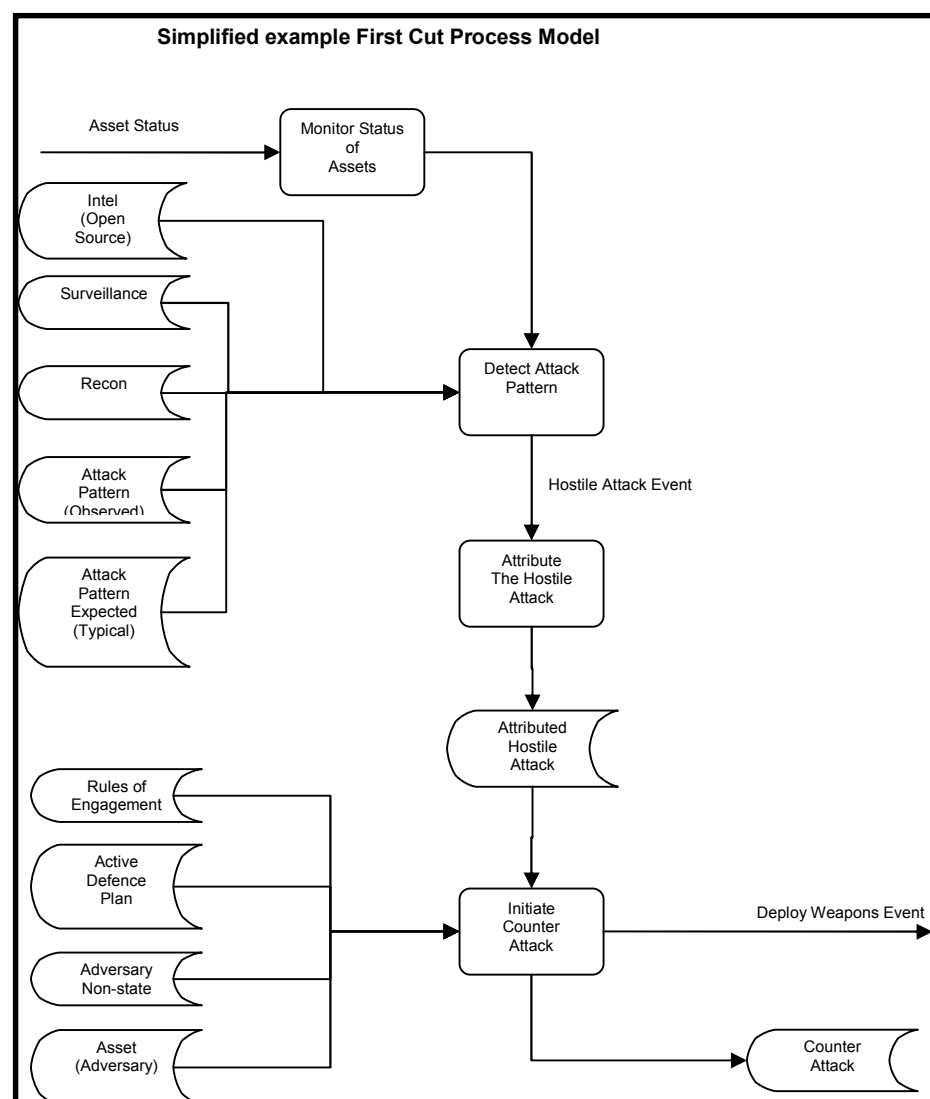
- Citizens
- Non-state Actors
- State Actors (Adversary)
- Special Interest Groups
- Criminal organizations
- Individual Hackers
- Military organizations (ours or friendly or adversary)
- Critical Infrastructure Systems
- Law Enforcement Organizations
- Commercial Companies
- Intelligence and Secret Services (espionage, green ops, black ops, and subversion)

Note: This is not an exhaustive list, just a sample.

The following is a simplified subset of the process model in Appendix 15 First Cut Process Model Cyber War – complete. This model is used to illustrate how this technique and enterprise architecture approach could be used in analysing the essential processes of a cyber war organization, such as US Cyber Command.

There are two sets of missions. One is a defensive mission and the other one is an offensive mission. The defensive mission would require some infrastructure support such as “network-to-defend-a-network”, deployed sensors, monitoring, reporting, analysing, and managing systems etc. Usually there would be a national or a domain specific Cyber Operations Centre staffed with experts 24x7.

The Cyber Operations Centre would monitor the status and analyze anomalies and events. The analysts and other experts would try to attribute the attacks and initiate counter measures. Counter measures may include active defence, counter attack in other words. The counter attack may be cyber-to-cyber, cyber-to-physical, physical-to-cyber, or physical-to-physical.



The following narrative aims to explain the basic concepts of a very simplified model of cyber war. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique.

The following are some possible interpretations of the process model based on my understanding of the material I have researched up to this point.

This process model indicates that assets are monitored in real-time or near real-time. When anomalies are detected, an attempt is made to analyse the available data and the context of the anomaly, to determine if the anomaly and context information matches a known attack pattern. The implications of the detected anomaly or event with its context are extrapolated to estimate the potential impact and cascading possible implications almost in real time as an attack develops.

When certain conditions are met, such as attack pattern matching, linking an attack to specific assets and states, and depending on the rules of engagement, the active defence plan could be initiated. If the rules of engagement require, and the situation warrants it, a counter attack is initiated and monitored.

Another facade of Cyber Operations is its support role for other dimensions of the armed forces and law enforcement organizations. This support role is in deploying cyber attack(s) to the relevant capabilities of adversaries to provide an advantage for the other dimensions friendly armed forces, secret services, and law enforcement agencies.

All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

4.2. Cyber Intelligence, Espionage and Subversion

Cyber Intelligence is a very easy and cost effective way of collecting intelligence (open source) over the internet. It is usually the first activity for any cyber offence or assault.

Some of the simplest attack techniques e.g. password guessing or social engineering are based on gathering intelligence on the internet. The websites of the target organization, social networking sites about the target people and search engines are sources of very rich intelligence.

Cyber Espionage -covert and illegal (including covert operations e.g. green ops, black ops, sabotage, insurgency, misinformation war, subversion), is using hacking or penetration testing process, techniques, and tools to steal sensitive and confidential or secret data.

Furthermore, today an intelligence and espionage organization requires top-notch information security capabilities and hacking skills for Cyber Intelligence and Espionage or for subversive operations. [138 pages 103 to 109] Attacks not always perpetrated by foreign states but sometimes by foreign non-state actors or foreign organizations [157]

Misinformation War emerges as the preferred technique to subvert, especially by democratic states. The following quote emphasizes the point of view of some states and organizations.

“Deception is a state of mind and the mind of state”

James Jesus Angelton³,
Head of CIA Counter Intelligence
1954 – 1974 [127, 128, 129]

Unfortunately most of the counter intelligence organizations remain ineffective and weak when defending against such assaults. Some additional points regarding Cyber Counter Intelligence are in [108].

Categorized by General Michal Hyden as Cyber-on-the Cyber exploits [106], some real life examples of Industrial and Cyber Espionage are provided in Appendix 23. Industrial Espionage Notable cases. [144]

³ The founder of Gladio subversive organization starting with Italy, and rest of the other NATO countries later.

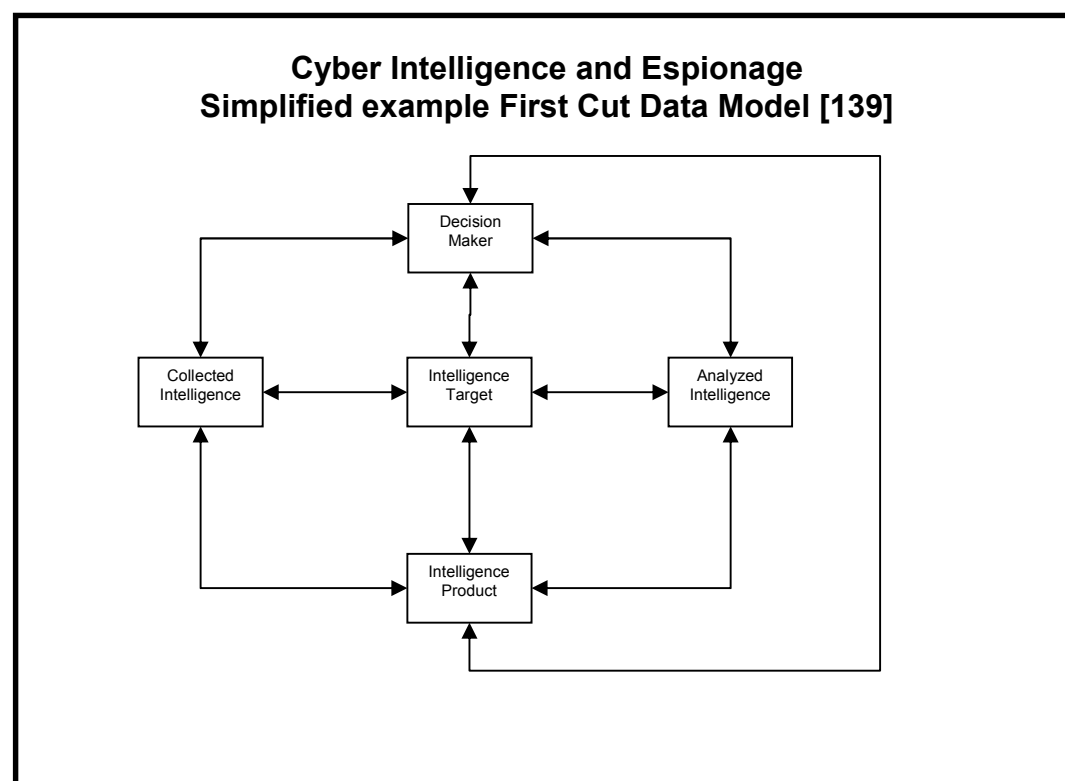
4.2.1 The Objectives of Intelligence, Espionage and Subversion Operations

Based on my investigation of multiple sources, the following emerges as high-level objectives of Intelligence and Espionage activities. [123, 137, 138]

- Avoid strategic surprise
- Serve as a source of organizational memory –a knowledge repository- to states where policy makers come and go
- Provide deep expertise in relevant issues, countries, actors, etc.
- Assist and enable the policy makers
- Protect confidentiality of data
- Protect the confidentiality of sources of intelligence – informants, whistle blowers, double agents, assets developed in other organizations or countries
- Protect confidentiality of intelligence requirements or needs
- Protect confidentiality of espionage methods

One can observe from the above intelligence and espionage objectives, that there is quite a bit of overlap with Information Security. The cyber space is a significant zone of conflict. [138 pages 103 to 109] [157] [127, 128, and 129] [108]

4.2.2 First Cut Data Model



The following narrative aims to explain the basic concepts of a very simplified model of cyber intelligence, espionage, and subversion. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique.

Overview of the some of the Entity Types:

This data model is based on a “Target Centric Approach” to intelligence rather than a traditional Intelligence Cycle approach.

This approach requires everyone from different perspectives to work on the entity type ***Intelligence Target***. They build up the picture and add to the contents from different perspectives over time. The entity type ***Intelligence Target*** is like a magical shoebox to store facts and knowledge. The entity type ***Decision Maker*** represents the data about the decision maker or policy maker. This may be a set of requirements, questions, feedback etc.

The ***Collected Intelligence*** represents the raw data and facts about a specific ***Intelligence Target***. The ***Analyzed Intelligence*** represents the analysis of ***Collected Intelligence***, but it is not produced as an ***Intelligence Product*** yet. These are some of the possible interpretations of the entity types.

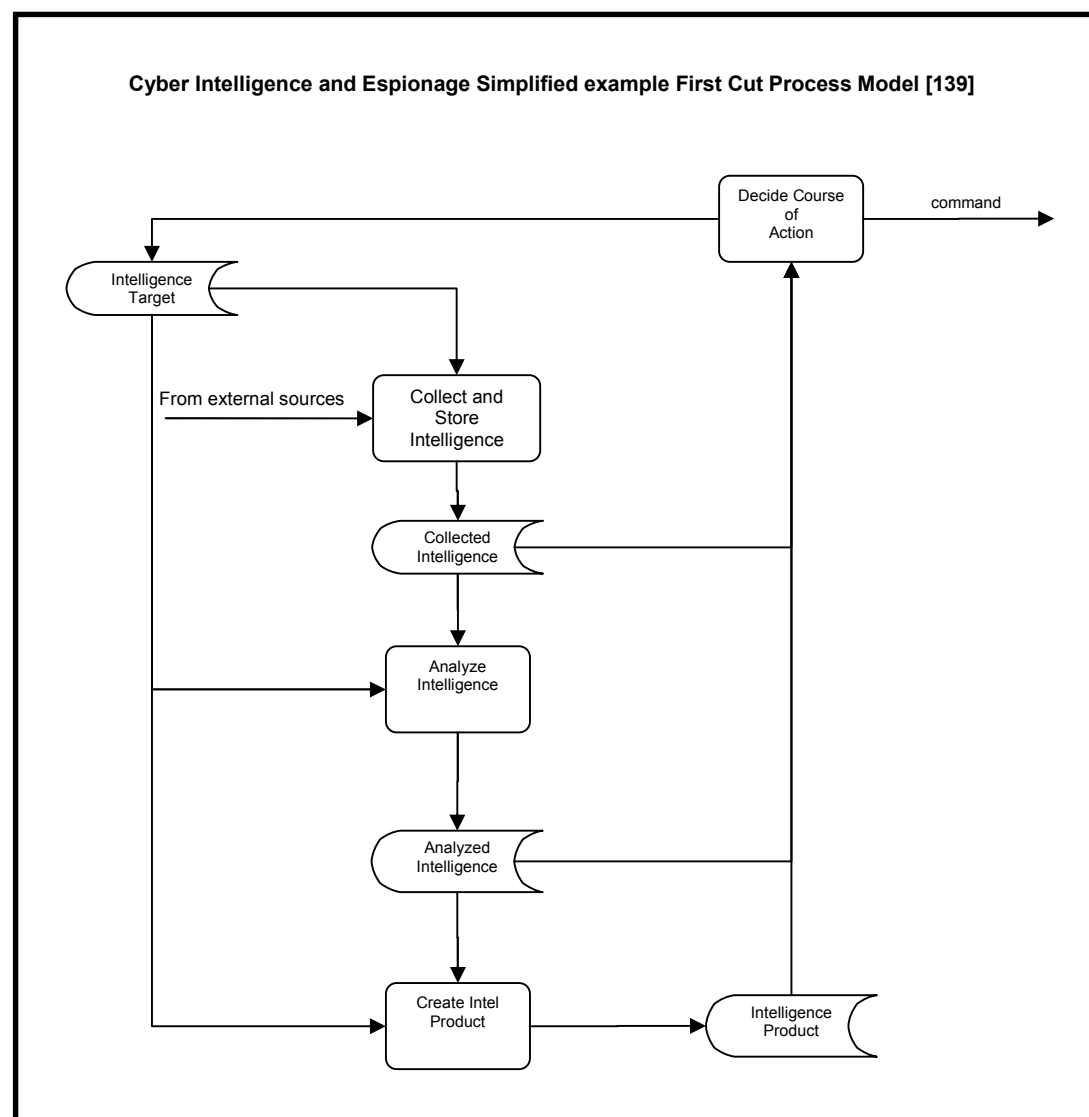
Overview of the some of the Relationships:

The relationship between ***Decision Maker*** and ***Intelligence Target*** represents the targets which that decision maker is interested in or may be interested in. In a full-blown model, the strength of the relationship or type of relationship, or relationship attributes may indicate the importance or priority of the target.

The relationship between the ***Intelligence Target*** and the ***Collected Intelligence*** represents the collected raw unanalyzed intelligence about the specific intelligence target. This relationship gives everyone an opportunity to access the raw intelligence without waiting for analysis or production. This is an improvement over a classical intelligence cycle approach, which gives everyone an opportunity to see the facts behind the analysis and intelligence product. These are some possible interpretations of the relationships.

All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

4.2.3 First Cut Process Model



The following narrative aims to explain the basic concepts of a very simplified model of cyber intelligence, espionage, and subversion. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique.

This process model is based on a “Target Centric Approach” to intelligence rather than the traditional Intelligence Cycle approach. This approach requires everyone from different perspectives to work on the data store **Intelligence Target**. They build up the picture and add to the contents from different perspectives over time.

The ultimate objective is to enable and initiate decision-making; this is represented with the process box **Deciding Course of Action**. The intelligence requirement for **Deciding Course of Action** or the interests of the decision makers are represented by the data store **Intelligence Target**. The **Collect and Store Intelligence** process uses data contents of the **Intelligence Target** data store to determine how to prioritize intelligence collection activities and what intelligence to collect.

What makes this approach unique compared to other intelligence approaches is that the data stored in **Collected Intelligence**, **Analyzed Intelligence**, and **Intelligence Product** data stores are available to the **Decide Course of Action** process all the time.

I am assuming the rest of the processes are obvious and do not require any explanation. All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

4.3. Cyber Crime

4.3.1 The Objectives of Cyber Crime Organizations

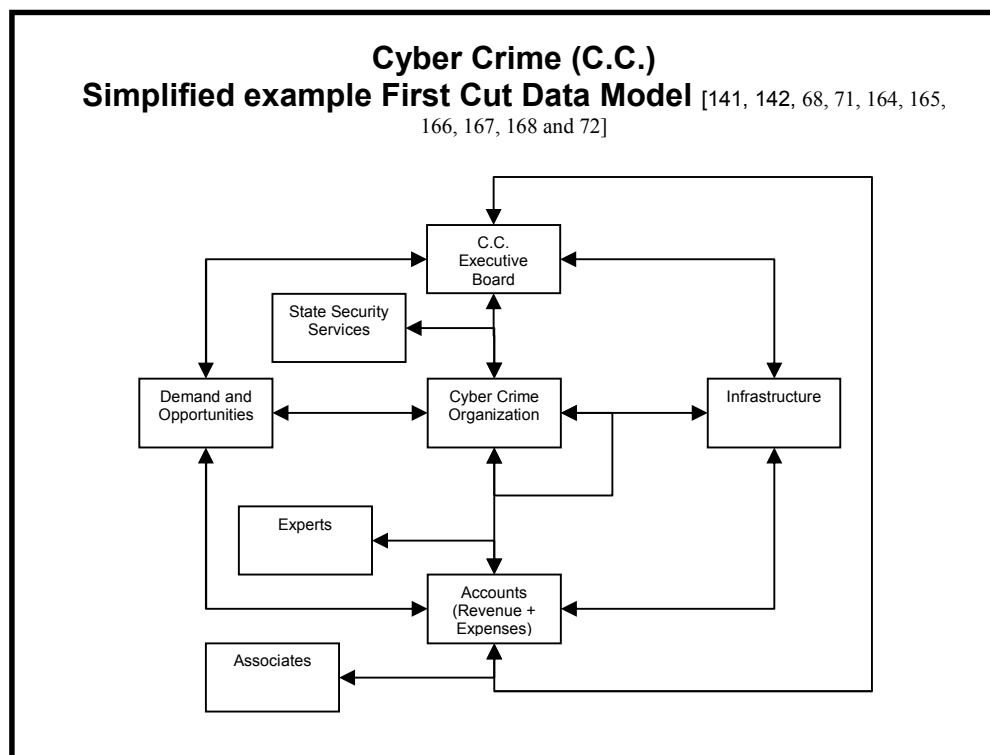
According to the sources reviewed, the primary objective of a cyber criminal organization is profit, but there are also secondary objectives too. The following is a consolidated list of objectives for cyber crime organizations: [141, 142, 68, 71, and 72]

- Protection from the law enforcement
- Profit or Financial Gain [141 page 49 – 51 and Appendix A Tables 3 and 4 in Appendix A]
- Material gain e.g. botnets, advanced crimeware, crime infrastructure, valuable data, bulletproof hosting
- Protection of markets and territory – protection of monopolistic status

The resources reviewed suggest that there are two different types of cyber crime business models or operations. The first kind of cyber crime business is a passive support role, providing the infrastructure such as bulletproof internet services and criminal tools only (crimeware). The second kind of cyber crime business is an active one, an actual execution of the attacks using the rented infrastructure and rented or purchased tools or crime ware.

I have not found any cyber crime case with cyber-on-physical assault or any offence intending to destroy or sabotage yet. Most likely, there is no market for it or risks are too high for them to accept. [142]

4.3.2 First Cut Data Model



The following narrative aims to explain the basic concepts of a very simplified model of cyber crime. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique.

Overview of some of the Entity Types:

The following are some of the possible interpretations of the entity types modelled in this section.

Based on my understanding of the material there are some types of ‘big bosses’ in Cyber Crime. (I have represented them with the entity type **C.C. Executive Board**. According to [141 Appendix A Tables 3 and 4]), regardless of the organizational structure of the crime organization, whether it is hierarchical, networked, an ad hoc temporary team formed for a project, or a loosely associated group of people who work collaboratively. There is always a set of core people which directs the activities of a criminal organization. Cyber Crime organizations in North America are less hierarchical and more entrepreneurial. On the other hand, the cyber crime organizations in Russia and Eastern Europe exhibit a more hierarchical structure, command control communication, and strong discipline enforcement.

An important point is, the cyber crime exists because there is either a demand for the products and services or an opportunity to make money. I have represented that concept as the entity type ***Demand and Opportunities***.

The hierarchical, network, or other forms of cyber crime organizational structure are modelled as the entity type ***Cyber Crime Organization***.

In Cyber Crime, it looks like there are areas of expertise and loose-associations. These concepts are represented as ***Experts*** and ***Associates*** in the model. The first entity type represents the skill base and different expertise areas. The second entity type models the people who like to work together in cyber crime projects or offences. They may interact with, or know each other only in cyberspace. Some may interact with or know each other in real life or only in cyber or both. This could be one of the variables to attribute their offences. [141 pages 49 – 51 Appendix A Tables 3 and 4]

Part of the Cyber Crime business model is that there must be a flow of money. There must be rules and processes that determine how the money is controlled and accounted for. This is the most important aspect of the business model. This aspect is represented as ***Accounts (Revenue and Expenses)*** entity type in the data model.

Overview of some of the Relationships:

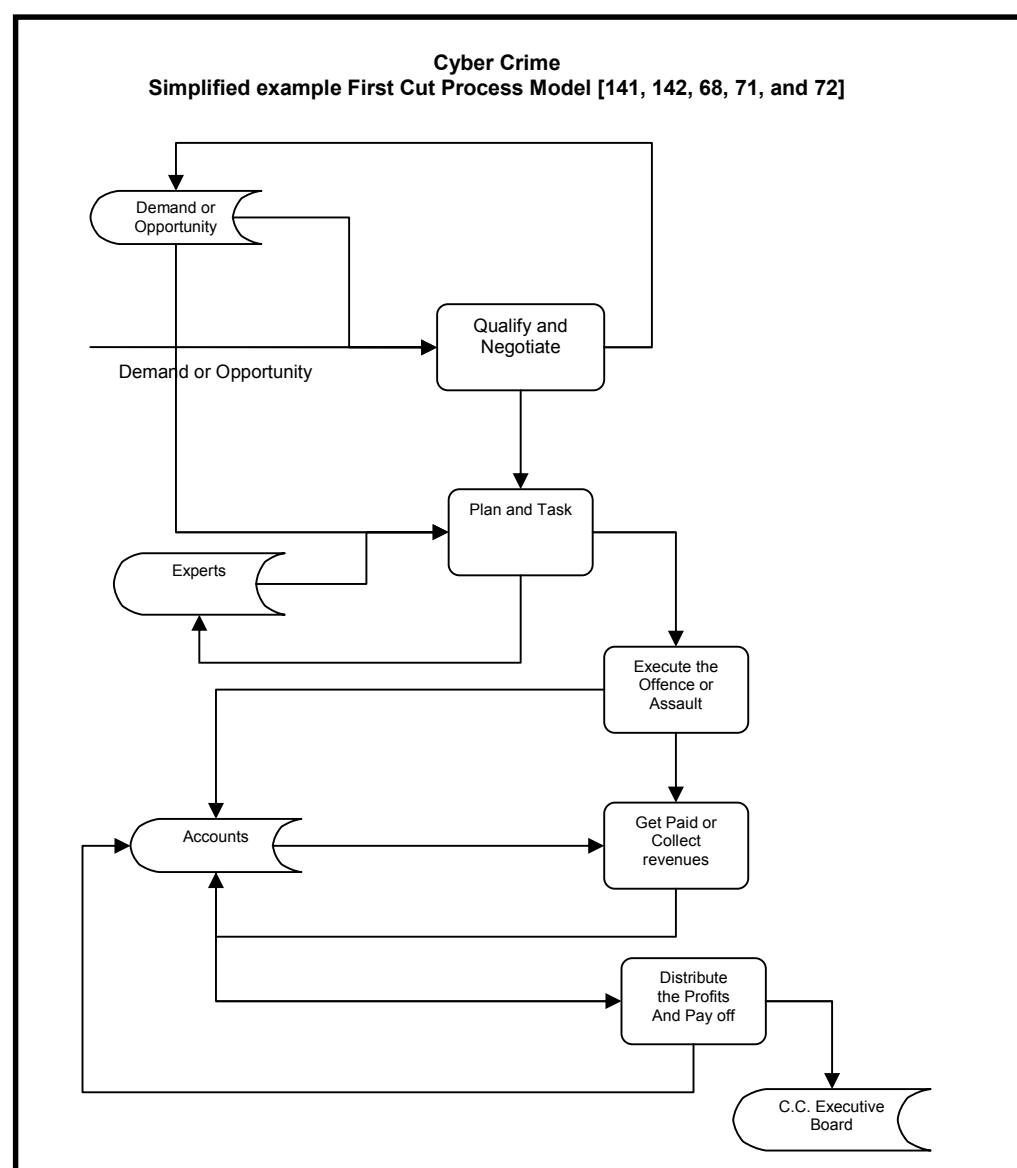
The relationships from entity type ***Cyber Crime Organization*** to entity types ***C.C Executive Board***, ***Infrastructure***, ***Accounts***, ***Experts***, ***Demands and Opportunities*** represent relationships with different time horizons and longevity. Existence of ***Infrastructure*** may indicate long-term investment and desire to exist for a long period of time. These are some possible interpretations of the relationships, which should be investigated and verified by the experts in a full-scale enterprise architecture project.

The relative strength of relationships between entity type ***State Security Services*** and ***Cyber Crime Organization*** and the relationship between ***the C.C. Executive Board*** and ***Cyber Crime Organization*** could be a significant indicator of who is in charge and when. This could be a useful relationship to explore further and collect information from all means possible, as part of an attribution analysis.

All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

The real life examples of cyber criminal organizations are provided in Appendix 44. Known Cyber Criminal Organizations and in references [158, 159, 160, and 161]

4.3.3 First Cut Process Model



The following narrative aims to explain the basic concepts of a very simplified model of cyber crime. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique.

These are some possible interpretations of the process model. The Cyber Crime Value Chain starts with some form of portfolio analysis, qualifying the opportunities and negotiating the price and how the loot would be divided. These activities are represented as the process box **Qualify and Negotiate**.

The next step upon successful qualification and negotiation is **Plan and Task**. During a Plan and Task phase, it is possible to go back to a previous process, re-qualify, and renegotiate like in any other business. Typical targets according to [142] are outputs of

computer systems (print files too), stored data, unauthorized access to infrastructure for criminal use, unauthorized access to software and tools and secure criminal communication. All of these are considered Cyber-on-cyber offences or assaults. [142]

The actual criminal activity would then take place as depicted by the process **Execute the Offence or Assault**. The typical assault techniques employed by Cyber Criminals are Social Engineering, Multi Vector Attack, Malware, Phishing, bribing, and corrupting the law enforcement organizations. [141 Appendix A Table 3 and 4]

Also, during the criminal operations it is most likely that expenses regarding the project or operation could be tracked and recorded in the data store **Accounts**.

The most significant processes are **Get Paid or Collect Revenue** and **Distribute the Profits and Payoff**. The accountants and accounts of any criminal organization will be the most sought after prize for the competitors and for the law enforcement. Most likely it could be well protected and encrypted. A counter offensive could be getting access to accounting, banking, and customer data.

Obtaining protection from the law enforcement is vital for crime organizations. This is usually achieved by doing favours for the state security organization in Russia and China and in return receiving state protection. In other places this is mostly achieved by corrupting members of law enforcement organizations

As in all other models, the models, matrix analysis, and explanations are my interpretation of the material I have researched. The real life examples of cyber criminal organizations are provided in Appendix 44. Known Cyber Criminal Organizations and in references [158, 159, 160, and 161]

4.4. Conceptual Analysis: The Main Points -Summary

The objective of this chapter is to demonstrate how investigating the two columns of row 2 of Zachman's Framework could be used to analyse and represent knowledge of cyber struggle. The columns are What (Data) and How (Process). We have completed this investigation and created the models for Cyber War; Cyber Intelligence, Espionage, and Subversion and Cyber Crime.

We have created a first cut conceptual data model using an entity-relationship modelling technique and process models using a Data Flow Diagramming (DFD) technique. The data models identified and highlighted the most important concepts and relationships among those concepts for each subject matter. In the same way the process models identified and highlighted the most important processes, data flows, and data stores for each subject matter. We have discussed the high-level meaning and interpretation of the entity types, relationships, and organizational processes for each subject matter

We have completed our preparation work to establish the ground for the next chapter where we will use matrices to investigate the alignments and dependencies among these artifacts, specifically the objectives, entity types and processes for each subject matter.

5. Synthesis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework

There are three matrices in this chapter synthesising what we have discovered and analysed in the previous chapters. The aim of these matrices is to demonstrate the approach and how it could be implemented to the Cyber Offences and Assaults. It is not intended to prove any other point or conclusion, just to demonstrate the approach since the simplified models included in the previous chapters are not detailed and complete enough to support a solid conclusion about the subject matter. Due to limitations of time and space, detailed models could not be included or produced in the main body.

A detailed explanation of the approach used in this chapter is documented in [Appendix 45. Overview of the Approach: Synthesis](#)

The following are very simplified matrices to illustrate the approach I have created for this project based on the enterprise architecture methodology. Only small subset versions of these matrices are created to show a basic and mock-up demonstration of the technique. All the models, matrix analysis, and explanations are my interpretation of the material I have researched.

5.1.WHY: (Offence Types) (Objectives) x (Offence Types) (Objectives) Matrix – Sample

The following narrative aims to explain the basic concepts of a very simplified model of the subject matter. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique according to the project objectives.

In this matrix we are comparing similarities and differences of the objectives of different Offence Types. The Offence Types are Cyber War, Cyber Intelligence, Espionage and Subversion, and Cyber Crime. We have analysed these Offence Types in the previous chapters.

The (Offence Types) (Objectives) x (Offence Types) (Objectives) Matrix has identical rows and columns. Since the meaning of the similarity is the same from both directions, we only need the half of the matrix. We will use this matrix to show similarities and differences between the objectives of Cyber War, Cyber Intelligence and Espionage, and Cyber Crime. If there is a strong similarity between the Objectives of these Offence Types, then there is a strong case that the business or mission of these organizations are

similar too. The cell values would indicate the degree of conceptual similarity or a common parent objective.⁴

A very simple classification is chosen. The values in the cells are conceptually equal, conceptually similar, or conceptually different (no common parent objective). The symbol “☑” would indicate conceptually equal. The symbol “≈” would indicate conceptually similar. The symbol “⊗” would indicate the difference.

The following are basic matrices to illustrate the approach created for this project based on the enterprise architecture methodology.

⁴ When the objectives of an organization are modelled, the objectives of the organization could be represented as a hierarchy. The parent, a more generic objective, is decomposed into more detailed and specific child objectives (Management by Objectives) [155].

Objectives																	
			Cyber War (State on State)					Cyber Intelligence and Espionage					Cyber Crime				
			Replace boots on the ground (US)	Make up for the inferior armed forces relative to US (China and Russia)	Make up for the weak conventional armed forces relative to nonnuclear states. (Russia)	Reduce losses of conventional forces (US, Russia, China)	Cyber Defense	Strategic Intelligence	Misinformation War	Tactical Intelligence	Operational Intelligence	Sabotage Black Ops	Protection from law enforcement	Profit	Material Gain	Protection of Market share and Territory	
Objectives	Cyber War (State on State)	Replace boots on the ground (US)						☒	☒	☒	~	~	☒	☒	~	☑	
		Make up for the inferior armed forces relative to US (China and Russia)						☒	~	~	~	☑	☒	☒	~	☑	
		Make up for the weak conventional armed forces relative to nonnuclear states. (Russia)						☒	~	~	~	☑	☒	☒	☑	☑	
		Reduce losses of conventional forces (US, Russia, China)						☒	~	~	☑	☑	~	~	~	☒	
		Cyber Defense						☒	☒	~	~	☒	☒	~	~	☑	
	Cyber Intelligence and Espionage	Strategic Intelligence												~	~	☒	☑
		Misinformation War												☒	☒	☒	~
		Tactical Intelligence												☒	☒	☒	~
		Operational Intelligence												~	☒	☒	☒
		Sabotage Black Ops												☒	☒	☒	~
	Cyber Crime	Protection from law enforcement															
		Profit															
		Material Gain															
		Protection of Market share and Territory															

5.2. WHAT: (Offence Types) (Objectives) x (Entity Types) Matrix – Sample

The following narrative aims to explain the basic concepts of a very simplified model of cyber war. The model is not intended to be complete or conclusive. The model is just to demonstrate the technique according to the project objectives.

There are two reasons to create this matrix. The first one is to verify the alignment between the entity types and objectives.

The second one is a comparison of conceptual and semantic similarities of entity types of different cyber Offence Types - Cyber War, Cyber Intelligence and Espionage, and Cyber Crime. This is my extension of the normal enterprise architecture methodology.

The WHAT Matrix is created to model the alignment or misalignment between Entity Types and the Objectives of the original cyber Offence Type the entity type to which it belongs. The columns indicate the Objectives of each cyber Offence Type and the rows indicate the entity types modelled in the sample data models for each cyber Offence Type in the previous chapter. The Cell values indicate support or alignment between objectives and entity types for the same Offence Type. In other words, how well for example, the entity types discovered for Cyber War aligns with or supports Cyber Intelligence and Espionage or Cyber Crime Objectives. This perspective of the model indicates similarity across the three Offence Types.

For the first view of the matrix model, where the alignment between the objectives and entity types of the same Offense Type is modelled, if an Entity Type is supporting an Objective then this alignment is indicated with the symbol “☑”; if it is not that then it is indicated with the symbol “☒”.

For the second view, where the entity types of different Offence Types are compared, the following distinctions are made: the symbol “☑” would indicate conceptually equal. The symbol “~” would indicate conceptually similar. The symbol “☒” would indicate the difference.

The following is a basic matrix to illustrate the approach created for this project based on the enterprise architecture methodology.

Objectives															
		Cyber War (State on State)					Cyber Intelligence and Espionage					Cyber Crime			
	Entity Types	Replace boots on the ground (US)	Make up for the inferior armed forces relative to US (China and Russia)	Make up for the weak conventional armed forces relative to nonnuclear states. (Russia)	Reduce losses of conventional forces (US, Russia, China)	Cyber Defense	Strategic Intelligence	Misinformation War	Tactical Intelligence	Operational Intelligence	Sabotage Black Ops	Protection from law enforcement	Profit	Material Gain	Protection of Market share and Territory
Cyber War (State on State)	Attack	☑	☑	☑	☑	?	☑	☑	☑	☑	☑	☑	~	~	☑
	Detection	☑	☑	☑	~	☑	☑	☑	~	☑	☑	☑	☑	☑	~
	Attack Pattern - observed	☑	☑	☑	~	☑	☑	☑	☑	☑	☑	☑	☑	☑	~
	Attribution	☑	☑	☑	☑	☑	☑	☑	~	☑	☑	☑	☑	☑	☑
	Attack Pattern - expected	☑	☑	☑	☑	☑	☑	☑	~	☑	☑	☑	☑	☑	☑
	Adversary – non-state	☑	☑	☑	☑	☑		☑	☑	☑	☑	☑	☑	☑	☑
	Puppet Master	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	~	~	~
Cyber Intelligence and Espionage	Intelligence Target	☑	☑	☑	☑		☑	☑	☑	☑	☑	☑	☑	☑	☑
	Decision Maker	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	~	~	~	~
	Collected Intelligence	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Analyzed Intelligence	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	~	~	☑
	Intelligence Product	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	~	~	~	☑
Cyber Crime	C.C. Executive Board	☑	☑	☑	~	☑	☑	☑	~	~	☑	☑	☑	☑	☑
	Cyber Crime Organization	☑	☑	☑	~	?	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Demand and Opportunities	?	☑	☑	?	☑	☑	☑	☑	☑	☑	?	☑	☑	☑
	Infrastructure	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Accounts	☑	☑	☑	☑	☑	☑	☑	☑	☑	?	☑	☑	☑	?
	Experts	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	Associates	?	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
	State Security Services	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑

5.3. HOW: (Offence Types) (Objectives) x (Process Matrix) – Sample

The following narrative aims to explain the basic concepts of a very simplified model of cyber war. The model is not intended to be complete or conclusive. The models are just to demonstrate the technique according to the project objectives.

There are two reasons to create this matrix. The first one is to verify the alignment between the processes and the objectives.

The second one is to compare the conceptual and semantic similarities of the processes belonging to different Offence Types - Cyber War, Cyber Intelligence and Espionage, and Cyber Crime. This is my extension of the normal enterprise architecture methodology.

In other words, how well for example the processes discovered for Cyber War aligns with or supports the Cyber Intelligence and Espionage or Cyber Crime Objectives. This perspective of the model indicates similarity across the three Offence Types.

The HOW Matrix is created to model the alignment or misalignment between Processes and the Objectives of the same cyber Offence Types - Cyber War, Cyber Intelligence and Espionage, and Cyber Crime. The columns indicate the Objectives of each cyber Offence Type and the rows indicate the processes modelled in the sample process models included in the previous chapter.

A very simple classification is chosen.

For the first view of the matrix model, where the alignment between the objectives and process of the same Offense Type is modelled, if a process is supporting an Objective then this alignment is indicated with the symbol “☑”; if it is not that then it is indicated with the symbol “☒”.

For the second view, where the processes of different cyber Offence Types are compared, the following distinctions are made: the symbol “☑” would indicate conceptually equal. The symbol “≈” would indicate conceptually similar. The symbol “☒” would indicate the difference.

The following is a basic matrix to illustrate the approach created for this paper based on the enterprise architecture methodology.

Objectives															
		Cyber War (State on State)					Cyber Intelligence and Espionage					Cyber Crime			
	Processes	Replace boots on the ground (US)	Make up for the inferior armed forces relative to US (China and Russia)	Make up for the weak conventional armed forces relative to nonnuclear states. (Russia)	Reduce losses of conventional forces (US, Russia, China)	Cyber Defense	Strategic Intelligence	Misinformation War	Tactical Intelligence	Operational Intelligence	Sabotage Black Ops	Protection from law enforcement	Profit	Material Gain	Protection of Market share and Territory
Cyber War (State on State)	Monitor Status of Assets	☒	☒	☒	☒	☒	☒	☒	☒	☒	?	☒	☒	☒	☒
	Detect Attack Pattern	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Attribute the Hostile Attack	☒	☒	☒	?	☒	?	☒	☒	☒	☒	☒	☒	☒	☒
	Initiate Counter Attack	☒	☒	☒	☒	☒	?	☒	?	?	☒	☒	☒	☒	☒
Cyber Intelligence and Espionage	Collect and Store Intelligence	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Analyze Intelligence	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	?	☒	☒	☒
	Create Intel Product	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	?	☒	☒	☒
	Decide Course of Action	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	?	☒	☒	☒
Cyber Crime	Qualify and Negotiate	☒	☒	☒	☒	☒	☒	☒	☒	☒	?	☒	☒	☒	☒
	Plan and Task	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Execute the Offence or Assault	☒	☒	☒	☒	?	☒	☒	☒	☒	☒	☒	☒	☒	☒
	Get Paid or Collect revenues	☒	☒	☒	☒	☒	☒	?	☒	☒	☒	☒	☒	☒	☒
	Distribute the Profits and Pay Off	☒	☒	☒	☒	?	☒	☒	☒	☒	☒	☒	☒	☒	☒

6. Conclusion

6.1. The Purpose of this Project

The major motivation behind this project is to create a reference blueprint for the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime. The purpose of the blueprint is to contribute to the security of citizens of smaller free and independent states and to enhance the cyber deterrence capabilities of states such as Latvia, Lithuania, Georgia, Ukraine, and Moldavia. This project is only a very humble beginning. I hope to build on this foundation. The intermediate goals are to:

- Establish a foundation to build capabilities in Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime fighting
- Explore the possibility of using software engineering models as an aid to represent knowledge
- Provide training about the subject matter

6.2. The Main Findings

It is demonstrated with the sample models, that a very high level blueprint of the foundation for enterprise architecture is established. The data modelling, process modelling, and matrix analysis are effective tools to analyse and represent knowledge about the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime.

As one would observe from the sample data, process, and matrix models, there are significant similarities and overlaps among the three subject areas. These models, anecdotal evidence, and materials researched, indicate a critical need to integrate the capabilities of law-enforcement, secret services, and military with clearly defined responsibilities. Common integrated enterprise architecture for the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime is invaluable in building cyber capabilities and training programs.

It is difficult to differentiate between crime and attack. It is also difficult to differentiate between cyber espionage attack or cyber-on physical destructive attack. Furthermore, to complicate things, a multi-vector persistent attack could start as cyber crime, turn into cyber espionage and lay the ground work for a catastrophic cyber attack.

Over multiple phases of an attack, a simple cyber incident event could be transferred from being the responsibility of law-enforcement, to the secret services or to the military for active defence. This near real-time seamless transfer is critical in cyberspace. These capabilities require a common integrated enterprise architecture.

The False Flag Operations are a preferred attack tactic. The Cyber weapons and attacks are emerging as new tools for covert attacks and covert wars to undermine states, companies, or organizations. Cyber weapons and attacks offer two distinct advantages:

- Plausible deniability by a state via the use of non-state actors
- Almost no physical, digital evidence or other evidence is left behind for a decisive attribution to a state, especially when the territories and assets of intermediary states are used.

The answer to the question of how to build an effective Cyber Warfare capability is answered at a very high level.

- Align the bulk of the offensive and defensive capabilities with the Cyber Intelligence, Espionage, and Sabotage organization.
- deploy operational offensive and defensive capabilities with the dimensions of the armed forces
- assign the initial detections, impact assessment, and attribution to the law-enforcement for civilian and non-military infrastructure
- establish an integrated common architecture and platform for cyber defence and cyber offence systems, tools, procedures and techniques for all of the organizations
- ensure that seamless near real time incidents data could be shared and jointly analysed, similar to “target-centric-intelligence”.

The current reality requires the citizens to have to defend themselves and their country. The legitimacy of war, espionage, and crime are very subjective. From one perspective, what is crime against humanity; from another perspective it is acceptable collateral damage. The implications of this lack of a common moral view and lack of common legitimacy standards for the time being is boiling over to the website attacks. But, as frustrations fester more over the coming decades due to perceived injustices, these attacks could easily take the form of successful cyber-on-physical attacks.

6.3. The Main Results

6.3.1 Results from the Synthesis Matrices

In this subsection 6.3, we have mainly answered three questions.

1. What is the degree of similarity among the Objectives of :
 - Cyber War
 - Cyber Intelligence, Espionage, and Subversion
 - Cyber Crime?
2. What is the degree of alignment and support provided by the entity types for the Objectives of other cyber Offence Types?
3. What is the degree of alignment and support provided by the processes for the Objectives of other cyber Offence Types?

6.3.2 The Motivations: The WHY Matrix - What is the degree of similarity among the Objectives⁵?

We have focused on the motivation (WHY) mostly in the first row of Zachman's Framework. If most of the objectives of Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime are the same or similar, this could be interpreted as a strong similarity among the Cyber War, Cyber Intelligence, and Cyber Crime organizations.

The common motivation behind Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime appears to be the same or very similar. The purpose of Cyber Operations is to gain advantage over adversaries in the following areas:

- Economic - profit, market share, resources
- Political - influence, control, military superiority
- Military – reduce losses, make up for strategic weakness, compensate for tactical inferiority

Support for this conclusion is provided in the section below.

In the WHY Matrix we have observed the following:

The Cyber War and Cyber Intelligence and Espionage

The similarity measure of the objectives between the Cyber War and Cyber Intelligence and Espionage is 16 out of 25.

The difference measure of the objectives between the Cyber War and Cyber Intelligence and Espionage is 9 out of 25.

This indicates that the objectives of the Cyber War and Cyber Intelligence and Espionage are more similar than different. The implication of this is that there are opportunities to integrate and consolidate the infrastructure, operations, and organizations of Cyber War and Cyber Intelligence and Espionage to achieve a greater level of effectiveness and efficiency.

The Cyber War and Cyber Crime

The similarity measure of the objectives between the Cyber War and Cyber Crime is 12 out of 20.

⁵ The hierarchy of objectives of the current models is kept at a single level. There are two reasons for this. The first reason is to keep the sample matrix simple. The second reason is that we do not have more in-depth knowledge at this moment to specify a complete hierarchy or knowledge to compare them.

The difference measure of the objectives between the Cyber War and Cyber Crime is 8 out of 20.

My interpretation of the above measures is that there is similarity between cyber war and cyber crime. Often those involved collaborate e.g. in Russia and China to take advantage of the plausible deniability; state organization's need disguise of cyber crime organizations as we have seen in many examples e.g. attack on Estonia and Georgia.

The Cyber Intelligence and Espionage and Cyber Crime

The similarity measure of the objectives between the Cyber Intelligence and Espionage and Cyber Crime is 7 out of 20.

The difference measure of the objectives between the Cyber Intelligence and Espionage and Cyber Crime is 13 out of 20.

The above measures indicate a difference in the objectives of the Cyber Intelligence and Espionage and Cyber Crime.

This could be due to simplified modelling or faulty cell values. Based on anecdotal evidence, it is claimed that there is strong collaboration between state security organizations and cyber crime organizations in Russia and China.

The overall measurement of similarity is 35 out of 65 and difference is 30 out of 65 in all of the Offence Types. This implies a degree of similarity among the objectives of the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime.

6.3.3 The Organizational Concepts and Data: The WHAT Matrix - What is the degree of alignment and support provided by the entity types?

The purpose of conceptual data models is to understand and document the concepts and terminology used for each of the cyber offence and assault areas separately. According to the enterprise architecture practice, the conceptual data models constitute the bedrock foundation of any business or organization. In the long-run, the foundation of the conceptual data models would not change, unless the organization changes the industry it is in. Based on this principle, if we could demonstrate similarity⁶ among the data models in Chapter 4, then we can assert that there are similarities among these organizations or their missions.

⁶ If most of the entity types of Cyber War, Cyber Intelligence and Espionage, and Crime are the same or similar, this could be interpreted as a strong similarity among Cyber War, Cyber Intelligence, and Cyber Crime. Also see Normalization Rules, Relational Algebra C. J. Date

When there are conceptual or semantic similarities among entity types belonging across multiple businesses or missions, this would be considered a strong indication that these businesses or missions are the same. Furthermore, in these situations there is an opportunity to integrate business or organizational practices and systems for greater efficiency and effectiveness. This is commonly referred to as breaking down the silos. The implication is a common data architecture which could be implemented for Cyber War; Cyber Intelligence, Espionage, and Subversion; and Cyber Crime organizations.

Ideally this comparison should be completed at a representative data element level, unique identifier level, and entity type level by comparing the organizational definitions of the entity type to entity type.

In the WHAT Matrix we have observed the following:

The overall measurement of similarity is 196 out of 280 and difference is 65 out of 280 in all of the Offence Types. This implies a degree of similarity among the entity types of the Cyber War, Cyber Intelligence and Espionage, and Cyber Crime.

This indicates a very strong similarity of the businesses they are in or the missions they are trying to fulfill since these organizations share the same the concepts and terminology used in describing what their business or organization is all about. In other words these organizations share the same DNA.

6.3.4 The Organizational Process and Value Chain: The HOW Matrix - What is the degree of alignment and support provided by the processes?

First Cut Process models are created to understand and describe the conceptual organizational processes independent of organizational structure, specific technology, or systems. The aim is to visually model the organizational processes using a Data Flow Diagramming technique [18, 19].

The HOW Matrix relates organizational processes to organizational objectives. The processes modelled in each specific area are related to the objectives of that area first and then the objectives of other areas.

Support or alignment across different cyber Offence Types indicates process similarity. Inversely, the lack of support or alignment could be an indication of differences among cyber Offence Types.

When there are process similarities across multiple businesses or missions, this could be considered a strong indication that these businesses or missions are the same. If

most of the processes of Cyber War, Cyber Intelligence and Espionage⁷, and Crime are the same or similar, this could be interpreted as a strong similarity among the Cyber War, Cyber Intelligence, and Cyber Crime organizations.

Furthermore, under these situations there is an opportunity to integrate business or organizational practices and systems for greater efficiency and effectiveness. This is commonly referred as breaking down the silos. In this case the same systems, strategies, tactics, techniques, tools could serve all of the Offence Types.

We have discovered similarities in the operational processes supporting Cyber War, Cyber Intelligence, Espionage and Subversion and Cyber Crime organizations. This is a good indication that they are in similar types of businesses or operations with similar operational procedures.

In the HOW matrix we have observed the following:

The overall measurement of similarity is 123 out of 182 and the difference is 43 out of 182 in all of the Offence Types. This implies a degree of similarity among the processes of the Cyber War, Cyber Intelligence and Espionage, and Cyber Crime.

The above measures indicate a very strong similarity of the processes enabling these organizations to fulfill their objectives or organizational missions. Therefore they are in the same industry and in the same business.

There are strong similarities between the organizational processes of Cyber War, Cyber Intelligence and Espionage, and Cyber Crime. This is a very strong indication that the business these organizations in are similar and they go about operating in similar ways.

Note:

Some of the common examples of the Crimeware or Cyber Weapons, Tools, Techniques, Tactics used for the cyber offences and assaults of any kind are as follows:

- Web Hacking – e.g. SQL injection, XSS, password cracking,
- Social Engineering
- Hacking Techniques and Tools
- Weaponized Malware – e.g. Stuxnet
- The context level approach is summarized in the First Cut Process Model

Even though most of the process details, techniques and tools are the same, there are differences between covert cyber offence and assault and overt cyber offence and assault.

⁷ Note: Since we have not included the defensive responsibilities of Cyber Intelligence and Espionage, e.g. keeping secrets, protection of confidentiality, those similarities do not appear on the matrix.

The Covert versus Overt Cyber Operations:

Most of the cyber offences and assaults have taken place as covert operations with plausible deniability e.g. CIA operation against a Soviet pipeline, Chinese espionage, Russian DOS / DDOS, etc. The only overt operation example available through open source documents is the US and NATO information operation against the Serbian air defense system.

6.3.5 Summary of Main Results from the Synthesis Matrices

We have seen above, cumulative evidence that there are strong similarities between the organizational objectives, organizational concepts, and organizational process of the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime organizations.

First we have observed a similarity of objectives. Then we have observed a similarity of concepts and terminology. Finally we have observed a similarity of the processes. All of these observations together indicates that a common enterprise architecture exists for Cyber War, Cyber Intelligence and Espionage, and Cyber Crime organizations.

6.3.6 Additional Observations and Conclusions

Even though we are not investigating the other columns of Zachman's Framework, the following are some observations regarding the WHO, WHEN and WHERE columns.

6.3.6.1 Who

During the data modelling activities we have also discovered who the players are in each cyber offence area. This understanding is abstracted to the following actors. This abstraction partially covers the (WHO) column of Zachman's Framework.

(WHO) The Actors are

- Nation State
- Non-State Actors acting on behalf of a state
- Self Organizing Groups – independent of any state (Hactivists)
- Individuals

6.3.6.2 When

Regarding timing, the sequence of activities, and organizational cycles the following observations are made:

(WHEN):

- Cyber Conflict becomes Cyber War: when hostilities are aggravated and may follow the following phases:
 - Misinformation and propaganda war: nonstop 7x24
 - Web defacing: as hate and anger increases

- DOS / DDOS; when tensions increase and armed conflict (hard attack or kinetic attack) is possible or imminent
- Computer Network Operations: Synchronized with the hard attack or kinetic operations (time and place)
- Organized Crime / Cyber crime: nonstop 7x24
- Espionage and Subversion (including misinformation war): nonstop 7x24

The implication of these points are that cyber war (state-on-state) may or may not occur at a given time, or may occur very infrequently but cyber espionage, cyber subversion, and cyber crime are happening every where all the time 7x24.

6.3.6.3 Where

Some aspects of the cyber space is unique and one such aspect is location or territory. We have left out some of the columns of Zachman's Framework, one of them being Location (WHERE), but as we have seen in the complete first cut data models this aspect is quite important for cyber operations. If the territory is clearly identified, this would implicate a state. This is not desirable for the attacking states in cyber space. Here is a quick overview of the important point of the (WHERE) column for cyber space.

Since the Attackers will most likely cover their tracks and obfuscate the real origin of the attack via cutoff organizations and intermediaries, the question of Attribution and forensic analysis are critical components of the active defence strategy.

Since the False Flag Operations are a preferred attack tactic, there two fundamental questions from the defender's perspective, especially when they are required to use active defence operations. From where is the attack originating? Is this an innocent intermediary or the real attacker?

(WHERE): The most significant Location aspects of Cyberspace are

- The False Flag Operations - Where is the attack really originating?
- Global
- Local to targeted area or (cyber operations in support of the law enforcement or the secret services)
- Operational theatre for the other dimensions of military
- Area targeted by hard attack or kinetic force

6.3.6.4 Additional Observations for Cyber War and Active Defence

Detecting an Attack and Attribution of the detected Attack is at the heart of legitimate cyber warfare where a state could invoke the right to self-defence under the UN Charter or International Criminal Court agreement –Sudan, Israel, and the US do not accept the jurisdiction of the court.

I think this would require couple of things.

- One possibility is similar to a UN Cease Fire. Observers in frontlines who are documenting evidence of who is shooting at whom and when, similarly an

international independent organization monitoring cyber space and cyber attacks could be established.

- An independent international organization responsible for conducting investigation and attribution of cyber attacks or
- a set of collaborating states, such as EU, Canada, Japan, New Zealand, Australia, UK who are independently monitoring, witnessing, and documenting cyber attacks to other states,
- even helping each other to triangulate the real source of the attack.

Regardless, this area will require major investment in digital forensics, network forensics, and network monitoring technologies. Almost real-time attribution by multiple states would be the ideal solution. In one sense, states should provide early warning and detection services free of charge to each other, like neighbourhood watch. However, in order to be credible, these must be developed similar to open source, with no dominating state or company, and no patent or commercial protection. So any one could verify the Attacks and the findings are freely used by all states. Otherwise, the idea of active defence and legally justifiable cyber counter attack will remain elusive. [139, 140]

In order to take full advantage of cyber military operations capabilities, it may be required to educate and train of all of the commanding officers in other dimensions (Navy, Air force, Army, and Marines) regarding cyber operational support capabilities. In order to take full advantage of cyber attack capabilities synchronized with hard or kinetic operations, such as cyber-on-cyber or cyber-on-physical, the commanding officers should be aware of them during the planning stages of their operations.

6.4. The Project Objectives and the Project Results

Topic Objectives: To establish a foundation to develop a Cyber War, Cyber Espionage, Cyber Counter Insurgency Course (s).

I believe a foundation for analysing, organizing knowledge, and teaching has emerged. I think this foundation could be used as teaching material in an introductory course.

However from an industrial perspective, I feel I have scratched the surface of these topics and more detailed research and work is required to bring a level of completeness required for industrial strength architecture.

Topic Objectives: To explore the possibility of using software engineering models as an aid to teaching Information Security Related Subjects.

I have found starting with the context and motivation first, as prescribed by Zachman's Framework, is very helpful to focus the research and modelling effort. This is especially true for such a very wide and complex area rich with technical details. Moreover representing the static and the long-range stable perspective in data models is very helpful in understanding the fundamental concepts and terminology of

the subject matter. I believe in understanding the simpler static parts before trying to understand the complex dynamic behaviour of a system.

Topic Objectives: To examine the subject matter from a new perspective

I am not certain about this; the simple answer would be a yes. Since I have only been able to use less than one fifth of the research material I have found, this may be true but it requires a more complete analysis of the all the open source material available.

Also, most likely internal and confidential works must have been carried out to develop a better enterprise architecture in this area.

Topic Objectives: To Apply knowledge and experience in enterprise architecture, data modelling, and process modelling to the topic.

This is clearly achieved and demonstrated at a higher level than typical industrial strength work. Given the time and space limitations, I believe expecting to achieve more than this is not realistic. A typical enterprise architecture project is usually assigned 3 to 7 people and would continue for about 12 – 18 months.

Scope Objectives: How to build an effective Cyber Warfare capability?

Only a very high level answer has emerged:

- Align the bulk of the offensive and defensive capabilities with the Cyber Intelligence and Espionage organization
- Deploy operational offensive capabilities with the dimensions of the armed forces
- Assign the initial detections, impact assessment, and attribution to the law-enforcement.
- All of the organizations should be using systems, tools, procedures and techniques that are integrated into a common architecture and platform,
- Where seamless near real time incidents data could be shared and jointly analysed; similar to “target-centric-intelligence”.

But lower level details of techniques, tactics, and tools are not covered due to lack of time and space. In the references and appendix sections I will try to point out some of the relevant resources.

Scope Objectives: How to conduct Cyber Espionage?

This is a two part question. The first part is how to conduct espionage. The first part is a more complex and elusive topic. The second part is how to conduct cyber espionage. I have only been able to cover the first part at a very high level. More detailed enterprise architecture analysis of the area is required. In one sense the second part is a simple technical question. I could re-word it as – How does one hack into a computer network and steal data?

The challenging part is the first part. One has to know what data to steal, how to verify and correlate the data, how to analyse and interpret it, and produce the finished

intelligence report. Then how would one make sure that the decision makers effectively use the knowledge provided by the intelligence organization?

Scope Objectives: How to conduct Cyber Counter Intelligence ? (Partially out of scope at this time)

Since I have run out of time and space, unfortunately, this area is not addressed in the report, even though I have found good open source material.

Scope Objectives: How to fight Insurgency using the Cyber Warfare Capabilities? (Partially out of scope at this time)

Since I have run out of time and space, unfortunately, this area is not addressed in the report, even though I have found good open source material.

6.5. Contribution to Knowledge

The answer to the question as to whether or not I have contributed to knowledge about Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime, I believe should be no.

I do not know everything there is to know about the topics, therefore the answer must be no. There must be and there are practitioners with years of experience, according to job requirements ads for government organizations and news of cyber crime activity. Obviously these experts and their management must know more than what is available in the open source documents.

I believe that I have not covered an adequate amount of open source resources to answer this question with any degree of confidence. I do not know the complete universe of open source knowledge to make any claim. Since I have only been able to use less than one fifth of the material I have found, a viable answer requires more complete coverage of the all the open source material available.

Also, one would think, it is most likely that internal and confidential work must be carried out or being carried out to develop a better enterprise architecture in the government organizations and agencies. I think I have just scratched the surface of the relevant knowledge. Since most of the government organizations and agencies would keep their work in this area confidential, as a civilian I could not answer this question.

I do know enterprise architecture methodology and techniques. I believe that in this project I have expanded its application to a different kind of problem and also enhanced the practice. I can at least claim a very unique application of enterprise architecture practice and Zachman's Framework.

I do not have access to facts on how much the relevant organizations know about the enterprise architecture practice. Most likely with the resources available to NSA, DOD, CIA or similar agencies; they could afford to hire the best and the brightest in the world.

Regarding different findings, my observations of what is announced by the policy makers in the US as Cyber Strategy seems to contradict the conclusions of this report.

The decisions the policy makers make are always quite puzzling and curious. The question however remains the same – What were they thinking? This is true of most of the organizational structure announced, appointments made, and cyber operations centres opened, especially in the USA. Why would one further destroy the unity of command and split responsibilities into more ill defined pieces and create more ill defined interfaces.

6.6. The Future of the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime

The value of a common integrated enterprise architecture of the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime

There would be many defence contractors and software vendors who would like to grab a share of this market. They would offer products and services for - the Cyber War; Cyber Intelligence, Espionage, and Sabotage organizations. If these products and services are developed independently, without conforming to a common architecture, the most likely scenario is that they will be incompatible and moreover their inter-operability may negatively impact each other. This would provide a set of new vulnerabilities and attack surfaces. On the other hand, if a common architecture is developed, it would not remain secret for long.

The other implication of a common integrated architecture is in the implementation strategy. Based on a common integrated architecture, it would be possible to develop a reuse framework and reusable components. One such framework could be for cyber operations centres, management, monitoring, detection, attribution capabilities or managing the cyber battlefield. The other framework could be a framework for cyber weapons and tools development. Similar research and development is expected to continue in crimeware and crime infrastructure development too. Most likely some crimeware products and services would emerge as market leaders.

It is quite possible that the cyber attack infrastructure and cyber weapons could reduce the cost of spending on armed forces since the material cost of manufacturing, distribution, or logistics is significantly cheaper for cyber weapons than hard (kinetic) weapons. Also, there would be the temptation to deploy them more often than a conventional dimension force because of the covert nature of cyber offences and assaults.

There are two social and political relevant trends.

The first trend is in the 21st century as we are left with less real democratic states than 20th century and states become openly more oppressive [156, 157]. The second trend is that cyber citizen groups and cyber activists have emerged. They are trying to expose and counterbalance oppressive states, such as assistance provided to Iranian, dissidents or Wikileaks.

It is most likely with hactivism and self organizing groups in cyberspace the political, would power shift to ordinary citizens.

Concluding Remarks:

I have demonstrated that the enterprise architecture methodology together with the sample models, the data models, process models, and matrix analysis are effective tools to analyse and represent knowledge about the Cyber War; Cyber Intelligence, Espionage and Subversion; and Cyber Crime.

I have realised an important aspect, which is not explicitly stated in any of the material I have researched. This important aspect is, over multiple phases of an attack, a simple cyber incident event should be transferred from being the responsibility of law-enforcement, to the secret services or to the military for active defence. This near real-time seamless transfer is critical in cyberspace. Because of the requirement for these capabilities, it is necessary to create a common integrated enterprise architecture.

The feasibility of developing such a common enterprise architecture from open source resources is positively demonstrated in this project. The set of models and artifacts provides a mechanism to represent knowledge, correlate knowledge, and integrate knowledge, and create knowledge. In my opinion, a beginning of viable solution has emerged. Out of this set of artifacts it is possible to build multiple roadmaps according to cyber battlefield requirements.

I believe it is critical to develop the enterprise architecture based roadmap to defend medium and small size democracies. I would like to continue this research and develop a detailed enterprise architecture for Cyber Crime; Cyber Intelligence, Espionage and Subversion; and Cyber War as either part of a PhD or R&D project.

This project is only a very humble beginning. I hope to build on this foundation in the near future.

References

No:	Reference		Type	Subject	Applicable Sections	Comments
[1]	IBM, Business Systems Planning, Information Systems Planning Guide, Fourth edition July 1984		Book	Enterprise Architecture	1.4 Methodology Overview	
[2]	Thomas E. Gallo, Strategic Information Management Planning, Prentice Hall, Englewood Cliffs, New Jersey 07632, 1988		Book	Enterprise Architecture	1.4 Methodology Overview	
[3]	Steven H. Spewak with Steven C. Hill, Enterprise Architecture Planning, Developing a Blueprint for Data, Applications and Technology, QED Publishing Group, 1992		Book	Enterprise Architecture	1.4 Methodology Overview	
[4]	S. H. Spewak, Enterprise Architecture Planning: Developing a Blueprint for Data, Applications and Technology, John Wiley & Sons, Oct 1993		Book	Enterprise Architecture	1.4 Methodology Overview	
[5]	A. B. Scott, An Introduction To Enterprise Architecture: Second Edition, AuthorHouse; Sep 2005		Book	Enterprise Architecture	1.4 Methodology Overview	
[6]	J. W. Ross, P. Weill, and D. C. Robertson, Enterprise Architecture as Strategy: Creating a Foundation for Business Execution, Harvard Business School Press; Aug 2006		Book	Enterprise Architecture	1.4 Methodology Overview	
[7]	T. Graves, Everyday Enterprise-Architecture: Sensemaking, Strategy, Structures and Solutions, Tetradian Books, April 2010		Book	Enterprise Architecture	1.4 Methodology Overview	
[8]	L. Kappelman, The SIM Guide to Enterprise Architecture, CRC Press; 27 Oct 2009		Book	Enterprise Architecture	1.4 Methodology Overview	
[9]	D. F.X. Mathaisel, Sustaining the Military Enterprise: An Architecture for a Lean Transformation, Auerbach Publications; Jan 2008		Book	Enterprise Architecture	1.4 Methodology Overview	An example of EA initiative in military
[10]	R. O. Tekes, "Linking Strategic Business Management Planning and Information Architecture based Strategic I/S Planning". Presentation at IBM Information Resource Management Interdivisional Technical Liaison, Toronto, October 1989		Conference proceeding	Enterprise Architecture	1.4 Methodology Overview	
[11]	J. A Zachman, A framework for information systems architecture, IBM Los Angeles Scientific Center, 1986		Report	Enterprise Architecture	1.4 Methodology Overview	The first publication about Zachman's Framework, which defines rows, columns, cells and relationships
[12]	C. O'Rourke, N. A. Fishman and W. Selkow, Enterprise Architecture Using the Zachman Framework (MIS), Course Technology Inc., April 2003		Book	Enterprise Architecture	1.4 Methodology Overview	

No:	Reference		Type	Subject	Applicable Sections	Comments
[13]	W H. Inmon, J Zachman and J Geiger, Data Stores, Data Warehousing and the Zachman Framework: Managing Enterprise Knowledge (McGraw-Hill Series on Data Warehousing & Data Management), Osborne/McGraw-Hill, Jun 1997		Book	Enterprise Architecture	1.4 Methodology Overview	
[14]	J. A Zachman, Zachman Framework: Enterprise Architecture Framework, Enterprise Architecture, View Model, Reification, Methodology, IBM, Betascript Publishing, ????		Book	Enterprise Architecture	1.4 Methodology Overview	
[15]	M. Flavin, Fundamental Concepts of Information Modelling, Yourdon Press Computing Series, Prentice Hall Inc., 1981.		Book	Data	1.4 Methodology Overview	
[16]	S. Shlaer and S J. Mellor, Object-oriented Systems Analysis: Modelling the World in Data (Yourdon Press Computing), Prentice Hall, April 1988		Book	Data	1.4 Methodology Overview	
[17]	S. Hoberman, D. Burbank and C. Bradley, Data Modeling for the Business: A Handbook for Aligning the Business with IT Using High-Level Data Models, Technics Publications, LLC, Mar 2009		Book	Data	1.4 Methodology Overview	
[18]	E. Yourdon, Modern Structured Analysis, Yourdon Press Computing Series, Prentice Hall Inc., 1989		Book	Process	1.4 Methodology Overview	
[19]	P. J. Plauger and T. DeMarco, Structured Analysis and System Specification (Yourdon Press Computing Series), Prentice-Hall, May 1979		Book	Process	1.4 Methodology Overview	
[20]	Mustafa Kemal Atatürk, http://en.wikiquote.org/wiki/Atat%C3%BCrk		Internet source wikiquote.org	Background	2. The Background and Continuum	
[21]	Dwight D. Eisenhower, http://en.wikiquote.org/wiki/Dwight_D._Eisenhower		Internet source wikiquote.org	Background	2. The Background and Continuum	
[22]	R. Walton, Why Information Security?, Walto-Mackenzie Limited, October 2010	Page 2 Preliminary Remarks	Lecture Notes	Background	2. The Background and Continuum	
[23]	F. Engels, The Origin of the Family, Private Property, and the State (1884), http://en.wikipedia.org/wiki/The_Origin_of_the_Family,_Private_Property_and_the_State		Book	Background	2. The Background and Continuum	
[24]	Author unknown, Introduction to Social and Political Sciences, METU Ankara, 1969 ?		Lecture Notes	Background	2. The Background and Continuum	

No:	Reference		Type	Subject	Applicable Sections	Comments
[25]	British Secret Intelligence in WWII, They were the English spies before "James Bond." They operated in the shadows with innocuous names like the Special Operations Executive, MI-5 and MI-6, but their missions were deadly serious. Amazing facts that are stranger than fiction in the storied history of Britain's intelligence service during the Second World War. Series 1 : Episode 3 on Content Film, Duration: 51:57; Published: 24/01/11 http://video.uk.msn.com/watch/video/british-secret-intelligence-in-wwii/1gekb7df4 http://www.amazon.co.uk/dp/B004GXY9N6/ref=nosim?tag=l076-21		DVD	Background	2. The Background and Continuum	
[26]	H. Melzig, Atatürk's political Testament, English Edition, Kenan Printing House Istanbul, 22 May 1943, Printed 99 copies		Research Paper	Background	2. The Background and Continuum	
[27]	Charter of United Nations, CHAPTER I: PURPOSES AND PRINCIPLES, UN, http://www.un.org/en/documents/charter/chapter1.shtml		International agreement	Background	2. The Background and Continuum	
[28]	Charter of United Nations,, CHAPTER VII: ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION, UN, http://www.un.org/en/documents/charter/chapter7.shtml		International agreement	Background	2. The Background and Continuum	
[29]	The International Criminal Court (ICC), http://www.icc-cpi.int/Menu/ICC/About+the+Court/		International agreement	Background	2. The Background and Continuum	
[30]	Article 8 bis Crime of aggression, The International Criminal Court (ICC), http://www.icc-cpi.int/NR/rdonlyres/336923D8-A6AD-40EC-AD7B-45BF9DE73D56/0/ElementsOfCrimesEng.pdf		International agreement	Background	2. The Background and Continuum	
[31]	W. Raleigh, England and the War, http://www.authorama.com/england-and-the-war-3.html		Moral and Political	Background	2. The Background and Continuum	
[32]	Might is right has become the Obama doctrine, http://www.thisislondon.co.uk/standard/article-23952628-might-is-right-has-become-the-obama-doctrine.do	Might Is Right	News	Background	2. The Background and Continuum	
[32a]	ALGERIE - Les Auschwitz de la France en Algerie, http://www.youtube.com/watch?v=RGLrdjkcLdM&feature=related		Internet source	Background	2. The Background and Continuum	

No:	Reference		Type	Subject	Applicable Sections	Comments
[33]	CRIMES DE LA FRANCE AU MAROC, http://www.youtube.com/watch?v=JwEXHJTmyM		News	Background	2. The Background and Continuum	
[34]	Judges Defer Decision on WikiLeaks Founder's Extradition, http://www.voanews.com/english/news/europe/Judges-Defer-Decision-on-WikiLeaks-Founders-Extradition-125505878.html		News	Background	2. The Background and Continuum	
[35]	Dominique Strauss-Kahn: 'Doubts' on maid's credibility, http://www.bbc.co.uk/news/world-us-canada-13986970		News	Background	2. The Background and Continuum	
[36]	M. Cronin, U.S. Cyber Strategy: The Perils of Deterrence, World Politics Review LLC., 10 Jun 2011, http://www.worldpoliticsreview.com/articles/9126/u-s-cyber-strategy-the-perils-of-deterrence		Briefing News	Direction	3. Analysis: Strategic Scope	
[37]	J. N. Hoover, U.S. Military Outlines Cyber Security Strategy, InformationWeek, July 14, 2011 04:01 PM, http://www.informationweek.com/news/government/security/231001814		News	Direction	3. Analysis: Strategic Scope	
[38]	J. Healey, Select Foreign Response to the U.S. International Cyber Strategy, Atlantic Council, May 31, 2011, http://www.acus.org/new_atlanticist/select-foreign-response-us-international-cyber-strategy		Blog	Direction	3. Analysis: Strategic Scope	
[39]	Wikipedia®, United States Cyber Command, http://en.wikipedia.org/wiki/United_States_Cyber_Command		Internet source	Direction	3. Analysis: Strategic Scope	
[40]	L. Page, US Cyber Command becomes 'fully operational', the Register, Posted in Enterprise Security, 4th November 2010 15:00 GMT, http://www.theregister.co.uk/2010/11/04/cyber_command_go/		News	Direction	3. Analysis: Strategic Scope	
[41]	U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010 http://www.stratcom.mil/factsheets/Cyber_Command/		Government	Direction	3. Analysis: Strategic Scope	
[42]	"New Cyber Warfare Branch Proposed". Blogs.govinfosecurity.com. 2009-03-25. Retrieved 2010-07-10.		Internet source	Direction	3. Analysis: Strategic Scope	
[43]	E. Nakashima (2010-03-19). "Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies". The Washington Post. Retrieved 2010-07-10.		Internet source	Direction	3. Analysis: Strategic Scope	
[44]	U.S. Cyber Command (USCYBERCOM or CYBERCOM), http://www.stratcom.mil/factsheets/cyber_command/		Government	Direction	3. Analysis: Strategic Scope	
[45]	Wikipedia®, United States Strategic Command, http://en.wikipedia.org/wiki/United_States_Strategic_Command		Internet source	Direction	3. Analysis: Strategic Scope	

No:	Reference		Type	Subject	Applicable Sections	Comments
[46]	United States Strategic Command, http://www.stratcom.mil/		Government	Direction	3. Analysis: Strategic Scope	
[47]	G. Conti and B. Surdu; "Army, Navy, Air Force, Cyber: Is it Time for a Cyberwarfare Branch of the Military;" Information Assurance Newsletter, Vol. 12, No. 1, Spring 2009, pp. 14–18 http://www.rumint.org/gregconti/publications/2009_IAN_12-1_conti-surdu.pdf .		Internet source	Direction	3. Analysis: Strategic Scope	
[48]	Wikipedia®, Cyberwarfare in the United States, http://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States		Internet source	Direction	3. Analysis: Strategic Scope	
[49]	Hancock, Bill. "Security Views." Computers & Security 18 (1999): 553-64. ScienceDirect. Web. 11 October 2009. < http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6V8G-463GSGP-2-1&_cdi=5870&_user=47004&_orig=search&_coverDate=12%2F31%2F1999&_sk=999819992&view=c&wchp=dGLzVlz-zSkWA&md5=a6d6590f9a8954864a1abbd91dd0a981&ie=/sdarticle.pdf >.		Internet source	Direction	3. Analysis: Strategic Scope	In 1998, in order for US and NATO to bomb Serbia successfully in Kosovo, the USA needed to hack the Serbian air defense system and trick the Serbian Air Traffic Control.
[50]	Wikipedia®, Space and Naval Warfare Systems Command, http://en.wikipedia.org/wiki/Space_and_Naval_Warfare_Systems_Command		Internet source	Direction	3. Analysis: Strategic Scope	
[51]	Space and Naval Warfare Systems Command, http://www.public.navy.mil/spawar/Pages/default.aspx		Government	Direction	3. Analysis: Strategic Scope	
[52]	P. Jackson, Meet USCybercom: Why the US is fielding a cyber army, BBC News, 09:27 GMT, Monday, 15 March 2010, http://news.bbc.co.uk/1/hi/technology/8511711.stm		News	Direction	3. Analysis: Strategic Scope	Their weapon of "precision disruption" has the potential to be more efficient, more effective, less damaging, less life-threatening than a kinetic weapon," he says. But as with pilots and warship commanders, as US cyber warriors get stronger, so may their potential adversaries.
[53]	Wikipedia®, National Security Agency, http://en.wikipedia.org/wiki/NSA		Internet source	Direction	3. Analysis: Strategic Scope	
[54]	NSA, http://www.nsa.gov/		Home Page	Direction	3. Analysis: Strategic Scope	
[55]	N. Doyle, Leak exposes NSA's 200 MW cyberwar centre, atomicnews, 21 Jun 2011, http://atomicnews.info/cyberwar/leak-exposes-nas-200-mw-cyberwar-centre/		Internet source	Direction	3. Analysis: Strategic Scope	
[56]	M. Pillsbury, CHINA'S MILITARY STRATEGY TOWARD THE U.S., A View from Open Sources, http://www.uscc.gov/researchpapers/2000_2003/pdfs/strat.pdf		Government	Direction	3. Analysis: Strategic Scope	

No:	Reference		Type	Subject	Applicable Sections	Comments
[57]	TheFreeDictionary, Revolution in Military Affairs, http://encyclopedia.thefreedictionary.com/Revolution+in+Military+Affairs		Internet source	Direction	3. Analysis: Strategic Scope	In 1997, the United States Army mounted an exercise code-named "Force 21", to test the application of digital technologies in warfare. The goal of Force 21 was to improve the communications and logistics through the application of computers and information technology generated in the private sector and adapted for military use.
[58]	D. M. Finkelstein, CHINA'S NATIONAL MILITARY STRATEGY, RAND.ORG, http://www.rand.org/pubs/conf_proceedings/CF145/CF145.chap7.pdf		Internet source	Direction	3. Analysis: Strategic Scope	
[59]	Reuters, US and China face vast divide on cyber issues, defenceWeb, Friday, 15 July 2011 12:14, http://www.defenceweb.co.za/index.php?option=com_content&view=article&id=17229:us-and-china-face-vast-divide-on-cyber-issues&catid=48:Information%20&%20Communication%20Technologies&Itemid=109	News	News	Direction	3. Analysis: Strategic Scope	For two years, academic experts from the United States and China have quietly held talks on cyber-security, straining to establish rules of the road in a realm that has proven a persistent irritant between the world's two largest economies.
[60]	IBD Editorials, A Cyber-Pearl Harbor On Horizon?, Investor's Business Daily, Inc., Posted 07/15/2011 06:42 PM ET, http://www.investors.com/NewsAndAnalysis/Article/578532/201107151842/A-Cyber-Pearl-Harbor-On-Horizon-.htm		Internet source	Direction	3. Analysis: Strategic Scope	
[61]	J. Fritz BS (St. Cloud), MIR (Bond), HOW CHINA WILL USE CYBER WARFARE TO LEAPFROG IN MILITARY COMPETITIVENESS, Culture Mandala, Vol. 8, No. 1, October 2008, pp.28-80, http://www.international-relations.com/CM8-1/Cyberwar.pdf		Magazine	Direction	3. Analysis: Strategic Scope	
[62]	Z. Rochner, Russia's Military Strategy, Global Power and Strategy Analysis: Know Your World, August 9, 2009, http://gpsanalysis.com/?p=25		Internet source	Direction	3. Analysis: Strategic Scope	
[63]	WAR.WIRE, New Russian military strategy names NATO as chief threat, www.spacewar.com , MOSCOW, Feb 5 (AFP) Feb 05, 2010, http://www.spacewar.com/afp/100205164908.2zmdxhbb.html		Internet source	Direction	3. Analysis: Strategic Scope	Since the 1991 Soviet collapse, Russian military planners have relied increasingly on the country's huge nuclear deterrent as the capabilities of its conventional forces have deteriorated. Efforts to develop a new military doctrine in recent years have coincided with plans for a radical modernisation of Russia's armed forces.

No:	Reference		Type	Subject	Applicable Sections	Comments
[64]	J. B. Spero, RUSSIAN MILITARY CHALLENGES TOWARD CENTRAL-EAST EUROPE, http://www.google.co.uk/url?sa=t&source=web&cd=29&ved=0CE4QFjAIOBQ&url=http%3A%2F%2Fkms1.isn.ethz.ch%2Fserviceengine%2FFiles%2FISN%2F118966%2Fchaptersection_singledocument%2Fabb08d-e14b-4d8f-b7eb-a081c9a628d9%2Fen%2FChapter_7.pdf&rct=j&q=%22russian%20military%20strategy%22&ei=tMshTo2jloaFhQf3zYTRAw&usg=AFQjCNG264VGMa350gac3xWYsHzBYCjgCA&cad=rja		Book chapter	Direction	3. Analysis: Strategic Scope	
[65]	Curzon, Contemplating Georgia, Part 4: Scrutinizing the Russian Military, ComingAnarchy.com, Posted on 8/28/2008, http://cominganarchy.com/2008/08/28/contemplating-georgia-part-4-scrutinizing-the-russian-military/		Blog	Direction	3. Analysis: Strategic Scope	
[66]	R. D. Kaplan, America's Elegant Decline, The Atlantic Monthly Group, November 2007 ATLANTIC MAGAZINE, http://www.theatlantic.com/magazine/archive/2007/11/america-8217-s-elegant-decline/6344/		Magazine article	Direction	3. Analysis: Strategic Scope	
[67]	C. M. Grabo, Anticipating Surprise: Analysis for Strategic Warning, University Press of America, Sep 2004, http://www.gpnsec.org/public/index.php?cmd=file&id=39_len		Book	Approach	3. Analysis: Strategic Scope	
[68]	Wikipedia®, Cyberwarfare in Russia, http://en.wikipedia.org/wiki/Cyberwarfare_in_Russia		Internet source		3. Analysis: Strategic Scope	“According to some reports, under SORM-2 Russian Internet service providers (ISPs) must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages and web use. The device, which has been estimated to cost \$10,000-\$30,000, must be installed at the ISPs expense. Other reports note that some ISPs have had to install direct communications lines to the FSB and that costs for implementing the required changes were in excess of \$100,000.”
[69]	Wikipedia®, SORM, http://en.wikipedia.org/wiki/SORM				3. Analysis: Strategic Scope	

No:	Reference		Type	Subject	Applicable Sections	Comments
[70]	Wikipedia®, Federal Security Service (Russia), http://en.wikipedia.org/wiki/Federal_Security_Service_%28Russia%29		Internet source		3. Analysis: Strategic Scope	<p>“Targeted killing</p> <p>In the summer of 2006, the FSB was given the legal power to engage in targeted killing, and hunt down and kill terrorism suspects overseas if ordered to do so by Russia's president.[33]</p> <p>In July 2006, Chechen militant Islamist Shamil Salmanovich Basayev, responsible for the 2002 Moscow theater hostage crisis that led to 129 civilian deaths and the 2004 Beslan school hostage crisis that led to 385 deaths, was killed in the village of Ekazhevo, in Ingushetia. The FSB, following him with a drone, spotted his car approach a truck laden with explosives that the FSB had prepared, and by remote control triggered a detonator that the FSB had hidden in the explosives.[34][35][36]</p> <p>The Russian ambassador to the United Nations, Vitaly Churkin, said:</p> <p>"He is a notorious terrorist, and we have very clearly and publicly announced what is going to happen to notorious terrorists who commit heinous crimes of the type Mr. Basayev has been involved in."[37]”</p>
[71]	Wikipedia®, Active measures, http://en.wikipedia.org/wiki/Active_measures		Internet source		3. Analysis: Strategic Scope	
[72]	J. Carr, Inside Cyber Warfare, O'Reilly Media Inc., 2010		Book	Cyber Conflict	5. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[73]	US Government, Jobs Site; search for Intelligence Specialists; http://jobsearch.usajobs.gov/search.aspx?q=INTELLIGENCE+SPECIALIST+%28OPERATIONS%29+&where=&brd=3876&vw=b&FedEmp=N&FedPub=Y		Government	Skills	Appendix: Skills	Future Research: Consolidating an Overview of Required Skills for future training programs
[74]	R. O. Tekes, “Enterprise Architecture as a critical component of Strategic Business Management”. Presentation at Enterprise Architecture Symposium (EAS), Toronto, March 29, 2010, Time: 10:45 AM EST,			Enterprise Architecture	1 Introduction - Methodology	Entire presentation is available upon request from otekas@gmail.com

No:	Reference		Type	Subject	Applicable Sections	Comments
[75]	Magna Carta, http://www.historylearningsite.co.uk/magna_carta.htm		Internet source	Context	2. The Background	The Magna Carta was signed in June 1215 between the barons of Medieval England and King John. "Magna Carta" is Latin and means "Great Charter". The Magna Carta was one of the most important documents of Medieval England. It was signed between the barons and John at Runnymede near Windsor Castle. The document was a series of written promises between the king and his subjects that he, the king, would govern England and deal with its people according to the customs of feudal law. Magna Carta was an attempt by the barons to stop a king - in this case John - abusing his power with the people of England suffering.
[76]	Magna Carta, http://en.wikipedia.org/wiki/Magna_Carta		Internet source	Context	2. The Background	Lord Denning described it as "the greatest constitutional document of all times – the foundation of the freedom of the individual against the arbitrary authority of the despot".[1] In a 2005 speech,
[77]	D. Danziger & J. Gillingham, "1215: The Year of Magna Carta"(2004 paperback edition) p278		Book	Context	2. The Background	
[78]	Wikipedia, Operation Gladio, http://en.wikipedia.org/wiki/Operation_Gladio		Internet source	Context	2. The Background	
[79]	C. Floyd, The New US Sponsored Gladio: Sword Play: Attacking Civilians to Justify "Greater Security", Centre for Research on Globalisation, www.globalresearch.ca , 20 February 2005, http://www.globalresearch.ca/articles/FLO502B.html		News	Context	2. The Background	"You had to attack civilians, the people, women, children, innocent people, unknown people far removed from any political game. The reason was quite simple: to force ... the public to turn to the state to ask for greater security."
[80]	Time Watch, BBC, Operation Gladio [BBC Timewatch, 1992] State-Sponsored Terrorism in Europe, http://www.youtube.com/watch?v=7fB6nVivJcM		Documentary	Context	2. The Background	
[81]	Time Watch, BBC, Operation Gladio [BBC Timewatch, 1992] State-Sponsored Terrorism in Europe, http://video.google.com/videoplay?docid=264709845600167246#		Documentary	Context	2. The Background	
[82]	R. Dallaire, Shake Hands With The Devil: The Failure of Humanity in Rwanda, Arrow (3 Feb 2005)		Book	Context	2. The Background	

No:	Reference		Type	Subject	Applicable Sections	Comments
[83]	Wikipedia, Lewis MacKenzie, http://en.wikipedia.org/wiki/Lewis_MacKenzie		Internet source	Context	2. The Background	The 2000 book The Lion, the Fox, and the Eagle by Carol Off, which devotes a third of its content to MacKenzie's role in Yugoslavia, claims that MacKenzie was willfully ignorant of the Bosnian political situation and was manipulated into being a vehicle of pro-Serb propaganda.[9] In 1993, investigative reporter and Pulitzer prize winning journalist Roy Gutman accused Mackenzie of receiving funds from "SerbNet", a Serbian-American lobbyist group. In response MacKenzie said he had done nothing unethical or improper, although UN officials criticised his "lack of judgment" in the matter.[10]

No:	Reference		Type	Subject	Applicable Sections	Comments
[84]	Wikipedia, Taksim Square massacre, http://en.wikipedia.org/wiki/Taksim_Square_massacre		Internet source	Context	2. The Background	<p>some 20 snipers were detained by the gendarmerie and handed over to the police. However, none of them appeared in the records of the police. This information comes from the prosecutor investigating the Taksim Square Massacre, Çetin Yetkin. He said that Lieutenant Abdullah Erim made the detentions and handed the detainees over to the police officers Muhsin Bodur and Mete Altan (who after the military intervention of 12 September 1980 worked in the political department of Istanbul Police HQ). Both officers rejected the claim that they had been involved.[8] Former Turkish prime minister Bülent Ecevit recalled he had learned of the existence of Counter-Guerrilla, the Turkish "stay-behind" armies for the first time in 1974.[13] At the time, the commander of the Turkish army, General Semih Sancar, had allegedly informed him the US had financed the unit since the immediate post-war years, as well as the National Intelligence Organization (Turkish: Millî İstihbarat Teşkilâtı, MIT). Ecevit declared he suspected Counter-Guerrilla's involvement in the 1977 Taksim Square massacre in Istanbul, The next year, the demonstrators were met with bullets. According to Ecevit, the shooting lasted for twenty minutes, yet several thousand policemen on the scene did not intervene. This mode of operation recalls the June 20, 1973 Ezeiza massacre in Buenos Aires, when the Argentine Anticommunist Alliance (aka Triple A), founded by José Lopez Rega (a P2 member), opened up fire on the left-wing Peronists. According to an article in the leftist pro-Kurdish Kurtuluş magazine,[14] MIT deputy chief Hiram Abas was present on the May Day massacre. (Swiss historian Daniele Ganser says that Abas was a CIA agent;[15] the CIA's station chief in Istanbul, Duane Clarridge, spoke glowingly of him.[16]) The Hotel International, from which the shots were fired, belonged to ITT Corporation, which had already been involved in financing the September 11, 1973 coup against Salvador Allende in Chile and was on good terms with the CIA. Hiram Abas had been trained in the US in covert action operations and as an MIT agent first gained notoriety in Beirut, where he co-operated with the Mossad from 1968 to 1971 and carried out attacks, "targeting left-wing youths in the Palestinian camps and receiving bounty for the results he achieved in actions".[14]</p>

No:	Reference		Type	Subject	Applicable Sections	Comments
[85]	http://www.businesssturkeytoday.com/ , Tens of thousands fill İstanbul's Taksim Square on May Day , http://www.businesssturkeytoday.com/tens-of-thousands-fill-istanbuls-taksim-square-on-may-day/		Internet source	Context	2. The Background	
[86]	Wikipedia, Minutemen, http://en.wikipedia.org/wiki/Minutemen		Internet source	Context	2. The Background	
[87]	ushistory.org, Minutemen, http://www.ushistory.org/people/minutemen.htm		Internet source	Context	2. The Background	
[88]	Wikipedia, Airbus affair, http://en.wikipedia.org/wiki/Airbus_affair		Internet source	Context	2. The Background	
[89]	CBC News, Mulroney-Schreiber affair, http://www.cbc.ca/news/canada/story/2009/03/27/f-mulroney-schreiber.html		Internet source	Context	2. The Background	
[90]	Wikipedia, Ergenekon (organization), http://en.wikipedia.org/wiki/Ergenekon_(organization)		Internet source	Context	2. The Background	
[91]	Wikipedia, Ergenekon (material evidence), http://en.wikipedia.org/wiki/Ergenekon_(material_evidence)		Internet source	Context	2. The Background	
[92]	G. H. Jenkins, Between Fact and Fantasy: Turkey's Ergenekon Investigation, http://www.silkroadstudies.org/new/docs/silkroadpapers/0908Ergenekon.pdf		Internet source	Context	2. The Background	
[93]	Wikipedia, Sivas massacre, http://en.wikipedia.org/wiki/Sivas_massacre		Internet source	Context	2. The Background	
[94]	YouTube, sivas madimak, http://wn.com/Sivas_Madimak		Internet source	Context	2. The Background	
[95]	Wikipedia, International Criminal Court, http://en.wikipedia.org/wiki/International_Criminal_Court#Membership		Internet source	Context	2. The Background	As of June 2011, 114 states are members of the court, including all of South America, nearly all of Europe and roughly half the countries in Africa.[8] Three of these states— <i>Israel</i> , Sudan and the <i>United States</i> —have " unsigned " the Rome Statute, indicating that they no longer intend to become states parties and, as such, they have no legal obligations arising from their former representatives' signature of the statute.[8][13]

No:	Reference		Type	Subject	Applicable Sections	Comments
[96]	G. Friedman, Never Fight a Land War in Asia, STRATFOR', March 1, 2011 0947 GMT, http://www.stratfor.com/weekly/20110228-never-fight-land-war-asia?utm_source=GWeekly&utm_medium=email&utm_campaign=110301&utm_content=readmore&elq=2207179eed8b48d1a9ac44112f28bc64		Magazine Intel report	Context	2. The Background	U.S. Secretary of Defense Robert Gates, speaking at West Point, said last week that "Any future defense secretary who advises the president to again send a big American land army into Asia or into the Middle East or Africa should have his head examined." In saying this, Gates was repeating a dictum laid down by Douglas MacArthur after the Korean War, who urged the United States to avoid land wars in Asia.
[97]	E. Yourdon, Decline and Fall of the American Programmer, Prentice Hall; 1 edition (June 16, 1993)		Book	Context	2. The Background	
[98]	Wikipedia, Decline and Fall of the American Programmer, http://en.wikipedia.org/wiki/Decline_and_Fall_of_the_American_Programmer		Internet source	Context	2. The Background	
[99]	US Department of Homeland Security, http://www.dhs.gov/index.shtm		Government	Context	2. The Background	
[100]	NSA, NSA/CSS Mission, Vision, Values, http://www.nsa.gov/about/values/index.shtml		Government	Context	2. The Background	
[101]	C. R. Duke, BRIDGING THE GAP IN THE REALM OF INFORMATION DOMINANCE: A CONCEPT OF OPERATIONS FOR THE NAVAL POSTGRADUATE SCHOOL CENTER FOR CYBER WARFARE, NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA, https://hsdl.org/?view&doc=131933&coll=limited		Thesis	Context	2. The Background	
[102]	D. Goodin, Georgian cyber attacks launched by Russian crime gangs With help from Twitter, Facebook and Microsoft, the Register, Posted in Security, 18th August 2009 00:23 GMT, http://www.theregister.co.uk/2009/08/18/georgian_cyber_attacks/		News	Context	2. The Background	
[103]	S. GORMAN, Hackers Stole IDs for Attacks, The wall Street Journal Europe, http://online.wsj.com/article/SB125046431841935299.html#articleTabs%3Darticle		News	Context	2. The Background	Technique used by Russian hackers when they have attacked Georgia
[104]	airforce-technology.com, E-3 AWACS Airborne Warning and Control System, USA, http://www.airforce-technology.com/projects/e3awacs/				2. The Background	
[105]	Wikipedia, Active measures, http://en.wikipedia.org/wiki/Active_measures				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	

No:	Reference		Type	Subject	Applicable Sections	Comments
[106]	D. Athow, Former NSA & CIA Director Suggests Employing Mercenaries For Cyberwarfare, ITPortal, 01 August, 2011, http://www.itproportal.com/2011/08/01/former-nsa-cia-director-suggests-employing-mercenaries-cyberwarfare/				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[107]	ASF2011: Cyber Security, Bloomberg's Allan Holmes moderates a conversation with former CIA Director Gen. Michael V. Hayden, Dell SecureWorks' Jon Ramsey, and AGT International's Mati Kochavi, YouTube, http://www.youtube.com/watch?v=yoWkAVXmSs0&feature=player_embedded				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[108]	Treadstone, Cyber Counterintelligence Doctrine - Treadstone 71, http://www.youtube.com/watch?v=5baUvUo76IY&feature=related				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	Cyber Counterintelligence activities as a component of strong cyber security practices must be examined, strategically deployed, operational delivered and continuously enhanced as a method of both active defensive and offense. It is time we expanded our approach from 'see, detect and arrest' to one that is proactive and aggressive. It is time to drive offensive cyber operations as part of our cyber DNA.
[109]	US Army, Counter-Intelligence Special Operations, http://www.youtube.com/watch?v=LyumoOw0voU&feature=related				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	This film explains surveillance techniques

No:	Reference		Type	Subject	Applicable Sections	Comments
[110]	YouTube, Cyber Security Operations Centre, http://www.youtube.com/watch?v=SVGvQxJEZ5M&feature=related				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	The Cyber Security Operations Centre, located in the Defence Signals Directorate, was officially opened by the Minister for Defence, Senator John Faulkner, on 15 January 2010. The Cyber Security Operations Centre provides comprehensive understanding of cyber threats to Australian interests and coordinates responses to cyber incidents of national importance. It is staffed by information technology experts, engineers and analysts from the Defence Signals Directorate, Defence Intelligence Organisation, Australian Defence Force and scientists from the Defence Science and Technology Organisation.
[111]	YouTube, How the CIA's Covert Operations Work, http://www.youtube.com/watch?v=wRS-3FUhUaY&feature=related			Covert Ops	4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[112]	YouTube, Counter-Intelligence Survey Report, http://www.youtube.com/watch?v=KD2WkbFVkw&feature=relmfu			Security Assessment	4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[113]	Sandia National Laboratories, Physical-Cyber Operations Analysis & Visualization, http://www.youtube.com/watch?v=m8_0tHxqFFw&feature=related			Joint Analysis of Battle Fields- Real and Cyber	4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	Analysis and visualization of dynamic physical-cyber operations is difficult to achieve. As one solution, Sandia has applied its flexible Umbra environment that allows modeling and simulation of physical, cyber, and human cognitive elements as a flexible dynamic interaction event visualizer. Dynamic visualization allows analysts to understand operational relevance and detect patterns in behavior displayed at rates faster, slower or equal to real time.

No:	Reference		Type	Subject	Applicable Sections	Comments
[114]	YouTube, CNN: Cyber Security and the Aurora Vulnerability, http://www.youtube.com/watch?v=C2qd6xXbySk&feature=related				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	Cyber on Physical Attack = Physical Destruction
[115]	YouTube, ECHELON Locations (Google Earth), http://www.youtube.com/watch?v=pF5mrwS1Nz0&feature=related				2. The Background	ECHELON LOCATIONS: RAF Menwith Hill (North Yorkshire, UK) GCHQ Bude (Cornwall, UK) Sugar Grove (West Virginia, US) Naval Security Group Activity Sabana Seca (Puerto Rico, US) (*decommissioned) Yakima Training Center (Washington, US) GCSB Waihopai (Marlborough, NZ) Pine Gap (Northern Territory, AU) Australian Defence Satellite Communications Station (Western Australia, AU) Chung Hom Kok (Hong Kong, HK)(*decommissioned) Misawa Air Base (Aomori, JP) Ayios Nikolaos Station (Cyprus, UK) Bad Aibling Station (Bavaria, DE) Griesheim Site (Hesse, DE) Canadian Forces Station Leitrim (Ontario, CA) NSA Headquarters, Fort Meade (Maryland, US) Gordon Regional Security Operations Center (Georgia, US) Medina Regional Security Operations Center (Texas, US) Buckley Air Force Base (Colorado, US) Kunia Regional Security Operations Center (Hawaii, US) Naval Computer and Telecommunications Station Guam (Guam, US) Shoal Bay Receiving Station (Northern Territory, AU)
[116]	US Army, FM 31-15, Operations Against Irregular Forces, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA310713&Location=U2&doc=GetTRDoc.pdf				2. The Background	

No:	Reference		Type	Subject	Applicable Sections	Comments
[117]	Wikipedia, 1971 Turkish coup d'état (12 Mart) , http://en.wikipedia.org/wiki/1971_Turkish_coup_d'%C3%A9tat			Gladio 12.March. 1971 coup d'état	2. The Background	<p>After the Israeli consul was abducted on 17 May, hundreds of students, young academics, writers, trade unionists and Workers' Party activists—not just leftists but also people with liberal-progressive sympathies—were detained and tortured. The consul was shot four days later after a daytime curfew had been announced.[11]</p> <p>For the next two years, repression continued, with martial law renewed every two months.[12] Constitutional reforms repealed some of the essential liberal fragments of the 1961 Constitution and allowed the government to withdraw fundamental rights in case of "abuse".[2] Journalist Uğur Mumcu (assassinated in 1993) later wrote that he had been arrested and tortured after the coup by people declaring themselves as belonging to Counter-guerilla (the name of the Turkish Gladio).[13]</p> <p>Ferit Melen, who made little impression, took over the premiership in April 1972,[12] followed a year later by Naim Talu, whose main task was to lead the country to elections. (An important reassertion of civilian influence took place in March-April 1973, when Demirel and Ecevit, normally at odds, both rejected the generals' choice for president, instead having Fahri Korutürk elected to the post by the Assembly.[14]) By summer 1973, the military-backed regime had achieved most of its political tasks. The constitution was amended so as to strengthen the state against civil society; special courts were in place to deal with all forms of dissent quickly and ruthlessly (these tried over 3,000 people before their abolition in 1976); the universities, their autonomy ended, had been made to curb the radicalism of students and faculty; radio, television, newspapers and the constitutional court were curtailed; the National Security Council was made more powerful; and, once the Workers' Party was dissolved in July 1971, the trade unions were pacified and left in an ideological vacuum.[15][16] That May, Necmettin Erbakan's National Order Party had been shut down, which the government claimed showed its even-handedness in the anti-terror campaign, but he was not tried and allowed to resume his activities in October 1972; the National Action Party and the right-wing terrorists who worked under its aegis were left conspicuously alone.[17]</p> <p>In October 1973, Ecevit, who had won control of the Republican People's Party from İnönü, won an upset victory. Nevertheless, the very same problems highlighted in the memorandum re-emerged. A fragmented party system and unstable governments held hostage by small right-wing parties contributed to political polarization.[2]</p> <p>The economy deteriorated, the Grey Wolves escalated and intensified political terrorism as the 1970s progressed, and left-wing groups too carried out acts aimed at causing chaos and demoralization.[18] In 1980, seeking once again to restore order, the military carried out yet another coup.</p>

No:	Reference		Type	Subject	Applicable Sections	Comments
[118]	Wikipedia, Torture in Turkey, http://en.wikipedia.org/wiki/Torture_in_Turkey				2. The Background	The government under Recep Tayyip Erdoğan declared zero tolerance against torture in 2004,[2] but instances of torture seem to be on the rise since 2005.[3] ^ a b Freedom House, Freedom in the World 2009 - Turkey , 16 July 2009; accessed on 23 October 2009
[119]	Wikipedia, 1980 Turkish coup d'état, http://en.wikipedia.org/wiki/1980_Turkish_coup_d'%C3%A9tat				2. The Background	
[120]	Wikipedia, Kenan Evren, http://en.wikipedia.org/wiki/Kenan_Evren		Internet source	Agent of Influence	2. The Background	He was the commander of Operation Gladio's Turkish branch; the Counter-Guerrilla. The Counter-Guerrilla was an anti-communist "stay-behind" guerrilla force set up with the support of NATO.[2] He became Chief of General Staff in March 1978.[1] The Central Intelligence Agency's Ankara bureau chief at the time, Paul B. Henze, received a call from the White House Situation Room saying "Paul, your guys have done it", while President Jimmy Carter was watching Fiddler on the Roof at the Kennedy Center.[3][4]
[121]	Feza Gazetecilik A.Ş., Sept. 12 coup admiral dies at 87 before trial, TODAYSZAMAN.COM, 30 May 2011, Monday, http://www.todayszaman.com/news-245567-sept-12-coup-admiral-dies-at-87-before-trial.html		News		2. The Background	Prosecutor Murat Demir, appointed last month by the Ankara Chief Prosecutor's Office to investigate the coup, earlier this month decided he did not have jurisdiction in the case because it concerns offenses such as “staging a coup” and “destroying the constitutional order through the use of force.”
[122]	http://www.au.af.mil , Intelligence Support to Contemporary Information Operations, http://www.au.af.mil/info-ops/iosphere/07spring/iosphere_spring07_sloggett.pdf				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[123]	M. A. Duvenage, Intelligence Analysis in the Knowledge Age Duvenage, STELLENBOSCH UNIVERSITY, http://scholar.sun.ac.za/bitstream/handle/10019.1/3087/Duvenage,%20M.A.pdf?sequence=1				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	

No:	Reference		Type	Subject	Applicable Sections	Comments
[124]	A. Manes, J. Golbeck, and James Hendler, Semantic Web and Target-Centric Intelligence, University of Maryland, College Park, http://www.mindswap.org/papers/2005/IUI_Final.pdf				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[125]	Dr. T. O'Connor, THINKING LIKE AN INTELLIGENCE ANALYST, North Carolina Wesleyan College, http://werzit.com/intel/intel/papers/Thinking%20Like%20an%20Intelligence%20Analyst.pdf				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[126]	Wikipedia, Intelligence cycle (target-centric approach), http://en.wikipedia.org/wiki/Intelligence_cycle_(target-centric_approach)				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[127]	Spartacus Educational, James Jesus Angleton, http://www.spartacus.schoolnet.co.uk/SSangleton.htm				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[128]	Wikipedia, James Jesus Angleton, http://en.wikipedia.org/wiki/James_Jesus_Angleton				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[129]	CIA, The James Angleton Phenomenon, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol53no4/201ccunning-passages-contrived-corridors201d.html				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[130]	ASDReports.com / ASDMedia BV - The Netherlands, Cyberwarfare Market 2008-2018,					

No:	Reference		Type	Subject	Applicable Sections	Comments
[131]	D. Williams, Spymaster sees Israel as world cyberwar leader, Thomson Reuters, TEL AVIV Tue Dec 15, 2009 1:47pm EST , http://www.reuters.com/article/2009/12/15/us-security-israel-cyberwarfare-idUSTRE5BE30920091215				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	Cyberwarfare teams nestle deep within Israel's spy agencies, which have extensive experience in traditional sabotage techniques and are cloaked in official secrecy and censorship. They can draw on the know-how of Israeli commercial firms that are among the world's hi-tech leaders and whose staff are often veterans of elite computer units in the conscript army. Technolytics Institute, a private U.S. consultancy, last year rated Israel the sixth-biggest "cyberwarfare threat," after China, Russia, Iran, France and "extremist/terrorist groups."
[132]	Wikipedia, Security Operations Center, http://en.wikipedia.org/wiki/Security_Operations_Center				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[133]	R. Bidou, Security Operation Center Concepts & Implementation, http://www.iv2-technologies.com/SOCCConceptAndImplementation.pdf		Technical paper		4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[134]	d3security.com, virtual Security Operations Center, http://www.futureshield.com/brochures/D3_brochure.pdf				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[135]	Wikipedia, Information Security Operations Center,				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[136]	RAND National Security Research Division, Assessing the Tradecraft of Intelligence Analysis, http://www.rand.org/pubs/technical_reports/2008/RAND_TR293.pdf				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	

No:	Reference		Type	Subject	Applicable Sections	Comments
[137]	R. Z. George and J. B. Bruce editors, Analyzing Intelligence Origins, obstacles, and innovation, In cooperation with the Center for Peace and Security Studies Edmund A. Walsh School of Foreign Service Georgetown University, 2008 , http://depositfiles.com/en/files/aqdt7n73f , http://avaxhome.ws/ebooks/1589012011.html			Cyber Intelligence and Espionage	4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[138]	R. M. Clark, Intelligence Analysis: A Target-Centric Approach, CQ Press; 3rd Edition edition (15 Sep 2009)			Cyber Intelligence and Espionage	4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[139]	W. Gragido and J. Pirc , Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats, Syngress (7 Mar 2011)				4. Analysis: Enterprise Model Conceptual View – Row 2 of Zachman's Framework	
[140]	defensetech.org, Hezbollah's Cyber Warfare Program , http://defensetech.org/2008/06/02/hezbollahs-cyber-warfare-program/					
[141]	A Cevdalli, Leveraging The Multi-Disciplinary Approach to Countering Organised Crime, Department of Mathematics Royal Holloway, University of London, http://www.rhul.ac.uk/mathematics/techreports					
[142]	Wikipedia, Computer crime, http://en.wikipedia.org/wiki/Computer_crime					
[143]	Cabinet Office, The cost of cyber crime, http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime					
[144]	Wikipedia, Industrial espionage, http://en.wikipedia.org/wiki/Industrial_espionage					
[145]	The Technolytics Institute Cyber Warfare Center , Cyber Commander's eHandbook UPDATED (The Weaponry and Strategies of Digital Conflict and Cyber War, Version 2, The Technolytics Institute, 2010					
[146]	www.technolytics.com , The Right to Bear Cyber Arms, http://www.technolytics.com/Right_to_bear_cyber_arms_CCH9-2.pdf					
[147]	U.S. Government Printing Office, Tactical Level Commander and Staff Toolkit, http://usacac.army.mil/cac2/FM3-28/CommanderStaffDCSAHandbook.pdf					
[148]	US Army Training and Doctrine Command Deputy Chief of Staff for Intelligence Assistant Deputy Chief of Staff for Intelligence – Threats, Critical Infrastructure Threats and Terrorism, http://www.fas.org/irp/threat/terrorism/sup2.pdf					

No:	Reference		Type	Subject	Applicable Sections	Comments
[149]	US department of Navy, Navy Cyber Forces Total Cyber Force Mentorship Program, http://www.public.navy.mil/bupers-npc/officer/Detailing/IDC_FAO/IP/Documents/COMNAVCYBERFORINST%201500.1.pdf					
[150]	http://www.navy.gov.au , Warfare Officers Career Handbook, http://www.navy.gov.au/w/images/Warfare_Officers_Career_Handbook.pdf					
[151]	O. ORTIZ, JOINT INTERAGENCY COORDINATION GROUP – CYBER: EMPOWERING THE COMBATANT COMMANDERS AGAINST THE NO- BORDERS THREAT, NAVAL WAR COLLEGE Newport, R.I. , http://dodreports.com/pdf/ada503033.pdf					
[152]	M. Grégoire, Visualisation for Network Situational Awareness in Computer Network Defence, Defence R&D Canada – Ottawa , http://ftp.rta.nato.int/public/PubFullText/RTO/MP/RTO-MP-IST-043/MP-IST-043-20.pdf					
[153]	US, Intelligence, http://www.fas.org/irp/doddir/army/fm2-0.pdf					
[154]	US Navy, US Navy's Vision for Information Dominance, http://www.insaonline.org/assets/files/NavyInformationDominanceVisionMay2010.pdf					Navy's information capabilities will evolve from 20th century supporting functions to a main battery of 21st century American seapower. To be successful at 21st century warfare, the Navy will create a fully integrated C2, information, intelligence, cyberspace, environmental awareness, and networks operations capability and wield it as a weapon and instrument of influence. Information will be treated as a weapon across the full range of military operations. The transition to an information-centric Navy represents a new vision of who we are as a sea power.
[155]	G. S. Odiorne, Management by Objectives, Pitman Pub. Corp.; First edition (1965)				6. Conclusion	
[156]	S. S. Wolin, Democracy Incorporated: Managed Democracy and the Specter of Inverted Totalitarianism, Princeton University Press; 1 edition (1 Feb 2010)					
[157]	M. McDonald, The Armageddon Factor: The Rise of Christian Nationalism in Canada, Random House Canada (11 May 2010)					
[158]	Escrito por Juan Santana , Cyber-crime organizations: a specialist classification, Panda Security Insight, March 31st, 2010 http://www.pandainsight.com/en/cyber-crime-organizations-a-specialist-classification ,					

No:	Reference		Type	Subject	Applicable Sections	Comments
[159]	Criminal hacker, Top 10 posts in cybercriminal operations Cybercrime organizations often run like corporations, staffed by experts in specific jobs, http://www.amarjit.info/2010/03/top-10-posts-in-cybercriminal.html Monday, May 9, 2011					
[160]	http://www.net-security.org/ , Cybercrime organizational structures and modus operandi, Posted on 15 July 2008, http://www.net-security.org/secworld.php?id=6325					
[161]	Threat Research Team, Zeus: A Persistent Criminal Enterprise, A Trend Micro Research Paper I March 2010, http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/zeusapersistentcriminalenterprise.pdf					
[162]	Wikipedia, List of criminal enterprises, gangs and syndicates, http://en.wikipedia.org/wiki/List_of_criminal_enterprises,_gangs_and_syndicates					
[163]	P. Williams, Organized Crime and Cyber-Crime: Implications for Business, CERT® Coordination Center,					
[164]	D E. Denning, Information Warfare and Security, Addison Wesley; 1 edition (10 Dec 1998)					
[165]	GJ Rattray, Strategic Warfare in Cyberspace, MIT Press; illustrated edition edition (1 Jun 2001)					
[166]	F. D. Kramer, S. H. Starr, and L. K. Wentz, Cyberpower and National Security (National Defense University, Potomac Books Inc; 1 edition (6 Nov 2009)					
[167]	Richard A Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do About It, ECCO Press,U.S. (15 May 2010)					
[168]	R.H. Anderson, Securing the U.S.Defense Information Structure: A Proposed Approach, RAND; illustrated edition edition (1 Sep 1999)					
[169]						
[170]						
[171]						
[172]						
[173]						
[174]						
[175]						
[176]						

No:	Reference		Type	Subject	Applicable Sections	Comments
[177]						
[178]						
[179]						
[180]						
[181]						
[182]						
[183]						
[184]						
[185]						
[186]						
[187]						
[188]						
[189]						
[190]	, http://www.rawstory.com/rawreplay/2011/07/former-bush-nsa-director-calls-for-digital-blackwater/					
[191]						
[192]						
[193]	M. V. Hayden, Gen USAF, Retired, The Future of Things “Cyber”, Strategic Studies Quarterly, Vol5 No1, Sprin 2011, http://www.au.af.mil/au/ssq/2011/spring/hayden.pdf		Government		Conclusion	“When speaking of the threat, citizens of a series of first-world nations recently asked whom they feared most in cyberspace, and the most popular answer was not China or India or france or Isreal. It was United States.”
[194]						
[195]						
[196]						
[197]	L Page, US cyberwar firing range to demo by July, the Register, 26th January 2011 12:21 GMT, http://www.theregister.co.uk/2011/01/26/cyber_range_demo_date_set/		News			
[198]						
[199]						
[200]	http://jobs.businessweek.com/a/all-jobs/list/q-intelligence+specialist+operations/l-baltimore,+md					

No:	Reference		Type	Subject	Applicable Sections	Comments
[201]	Dag Hammarskjöld, http://en.wikipedia.org/wiki/Dag_Hammarskj%C3%B6ld		Internet source			

Appendices

1. An Overview of Enterprise Architecture Approach and Zachman's Framework

During IBM years when John Zachman was working with different clients in different industries, he observed distinct patterns when organizations were tackling complex and large projects; for example designing and building aeroplanes, ships, and complex information system.

A typical approach is to build the simplest model of the problem including only the most relevant variables, then finding a solution to the problem at the most simplified level. During the next iteration one would add more detail and complexity to the model and develop a solution with those detailed variables and with a more complex model. Sometimes based on what is discovered at a lower level one may need to make corrections to the higher level model.

In other words, people would use levels of abstraction to architect, analyse, design, and build. These levels of abstractions in Zachman's Framework -contextual, conceptual, logical, and physical- are represented as rows.

He also observed during these endeavours that people tackle a distinct set of interrelated problems which could be summarized, into: Why are we doing this? What is this? How will this work? When should it happen? Who is responsible? Where should this be?

Out of these questions John created the columns: Why, What, How, When, Who, and Where. Then he observed during these large and complex projects that the deliverables match into the cells of the Framework matrix with rows and columns as described above. Usually these deliverables are considered artifacts which define and constitutes the whole.

The enterprise architecture [1,2,3,4,5,6,7,8,9,10] methodology is a way to investigate, analyse, and optimize how an organization may operate to fulfill its objectives and mission. Since the criminal, military, law enforcement, and secret service establishments are organizations too; their missions or objectives, data requirements, processes, organizational structures and skill requirements, locations, operational sequences and cycles could be analysed and optimized using the same framework or classification scheme.

At row 1 – Contextual Level: The aim is to investigate and document artifacts as defined by different columns of the Row 1 of the Architectural Framework. The main purpose at this level is to extract and understand organizational objectives and direction; and make sure everything else at the lower levels of abstraction aligns and supports the organizational objectives and direction.

At lower level rows of Zachman's Framework [11, 12, 13, 14] data models [15, 16, 17] are used to define organizational data requirements and Data Flow Diagrams [18, 19] are used to document organizational processes.

Through various matrices, relationships between artifacts (the cells of the framework) are analyzed, they are clustered according to rules, and a logical build sequence is established. The logical build sequence defines how various dimensions and specific requirements should be packaged without any constraints. As the next step, the logical build sequence is modified to take into account the situational constraints. Out of this work a series of projects are proposed to support organizational objectives and

direction. The series of proposed projects are modified according to the constraints placed by the environment. A diagrammatic depiction as a roadmap of this approach is provided as the second diagram in the Appendix 1.

All of the above activities are usually conducted during workshops, modelling sessions, and facilitated discussions (brain storming, and root-cause-analysis). However no such opportunity is available to this student; instead, published material will be used and gaps will be filled with assumptions. Moreover, since due to the enormous size of the scope and time limitations, the Swiss - chest technique will be used. Time to time certain gaps will be left or certain analysis will be skipped for future investigation beyond this project.

The first Diagram: Introduction to IS Strategic Planning - Levels of Abstraction

In this diagram levels of abstraction and relevant levels of detail is explained with an analogy to city plan, subdivision plan, and engineering blueprint of a building. A similar point of view is used in Enterprise Architecture approaches. The Enterprise Architecture deliverables represent the City Plan perspective. The Subdivision Plan represents project requirements perspective. The Engineering Blueprints represent the design perspective. As it is seen from the City Plan perspective plans area is much larger than the lower levels, but the detail is much less. Exactly the same thing applies to Enterprise Architecture deliverables.

The Second Diagram: Enterprise Architecture as IT Long range Planning

Here the diagram depicts the process of creating enterprise architecture. It starts with scope, then data requirements in the scope are investigated usually using conceptual data models. Later in parallel, resources are identified, management commitment is obtained, interviews of subject matter experts are conducted. Later models (data and process) are produced and based on the models architecture is deduced. According to the objectives, and taking the architecture as a base, and assessment is conducted –how well the architecture is meeting the objectives where are gaps, etc.-, recommendations are identified and approved, plans for project initiations are proposed – usually to a project management office or a executive steering committee-.

The Third Diagram:

Row 2 is defined as 20 – 30 thousand view of the enterprise. Row 2 aims to understand and document how entire enterprise or organization is independent of an organizational structure or any IT systems. On the other hand the Row 1 is considered a 60 thousand feet view of the entire organization independent of any constraints such as organizational structure or systems or budgetary constraints. The next level, Row 3 of Zachman's framework is a more detailed logical view of a Line-of-Business or Organizational subset or a project. This is similar to the requirements definition and analysis phase of a software development project. We will not explore Row 3 of Zachman's framework in this paper.

The Zachman's Framework consists of rows representing the levels of abstractions and columns representing the perspectives. The rows are: contextual, conceptual, logical, physical, and detailed (implementation) representation (e.g. source code).

The columns are: Why, What, How, When, Who, and Where.

The cells of the framework are pigeon holes for types of artifacts. For a specific cell one may use different techniques to represent that artifact of the cell. For example for conceptual data model cell, one may use Chen representation, Bachman representation, or IE representation. Or one may logically merge data and process columns and use object oriented modelling techniques.

The Fourth Diagram:

The fourth diagram indicates how the Zachman's Framework and normal Enterprise Architecture Methodology will be modified.

On Row 1 Scope (Contextual) the objectives and strategies of the major players (USA, Russia, and China) will be investigated and analysed. This investigation and analysis are on Chapter 3. The aim is to understand what the distinct objectives are for the major players. What strategies are they using (how do they allocate resources, organize resources, and direct them toward their aims) to achieve their objectives. How they are organizing their strategic resources. What responsibilities they are assigning to whom? How they have offended or attacked in the past (*modus operandi*) These would map to columns Why, Who, and How of Row 1.

On Row 2 of Zachman's Framework Enterprise Model (Conceptual) goal is understanding what are the important concepts; high level processes; high level organizations including responsibilities, and skills requirements. These map to the columns, What, How, Who of Row 2.

On Row 3 the Cyber Offence or Cyber Attack, in other words Cyber Warfare, Cyber Espionage, or Cyber Crime would be analysed in more detailed and modelled to capture the essence of organizations value chain. More detailed and complex models would be built to document and optimize the techniques, tools, tactics, and detailed data requirements, process definitions, organizational structures, roles and responsibilities, skills requirements, location requirements, organizational cycles and sequences, events. All of these would be analysed and modelled to represent an organization independent of a specific organizational structure, specific technology, or IT systems implantation. Unfortunately, this level of analysis and modelling is out of scope.

One may also use a similar approach when collecting and analysing intelligence, surveillance, reconnaissance activities to map a target organization and its IT Infrastructure Architecture.

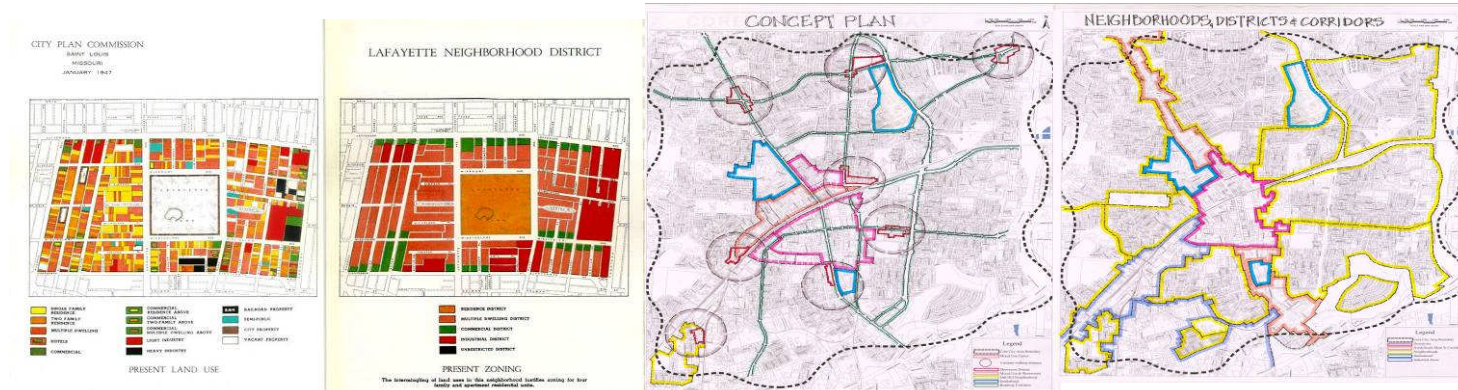
On Row 3 the Cyber Offence or Cyber Attack, in other words Cyber Warfare; Cyber Intelligence, Espionage, and Cyber Subversion; Cyber Crime would have been analysed in more detail.

Unfortunately, this level of analysis and modelling is out of scope. It is not possible due to the space and time limitations of an MSc.

Introduction to IS Strategic Planning

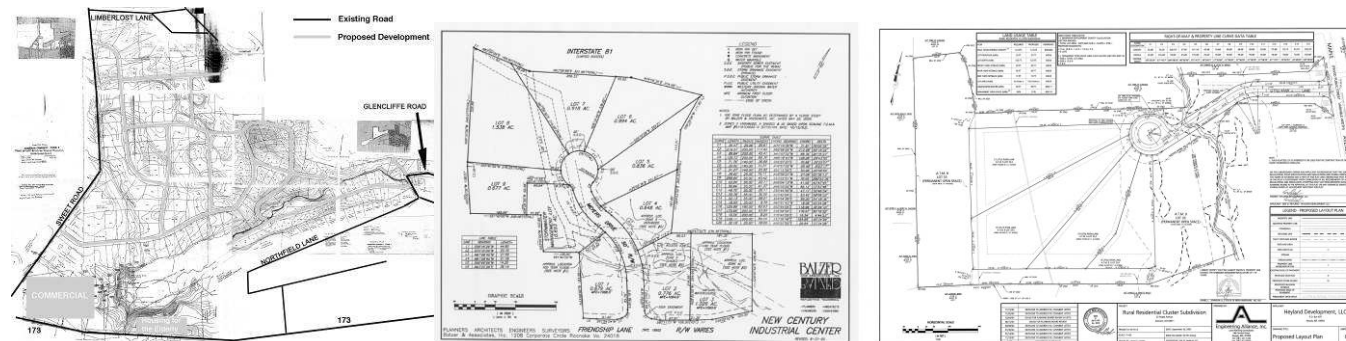
Levels of Abstraction

*Enterprise
Architecture
“the city plan”*



- Subdivisions
- Land use
- Traffic flow
- Utilities
- Infrastructure
- Land use code

*Solution
Architecture
“subdivision plan”*



- Lots
- Roads
- Common areas
- Utilities
- Infrastructure
- Municipal code

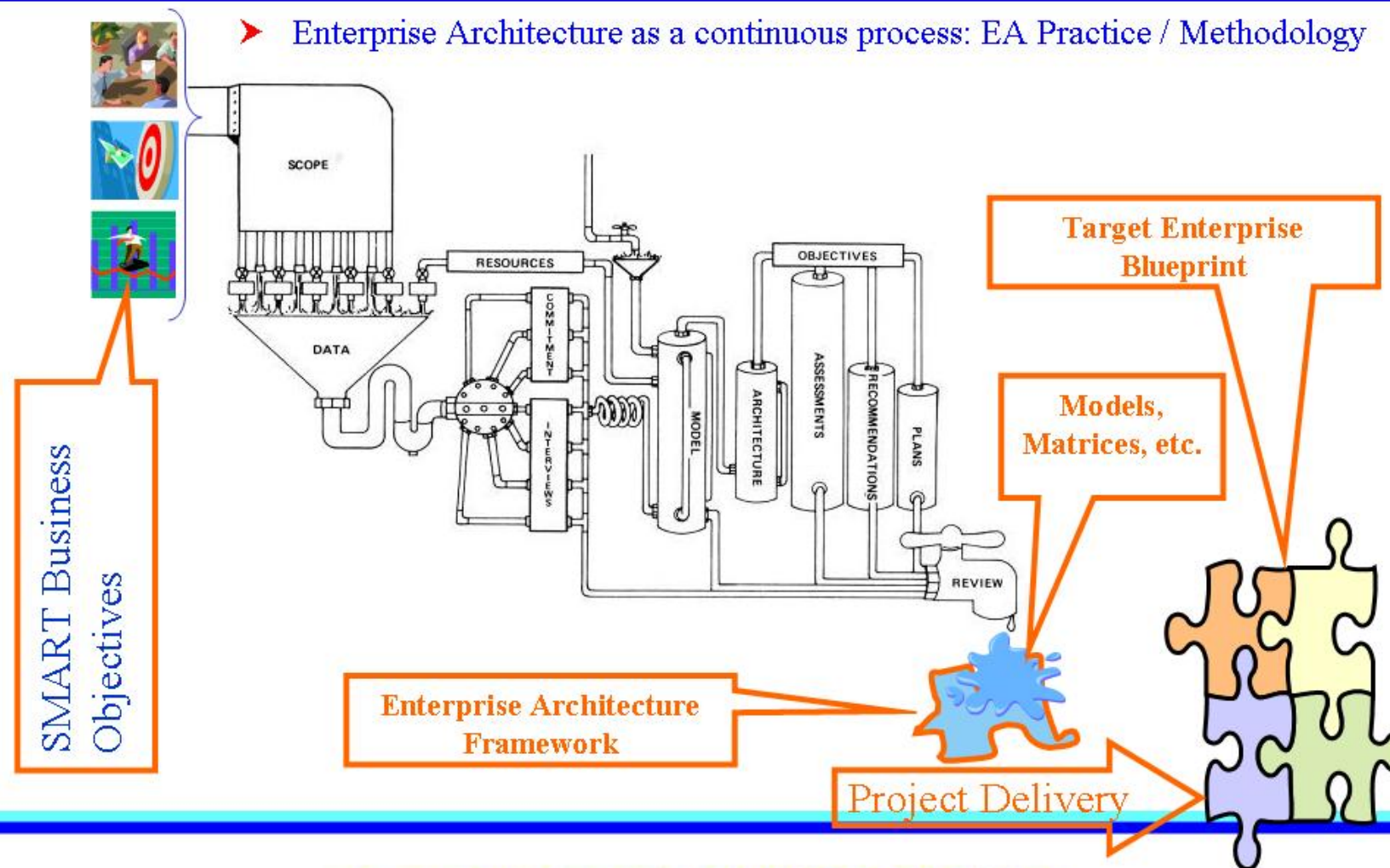
*Design
“engineering
blueprint”*



- Building use
- Lot placement
- Structure
- Municipal connections
- Building code

IV. Enterprise Architecture as IT Long-range Planning

➤ Enterprise Architecture as a continuous process: EA Practice / Methodology










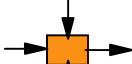

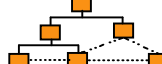


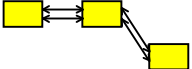
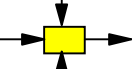
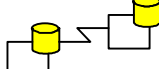
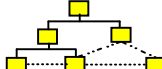

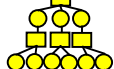
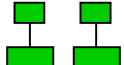
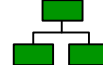










2011-07-29 15:25

- INTELLECTUAL PROPERTY OF ROTEK DOT CA LTD. -

29

[2], [74]

ENTERPRISE ARCHITECTURE - A FRAMEWORK TM

	DATA <i>What</i>	FUNCTION <i>How</i>	NETWORK <i>Where</i>	PEOPLE <i>Who</i>	TIME <i>When</i>	MOTIVATION <i>Why</i>	
SCOPE (CONTEXTUAL)	List of Things Important to the Business 	List of Processes the Business Performs 	List of Locations in which the Business Operates 	List of Organizations Important to the Business 	List of Events Significant to the Business 	List of Business Goals/Strat 	SCOPE (CONTEXTUAL)
<i>Planner</i>	ENTITY = Class of Business Thing	Function = Class of Business Process	Node = Major Business Location	People = Major Organizations	Time = Major Business Event	Ends/Mean=Major Bus. Goal/ Critical Success Factor	<i>Planner</i>
ENTERPRISE MODEL (CONCEPTUAL)	e.g. Semantic Model 	e.g. Business Process Model 	e.g. Business Logistics System 	e.g. Work Flow Model 	e.g. Master Schedule 	e.g. Business Plan 	ENTERPRISE MODEL (CONCEPTUAL)
<i>Owner</i>	Ent = Business Entity ReIn = Business Relationship	Proc. = Business Process I/O = Business Resources	Node = Business Location Link = Business Linkage	People = Organization Unit Work = Work Product	Time = Business Event Cycle = Business Cycle	End = Business Objective Means = Business Strategy	<i>Owner</i>
SYSTEM MODEL (LOGICAL)	e.g. Logical Data Model 	e.g. Application Architecture 	e.g. Distributed System Architecture 	e.g. Human Interface Architecture 	e.g. Processing Structure 	e.g., Business Rule Model 	SYSTEM MODEL (LOGICAL)
<i>Designer</i>	Ent = Data Entity ReIn = Data Relationship	Proc. = Application Function I/O = User Views	Node = I/S Function (Processor, Storage, etc.) Link = Line Characteristics	People = Role Work = Deliverable	Time = System Event Cycle = Processing Cycle	End = Structural Assertion Means = Action Assertion	<i>Designer</i>
TECHNOLOGY MODEL (PHYSICAL)	e.g. Physical Data Model 	e.g. System Design 	e.g. Technology Architecture 	e.g. Presentation Architecture 	e.g. Control Structure 	e.g. Rule Design 	TECHNOLOGY MODEL (PHYSICAL)
<i>Builder</i>	Ent = Segment/Table/etc. ReIn = Pointer/Key/etc.	Proc. = Computer Function I/O = Data Elements/Sets	Node = Hardware/System Software Link = Line Specifications	People = User Work = Screen Format	Time = Execute Cycle = Component Cycle	End = Condition Means = Action	<i>Builder</i>
DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)	e.g. Data Definition 	e.g. Program 	e.g. Network Architecture 	e.g. Security Architecture 	e.g. Timing Definition 	e.g. Rule Specification 	DETAILED REPRESENTATIONS (OUT-OF-CONTEXT)
<i>Sub-Contractor</i>	Ent = Field ReIn = Address	Proc. = Language Stmt I/O = Control Block	Node = Addresses Link = Protocols	People = Identity Work = Job	Time = Interrupt Cycle = Machine Cycle	End = Sub-condition Means = Step	<i>Sub-Contractor</i>
FUNCTIONING ENTERPRISE	e.g. DATA	e.g. FUNCTION	e.g. NETWORK	e.g. ORGANIZATION	e.g. SCHEDULE	e.g. STRATEGY	FUNCTIONING ENTERPRISE

John A. Zachman, Zachman International (810) 231-0531

ENTERPRISE ARCHITECTURE - A FRAMEWORK™



Introduction

Types of Structured Analysis Models

- Process Model: The graphic representation and related definitions of the business activities required to achieve the mission and objective of the business
- Data Model: The graphic representation and related definitions of the essential groups of facts and their structure to support the activities and management of the business.

2011.03.27.

21

Introduction

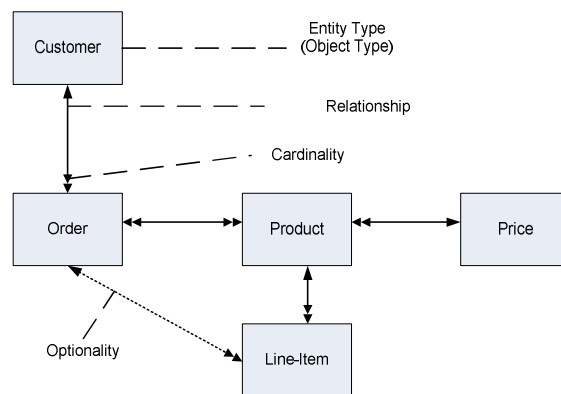
Levels of Abstraction

- Conceptual:
 - Define the purpose and the objectives of the organization or business unit under study (global view)
 - Model used mainly for representation, in order to communicate a reality to a group of people
 - It is a Computational Independent Model (CIM)
 - Audience: It is Investors and business owners view
- Logical:
 - Identify all the necessary elements of the required to define and specify a solution
 - Model used to verify the presence and the coherent arrangement of all the components of the organization or business unit under study
 - It is a Platform Independent Model (PIM)
 - Audience: It is Project requirements Analysis view
- Physical:
 - Integrate the constraints of the IT environment and of the IT Infrastructure (S/W, M/W, H/W, etc.) in order to build an efficient information system aligned with business drivers
 - Model used for construction purposes
 - It is a Platform Specific Model (PSM)
 - Audience: It is Designers and Infrastructure Architects view

2011.03.27.

22

Introduction to Data Modeling Entity Relationship Diagram



2011.03.27.

68

Introduction to Data Modeling Meaning of Entity Relationship Modeling Symbols

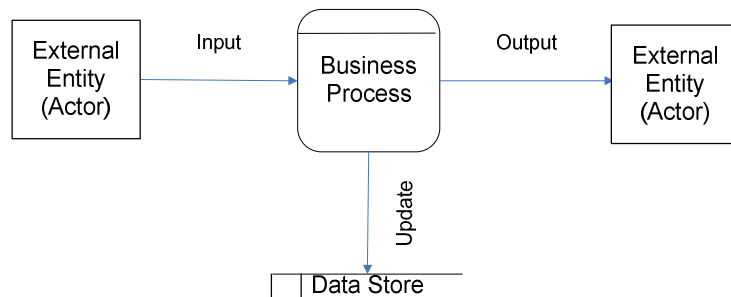
- **Entity Type:** Something business needs to, or wants to keep data about. A representation of business reality, as perceived by the business and data architect, characterized by:
 - Its value for the enterprise
 - Its stability in reality
 - Its instances exist independently within the data model
 - something business wishes to keep data or know facts about
- **Relationship:** An association between two or more entity types. Examples are one-to-one, one-to-many, and many-to-many. A representation of relationships, business policies and rules as perceived by the business and data architect, characterized by:
 - Its value for the enterprise
 - Its stability in reality
 - Its dependent existence within the data model

2011.03.27.

70

Basic DFD Modeling

Basic DFD Model:



2011.03.27.

30

Basic DFD Modeling

DFD Symbols*

Meaning	Symbol
Data Flow: A pipeline through which packets of data flows	
Process: A business process which transforms input data to output	
External Entity: Out of scope external source or destination of data flows or event flows (UML Actor), e.g. Organization, System, or role	
Data Store:	

*Gane & Sarson

2011.03.27.

29

2. Some Political Thoughts on Injustice, Use of Violence, and Subversion of Democracy

Here are some quotes from Dwight D. Eisenhower some going back to 1948, not so distance past.

First Inaugural address (20 January 1953)

“We must be ready to dare all for our country. For history does not long entrust the care of freedom to the weak or the timid. We must acquire proficiency in defense and display stamina in purpose. We must be willing, individually and as a Nation, to accept whatever sacrifices may be required of us. A people that values its privileges above its principles soon loses both. These basic precepts are not lofty abstractions, far removed from matters of daily living. They are laws of spiritual strength that generate and define our material strength. Patriotism means equipped forces and a prepared citizenry. Moral stamina means more energy and more productivity, on the farm and in the factory. Love of liberty means the guarding of every resource that makes freedom possible—from the sanctity of our families and the wealth of our soil to the genius of our scientists.” [21]

“I like to believe that people in the long run are going to do more to promote peace than our governments. Indeed, I think that people want peace so much that one of these days governments had better get out of the way and let them have it.” [21]

“Speech to the American Society of Newspaper Editors ["The Chance for Peace"](#) (16 April 1953)” [21]

“No people on earth can be held, as a people, to be an enemy, for all humanity shares the common hunger for peace and fellowship and justice. ... No nation's security and well-being can be lastingly achieved in isolation but only in effective cooperation with fellow-nations.” [21]

“Every gun that is made, every warship launched, every rocket fired signifies, in the final sense, a theft from those who hunger and are not fed, those who are cold and are not clothed. This world in arms is not spending money alone. It is spending the sweat of its laborers, the genius of its scientists, the hopes of its children. The cost of one modern heavy bomber is this: a modern brick school in more than 30 cities. It is two electric power plants, each serving a town of 60,000 population. It is two fine, fully equipped hospitals. It is some fifty miles of concrete pavement. We pay for a single fighter plane with a half million bushels of wheat. We pay for a single destroyer with new homes that could have housed more than 8,000 people. This is, I repeat, the best way of life to be found on the road the world has been taking. This is not a way of life at all, in any true sense. Under the cloud of threatening war, it is humanity hanging from a cross of iron. ... Is there no other way the world may live?” [21]

“Speech in Ottawa (10 January 1946), published in Eisenhower Speaks : Dwight D. Eisenhower in His Messages and Speeches (1948) edited by Rudolph L. Treuenfels” [21]

“I hate war as only a soldier who has lived it can, only as one who has seen its brutality, its stupidity.” [21]

“The White House Years: Mandate for Change: 1953–1956: A Personal Account (1963), p. 331” [21]

“Un-American activity cannot be prevented or routed out by employing un-American methods; to preserve freedom we must use the tools that freedom provides.” [21]

I wonder what Mr. Dwight D. Eisenhower would think about torturing enemy soldiers or the Patriot Act – indefinite detention without any charges-.

“The White House Years: Mandate for Change: 1953–1956: A Personal Account (1963), pp. 312-313” [21]

“Secretary of War [Stimson](#), visiting my headquarters in Germany, informed me that our government was preparing to drop an atomic bomb on Japan. I was one of those who felt that there were a number of cogent reasons to question the wisdom of such an act. ...the Secretary, upon giving me the news of the successful bomb test in New Mexico, and of the plan for using it, asked for my reaction, apparently expecting a vigorous assent.

During his recitation of the relevant facts, I had been conscious of a feeling of depression and so I voiced to him my grave misgivings, first on the basis of my belief that Japan was already defeated and that dropping the bomb was completely unnecessary, and secondly because I thought that our country should avoid shocking world opinion by the use of a weapon whose employment was, I thought, no longer mandatory as a measure to save American lives. It was my belief that Japan was, at that very moment, seeking some way to surrender with a minimum loss of 'face'. The Secretary was deeply perturbed by my attitude...” [21]

“On his stated opposition to the use of the atomic bomb against the Japanese at the end of World War II, as quoted in Newsweek (11 November 1963)” [21]

“I was against it on two counts. First, the Japanese were ready to surrender, and it wasn't necessary to hit them with that awful thing. Second, I hated to see our country be the first to use such a weapon.” [21]

“[Farewell address \(17 January 1961\)](#)” [21]

“Now this conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence — economic, political, even spiritual — is felt in every city, every Statehouse, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources, and livelihood are all involved. So is the very structure of our society.

In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the [military-industrial complex](#). The potential for the disastrous rise of misplaced power exists and will persist. We must never let the weight of this combination endanger our liberties or democratic processes.” [21]

“Remarks at Fourth Annual Republican Women's National Conference (6 March 1956)” [21]

“If a political party does not have its foundation in the determination to advance a cause that is right and that is moral, then it is not a political party; it is merely a conspiracy to seize power.” [21]

“News Conference of (11 August 1954)” [21]

“All of us have heard this term "[preventive war](#)" since the earliest days of Hitler. I recall that is about the first time I heard it. In this day and time, if we believe for one second that nuclear fission and fusion, that type of weapon, would be used in such a war — what is a preventive war?

I would say a preventive war, if the words mean anything, is to wage some sort of quick police action in order that you might avoid a terrific cataclysm of destruction later.

A preventive war, to my mind, is an impossibility today. How could you have one if one of its features would be several cities lying in ruins, several cities where many, many thousands of people would be dead and injured and mangled, the transportation systems destroyed, sanitation implements and systems all gone?

That isn't preventive war; that is war.

I don't believe there is such a thing; and, frankly, I wouldn't even listen to anyone seriously that came in and talked about such a thing.

... It seems to me that when, by definition, a term is just ridiculous in itself, there is no use in going any further.

There are all sorts of reasons, moral and political and everything else, against this theory, but it is so completely unthinkable in today's conditions that I thought it is no use to go any further.” [21]

"DWIGHT D. EISENHOWER, State of the Union Address, Jan. 9, 1958" [21]

"We could make no more tragic mistake than merely to concentrate on military strength. For if we did only this, the future would hold nothing for the world but an Age of Terror."

"If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking... is freedom." Dwight D. Eisenhower [21]

"TV talk with [Prime Minister Macmillan](#) (31 August 1959), "[Selected Quotations](#)". *Eisenhower Archives*. Eisenhower Library. Archived from [the original](#) on 2007-02-08. Retrieved on 2007-04-01." [21]

"I like to believe that people in the long run are going to do more to promote peace than our governments. Indeed, I think that people want peace so much that one of these days governments had better get out of the way and let them have it." [21]

"Never let yourself be persuaded that any one Great Man, any one leader, is necessary to the salvation of America. When America consists of one leader and 158 million followers, it will no longer be America." [Dwight D. Eisenhower](#) [21]

About 15 20 year before Dwight D. Eisenhower, another General and President, Mustafa Kemal Atatürk, echoed the same ideas and feelings

"Millet hayatı tehlikeye maruz kalmayınca, savaş cinayettir. (Unless a nation's life faces peril, war is murder.)"

*"["Adana Çiftçileriyle Konuşma" \(16 March 1923\)](#); English translation as delivered in [an address by Talat S. Halman \(10 November 1995\)](#), quoted in *The Turkish Times* (1 December 1995)"* [20, 26]

"Yurtta Barış, Dünyada Barış (Peace at home, peace in the world.)"

"Maxim which became the motto of the Republic of Turkey; quoted in many sources including, *Atatürk* (1963) by Uluğ İğdemir, p. 200; and *Small Nations and Great Powers: A Study of Ethnopolitical Conflict in the Caucasus* (2000) by [Svante E. Cornell](#), p. 287" [20, 26]

"Mankind is a single body and each nation a part of that body. We must never say "What does it matter to me if some part of the world is ailing?" If there is such an illness, we must concern ourselves with it as though we were having that illness."

As quoted by [Paul Wolfowitz](#) in an [address to the Washington Institute for Near East Policy, Washington, D.C. \(13 March 2002\)](#) [20, 26]

3. The Crime of Aggression: UN Charter

The Crime of Aggression

As one could deduct from the UN Charter and International Criminal Court website; aggression is defined as a Crime even though currently powerful nations act based on might-is-right principal without any consequence.

The UN Charter, CHAPTER I: PURPOSES AND PRINCIPLES

"Article 1

2011-08-31 13:09:53

Final Draft Osman Tekes 20110831

The Purposes of the United Nations are:

- 1 To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace;
- 2 To develop friendly relations among nations based on respect for the principle of equal rights and self-determination of peoples, and to take other appropriate measures to strengthen universal peace;
- 3 To achieve international co-operation in solving international problems of an economic, social, cultural, or humanitarian character, and in promoting and encouraging respect for human rights and for fundamental freedoms for all without distinction as to race, sex, language, or religion; and
- 4 To be a centre for harmonizing the actions of nations in the attainment of these common ends.

Article 2

The Organization and its Members, in pursuit of the Purposes stated in Article 1, shall act in accordance with the following Principles.

- 1 The Organization is based on the principle of the sovereign equality of all its Members.
- 2 All Members, in order to ensure to all of them the rights and benefits resulting from membership, shall fulfill in good faith the obligations assumed by them in accordance with the present Charter.
- 3 All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.
- 4 All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.
- 5 All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action.
- 6 The Organization shall ensure that states which are not Members of the United Nations act in accordance with these Principles so far as may be necessary for the maintenance of international peace and security.
- 7 Nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII. " [27]

CHAPTER VII: ACTION WITH RESPECT TO THREATS TO THE PEACE, BREACHES OF THE PEACE, AND ACTS OF AGGRESSION [28]

4. The Crime of Aggression: The International Criminal Court

The International Criminal Court (ICC) [29]

Article 8 bis⁷⁴

Crime of aggression

Introduction

1. It is understood that any of the acts referred to in article 8 *bis*, paragraph 2, qualify as an act of aggression.
2. There is no requirement to prove that the perpetrator has made a legal evaluation as to whether the use of armed force was inconsistent with the Charter of the United Nations.
3. The term "manifest" is an objective qualification.
4. There is no requirement to prove that the perpetrator has made a legal evaluation as to the "manifest" nature of the violation of the Charter of the United Nations.

Elements

1. The perpetrator planned, prepared, initiated or executed an act of aggression.
2. The perpetrator was a person in a position effectively to exercise control over or to direct the political or military action of the State which committed the act of aggression.

3. The act of aggression – the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations – was committed.
4. The perpetrator was aware of the factual circumstances that established that such a use of armed force was inconsistent with the Charter of the United Nations.
5. The act of aggression, by its character, gravity and scale, constituted a manifest violation of the Charter of the United Nations.
6. The perpetrator was aware of the factual circumstances that established such a manifest violation of the Charter of the United Nations. [30]

5. Continuum One: The Scale of Escalation - Intensity of Coercion

As an example of the scale of escalation, the following list is provided. The policy makers have all these options available at their disposal. They may use one or a combination as the situation warrants. These are the means available to fulfil political or other ends

Some believe that, if one assumes the following is a very simplistic depiction of available means:

- 1. Politics** - negotiations or international political processes: the legitimate and non-violent practices of getting what you want or allocating resources and privileges [24]
- 2. Policing** – enforcing laws of a state domestically or internationally
- 3. Customs and Border Police** – controlling the borders of a state and what is being brought in
- 4. Intelligence** – open sources passive and legal collection of data, information, or knowledge
- 5. Cyber Weapons and Cyber Command**
- 6. Intelligence** – use of active intelligence for competitive advantage
- 7. Surveillance** – watching state of affairs more actively
- 8. Counter Intelligence** – controlling or reducing acts of subversion, espionage, and illegal influences
- 9. Espionage** – collection of intelligence via illegal means and ways
- 10. Information War** – controlling media, propaganda, and misinformation (part of subversion)
- 11. Subversion** – false flag operations
- 12. Special Ops** – subversion, green ops, or black ops
- 13. Total War**
 - Air force
 - Navy

- Marines
- Army
- Space weapons and Space Command
- Nuclear Weapons and Nuclear Command (NCCS in US)

An example of how force could be applied with escalating intensity without going into open warfare is depicted in the following documentary.

According to the documentary “*British Secret Intelligence in WWII*” [25] the top-level organizations and their responsibilities were:

Special Operations Executive (SOE)

The common activities are:

- Sabotage
- Irregular Warfare
- Agent Provocateurs to use the locals to fight for them
- Providing money, resources, training, operational plans to insurgency operations of the adversaries

Operations Theatre: pretty much everywhere

British Security Coordination

The common activities are:

- Information War and propaganda to change the public opinion
- Developing Agents-of-Influence (Rockefellers) to obtain favourable support from politicians and Government
- Planning and conducting secret propaganda
- Manipulating US political process
- Subverting the will of Americans
- Planting operatives in the pole companies
- Manipulating pole results
- Organizing engineered demonstrations

Operations Theatre: USA

6. United States Strategic Command (STRATCOM)

United States Strategic Command (STRATCOM):

“It is charged with space operations (such as [military satellites](#)), information operations - *Department of Defense Information Operations* -(such as [information warfare](#)), [missile defense](#), global [command and control](#), intelligence, surveillance, and reconnaissance ([C⁴ISR](#)), global strike and [strategic deterrence](#) (the [United States nuclear arsenal](#)), and combating [weapons of mass destruction](#).” [45]

Mission statement:

‘USSTRATCOM promotes global security for America: The missions of U.S. Strategic Command are to deter attacks on U.S. vital interests, **to ensure U.S. freedom of action**

in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations, to synchronize global missile defense plans and operations, to synchronize regional combating of weapons of mass destruction plans, to provide integrated surveillance and reconnaissance allocation recommendations to the SECDEF, and to advocate for capabilities as assigned.” [45]

7. USCYBERCOM High Level Mission Statement and Organizational Structure

“The central cyber command coordinates the activities of the separate US armed services' **cyber forces** - the 24th Air Force and corresponding **cyber formations** in the US Navy, Army, and Marine Corps. It will also work closely with the NSA (formally speaking a "combat support agency" of the Defense Department) and will cooperate with the Department of Homeland Security.” [39]

“The cyber command is responsible for defending the .mil domain, while .gov comes under the DHS. Both agencies' role in other parts of the internet is yet to become clear, though it is evident that the military **cyber warriors** will maintain the ability to attack the networks of others as well as defending their own. (The 24th AF contains an entire unit, the 67th **Network Warfare Wing**, dedicated to nothing else - though it has a subsidiary role in red-teaming friendly networks when there are no enemies to attack.)” [39]

Mission

"USCYBERCOM plans, coordinates, integrates, synchronizes and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, **conduct full spectrum military cyberspace operations** in order to enable actions in all domains, ensure US/Allied **freedom of action in cyberspace and deny the same to our adversaries.**"[39]

“Service components

U.S. Cyber Command is composed of several service components, units from military services who will provide Joint services to Cyber Command.

- [Army Cyber Command/2nd Army \(Army\)](#)
 - [Army Network Enterprise Technology Command / 9th Army Signal Command](#)
 - Portions of [1st Information Operations Command \(Land\)](#)
 - [United States Army Intelligence and Security Command](#) will be under the operational control of ARFORCYBER for cyber-related actions. ^{[5][6][7]}
- [Fleet Cyber Command/10th Fleet \(Navy\)](#) ^{[8][9]}
 - [Naval Network Warfare Command](#)
 - Navy Cyber Defense Operations Command

- Naval Information Operation Commands
 - Combined Task Forces
- [Air Forces Cyber Command/24th Air Force \(Air Force\)](#)^{[10][11]}
 - [67th Network Warfare Wing](#)
 - [688th Information Operations Wing](#)
 - [689th Combat Communications Wing](#)
- [United States Marine Corps Forces Cyberspace Command \(Marine Corps\)](#)^[12] “ [39]

8. Some examples of Skills sought in Cyber Warriors

“Space and Naval Warfare Systems Command

New Professional Program (NP)

Permanent full-time positions available for graduates with BS/MS or PhD degrees in the fields of Electrical Engineering, Computer Engineering, Computer Science and other key science and technology careers.” [51]

Job Title: INTELLIGENCE SPECIALIST (OPERATIONS)

Department: Department Of The Army

Agency: Army Intelligence and Security Command

Job Announcement Number: WTST11830405

SALARY RANGE: \$62,467.00 - \$115,742.00 /year

OPEN PERIOD: Wednesday, March 23, 2011 to Thursday, July 21, 2011

SERIES & GRADE: IA-0132-03/03

POSITION INFORMATION: - This is a Permanent position. -- Full Time

DUTY LOCATIONS: 1 vacancy - MD - Anne Arundel County

WHO MAY BE CONSIDERED: US Citizens and Status Candidates

JOB SUMMARY:

Civilian employees serve a vital role in supporting the Army mission. They provide the skills that are not readily available in the military, but crucial to support military operations. The Army integrates the talents and skills of its military and civilian members to form a Total Army. Changes to the Job Announcement: This is an Occupational Band 03 job in DCIPS. Band 03 duties are at the Full Performance work level, and equal to those at GS/GG 11/12/13. Salary will be set within the band equal to a GS/GG grade based on the selectee's quals in relation to the job. Organization(s):

US Army Intelligence & Security Command (INSCOM), Cyber Brigade, Fort Meade, MD

About the Position: Serves as a Cryptologic Cyberspace Operations Specialist, 1st Cyber Battalion, 1st Cyber Brigade. Duties involve conducting analysis, collection operations of digital networks, and support in the planning of Cyber Warfare activities. Uses information collected from a variety of computer network defense and SIGINT resources to identify, analyze, and report events that occur on digital networks. Exploits captured media and/or investigates computer security incidents in order to derive useful intelligence and/or enable mitigation of network vulnerabilities. Actions support development of cyberspace operations and plans as well as the integration and synchronization of diverse operational capabilities to achieve assigned missions. The expected contribution of the selectee in the new position based on personal qualifications, including knowledge, capability to deal with complexity, broad scope and responsibility, and impact mission will be evaluated for pay setting purposes.

Duties

Additional Duty Location Info:

You will conduct computer (network and infrastructure) analysis to enable Cyber Warfare effects in support of national and theater intelligence requirements. You will leverage information derived from a variety of computer network defense and SIGINT resources to identify events that occur on computer networks. You will initiate actions to identify, assess, report, and brief on foreign computer network capabilities, vulnerabilities, and personalities that could pose a threat to U.S. computers, communications, and operations. You will investigate computer security incidents and operate automated data processing equipment. You will perform analysis, strategies and operations for the control and application of cyber capabilities. You will assist with integrating Cyberspace Operations capabilities into operations/exercise design and integrating/synchronizing Cyber-related effects. You will prepare review, evaluate and publish technical, time sensitive reports, and event reports.

Qualifications and Evaluations

QUALIFICATIONS REQUIRED:

SPECIALIZED EXPERIENCE: Progressively responsible experience is that which has included intelligence-related research, analysis, collections and /or operations. This experience should have included intelligence analysis and/or production, intelligence collection and/or operations, counterintelligence, or threat support directly related to the position to be filled. Creditable specialized experience may include previous military intelligence experience, experience gained in the private sector or in another government agency as long as it was at a level at least equivalent to the next lower band in the series. This experience should demonstrate: Knowledge of intelligence processes, cycle and organizations; Knowledge of and/or ability to use research tools such as library holdings, photographs, statistics, graphics and maps; Knowledge of the systems, procedures and methods of analyzing, compiling, reporting and disseminating intelligence data; and/or Knowledge of organization(s) for and methods of collecting and analyzing intelligence data.

At a minimum your resume must reflect one year of demonstrated experience performing the duties listed above (specialized experience) which must be comparable to the next lower GGE/Band. You must document that you have a current successful performance evaluation. Education may be substituted for experience for some positions. If you feel your education is relevant to the position being filled, you must include college/university, dates attended, degree achieved, semester hours earned, GPA, major field of study, specific courses and course hours in your major on your resume.

EDUCATION SUBSTITUTION: Lower end of band - Ph.D. or equivalent degree

Must be able to obtain and maintain a TOP SECRET security clearance based on SBI and eligibility for Sensitive Compartmented Information (SCI).

2011-08-31 13:09:53

Final Draft Osman Tekes 20110831

Must successfully pass an initial and periodic counterintelligence scope polygraph examination.

In accordance with Change 3 to AR 600-85, Alcohol and Drug Abuse Prevention and Control Program, employee must successfully pass a urinalysis screening for illegal drug use prior to appointment and periodically thereafter.

All INSCOM employees may be subject to extended TDY or worldwide deployments during crisis situations to perform mission essential functions as determined by management.

Stress is inherent in the nature of work: The many short-suspense actions and pressures of time from nearly all contacts contribute to heightened demands. Under crisis operations, may be subject to short notice expanded hours and possible recall situations and irregular work hours, including weekends and holidays.

APPLICANTS WHOSE SELF-NOMINATIONS ARE RECEIVED BY THE CUT-OFF DATE WILL BE CONSIDERED FIRST.

APPLICANTS WHOSE SELF-NOMINATIONS ARE RECEIVED AFTER THE CUT-OFF DATE AND PRIOR TO THE CLOSING DATE WILL ONLY BE CONSIDERED IF THE SUPPLY OF CANDIDATES IS EXHAUSTED AND/OR THERE ARE ADDITIONAL VACANCIES TO FILL.

Your pay will be set within the range specified in this vacancy announcement and will be based on your qualification, education, experience, training, and availability of funds.

Quality of experience relates to how closely or to what extent an applicant's background and recency of experience, education, and training are relevant to the duties and responsibilities of the announced position. Candidates must have the knowledge, skills, abilities and competencies to successfully perform the work of the position at the appropriate level. [73]

NSA currently has career development programs in the following areas:

“

- Acquisition & Business Management
- [Computer Science](#)
- Engineering
- Mathematics
- Cryptanalysis
- [Information Assurance Analysis](#)
- Intelligence Analysis
- Language Analysis
- Organizational Leadership Management
- Security and Counterintelligence
- Signals Analysis
- Office and Support Professionals
- Senior Technical Development Program
- Joint Duty Assignment Program” [54]

9. The Three Gaps in knowledge of China and “leap frog” weapons

“Three Gaps in Our Knowledge of the Chinese Military, According to DOD”[56]
“Where are the Gaps in Knowledge?

For each of the major topics of assessment just outlined, there are a number of more specific subjects on which better information would be very useful. In some cases, we are unlikely ever to obtain exactly the information we would want. If some knowledge gaps cannot be corrected, it is at least advantageous to be aware that they exist. In general, three kinds of gaps stand out.” [56]

“ Second, as might be predicted, we are less knowledgeable about things that are less visible or tangible — training, logistics, doctrine, command and control, special operations, mine warfare — than we are about airplanes and surface ships. [56]

Third, although we can identify emerging methods of warfare that appear likely to be increasingly important in the future — particularly missiles and **information warfare** — we cannot confidently assess how each side ’ s capabilities will develop or the interaction of measures and countermeasures that these emerging military competitions will generate.” [56]

“Investments Recommended by the RMA Advocates. The RMA (Revolution in Military Affairs) visionaries (represented in numerous articles and five books in 1997) have been calling since at least 1993 for China to attempt to leapfrog the United States in the next two decades by investing mainly in the most exotic advanced military technology, and in new doctrines and new organizations.” [56]

“Key Priorities for Chinese Defense Investment” [56]

“Leap Style Weapons - GAD Director Cao Gangchuan in 2001 “ [56]

“In May 2001, the Chinese press reported a new phrase used in a speech by the director of the General Armament Department General Cao Gangchuan. He called for “Leap Style Weapons” using a new acquisition process he called the Four Mechanisms, which were vaguely defined as a new process of monitoring, evaluation and special incentives. These concepts were familiar. As early as 1988, AMS authors had called for a Leap Style. “[56]

“A fifth asymmetrical approach will be for China to attack American naval command and information systems.” [56]

“In an article entitled “The Military Revolution in Naval Warfare,” Captain Shen Zhongchang and his co-⁵ authors list new technologies that will contribute to the defeat of the United States. They explain that protection of C3I is now so important that “the US Defense Department has invested \$1 billion in establishing a network to safeguard its information system.” However, the American system may not be so safe from attack. Captain Shen writes that there are many ways to destroy information systems such as:

- attacking radar and radio stations with smart weapons
- jamming enemy communication facilities with electronic warfare
- attacking communication centers, facilities and command ships
- destroying electronic systems with electromagnetic pulse weapons

- **destroying computer software with computer viruses.**
- developing directed energy weapons and electromagnetic pulse weapons. “ [56]

“In the summer 1996 issue of *China Military Science*, General Pan Junfeng was the first to propose that the United States could be defeated with Assassin’s Mace weapons. He explains three ways that in future wars American computers can be very vulnerable. “We can make the enemy’s command centers not work by changing their data system. We can cause the enemy’s headquarters to make incorrect judgments by sending disinformation. We can dominate the enemy’s banking system and even its entire social order.” General Pan puts forward five suggestions for ways in which China can strengthen its development and implementation of the RMA:

- Increase research on military doctrine
- Establish operational theory
- Train high-quality people in advanced degrees
- Establish combat laboratories and learn from the six laboratories the United States has created
- Create sha shou jian, or “Assassin’s Mace weapons.”” [56]

“Information Warfare As An Assassin’s Mace Weapon” [56]

“The April 1997 issue of the journal *Military Operational Art* carried a proposal by Admiral Yang Yushu of the East Sea Fleet of the PLA Navy to develop a kind of “**information warfare system**” which must have Assassin’s Mace weapons which could defeat enemy. “**Soft**” Kills by Assassin’s Mace Weapons In their 1997 book, *Sun Zi and High Tech Warfare*, Colonels Yue Shuiyu and Liang Jingming wrote that the future will require development of *Assassin’s Mace weapon* with special characteristics. They advocated **dividing warfare into ‘soft’ and ‘hard’ missions**, with the emphasis on “**soft**” **attack** as the mission for which Assassin’s Mace weapons would be most needed. In the January 1999 issue of *China Military Science*, General Fu Quanyou, Chief of the PLA General Staff wrote: “ In order for The Inferior to Defeat the Superior, first, we need to rely on high quality people; second , we need to rely on the smart combat doctrines; third, we need to rely on the high quality Assassin’s Mace weapons.”” [56]

“Information Warfare Requires Assassin’s Mace Weapons Colonel He Jiasheng, a senior editor from *Liberation Army Daily* wrote about leap-forward style “Assassin’s Mace weapons” as a part of Information Warfare in the February 2001 issue of *China Military Science*. He advocated at “focus on information warfare equipment and our **own Assassin’s Mace weapons.**”” [56]

“Special Forces and Network Assassin’s Mace Weapons The April 2, 2001 issue of *Liaowang* by the New China News Agency featured a PLA author’s proposal that “We can’t just use a keyboard and mouse in information warfare. We need special operations forces and direct destruction of the enemy network at headquarters, including research on Assassin’s Mace weapons to **attack the enemy’s network.**”” [56]

“In an article in the April 4, 2001 issue of *Liberation Army Daily*, Sheng Changxiang of the Academy of Engineering wrote that one Assassin’s Mace weapon that can win contemporary wars is equipment for the “protection of information,” the mission area of information security. “[56]

10. The Russian invasion of Georgia

“The Russian invasion of Georgia saw Moscow’s troops steamroll over Tbilisi’s soldiers with ease. But the end result of the invasion was never truly in doubt considering the relative size and strength of Russia compared to Georgia. And in fact, a joint analysis in Reuters by military analysts Aydar Buribaev (in Moscow), James Kilner (in Tbilisi), Oleg Shchedrov (in Sochi), written up by Christian Lowe, has a completely different analysis: Russia’s biggest combat operation since USSR occupied Afghanistan revealed terrifying weaknesses in its military strength.” [65]

“Here’s a summary of relevant points:

2011-08-31 13:09:53

Final Draft Osman Tekes 20110831

+ The Russian commander that spearheaded the invasion was wounded by a Georgian ambush attack on day two of the deployment. Later, Russian soldiers rode into battle riding on top of their armored personnel carriers instead of inside, because the flawed armour makes it highly vulnerable to rockets and land mines.

+ Four Russian aircraft, including one long-range supersonic bomber, were shot down by Georgia's air defenses, because the Russian military probably lacked the technology to locate and destroy Georgia's anti-aircraft platforms from a distance.

+ The troop deployment by Russia was many times that of the standing army of Georgia, but this was necessary because of a lack of long range offensive technology that could have reduced the required number of troops.

+ The invasion gave NATO planners an opportunity to carefully scrutinize Russian military strategy, hardware, and conduct. Current Russian tactics generally follow the Soviet pattern, with an air and artillery attack followed by the deployment of a large ground force, and in all practicality lack the sophistication of modern tech-heavy 21st century warfare." [65]

11. Russian attempts to upgrade nuclear capabilities

“With the recent failed launch of the Bulava missiles the Russian Federation has found itself in another political/military quandary. The failed tests were a gamble taken to reassure to the world the legitimacy of Russian military prowess, but instead it showed that the new military technology Russia has acquired is less than it initially seemed. This latest failure is just one of a long line of setbacks that have recently befallen the Russian military establishment, most of which have been tragic, like the Kursk or the Nord-Ost Theater siege, in which a nerve agent meant to pacify the hostages and their captors killed them.’ [62]

“The Bulava missile is a submarine based weapon, and is nearly impervious to current and future missile defense systems. It is estimated that each missile can carry up to ten reentry vehicles (100-150 kT yield) and has an operational range up to eight thousand kilometers. Currently, the Bulava is not deployed the Russian missile submarines, known as the Akula class. It is projected though that within the next year three brand new Borei class nuclear submarines will be equipped with sixteen missiles each. Basic arithmetic shows that the Russian Navy will then have the possibility of deploying four hundred eighty nuclear weapons at any given time. It is sufficient to say that this something **others should take notice of, which is exactly what the Russians want.**” [62]

”The Russian struggle for acceptance and legitimacy through the past two decades has been the trigger for every show of military force (note the pervasive use of force in Chechnya and Georgia) and weapons development since the end of the Cold War. The Bulava tests and the development of the Borei class submarine are no different; they are of the same ilk as the development of the ‘Father of All Bombs’ (a saucy play on the American ‘Mother of All Bombs’) and the reinstitution of strategic bomber flights throughout the world. What adds to this posturing by Russia is the recent announcement by American sources that two Akula class nuclear submarines have been detected within launch range of the American East Coast. The Russian Navy is showing that if it can place its twenty-eight year old Akula’s off the American coast then it will certainly be able to put its brand new ships within striking range as well. They are also showing they can have up to three hundred nuclear warheads in that region, ones that are designed to sneak through defense systems (not that the Eastern seaboard has any notable missile defense systems).” [62]

“Of course, this show of technology should not be taken out of context. The Russian Federation is not preparing a surprise nuclear blitz on Washington in reprisal for the end of the Cold War, and it likely has absolutely no intentions of using the Bulava for any offensive purpose. What should be taken from this posturing is that the Russian Federation does still have nuclear potential, and has made an impressive stride in cementing its own nuclear triad, something it lacked for a good portion of the Cold War. However, there are even caveats to go along with this observation. With a failure rate of roughly fifty percent during tests (likely because of a fast track testing program instituted in 2006), the Bulava will likely not be entering service in late 2009 as was initially predicted by the Russian Navy.” [62]

“These failures have also had a damaging effect on the Russian political/military psyche. Combined with **its lust for acceptance in the world power circles**, these failures have exacerbated what are likely feelings of inadequacy amongst the Russian military elite and frustration in the cadres of its political elites. History shows that prior failures have a strong effect on the Russian military strategy. The First Chechen War, though a tactical victory for Russia, was viewed as an embarrassing defeat by both the Russian populace and the global community as a whole. How was it that a rag tag confederation of clans had inflicted such heavy casualties on what was thought to have been one of the more powerful and apt militaries in the world? Why had Russia not taken lessons learned in Afghanistan? What had gone wrong? These questions were pondered by the rest of the world and that tore at the conscious of the Kremlin. The Second Chechen War demonstrated that. The First war had been a brutal exercise in nonchalance towards civilian casualties, and the Second took that to a new level. The increased use of indiscriminate bombings and a lackadaisical approach to troop control resulted in the sacking of Grozny and other cities in Chechnya, and eventually the complete pacification of the region. While disputed and attacked throughout the world for its brutality, annihilationist warfare was an ends that met its means. The reflection given to the First War by the Kremlin had helped it win the Second. The destruction in Chechnya has proven that the past dictates the future in Russian military strategy, and they are sure to not allow the failures continue.” [62]

“In the opinion of the analyst, the failures of the Bulava missiles, as well as other weapons platforms, shows that while Russia is experiencing difficulties, it is moving forward quickly in the spectrum of military hardware and that each failure is only adding a burning desire to succeed and more technical knowledge to the Russian arsenal. It is possible that the Russian military, if it can overcome its self perception issues and personnel problems, will become the preeminent force that it has always strived to be.” [63]

12. Analysis of Strategic Warning: Indication Intelligence

Some of the more difficult questions for defenders appears to be:

1. Could it be possible to detect strategic and tactical cyber attacks or operations in advance?
2. Could it be possible to detect strategic and tactical cyber attacks or operations, when the attack or when operation is taking place?
3. Could it be possible to discover and document strategic and tactical cyber attacks or operations took place in the past?

Answers to above questions are mostly technical and technological in nature Network Security offers Intrusion Detection and Prevention with limited success and Digital Forensics offers Network Forensics. We will investigate those later. But there is another approach based on a technique developed by the Defence Intelligence community, “Analysis of Strategic Warning” [67]

Even though the technique was developed for different purpose and era, it could be used in to determine possibility of a cyber attack or operation.

There are couple of reason we would like to review the background of conflicts and their history. Most likely most of the conflicts are managed and manipulated or are subverted by third parties to create opportunities for themselves. At the minimum they may employ misinformation war on cyber space and traditional media. Another reason some of these low level hostilities boil over to website attacks to DDOS attacks, especially certain anniversaries. Depending on ones location and vulnerabilities it is critical to understand the role of the history in cyber offences and assaults.

In attempts to predict cyber attacks, when one looks back the sequence of events, one would observe that the increasing political tensions and increase in hostile statements both by states and non-states agents has been precursor to cyber attacks. Also, when attributing and attack to a source in addition to understanding the technical evidence; analysis of political, social, and historical aspects are important as well. Cyber attacks do happen in a historical, social, and political context, and they are more likely when perceived injustices become more obvious. In some sense, some of the simpler exploitations like website attacks could be linked to previous real life events which are perceived as injustice by some.

Here is how I propose to modify the Indication Intelligence [67] technique:

Developing a list of political and social indicators; and measures for their intensity to be assessed over time.

Developing a list of technical (network, number of probes, websites offering tools, incitement, etc.) indicators and measures of intensity to be assessed over time

Developing government and organization specific indicator lists based on their past attacks and operations (e.g. for Russia based on Estonia and Georgia attacks)

Type of attack and changes in the attack type [72]

Attack tactics, techniques, and tools used [72]

Analyzing these indicators as time series and investigating the trends and rate of changes correlated with our own actions

Automating data collection via web crawlers

13. First Cut Data Model Cyber War – complete

When Row 2 of Zachman's Framework is investigated one would interview people representing at different organizational responsibilities and different organisational levels. For example people from marketing, finance, human resources, production, distribution, procurement, product planning, etc. would be interviewed to understand and document their operations. In order to build a coherent enterprise architecture these views must be integrated and a common language across the enterprise should be established.

People at different levels of organization are interviewed to understand the organization from different levels, such as a vice president's view, director's view, a manager's view, supervisor's view, staff's and worker's views. All of these views would focus on slightly different aspects of the area and most likely add different levels of detail.

Since using above approach is not possible at this time, instead the above knowledge of the topic would be extracted and deduced from publicly available sources.

In chapter four, a First Cut Data Models should have been created with the subject matter experts to inventory and define organizational concepts and terminology used by the practitioners and experts in these areas. Usually the entity types discovered during the development of a first cut data model is referred as candidate entity types; they are subjected to further definition, assignment of unique identifiers and representative data elements following rules of normalization. Then the conceptual data model would be a requirements definition for a database development (e.g. Enterprise Operational Data Store – Bill Inmon).

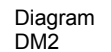
The boxes on the data model represent entity types and the lines represent the relationships. Usually cardinalities and optionality are also documented, but in this paper we will not go into those details. Cardinality indicates how many of one entity type is related to how many of other entity type. Usually 1 to N, N to 1, N to N, or a constraint number e.g. 3 to 1 or 3 to N. Optionality is indicated with 0, which means there could be an entity type or not. When the other entity type is created, the secondary entity type may, or may not exist or is not required. If the optionality is 1, it is mandatory, meaning the entity type must exist.

A set of data models will be created for Cyber Warfare, Cyber Espionage, and Cyber crime if time and space allow. The detailed models are in the appendix, and only simplified sample versions are in the main body of the paper.

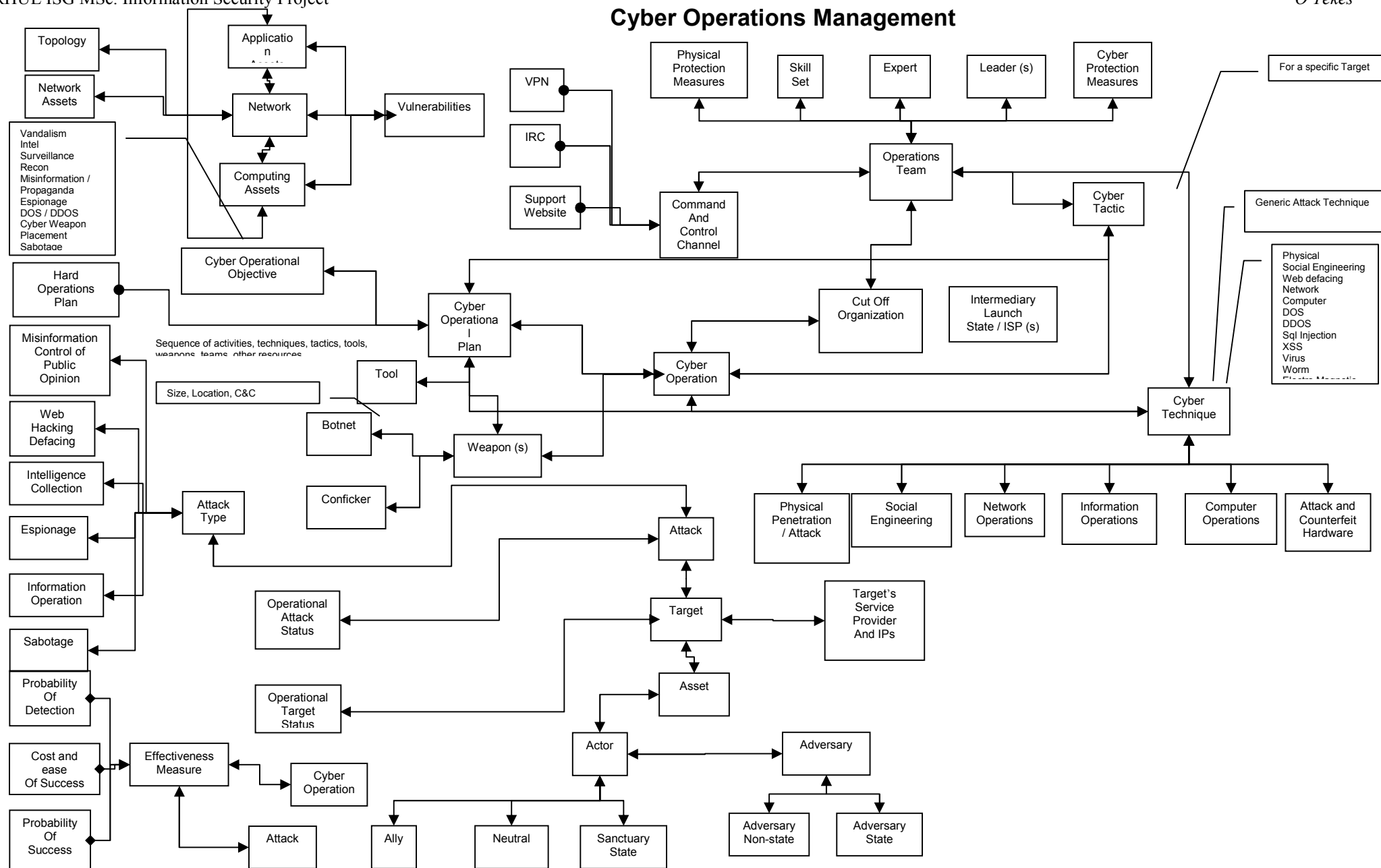
Based on the knowledge gathered from the books, articles, and other sources sample data models depicting interrelationships and dependencies are developed. This understanding is enhanced with the knowledge gained during the Penetration Testing and Digital Forensics courses.

Final Draft Osman Tekes 20110831





Cyber Operations Management

Diagram
DM3

14. Entity Types of First Cut Conceptual Data Model

	Entity Type Name	Explanation	Offence Types	Sub Type of	Diagram
1.	Surveillance	Remote or automated or in person observation of targets, organizations, and people. May include contents of websites, creation fo new websites, IRC channels, monitoring number of hits, number of times a website appears on a search, number of visits etc.			
2.	Operations Teams	Cyber Operations Team, hacking team			
3.	Rules of Engagement	A series of thresholds moving from realm of cyber crime to cyber warfare requiring immediate and urgent response to protect critical infrastructure or to protect un acceptable devastating impact			
4.	Adversary	A Digital Suspect or potential suspect [106]			
5.	Attack on H/W and Counterfeit H/W	Supply Chain Security			
6.	Zone of Conflict	Could be Geographic area, Location, Idea, Issue, etc. Needs further investigation in future			
7.	SOC	Information Security Operations Center . Security Operations Centre [132]			
8.	Event	Anomalies Types of events are: Network Event, Environmental Event, Computer Event (memory, cpu, etc.)			
9.	Management Systems	Network or Cyber Defense or Warfare Management			
10.	Analysis Systems	Analysis of Events or Anomalies			
11.	Private Network	Network to defend networks			
12.	Attack	Actual instance of an attack and related data			
13.	Technique	In general how an Attack is conducted, steps and phases e.g. in Penetration Testing or hacking, or Sequence of Scripts or activities used in a Social Engineering Attack, or Sending Phising emails to install trojans, etc.			
14.					
15.					
16.					
17.					
18.					
19.					

15. First Cut Process Model Cyber War – complete

In similar to first cut data models, matching conceptual process models are developed to define organizational process. In this paper data flow diagramming technique is used with event and control flows. In data flow diagrams, the rectangles with rounded corner represent the process. The arrows represent data flows and control flows. The data flows has defined data contents usually the elements of data model is used. Control flows or event flows may or may not have data contents. They represent near real time occurrence of an operational or control event. The event partitioning technique more appropriate to develop detailed models using a proper CASE tool.

The funny tubes represent data stores. Either the contents of data stores usually match to conceptual data model at entity type level or a set of entity types packaged together in one data store. (In proper DFD, data store representation is different then these funny tubes, but the correct data store symbol is not available in MS PowerPoint).

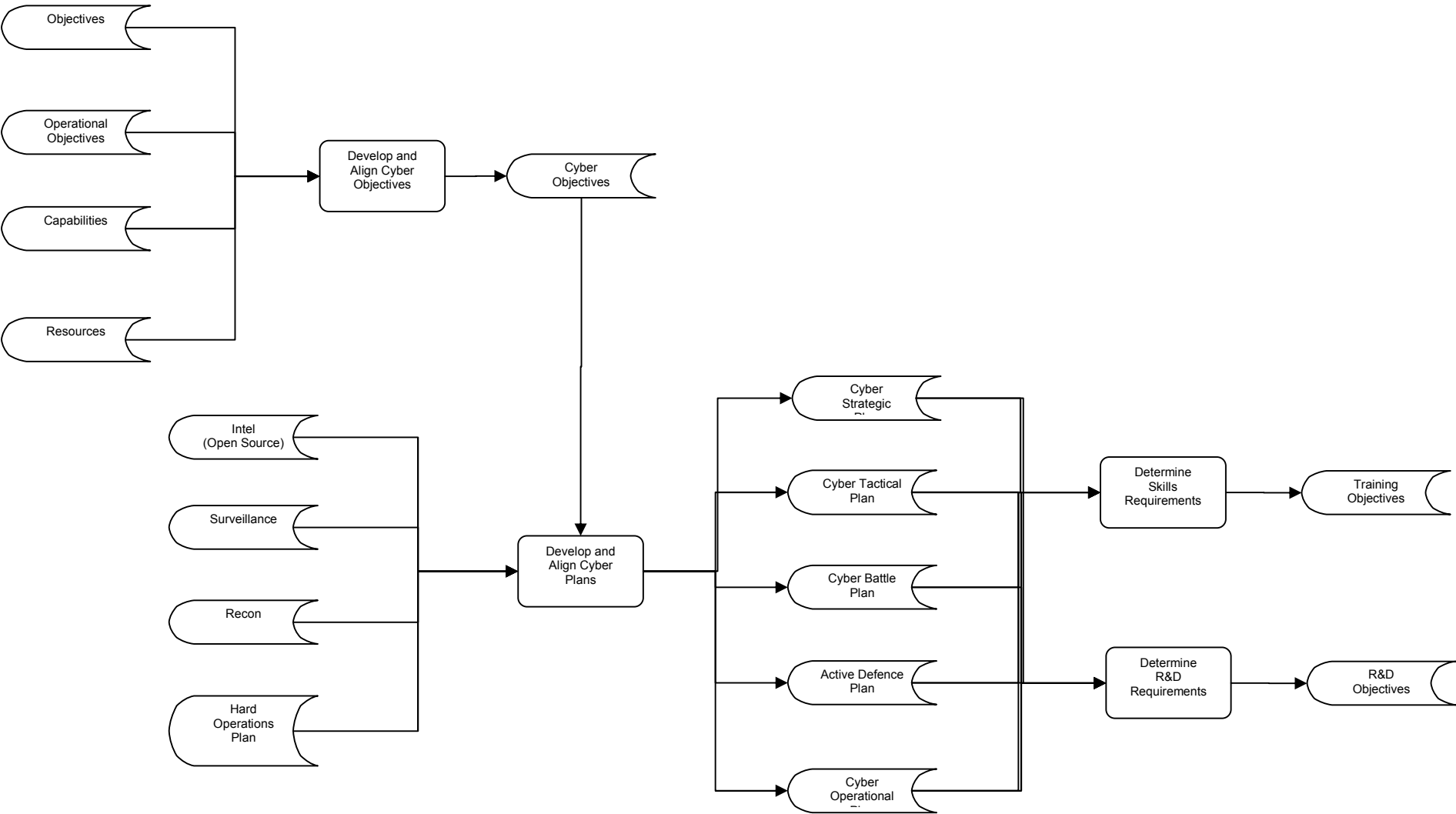
A set of process models will be created for Cyber Warfare, Cyber Espionage, and Cyber crime if time and space allows. The detailed models are in the appendix, and only simplified sample versions are in the main body of the paper.

We will develop two sample matrices. The first one is Entity Type by Objectives. Entity Types will be listed on the rows and objectives will be listed as columns. Cell values would indicate support or alignment. This matrix is useful in couple of ways, one to make sure there are entity types supporting all the objectives. This would assure we have completely covered the conceptual data scope to support the objectives. If there are entity types, which are not supporting specific objectives, this should be investigated and cause should be determined and documented. In similar fashion to above, a process versus objectives matrix is created similar and parallel analysis is completed on processes too.

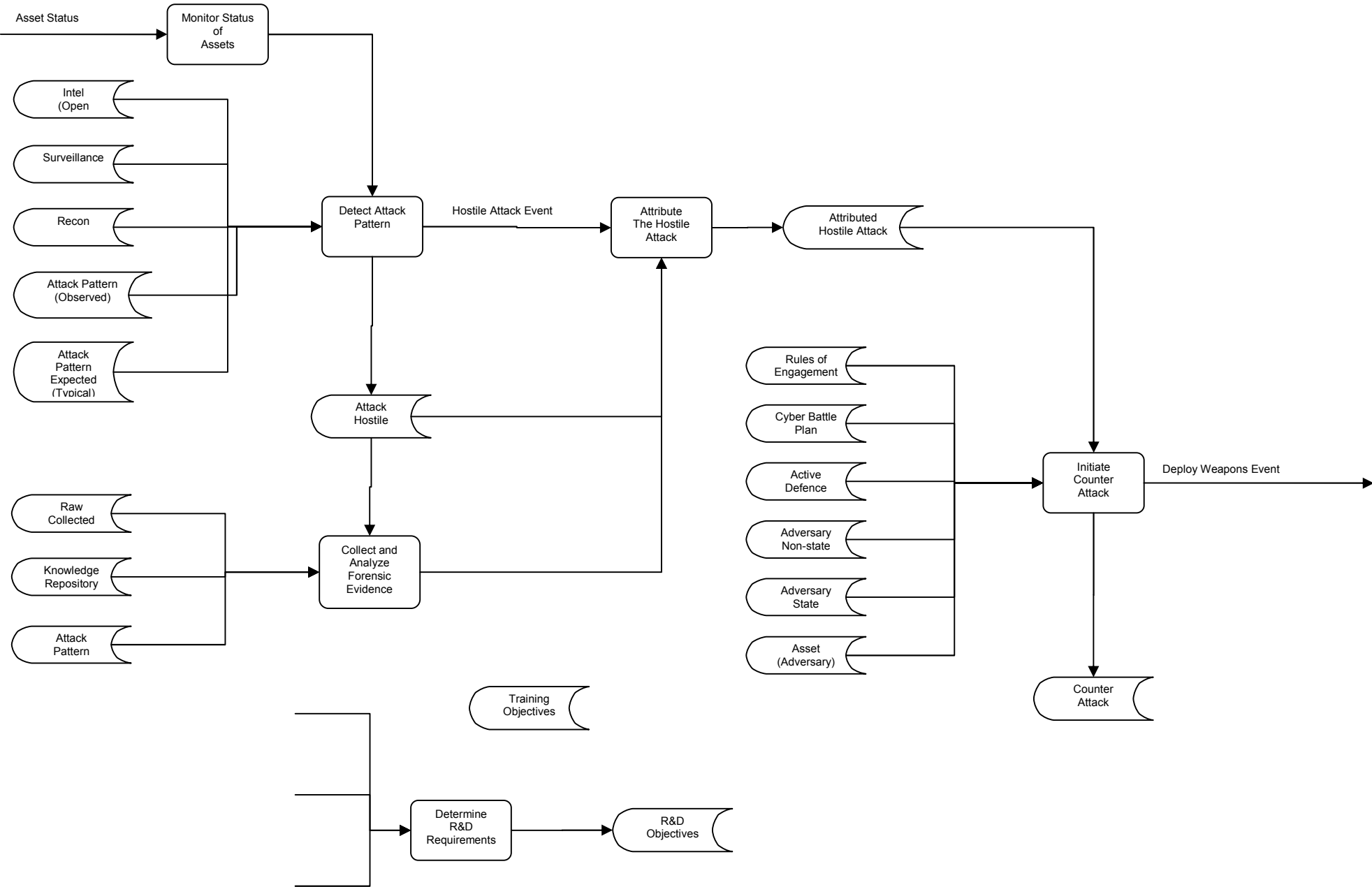
Only the very simplified versions of these matrices are created to show a mock-up version of the analysis.

Based on the knowledge gathered form the books, articles, and other sources sample these process models, are developed. This view will be enhanced with knowledge gained during the Penetration Testing and Digital Forensics courses time and space permitting.

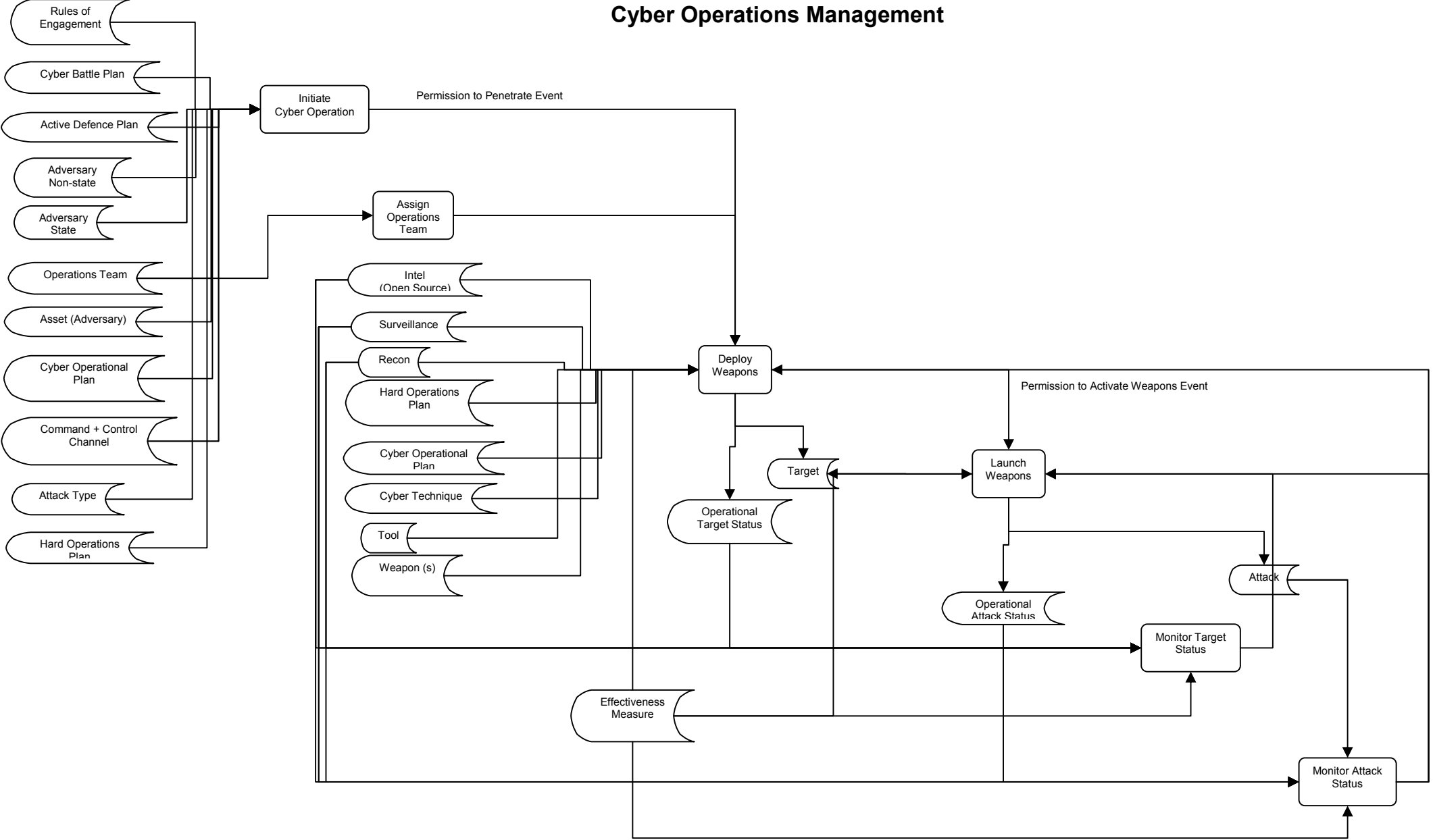
Planning, Preparation, and Training



Detection, Investigation, and Attribution



Cyber Operations Management



17. Former NSA & CIA Director Suggests Employing Mercenaries For Cyberwarfare



One of the architects of US foreign policy under George W. Bush, General Michael Hayden, suggested that the US Government should consider creating a "Digital Blackwater" during an open conversation with Bloomberg's Allan Holmes and several other cybersecurity specialists on stage, during an event called the Aspen Security Forum. Blackwater refers to the US private military group founded in 1997 and which has been renamed as Xe Services LLC, a move possibly linked with a number of high controversies that arose after the company expanded its security-related operations into Iraq and Afghanistan.

Recruiting mercenaries, Hayden suggested "might be one of those big new ideas in terms of how we have to conduct ourselves in this new cyber domain," referring to cyber warfare.

He continued by saying "You think back long enough in history and there are times when the private sector was responsible for its own defense," before adding "we may come to a point where defense is more actively and aggressively defined even for the private sector and what is permitted there is something that we would never let the private sector do in physical space".

Hayden went on to suggest the creation of a digital Blackwater, something that Xe might already be considering before hinting at what will happen next; "private sector expands to fill the empty space" before ominously claiming, "these are the kinds of things that are going to be put into play here very, very soon."

Hayden's comments should not be taken lightly because of his background as the Director of the CIA and also the National Security Agency under George W. Bush; both agencies have either been hacked or been heavily involved in cyber warfare. Under his leadership, both also significantly increased their partnerships with private military groups like Blackwater.

Recruiting whitehat hackers in the world of online security is nothing new, but Hayden suggests externalising the process of cyberwarfare away from the US government as it did with private military companies during the last decade. The complete discussion can be found below. [107]



Robinson Mitchell ★ 2 days ago

I agree with former Director Hayden's suggestion that the U.S. should hire private contractors as white hat hackers to combat the bad guys out there. I object to the use of the term "cybermercenaries" however. A cybermercenary is as likely to become a turncoat if he receives a better offer from the other side. A committed, dedicated professional who is committed to wiping out cyberterrorism is a very different sort of person than a cybermercenary. The mercenary mentality is something to be avoided at almost any cost. The white hats must be as carefully vetted and background checked as those working for the agencies Director Hayden previously led. We need professional "ideological white hats", not mercenaries.

Flag

Like ReplyReply



Lee Scott ★ 2 days ago

As a retired NSA official, I am not permitted to comment on this article. BUT, I am as discouraged with our government as most people and am a leading Progressive Movement blogger who tries to put the best articles in front of my growing audience. See www.d-daydems.blogspot.com for more.

Flag

Like ReplyReply



Zalice ★ 2 days ago

I have been contacted three times for such proposals. First one was by Israelies. I was at that time working for the French army. Once I left, I got contacted by the Chinese (this was in 2000.. 10 years ago they Chinese were already recruiting white/black hats). Recently, we saw french members of secret services get closer to some of our presentations mixing hardware hacking and BSD/Linux-based software and to my knowledge, no one accepted.

Governments don't like us because we are not little soldiers that went under training and we are not the kind of people that tolerate unskilled people, bullshit and shutting up. We are good but we are also blunt and we have no tolerance for people without high skills.

The army and those services are filled with incompetent people, and when they ask us to hack into some other government computers, most of the time they are slowing us down asking us to explain everything we do, while they are unable to understand 1 % of what we are doing. They make things go slow, and not how they should. We have to spend a lot of time doing things they don't need for the job to get done, and often they make stuff fail.

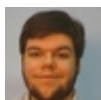
The Chinese on the other hand, they pay well. They give hardware. And they are interested in results. And they are listening to requests and getting things done. So they get all the data in their hands, and have been doing so for over 10 years. We did train a lot of chinese students before they were sent to work all over the world in companies, in order to steal information from corporate industries, and this dates back to 1999/2000. They stole everthing in electronic and technical data from companies all around.

We don't like governments. Too much incompetent people. They have a lot of trouble with out personalities (we say up loud what we thing and tell people that are not competent enough they need to move to another job) and most of us are Unix people, and we're rather paranoid all the time. So we work, as freelances, for money and most governments are getting new holes up their bottoms from us.

Flag

Like ReplyReply

Reactions



James Renken2 days ago

From twitter

"Employing mercenaries for cyberwarfare." <http://is.gd/lpLRvo> Riiight. Can I get a Tweet of Marque and Reprisal?

© 2008 — 2011 Net Communities. All rights reserved.

18. Gladio Organizational Structure

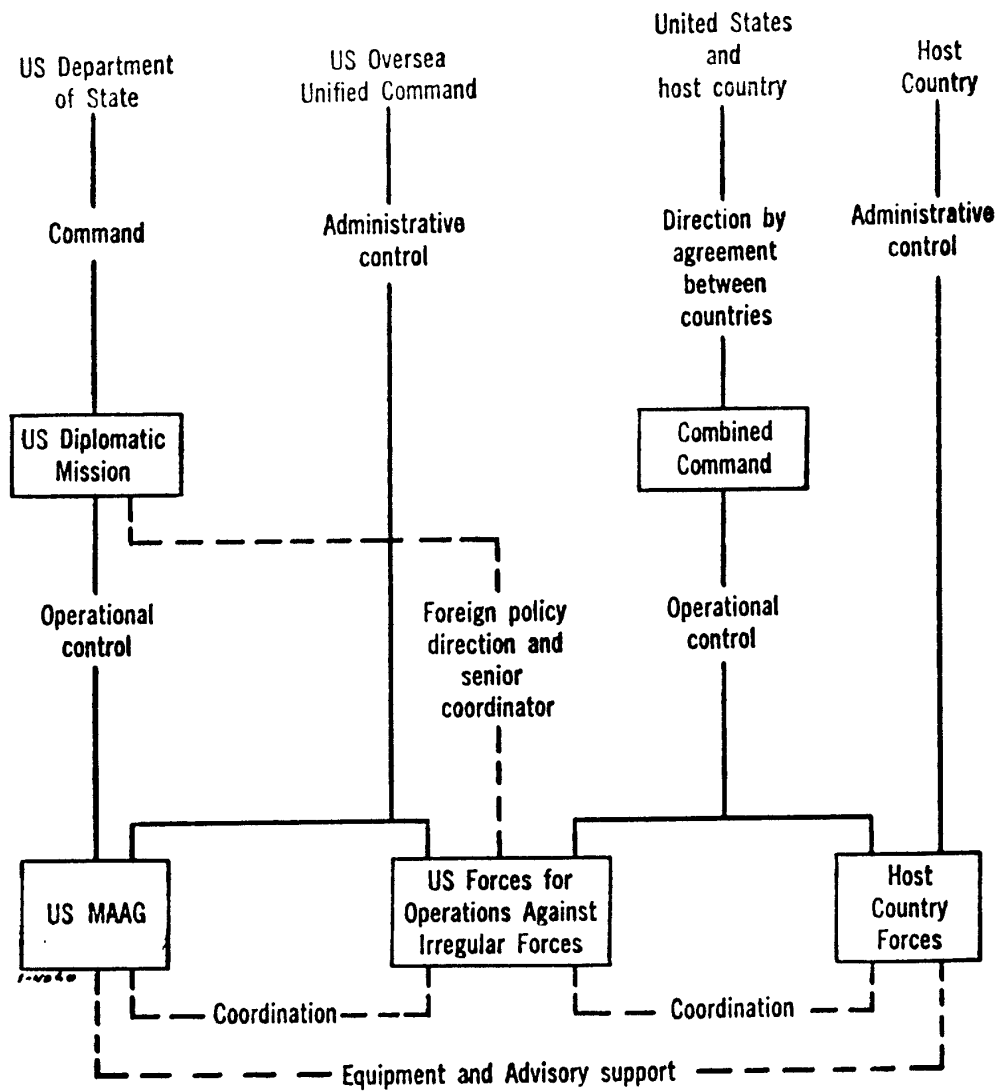


Figure 3. Possible relationships in a cold war situation.

19. Some examples of simple attack techniques

1. Building your criminal infrastructure with some one else's identity and money [103]

1. Step one: Steal identities and credit cards, if in hurry buy them
2. Step two: test the credit card numbers wit small item purchases.
3. Step three: Register domain names all over the world with stolen identities and credit card
4. Step four: make long term contract with hosting services companies in different parts of the world and pay in advance for long term contracts using the same stolen identities and credit card numbers. Do it quickly before the original owner discovers.

2. Example attacks on US Serviceman [72 page numbers]

3. ? Domain

4. Linkedin, facebook, and other social network sites with the information collected admin passwords are predicted from page 150

5 The last chapter [72]

More in [139 pages 68 – 73]

20. Cyberwarfare Market 2008-2018

Cyber attacks have for some time been no longer in the realm of fiction or film, but a cause for concern in the real world. Although annoying acts such as website defacements and virus spread have become fairly common, the cyber attacks in the Baltic state of Estonia in early 2007 managed to disrupt that country's financial system for a few weeks. There were concerns that this could be just the tip of the iceberg in computer network attacks; certainly, it was an event that showed how effective attacks on IT networks and systems could be, even at national level. Certainly, the consequences would be much more significant if those attacks had occurred on a greater scale, attacking central computers in government, policing and defence, in a nation or group of nations. It has been suggested that those attacks were a foretaste of what dedicated hackers belonging to terrorist groups or hostile powers could do, constituting a new form of warfare - cyberwarfare. Such threats would be far more serious than those of amateur hackers, despite the inconvenience these have caused. Furthermore, professional hacking groups or cells are likely to be far harder to repel, locate, close down, capture and convict. How can you compete with this?

In this new defence market report, Cyberwarfare, 2008-2018, visiongain analyses the cyberwarfare market in detail, covering its range from defensive to offensive capabilities. The cyberwarfare market is already large and growing, with most of the spending at present devoted to cyber defence. Visiongain expects the market to grow consistently from 2008 onwards. Rumours of developing cyber offensive capabilities and actions will further induce nations to do more to protect their vital networks, as well as stimulate the development of cyberwarfare capabilities as a natural progression in defence. The interest is strong among many nations to develop or improve their abilities to deal with cyberwarfare, providing significant opportunities for companies involved in computer protection and IT systems hardware, software and services in general. Are you and your company prepared to capture a key market share in these countries? How will your company best target these attacks?

There is now a realisation among many governments and militaries that "cyberspace" has become a new battleground, possibly on par with other recognised battle spaces in conventional warfare and defensive operations.

More detailed information on this report:

<http://www.asdreports.com/shopaff.asp?affid=21&id=312> [130]

21. Key Companies in Cyberwarfare and Cybersecurity [130]

- 6.1 3Com
- 6.2 BAE Systems
- 6.3 Bearing Point
- 6.4 Crypt
- 6.5 Cisco
- 6.6 Check Point
- 6.7 Cyber Defense Agency (CDA)
- 6.8 Juniper Networks
- 6.9 F-Secure
- 6.10 Lockheed Martin
- 6.11 McAfee
- 6.12 Northrop Grumman
- 6.13 PGP Corp
- 6.14 QinetiQ
- 6.15 Raytheon
- 6.16 SAIC
- 6.17 Secure Computing
- 6.18 Sophos
- 6.19 SPI Dynamics
- 6.20 SRA International
- 6.21 Symantec
- 6.22 Tata
- 6.23 TDi
- 6.24 Thales
- 6.25 Unisys [130]

From other sources:

Treadstone 71, LLC - <http://www.treadstone71.com/>

21. Spymaster sees Israel as world cyberwar leader [131]



1:47pm EST

2011-08-31 13:09:53

Final Draft Osman Tekes 20110831

By Dan Williams

TEL AVIV (Reuters) - Israel is using its civilian technological advances to enhance cyberwarfare capabilities, the senior Israeli spymaster said on Tuesday in a rare public disclosure about the secret program.

Using computer networks for espionage -- by hacking into databases -- or to carry out sabotage through so-called "malicious software" planted in sensitive control systems has been quietly weighed in Israel against arch-foes like Iran.

In a policy address, Major-General Amos Yadlin, chief of military intelligence, listed vulnerability to hacking among national threats that also included the Iranian nuclear project, Syria and Islamist guerrillas along the Jewish state's borders.

Yadlin said Israeli armed forces had the means to provide network security and launch cyber attacks of their own.

"I would like to point out in this esteemed forum that the cyberwarfare field fits well with the state of Israel's defense doctrine," he told the Institute for National Security Studies (INSS), a Tel Aviv University think tank.

"This is an enterprise that is entirely blue and white (Israeli) and does not rely on foreign assistance or technology. It is a field that is very well known to young Israelis, in a country that was recently crowned a 'start-up nation'."

Cyberwarfare teams nestle deep within Israel's spy agencies, which have extensive experience in traditional sabotage techniques and are cloaked in official secrecy and censorship.

They can draw on the know-how of Israeli commercial firms that are among the world's hi-tech leaders and whose staff are often veterans of elite computer units in the conscript army.

Technolytics Institute, a private U.S. consultancy, last year rated Israel the sixth-biggest "cyberwarfare threat," after China, Russia, Iran, France and "extremist/terrorist groups."

Noting that the United States and Britain are setting up cyberwarfare commands, Yadlin said Israel has its own "soldiers and officers" dedicated to this field.

He did not cite any specific targets for potential Israeli attacks. A military spokeswoman said the INSS speech was the first time that Yadlin, who has overall responsibility for Israeli intelligence, had discussed cyberwarfare in public.

"Preserving the lead in this field is especially important given the dizzying pace of change," Yadlin said.

Israel, which is assumed to have the Middle East's only atomic arsenal, has hinted it could attack Iranian facilities if international diplomacy fails to curb Tehran's nuclear designs. Israel bombed Iraq's nuclear reactor in 1981, a mission Yadlin took part in as an F-16 pilot.

But many experts believe the sites are too distant, dispersed and fortified for Israel's air force to take on alone. Washington has also voiced misgivings at the idea of open force.

"Cyberspace grants small countries and individuals a power that was heretofore the preserve of great states," Yadlin said.

"The potential exists here for applying force ... capable of compromising the military controls and the economic functions of countries, without the limitations of range and location." (Writing by Dan Williams; Editing by Alastair Macdonald)

22. Treadstone Cyber Counter Intelligence Doctrine [108]

Here are my notes from the training video created by the Treadstone 71, LLC:

Activities or steps of Cyber Counter Intelligence: [108]

1. Identify
2. Manipulate, Disrupt, and Neutralize
 - a. Penetrate
 - b. Deception – e.g. online media manipulation and redirection
 - c. Neutralize Adversary Operations
3. Recruit and induce defection using cyber persona
4. Leverage Denial, Deception, Counter Denial, Counter deception
 - a. Information war
 - b. Psychological Operations
 - c. Online media manipulation and redirection
5. Exploit - Collect Cyber Intelligence
 - a. Threat Information
 - b. Modus Operandi
 - c. Intelligence Requirements
 - d. Targeting
 - e. Objectives
 - f. Communications
 - g. Capabilities
 - h. Limitations
 - i. Linguistics
 - j. Attributable Hosting Locations
 - k. Vulnerabilities
6. CCI support - ??
7. Human Intel and cyber Intel support
8. ???

More information is available on Treadstone 71, LLC - <http://www.treadstone71.com/> and [108], [138 pages 33and 34]

23. Industrial Espionage Notable cases [144]

1. “France and the United States

In 1991 [Air France](#) was accused of helping its spy agency garner corporate secrets through installing microphones in its seats. Between 1987 and 1989, [IBM](#) and [Texas Instruments](#) were also thought to have been targeted by French spies with the intention of helping France's [Groupe Bull](#).^[35] In 1993, US aerospace companies were also thought to have been targeted by French interests.^[36] During the early 1990s, France was described as one of the most aggressive pursuers of espionage to garner foreign industrial and technological secrets.^[35] France accused the U.S. of attempting to sabotage its high tech industrial base.^[35] The government of France has been alleged to have conducted ongoing industrial espionage against American aerodynamics and satellite companies.^[37]

2. Volkswagen

In 1993, car manufacturer [Opel](#), the German division of [General Motors](#), accused [Volkswagen](#) of industrial espionage after Opel's chief of production, Jose Ignacio Lopez, and seven other executives moved to Volkswagen.^[11] Volkswagen subsequently threatened to sue for defamation, resulting in a four-year legal battle.^[11] The case, which was finally settled in 1997, resulted in one of the largest settlements in the history of industrial espionage, with Volkswagen agreeing to pay General Motors \$100 million and to buy at least \$1 billion of car parts from the company over 7 years, although it did not explicitly apologize for Lopez's behavior.^[38]

3. Hilton and Starwood

In April 2009 the US based [hospitality company](#) [Starwood](#) accused its rival [Hilton](#) of a "massive" case of industrial espionage. After being purchased by [private equity](#) group [Blackstone](#), Hilton employed 10 managers and executives from Starwood. Under intense pressure to improve profits, Starwood accused Hilton of stealing corporate information relating to its luxury brand concepts, used in setting up its own Denizen hotels. Specifically, former head of its [luxury brands](#) group, Ron Klein, was accused of downloading "truckloads of documents" from a laptop to his personal email account.^[39]

4. GhostNet

[GhostNet](#) was a 'vast surveillance system' reported by Canadian researchers based at the [University of Toronto](#) in March 2009. Using targeted emails it compromised thousands of computers in governmental organisations, enabling attackers to scan for information and transfer this back to a 'digital storage facility in China'.^[40]

5. Google and Operation Aurora

On January 13, 2010, [Google Inc.](#) announced that operators, from within China, had hacked into their Google China operation, stealing intellectual property and, in particular, accessing the email accounts of human rights activists.^{[41][42]} The attack was thought to have been part of a more widespread cyber attack on companies within China which has become known as [Operation Aurora](#).^[42] Intruders were thought to have launched a [zero-day attack](#), exploiting a weakness in the [Microsoft Internet Explorer](#) browser, the malware used being a modification of the [trojan Hydraq](#).^[21] Concerned about the possibility of hackers taking advantage of this previously unknown weakness in Internet Explorer, the Government of Germany, then France, issued warnings not to use the browser.^[43]

There was speculation that 'insiders' had been involved in the attack, with some Google China employees being denied access to the company's internal networks after the company's announcement.^{[44][45]} In

February 2010, computer experts from the U.S. [National Security Agency](#) claimed that the attacks on Google probably originated from two Chinese universities associated with expertise in computer science, [Shanghai Jiao Tong University](#) and the Lanxiang Vocational School, the latter having close links to the military.^[40]

Google claimed at least 20 other companies had also been targeted in the cyber attack, said by the London [Times](#), to have been part of an 'ambitious and sophisticated attempt to steal secrets from unwitting corporate victims' including 'defence contractors, finance and technology companies'.^{[42][41][43]} Rather than being the work of individuals or organised criminals, the level of sophistication of the attack was thought to have been 'more typical of a nation state'.^[41] Some commentators speculated as to whether the attack was part of what is thought to be a concerted Chinese industrial espionage operation aimed at getting 'high-tech information to jump-start China's economy'.^[46] Critics pointed to what was alleged to be a lax attitude to the intellectual property of foreign businesses in China, letting them operate but then seeking to copy or reverse engineer their technology for the benefit of Chinese 'national champions'.^[47] In Google's case, they may have been concerned about the possible misappropriation of source code or other technology for the benefit of Chinese rival [Baidu](#). In March 2010 Google subsequently decided to cease offering censored results in China, leading to the closing of its Chinese operation.

6. CyberSitter and 'Green Dam'

The US based firm [CyberSitter](#) announced in January 2010 that it was suing the Chinese government, and other US companies, for stealing its anti pornography software, with the accusation that it had been incorporated into China's [Green Dam](#) program, used by the state to censor Chinese^[48] citizens' internet access. CyberSitter accused Green Dam creators as having copied around 3000 lines of code. They were described as having done 'a sloppy job of copying,' with some lines of the copied code continuing to direct people to the CyberSitter website. The [attorney](#) acting for CyberSitter maintained "I don't think I have ever seen such clear-cut stealing".^[49]

7. USA v. Lan Lee, et al

The United States charged two former NetLogic Inc. engineers, Lan Lee and Yuefei Ge, of committing economic espionage against TSMC and NetLogic, Inc. A jury acquitted the defendants of the charges with regard to TSMC and deadlocked on the charges with regard to NetLogic. In May 2010, a federal judge dismissed all the espionage charges against the two defendants. The judge ruled that the U.S. Government presented no evidence of espionage.^[50]

8. Dongxiao Yue and 'Chordiant Software, Inc'

In May 2010, the federal jury convicted Chordiant Software, Inc., a U.S. corporation, of stealing Dr. Dongxiao Yue's JRPC technologies and used them in a product called 'Chordiant Marketing Director'. Dr. Yue previously filed lawsuits against Symantec corporation for a similar theft.^[51]

9. Stuxnet Worm

[Stuxnet](#) is a computer [worm](#) which affected [Iran's Bushehr nuclear power plant](#) in September 2010. Designed to target weaknesses in [Siemens](#) electronic industrial systems, it is thought to be capable of seizing control of industrial plants and to be the first 'worm' created for this purpose. The complexity of its design and targeted purpose left Western computer experts suggesting it could only have been the product of a "nation state". Mahmoud Liayi, from Iran's Ministry of Industries, is quoted as saying, "an electronic war has been launched against Iran". As well as targeting nuclear power stations, it is also capable of attacking systems which manage water supplies, oil rigs and other utilities.^[52]

10. Operation Payback

Distributed Denial of Service (DDoS) attacks were utilised by a network of [hackers](#), led by the self styled group '[Anonymous](#)', in orchestrating what was termed [Operation Payback](#), in December 2010.^[53] This

was aimed at sabotaging the websites of corporations such as [Mastercard](#), [Visa](#) and [Paypal](#), who had stopped [Wikileaks](#) donors using their financial services, allegedly under pressure from the United States Government^[53]. Thousands of people participating in the attacks did so through downloading the readily available [open source LOIC \(Low Orbit Ion Cannon\)](#) DDoS tool, leading to some commentators to note that, rather than worrying whether their credit card numbers had been hacked, parents should be concerned as to whether their teenage child was an amateur ['hacktivist'](#), possibly 'participating in a co-ordinated global attack on major financial institutions'^{[54][55]}. With Wikileaks founder [Julian Assange](#) in [Wandsworth prison](#) on charges of [sexual assault](#), the hackers threatened to bring down [United Kingdom](#) Government websites, should he be [extradited](#) to face charges in [Sweden](#)^[56]. However, 'Security experts' derided the idea that 'Operation Payback' was in any way comparable to [cyber warfare](#), claiming attacks of this kind were very common, and relatively harmless, only reaching the news in this case due to the association with Wikileaks^[53].

11. Chengdu J-20 stealth fighter jet

When it was unveiled in January 2010, the Chinese engineered [Chengdu J-20 stealth fighter jet](#) was speculated by [Balkan](#) military officials and other 'experts' as having been reverse engineered from the parts of a US [F-117 Nighthawk](#) stealth fighter shot down over [Serbia](#) in 1999. It was the first time such an aircraft had been hit. When the US jet was shot down, Chinese officials in the country were reported as having travelled around the region buying up parts of the aircraft from farmers. Representing 'dramatic progress' into cutting edge military technology for the Chinese, the Chengdu J-20 stealth fighter was thought to potentially pose a challenge to US air superiority. President [Milosevic](#) was known to have routinely shared captured military technology with Russian and Chinese allies. The Russian [Sukhoi T-50](#) prototype stealth fighter, unveiled in 2010, is likely to have been built from knowledge based on the same source^[57].

Chinese commentators contested claims this technology had somehow been stolen. A test pilot claimed that the J-20 was a "masterpiece" of home-grown innovation and that the F-117 technology was "outdated" even at the time it was shot down. An unnamed Chinese defence official protested to the official English language mouthpiece of the [Chinese Communist Party](#), the [Global Times](#), "It's not the first time foreign media has smeared newly-unveiled Chinese military technologies. It's meaningless to respond to such speculations,".^[58] [144]

24. The Humanistic View:

For some, the humanistic view represents an enlightened moral perspective, which is represented in historical documents like the Magna Carta, “Great Charter”. [75], [76]

“Lord Denning described it as “the greatest constitutional document of all times – the foundation of the freedom of the individual against the arbitrary authority of the despot”. [75], [76], [77]

Going back 1100s and 1200s people sought protection against despots and malicious state prosecution. Many leaders have echoed the desires for justice, fairness, dignity for all over the centuries. One of them is Dwight D. Eisenhower.

Here are some quotes from Dwight D. Eisenhower some going back to 1948, not so distance past relative to Magna Carta. He has seen the misery and human suffering wars brought to Europe. In addition to the devastation of WWII, Europe also lost the opportunity to grow and prosper during those war years and use of the resources wasted for the war effort.

“Speech to the American Society of Newspaper Editors ["The Chance for Peace"](#) (16 April 1953)” [21]

“No people on earth can be held, as a people, to be an enemy, for all humanity shares the common hunger for peace and fellowship and justice. ... No nation's security and well-being can be lastingly achieved in isolation but only in effective cooperation with fellow-nations.” [21]

“Every gun that is made, every warship launched, every rocket fired signifies, in the final sense, a theft from those who hunger and are not fed, those who are cold and are not clothed. This world in arms is not spending money alone. It is spending the sweat of its labourers, the genius of its scientists, the hopes of its children. The cost of one modern heavy bomber is this: a modern brick school in more than 30 cities. It is two electric power plants, each serving a town of 60,000 population. It is two fine, fully equipped hospitals. It is some fifty miles of concrete pavement. We pay for a single fighter plane with a half million bushels of wheat. We pay for a single destroyer with new homes that could have housed more than 8,000 people. This is, I repeat, the best way of life to be found on the road the world has been taking. This is not a way of life at all, in any true sense. Under the cloud of threatening war, it is humanity hanging from a cross of iron. ... Is there no other way the world may live?” Dwight D. Eisenhower [21]

Some economists have argued that any empire would decline if it spends more than 5 – 10 % of its GDP on the armed forces to maintain control over its empire. [*the book could not be identified at this time*]. As the spiral of heavier taxation starts to finance increasingly bigger armed forces to suppress increasing uprisings and insurgencies; As more revolts start in distant geographies, trade suffers and supply of raw materials suffer. Economy suffers due to decreased availability of capital to invest and grow. Unemployment rises, foreclosure of homes rises, and the economy stagnates and shrinks. In consequence ability sustain powerful armed forces shrink e.g. Soviet Russia.

“[Farewell address \(17 January 1961\)](#)” [21]

“Now this conjunction of an immense military establishment and a large arms industry is new in the American experience. The total influence — economic, political, even spiritual — is felt in every city, every Statehouse, every office of the Federal government. **We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications.** Our toil, resources, and livelihood are all involved. So is the very structure of our society. **In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought or unsought, by the [military-industrial complex](#).** The potential for the disastrous rise of misplaced power exists and will persist. **We must never let the weight of this combination endanger our liberties or democratic processes.”** Dwight D. Eisenhower [21]

Given that the American military was based on armed citizen, the Minute Man, [86, 87] large professional armed forces and an unimaginable amount of industrial resources being dedicated to the war effort was a new phenomena for America. Most likely the most didn't see the implications of this after the WWII. With at least half imaginary threat of the Red Peril, the Communist Threat, etc.; USA chose to allocate a large amount of its resources to dominate the Oceans, Skies of the world, and the Space. The US desire to dominate on one hand and other nations' need to access to resources, secure their territorial integrity, protect their political system and unity on the other hand have caused clandestine subversive operations, limited armed conflicts, subversive insurgency wars, and regional wars. It looks like this trend will continue in the future. We will discuss the role of cyber weapons (crimeware) and strategies, tactics, tools, and operations of cyber warfare in this context.

English Edition, Kenan Printing House Istanbul, 22 May 1943. [20, 26]

"Mankind is a single body and each nation a part of that body. We must never say "What does it matter to me if some part of the world is ailing?" If there is such an illness, we must concern ourselves with it as though we were having that illness."

As quoted by [Paul Wolfowitz](#) in an [address to the Washington Institute for Near East Policy, Washington, D.C. \(13 March 2002\)](#) [20, 26]

Both from the quotes of Dwight D. Eisenhower and Mustafa Kemal Ataturk, war and aggression are not acceptable conduct unless in self defence when ones country is under attack. More over wars do not solve anything. They are a wasteful use of scarce resources of the earth.

More of these quotes are available in Appendix 2 to emphasize the desirability of just and peaceful means of conflict resolution. There are various NGO organizations dedicated to this ideal, such as the "Trudeau Centre for Peace and Conflict Studies" [[Trudeau Centre for Peace and Conflict Studies](#) (PCS)]

25. The Crime of Aggression: The Analysis

The Crime of Aggression

At least some of the generals and presidents see war and aggression as a crime, so is UN Charter on the paper.

As one could deduct from the UN Charter and the International Criminal Court website; aggression is defined as a crime even though at this time powerful nations are acting based on might-is-right principal without any consequence.

In the first paragraph of Article 1 Chapter I: Purposes and Principles of the UN Charter, the Purpose of the United Nations is specified.

"To maintain international peace and security, and to that end: to take effective collective measures for the **prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, ... "** [27]

The purpose of UN described as prevention and removal of threats to peace and other breaches of the peace. One may consider that cyber attacks either by non-state actors or criminal organizations could be considered "**other breaches of the peace**" especially when such persistent attacks would harm a nation state or its economic activities or its citizens.

In the fourth paragraph of Article 2

"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations." [28]

There is a wide gap between the intended purpose of the UN and the current practice due to a variety of reasons. According to some critics, one of them is undemocratic veto powers of the permanent members of the Security Council. Thus if one of the perpetrators is a permanent member of the Security Council, it would block any UN action against itself by using Veto power, as they do quite often.

One of the principals of the UN charter is equality among states in one hand, but in practice the current arrangements give extraordinary powers to permanent members of the Security Council on the other hand. Some argue that concept of permanent membership violates the foundation of the UN. These kinds of contradictions and other “pragmatic measures” -like ability to withhold funding- hijack the basis on which the UN is supposedly built. [82]

Even one just considers these two purposes only; UN has miserably failed to achieve either of its objectives. There have been various state-over-state conflicts, proxy wars, and covert operations conducted by the permanent members of the Security Council. Cyber attacks or crime or misinformation campaigns to subvert democracies never even have been a UN priority. If a UN Administration through their indecision and inaction allowed genocides to take place [82] [83], it would be naïve to expect any solution from UN on Cyber aggression or Crime. The entire Article 1 and Article 2 of the UN Charter is in Appendix 3. [27, 28]

The other platform, which could address cyber aggression and crime, could be The International Criminal Court (ICC) [29]. In the Article 8 the **elements of the crime of aggression** [30] are defined. These elements are quite important for determining the attributions of an attack, invoking right-to-self-defence, and responding with counter attack using active-defence cyber operations.

“Elements”

“1. The perpetrator planned, prepared, initiated or executed an act of aggression.” [30]

This means a cyber attack must be planned, e.g. intelligence collection, network mapping initial recognisance, etc. Prepared may mean the infrastructure for an attack is established, e.g. botnet for DDOS, or training and coordination websites or IRC channels are established, etc. Executed as an act of aggression, if hundreds or thousands of people from a jurisdiction, which is under, control of a state is the source of a coordinated attack, if a common list of targets and tools provided; then deniability claim of a state would be not very convincing

“2. The perpetrator was a person in a position effectively to exercise control over or to direct the political or military action of the State which committed the act of aggression.” [30]

In case of Cyber Aggression, given that the major players have in place internet monitoring infrastructure or filtering systems in place e.g. SORM2 (Russia), Echelon (USA), or similar facilities in China, denying knowledge of an attack initiated from their own territory will not be very persuasive. Only two western democracies do not recognize the jurisdiction of ICC USA and Israel. [95 membership]

“5. The act of aggression, by its character, gravity and scale, constituted a manifest violation of the Charter of the United Nations.” [30]

Determining whether the threshold is breached to invoke the right-to-self-defence and initiate counter attack such as active-defence operations (cyber counter attack or hard attack) “gravity and scale” of the initial aggression must be determined and documented. The impact, duration, and intensity of the aggression should be the assessed to justify a counter attack.

26. The Anthropological perspective from Friedrich Engels

The Anthropological perspective:

"Engels emphasizes the importance not of primitive psychological development but rather of social relations of power and control over material resources, sometimes related to the development of new technologies." [23]

As Friedrich Engels argues in his book, *The Origin of the Family, Private Property, and the State*, in order to maintain control over material resources the clans or tribes select some men as warriors, most likely a group of men who hunt together. This was the beginning of the gang of warriors and plundering the resources of other clans or tribes. This phenomena lead to the rise of armies and kings.

Then the chain of logic is when clans have private property, this required a need for protection, the need for protection required warriors, when number of warriors increased, they required a permanent leader to coordinate their activities, similar to a group of hunters working together under one leader. The leader of warriors realized they have power over others, and they made themselves kings. Kings defined borders of their property, which lead concept country and state to govern it. [23]

27. Cyber Attacks could be classified as acts of war caused concern

"Last week's announcement by Pentagon officials that cyber attacks could be classified as acts of war caused concern among those who worry that the United States might act outside international law if it retaliates to such attacks with military force. Others assert the move amounts to little more than a money grab by budget-savvy advocates looking to foment fear and exploit public ignorance." [36]

28. The DOD's strategy is founded on five pillars

"The DOD's strategy is founded on five pillars: [37]

- treating cyberspace as an operational domain like land or sea,
- introducing improved defenses and new operating concepts for DOD networks,
- working with DHS and the private sector to secure critical infrastructure,
- working with the international community,
- and building a stronger cyber workforce and
- investing in cybersecurity research and development." [37]

29. U.S. Cyber Command, a new military unit

"Last year, for example, DOD [created](#) U.S. Cyber Command, a new military unit dedicated to protecting military networks from attack, and the DOD is now working to integrate cyber scenarios into its exercises and training, including the use of cyber red teams during war games. It also deepened its cooperation with the Department of Homeland Security, which protects the federal government's civilian networks from attacks." [37]

30. Chinese and Russian Response

Chinese and Russian Response: [38]

“The Obama Administration’s International Cyber Strategy, [launched last week](#), was met by the Russian and Chinese press with a mix of generally negative reactions. The most negative were rooted in **skepticism and mistrust** about U.S. motives as well as **perceived hypocrisy** underlying the proposed cyber standards.” [38]

“One Chinese outlet, the [Global Times](#), quoted an analyst (and offered no countering opinion) saying

The U.S. intends to keep its dominant role in the area by setting standards and rules ... the US masters a number of core technologies for cyberspace usage, and it aims to continuously consolidate its advantages.” [38]

31. Mistrust about the motives of the United States

“A column by Yu Xiaoqiu in the People’s Daily delved much deeper into mistrust about the motives of the United States: “

“On the so-called question of online freedom, the United States is likely to link it with human rights and subsidize the research and development of online cracking technology in a bid to open the gate of online information dissemination [to] developing nations. The "online warfare" of attacking and paralyzing the opponent's network and important information systems will also become its final military means to exert pressure on target nations. Under the pressure of the United States, the safeguarding of national interests and sovereignty in the field of information networks of all nations will be increasingly important, the competition and rivalry for information resources and markets will be more acute, and the controversies over Internet access control and anti-control will be more prominent.” [38]

32. Perceived hypocrisy of U.S.

“Skepticism was not solely rooted in mistrust of U.S. motives, however, it was engendered by **perceived hypocrisy** of U.S. calls to common cyber standards. Russian press added hypocrisy to the list of charges claiming that the strategy, which lays out fundamental concepts, such as an open Internet with guarantees for freedom of expression, was at odds with U.S. actions. Specifically, [Voice of Russia](#) said”: [38]

“The example of Wikileaks demonstrated that the US government was not eager to pay the price for global transparency.” [38]

“The other questionable point is the belief that the USA is responsible for the cyber attacks that sabotaged Iran’s nuclear facilities. While concerns about Iran’s nuclear programme couldn’t be described as groundless, calls for global internet security from a state that subscribes cyber attacks as a common tactic sounds hypocritical to say the least.” [38]

33. The international policy on the Internet should be a matter for the whole world

“The People’s Daily column by Yu Xiaoqiu described in more detail both why international agreement is important as well as how it agreement should be achieved through the United Nations.” [38]

“Although the Internet was invented by the Americans and most of the root servers are within their control, the rapid development of the Internet in recent years has been the achievement of the concerted

efforts of the international community, which is the common wealth of mankind and the new space for promoting world peace and development.” [38]

“The drafting of the international policy on the Internet should be a matter for the whole world and should strictly follow the "UN Charter" and other internationally acknowledged basic norms. The peaceful use of international information and cyberspace should be based on the safeguarding of sovereignty, interests, and security in the field of information of a nation as well as relevant resolutions and international treaties of the United Nations and the International Telecommunications Union.” [38]

34. Cultures of the Army, Navy and Air Force are incompatible with that of cyber warfare

“Some military leaders claim that the existing cultures of the Army, Navy and Air Force are fundamentally incompatible with that of cyber warfare,^[29] [48] and have suggested a fourth branch of the military, a cyber-warfare branch.^{[30][31]} LTC Gregory Conti and COL John "Buck" Surdu (chief of staff of the [United States Army Research, Development and Engineering Command](#)) stated that the three major services are "properly positioned to fight kinetic wars, and they value skills such as marksmanship, physical strength, the ability to leap out of airplanes and lead combat units under enemy fire. "Unfortunately," the two officers write, "these skills are irrelevant in cyber warfare. Technical expertise isn't highly valued in the three services. Just look at military uniforms: no decorations or badges honoring technical expertise", the officers point out. These officers suggest that "Ultimately, the role of fighting and winning in cyberspace is a military mission, which demands a military organization – one that can recruit, train and retain highly qualified cyber-warfare combatants." “ [39]

35. PRC may be a global power economically but its military lacks force projection

“The People’s Republic of China (PRC) may be a global power economically but its military lacks force projection beyond the Asia Pacific region. Its traditional military hardware is one to three generations behind the US and Russia. In light of these deficiencies it is probable that **cyber warfare will provide China with an asymmetric advantage to deter aggression from stronger military powers** as they catch up in traditional military capabilities. Cyber warfare would also allow China to leapfrog by means of technology transfer and exploiting adversary weaknesses. This investigation will address three primary questions: What is China’s current military capability? How would cyber warfare allow China to seriously advance its strategic abilities? And what is the evidence that China is headed in a cyber warfare direction?” [61]

36. Revolution in Military Affairs

“Many observers believe that Chinese concern with the RMA (Revolution in Military Affairs) and future warfare dates only from the Gulf War in 1991. However, one of China’s most important early studies of future warfare was published 13 years ago in 1988 by a team under the leadership of General Mi Zhenyu, a Vice President of the Academy of Military Science, entitled *China’s National Defense Development 3 Concepts*. He suggested:

- “China is in long term competition with other major powers.”

- “The gap between the weapons we now possess compared to those of advanced countries is twenty to twenty-five years.”
 - “If our objective is merely to shrink this discrepancy to ten to fifteen years, then from the point of view of effectiveness, it would seem to be higher than others. But from the point of view of competitive effectiveness, it would only be an impractical increase in quality, perhaps even a decrease.” “[56]
- “A fifth asymmetrical approach will be for China to attack American naval command and information systems.” [56]

37. Chinese military strategists view the world as a place basically hostile to Beijing’s national interests

“Jiang’s “caveat” is a relatively subdued echo of PLA concerns. For their part, **Chinese military strategists seem to view the world as a place basically hostile to Beijing’s national interests, especially China’s sovereignty.** It is a world where dangers to national security lurk everywhere. **The strategists view competition between nations for advantage as the norm and as a zero-sum equation (ni si wo huo).** Change in the global and regional security environment is viewed as constant and usually dangerous. **The absence of war does not mean the absence of hostility toward China.** And, over the horizon, today’s much-needed trade partners can slowly transform into serious economic, political, and military rivals. China’s Defense Minister General Chi Haotian is Beijing’s top military spokesman on these issues and he continues to be quite straightforward and frank in publicly highlighting the dangers that PLA planners see bubbling beneath the surface of a relatively peaceful world. As recently as March 1998, he underscored that pockets of antipathy toward China continue to require military vigilance:”

“Hostile international forces have never abandoned their strategic plot to westernize and split China, and the great cause of the motherland’s ultimate reunification has yet to be accomplished. Under the long, peaceful environment and the situation centering on economic construction, we must be prepared for danger in times of peace and enhance our awareness of hardship. We must not become intoxicated by songs and dances in celebration of peace.” [58]

38. US and China face vast divide on cyber issues

[US and China face vast divide on cyber issues](#) [59]

“But the military and espionage tracks have been hard going, highlighting what analysts say is a huge U.S.-China perception gap over values, capabilities, interests -- and even basic definitions of deterrence and cyber security.” [59]

“Analysts say China's People's Liberation Army believes its ability to attack U.S. cyber infrastructure compensates for its conventional military weakness compared to the United States.” [59]

39. Understanding of offensive operations

“ "I'm quite skeptical of the likelihood that any effective understanding of offensive operations can be reached with the Chinese government," said Stewart Baker, a former U.S. Department of Homeland Security official, now at the law firm Steptoe & Johnson.” [59]

“China's eagerness to acquire foreign technology also has inspired cyber intrusions that anger trade partners. Hackers based in China have been accused of trying to steal everything from Google's valuable search algorithm to manuals for U.S. satellites to gigabytes of proprietary business information from Western energy companies.”

“But China's spymasters, paradoxically for a centrally controlled government, do not keep a tight leash on hackers and others that they train, said Lewis, whose group will hold its next round of unofficial cyber-security talks later this year.” [59]

40. The high-value intellectual property theft

“Lewis said he was skeptical that Beijing was directing the high-value intellectual property theft or could stop it. “They do train people and they do use proxies but that doesn't mean that everyone is under their control,” he said.” [59]

“Even if the United States could verify that China was behind malicious cyber activity and Beijing had the capacity to rein it in, negotiations toward a cyber treaty might require concessions Washington would be loathe to put on the table.”

“Regardless of complaints or exaggerations of the threat, no one would like to give up their cyber weapons or capabilities. They are very attractive and convenient, with very flexible capabilities, almost limitless ways to use them.”

“Jack Goldsmith, an international law and cyber-security expert at Harvard Law School, says China and other countries would likely demand U.S. restraint in areas such as intelligence gathering and encouraging political activists who challenge curbs on Internet freedom.” [59]

41. Russia sees greater Euro-Atlantic threats moving farther east

“As the Russian military persists in trying to exploit Central-East European security dilemmas along Russia's western border, Russia sees greater Euro-Atlantic threats moving farther east. NATO's Central-East European enlargement not only includes countries bordering Ukraine and moving closer to the Caucasus (Georgia), but also encroaching upon the three Baltic countries that encircle Russia's Kaliningrad enclave. As a result, Russia's counter-NATO strategy still involves large-scale military exercises directed against former Soviet Republics along its western border.³⁵ Yet, East European and Eurasian energy security developments also influence Russian military planning for exercises directed more toward Central-East Europe. Consequently, the U.S. military force structure decline in Europe, and its post-9/11 focus on the Middle East and Southwest Asia enable Russia's military to reassert itself in Europe. Hence, Russian military strategy not only focuses on energy security along its western periphery in order to disrupt NATO planning, but it also remains part of the larger Russian national security strategy to exploit new Central-East European security dilemmas.” [64]

42. Cyberwarfare by Russian state

“Cyberwarfare by Russian state includes allegations of [denial of service attacks](#), [hacker attacks](#), dissemination of [disinformation](#) over the internet, [participation of state-sponsored teams in political blogs](#), internet [surveillance](#) using [SORM](#) technology, and [persecution of cyber-dissidents](#). According to investigative journalist [Andrei Soldatov](#),^[1] some of these activities are coordinated by the Russian [signals](#)

[intelligence](#), which is currently a part of the [FSB](#) but has been formerly a part of 16th [KGB](#) department, but others are directed by the [Russian Ministry of Internal Affairs](#).

Other than the allegations, there is no evidence that the Russian state is involved in cyberwarfare. Although Russia has denied any involvement cyberattacks in [Estonia](#) and [Georgia](#) in recent years, nobody believes that the attack emanated from anywhere else.” [68]

“Cyberattacks [68]

Main article: [2007 cyberattacks on Estonia](#)

Main article: [Cyber attacks during the 2008 South Ossetia war](#)

It has been claimed that Russian security services organized a number of [denial of service attacks](#) as a part of their [Cyber-warfare](#) against other countries,^[5] most notably [2007 cyber attacks on Estonia](#) and [2008 cyber attacks on Russia, South Ossetia, Georgia, and Azerbaijan](#) [4]. One of young Russian hackers said that he was paid by the [Russian state security services](#) to lead the hacker attacks on [NATO](#) computers. He was majoring computer sciences at the *Department of the Defense of Information*. His tuition was paid by the FSB.^[6]

At the same time, speaking of 2007 cyber attacks, Estonia's defence minister [Jaak Aaviksoo](#) admitted he does not possess evidence of official Russian government involvement in cyber attacks.^[7]

As to the 2008 cyber attacks on Georgia, an independent US-based research institute [US Cyber Consequences Unit](#) report stated the attacks had "little or no direct involvement from the Russian government or military". According to the institute's conclusions, some several attacks were carried from PCs of multiple users, located in Russia, Ukraine and Latvia. These people were willingly participating in cyber warfare, being Russia supporters during [2008 South Ossetia war](#). Some attacks also used botnets.^{[8][9]} “[68]

43. Overview of the Approach: Analysis

In chapter 4, we have developed some of the artifacts for the cells of Row 2 of Zachman’s Framework.

Row 2 is defined as 20 – 30 thousand feet view of the enterprise. Row 2 aims to understand and document how an entire enterprise or organization generates value independent of organizational structure or IT systems. On the other hand, Row 1 is considered a 60 thousand feet view of the entire organization independent of any organizational structure or systems or budgetary constraints. The next level, Row 3 of Zachman’s Framework is a more detailed logical view of a Line-of-Business or Organizational subset or a project. The Row 3 artifacts are similar to the deliverables of requirements definition and analysis phase of a software development project. We will not explore Row 3 of Zachman’s Framework in this paper.

When Row 2 of Zachman’s Framework is investigated, one would interview people representing different organizational responsibilities and different organisational levels. For example people from marketing, finance, human resources, production, distribution, procurement, product planning, and so forth. would be interviewed to understand and document their operations. Also, people with executive, director, manager, supervisor, and staff level responsibilities are interviewed from each function to understand and document their perspectives. In order to build a coherent enterprise architecture these views must be integrated and a common language across the enterprise should be established.

People at different levels of organization are interviewed to understand the organizational functions from different perspectives, such as vice president’s, a director’s, a manger’s, a supervisor’s, and staff and workers perspectives. All of these perspectives would focus on slightly different aspects of the functional area and most likely add different levels of detail. As expected the executive and director levels may focus on objectives, strategies, and future direction mostly. Management level interviews may focus on information requirements to manage their

function. The supervisor and staff interviews may provide knowledge about how the organization operates at the lowest level of detail possible.

Since using above approach is not possible at this time, instead the above knowledge about the topics, cyber war, cyber intelligence and espionage, and cyber crime would be extracted and deduced from publicly available sources.

Sample data models, process models, and matrices depicting interrelationships and dependencies are developed based on the knowledge gathered from the books, articles, and other sources. This view is enhanced with the knowledge gained during the Computer Crime, Penetration Testing, and Digital Forensics courses.

A first cut data model is created to identify important concepts and relationships among these concepts. Usually the terminology of a topic would identify important concepts of that topic. In order to manage and operate in that context one must understand these concepts and usually one must keep data about these concepts. Quite often these concepts would be translated into Entity Types of Entity-Relationship Data Models.

In this phase, a First Cut Data Models should have been created with the subject matter experts to inventory and define organizational concepts and terminology used by the practitioners and experts of these areas. Usually the entity types discovered during the development of a first cut data model are referred as candidate entity types; they are subjected to further definition and assignment of unique identifiers and representative attributes following rules of normalization. Then the data requirements documented in the conceptual data model would be the foundation for database development (e.g. Enterprise Operational Data Store – Bill Inmon <http://www.inmoncif.com/home/>).

The boxes on the data model represent entity types and the lines represent the relationships. Usually cardinalities and optionalities are also documented, but in this paper, we will not go into that level of detail. Cardinality indicates how many of one entity type related to how many of other entity type. Usually 1 to N, N to 1, N to N, or a constraint number e.g. 3 to 1 or 3 to N.

Optionality is indicated with 0, which means there could be an entity type or not. When the other entity type is created, the secondary entity type may, or may not exist or is not required. If the optionality is 1, it is mandatory, meaning the entity type must exist (referential integrity rules).

A set of data models is created for Cyber Warfare, Cyber Intelligence and Espionage (including covert operations e.g. green ops, black ops, sabotage, insurgency, misinformation war, and subversion), and Cyber Crime. The more detailed models are in the appendix, and only simplified sample versions are in the main body of the paper.

A First Cut Data Model identifies candidate entity types only and possible relationships between the candidate entity types. We will not describe the entity types. We will not assign representative entity attributes (data elements). We will not discover or create unique identifiers for these entity types. Without the three preceding activities, technically, it is not correct to claim that these are entity types.

Since the purpose of this first cut data model is to explore a basic understanding of the cyber war, these limitations are acceptable. The first cut data model will not be complete enough for database design phase.

A First Cut Process model is created to understand and describe the conceptual organizational processes independent of organizational structure, specific technology, or systems. The aim is to visually model the organizational processes using the Data Flow Diagramming technique [18, 19].

The conceptual process models are developed to define organizational processes. In this paper, data flow diagramming technique is used with event and control flows. In data flow diagrams, the rectangles with rounded corners represent the process. The arrows represent data flows and control flows. The data flows indicate specific data contents, which are generated together and logically related, and jointly represent a business or organizational meaning. The data flows may be assigned defined data contents. The data contents of dataflows usually consist of a set of either data elements, or entity types of the data model. The contents of dataflows should be described in the matching data model. Control flows or event flows may or may not have data contents. They represent near real time occurrence of an operational or control event. The event partitioning technique is more appropriate to

develop detailed models using a proper CASE tool. Since I do not have access to a CASE tool, the preferred level of technical precision is not achieved.

The funny tubes represent data stores. The contents of data stores usually represent a specific entity type of conceptual data model or a set of closely related entity types packaged together in one data store. (In the proper DFD diagram, the graphic representation of the data store is different than these funny tubes, but the correct data store symbol is not available in MS PowerPoint).

In order to define the scope of DFD model a context process model is created. The context model will show the external actors or things with which components inside the scope interact. In addition, the type and content of those interactions are specified. In one sense, context diagram would indicate the external interfaces of the subject matter under investigation. A DFD model is usually represented in multiple one page diagrams with accompanying process, dataflow, control flow, business event, and data store definitions.

44. Known Cyber Criminal Organizations

Cybercrime organizational structures and modus operandi

Posted on 15 July 2008.



Finjan announced the latest findings by its Malicious Code Research Center (MCRC). In its latest trends report for Q2 2008, the MCRC identifies and analyzes the latest Crimeware business operations, and provides a first-of-its-kind insider's look at the organizational structure of Cybercrime organizations. It all makes the cybercrime more successful and profitable than ever.

The report includes real documented discussions conducted by Finjan's researchers with resellers of stolen data and their "bosses", confirming Finjan's analysis of the current state of the cybercrime economy.

The report explores the trend of loosely organized clusters of hackers trading stolen data online being replaced by hierarchical cybercrime organizations. These organizations deploy sophisticated pricing models, Crimeware business models refined for optimal operation, Crimeware drop zones, and campaigns for optimal distribution of the Crimeware.

These cybercrime organizations consist of strict hierarchies, in which each cybercriminal is rewarded according to his position and task. The "boss" in the cybercrime organization operates as a business entrepreneur and does not commit the cybercrimes himself. Directly under him is the "underboss", acting as the second in command and managing the operation.

This individual provides the Trojans for attacks and manages the Command and Control (C&C) of those Trojans. "Campaign managers" reporting to the underboss lead their own attack campaigns. They use their own "affiliation networks" as distribution channels to perform the attacks and steal the data. The stolen data is sold by "resellers", who are not involved in the Crimeware attacks themselves.

As a preventative measure, businesses should look closely at their security practices to make sure they are protected. A layered security approach is a highly effective way of handling these latest threats, and applying innovative security solutions, such as real-time content inspection, designed to detect and handle them is a key factor in being adequately protected.

Top 10 posts in cybercriminal operations | Cybercrime organizations often run like corporations, staffed by experts in specific jobs

Monday, May 9, 2011

Criminal hacker organizations are operating with increasing corporate-like efficiency, specialization and expertise, according to the FBI.

From a business perspective, these criminal enterprises are highly productive and staffed by dedicated people willing to operate worldwide, around the clock "without holidays, weekends or vacations," according to Steven Chabinsky, deputy assistant director in the **FBI's cyber division**. "As a result, when an opportunity presents itself these criminals can start planning within hours."

"The cyber underground now consist of subject matter experts that can focus all their time and energy on improving their techniques, their goods and services," Chabinsky told an audience today at the FOSE conference, a government IT trade show, held here.

During the presentation, Chabinsky presented a list of the top 10 positions in cyber criminal organizations. They are:

1. **Coders/programmers**, who write the exploits and malware used by the criminal enterprise. Contrary to popular belief, Chabinsky noted that coders who knowingly take part in a criminal enterprise are not protected by the First Amendment.
2. **Distributors**, who trade and sell stolen data and act as vouchers for the goods provided by other specialists.
3. **Tech experts**, who maintain the criminal enterprise's IT infrastructure, including servers, encryption technologies, databases, and the like.
4. **Hackers**, who search for and exploit applications, systems and network vulnerabilities.
5. **Fraudsters**, who create and deploy various social engineering schemes, such as phishing and spam.
6. **Hosted systems providers**, who offer safe hosting of illicit content servers and sites.
7. **Cashiers**, who control drop accounts and provide names and accounts to other criminals for a fee.
8. **Money mules**, who complete wire transfers between bank accounts. The money mules may use student and work visas to travel to the U.S. to open bank accounts.
9. **Tellers**, who are charged with transferring and laundering illicitly gained proceeds through digital currency services and different world currencies.
10. **Organization Leaders**, often "people persons" without technical skills. The leaders assemble the team and choose the targets.

By Patrick Thibodeau. Patrick Thibodeau covers SaaS and enterprise applications, outsourcing, government IT policies, data centers and IT workforce issues for Computerworld.

Cyber-crime organizations: a specialist classification

Escrito por [Juan Santana](#)

March 31st, 2010

We have often described how online mafias are highly organized regarding strategic and operational vision, logistics and deployment. Not only do they seem like real companies, they are also international organizations operating across the globe.

The [FBI](#) has recently classified the different 'professional positions' they have encountered in the cyber-crime business, in an attempt to describe the most common figures that profit through online theft, extortion and fraud.

According to the FBI, cyber-crime organizations operate like companies, with experts specialized in each area and position. Yet unlike most companies, they don't have timetables, holidays or weekends.

The most common 'positions' or specializations according to the FBI are:

1. **Coders/programmers**, who develop the exploits and malware used to commit cyber-crime
2. **Distributors**, who collect and sell stolen data, acting as intermediaries
3. **Experts technicians**, who maintain the criminal "company's" infrastructure (servers, encryption technologies, databases, etc.)
4. **Hackers**, who search for exploit applications, and system and network vulnerabilities
5. **Fraudsters**, who create social engineering techniques and launch different attacks (phishing, spam, etc.)
6. **Hosted system providers**, who provide a safe environment to host illicit content on servers and pages
7. **Cashiers**, who control and provide victims' names and accounts to other criminals for a fee
8. **Money mules**, who carry out bank transfers between bank accounts
9. **Tellers**, who launder the money
10. **Organization Leaders**, who are usually normal people without technical knowledge who create a team and define the objectives

Cyber-crime organizations have a hierarchical structure whereby every action is performed by specialists. If you think about the different countries they are present in, you will get a clear idea of the number of people involved in these criminal activities, and who benefit from the anonymity provided by the Internet.

45. Overview of the Approach: Synthesis

The WHY Matrix is created to compare objectives of Cyber War, Cyber Intelligence and Espionage⁸⁹, and Cyber Crime organizations. The purpose of this matrix is to show conceptual similarities and differences between the Offence Types (Cyber War, Cyber Intelligence and Espionage, and Cyber Crime). The rows and columns are symmetric; they are structured the same way. The Objectives are grouped under different Offence Types. The cell values would indicate the degree of similarity or difference.

The WHAT Matrix serves two purposes. First, it is to model the alignment or misalignment between Entity Types and the Objectives of the original Offence Type entity type belongs. The Columns indicate the Objectives of each Offence Type and the rows indicate the entity types modelled in the sample data models for each Offence Type. The Cell values indicate support or alignment between objectives and entity types for the same Offence Type.

The second purpose is model alignment across different Offence Types. In other words, how well for example the entity types discovered for Cyber War aligns with or supports Cyber Intelligence and Espionage or Cyber Crime Objectives. This perspective of the model indicates similarity across the three Offence Types.

The cell values would indicate support for or alignment with the objectives of the original Offence Type where the entity type is modelled. This view of the matrix is useful in a couple of ways. The first one is to make sure that there are entity types supporting all the objectives. This would assure that we have completely covered the

⁸ The Cyber Intelligence and Espionage includes covert operations e.g. green ops, black ops, sabotage, insurgency, misinformation war, and subversion.

⁹ Note: Misinformation War could be offensive or defensive in cyber space. Both require resources and should be given priority especially to protect the democratic process in collaboration with counter espionage and subversion functions to identify and neutralize the agents of influence and other traitors.

2011-08-31 13:09:53

conceptual data scope to support the objectives. If there are entity types, which are not supporting specific objectives, this should be investigated and the cause should be determined and documented.

In similar fashion to the above, a process versus objectives matrix is created. The HOW Matrix serves two purposes too. The first purpose is to model the alignment or misalignment between processes and the Objectives of the original Offence Type the process belongs. The Columns indicate the Objectives of each Offence Type and the rows indicate the processes modelled in the sample process models for each Offence Type. The Cell values indicate support or alignment between processes and objectives of each Offence Type that process originally belongs.

The second purpose is to model alignment across different Offence Types. In other words, how well for example the processes discovered for Cyber War aligns with or supports the Cyber Intelligence and Espionage or Cyber Crime Objectives. This perspective of the model indicates similarity across the three Offence Types.

When there are processes similarities across multiple businesses or missions, this could be considered a strong indication that these businesses or missions are the same. Furthermore under these situations there is an opportunity to integrate business or organizational practices and systems for greater efficiency and effectiveness. This is commonly referred to as 'breaking down the silos'. In this case the same systems, strategies, tactics, techniques, and tools could serve all of the Offence Types.

The cell values would indicate support or alignment with the objectives of the original Offence Type where the process is modelled. This view of the matrix is useful in a couple of ways. The first one is to make sure that there are processes supporting all the objectives. This would assure we have completely covered the conceptual process scope to support the objectives. If there are processes, which are not supporting specific objectives, this should be investigated and the cause should be determined and documented.

Ideally this comparison should be completed at detailed process definition and input and output data flow levels.

A hierarchy of objectives could be developed with more detailed knowledge of Offence Types. This would require an in-depth understanding of the laws and regulations establishing the organization, the mission statement, the doctrine, and current strategy, tactics, and operations.

In addition, notes explaining the reasoning and evidence behind each cell value could be documented too. A set of matrices could cover the entire WHY (Motivation) column of the Zachman's Framework from the top to almost the bottom. It would be much preferable if a number of experts complete the matrices independently, and later consolidate the individual matrices into one with discussion and additional explanatory notes. The above are my extensions to typical Enterprise architecture methodology.

46. The most interesting questions about future developments in cyberspace are:

1. Looking to the future would cyber weapons and actions be a tool for liberation and self defence?
2. Would citizens use cyber weapons and actions for self defence or defence of other victims?
3. Would cyber actions be used for ensuring life, liberty pursuit of happiness and freedom for all?
4. Or cyberspace would be used as a tool of oppression and limiting freedoms?
5. Would cyber attack infrastructure and cyber weapons reduce the cost of defence? - Since the material cost of manufacturing, distribution, or logistics are significantly cheaper for cyber weapons than hard (kinetic) weapons