NATIONAL DEFENCE UNIVERSITY

TARGET AUDIENCE ANALYSIS IN CYBER DOMAIN

Thesis
Kapteeni
Miika Sartonen

Esiupseerikurssi 66
Ilmasotalinja

Huhtikuu 2014

Kurssi Esiupseerikurssi 66	Linja Ilmasotalinja
Tekijä Kapteeni Miika Sartonen	
Opinnäytetyön nimi **Target audience analysis in cyber domain**	
Oppiaine, johon työ liittyy Johtaminen ja sotilaspedagogiikka	Säilytyspaikka Maanpuolustuskorkeakoulun kurssikirjasto
Aika Huhtikuu 2014	**Tekstisivuja** 43 **Liitesivuja** 4

ABSTRACT

This thesis aims to find an effective way of conducting a target audience analysis (TAA) in cyber domain. There are two main focal points that are addressed; the nature of the cyber domain and the method of the TAA. Of the cyber domain the object is to find the opportunities, restrictions and caveats that result from its digital and temporal nature. This is the environment in which the TAA method is examined in this study. As the TAA is an important step of any psychological operation and critical to its success, the method used must cover all the main aspects affecting the choice of a proper target audience.

The first part of the research was done by sending an open-ended questionnaire to operators in the field of information warfare both in Finland and abroad. As the results were inconclusive, the research was completed by assessing the applicability of United States Army Joint Publication FM 3-05.301 in the cyber domain via a theory-based content analysis. FM 3-05.301 was chosen because it presents a complete method of the TAA process. The findings were tested against the results of the questionnaire and new scientific research in the field of psychology.

The cyber domain was found to be "fast and vast", volatile and uncontrollable. Although governed by laws to some extent, the cyber domain is unpredictable by nature and not controllable to reasonable amount. The anonymity and lack of verification often present in the digital channels mean that anyone can have an opinion, and any message sent may change or even be counterproductive to the original purpose.

The TAA method of the FM 3-05.301 is applicable in the cyber domain, although some parts of the method are outdated and thus suggested to be updated if used in that environment. The target audience categories of step two of the process were replaced by new groups that exist in the digital environment. The accessibility assessment (step eight) was also redefined, as in the digital media the mere existence of a written text is typically not enough to convey the intended message to the target audience.

The scientific studies made in computer sciences and both in psychology and sociology about the behavior of people in social media (and overall in cyber domain) call for a more extensive remake of the TAA process. This falls, however, out of the scope of this work. It is thus suggested that further research should be carried out in search of computer-assisted methods and a more thorough TAA process, utilizing the latest discoveries of human behavior.

KEYWORDS
Target audience analysis, psychological operations, cyber domain, information warfare

Kurssi Esiupseerikurssi 66	Linja Ilmasotalinja
Tekijä Kapteeni Miika Sartonen	
Opinnäytetyön nimi **Target audience analysis in cyber domain**	
Oppiaine, johon työ liittyy Johtaminen ja sotilaspedagogiikka	Säilytyspaikka Maanpuolustuskorkeakoulun kurssikirjasto
Aika Huhtikuu 2014	**Tekstisivuja** 43 **Liitesivuja** 4

TIIVISTELMÄ

Tämän opinnäytetyön tavoitteena on löytää tehokas tapa kohdeyleisöanalyysin tekemiseksi kybertoimintaympäristössä. Työssä keskitytään kahteen ilmiöön: kybertoimintaympäristön luonteeseen ja kohdeyleisöanalyysin metodiin. Kybertoimintaympäristön osalta tavoitteena on löytää sen digitaalisesta ja ajallisesta luonteesta juontuvat mahdollisuudet, rajoitteet ja sudenkuopat. Tämä on se ympäristö jossa kohdeyleisöanalyysiä tarkastellaan tässä työssä. Koska kohdeyleisöanalyysi kuuluu olennaisena osana jokaiseen psykologiseen operaatioon ja on onnistumisen kannalta kriittinen tekijä, käytettävän metodin tulee pitää sisällään kaikki oikean kohdeyleisön valinnan kannalta merkittävät osa-alueet.

Tutkimuksen ensimmäisessä vaiheessa lähetettiin avoin kysely informaatiosodankäynnin ammattilaisille Suomessa ja ulkomailla. Koska kyselyn tulokset eivät olleet riittäviä johtopäätösten tekemiseksi, tutkimusta jatkettiin tarkastelemalla Yhdysvaltojen armeijan kenttäohjesäännön FM 3-05.301 soveltuvuutta kybertoimintaympäristössä käytettäväksi teorialähtöisen sisällönanalyysin avulla. FM 3-05.301 valittiin koska se sisältää kokonaisvaltaisen kohdeyleisöanalyysiprosessin. Havaintoja verrattiin kyselytutkimuksen tuloksiin ja psykologian uusiin tutkimuksiin.

Kybertoimintaympäristö on tulosten perusteella nopea ja valtava, jatkuvasti muuttuva ja kontrolloimaton. Vaikkakin lait hallitsevat kybertoimintaympäristöä jossakin määrin, on se silti luonteeltaan ennakoimaton eikä sitä voida luotettavasti hallita. Digitaalisilla kanavilla usein läsnäoleva nimettömyys ja tiedon tarkastamisen mahdottomuus tarkoittavat että kenellä tahansa voi olla mielipide asioista, ja mikä tahansa viesti voi muuttua, jopa alkuperäiseen tarkoitukseen nähden vastakkaiseksi.

FM 3-05.301:n metodi toimii kybertoimintaympäristössä, vaikkakin jotkin osa-alueet ovat vanhentuneita ja siksi ne esitetään päivitettäväksi mikäli metodia käytetään kyseisessä ympäristössä. Kohdan kaksi kohdeyleisökategoriat korvattiin uusilla, digitaalisessa ympäristössä esiintyvillä ryhmillä. Lähestyttävyyden arviointi (kohta 8) muotoiltiin myös uudestaan, koska digitaalisessa mediassa pelkkä tekstin läsnäolo ei sellaisenaan tyypillisesti vielä riitä halutun viestin välittämiseen kohdeyleisölle.

Tietotekniikan edistyminen ja psykologian sekä sosiologian aloilla tehty tieteellinen tutkimus ihmisten käyttäytymisestä sosiaalisessa mediassa (ja yleensä kybertoimintaympäristössä) mahdollistavat koko kohdeyleisöanalyysiprosessin uudelleenrakentamisen. Tässä työssä sitä kuitenkaan ei voida tehdä. Siksi esitetäänkin että lisätutkimusta tulisi tehdä sekä tietokoneavusteisten prosessien että vielä syvällisempien kohdeyleisöanalyysien osalta, käyttäen hyväksi viimeisimpiä ihmisen käyttäytymiseen liittyviä tutkimustuloksia.

AVAINSANAT
kohdeyleisöanalyysi, psykologiset operaatiot, kybertoimintaympäristö, informaatiosodankäynti

INDEX

TARGET AUDIENCE ANALYSIS IN CYBER DOMAIN

1. INTRODUCTION

1.1 INTRODUCTION TO SUBJECT

Our daily environment is engulfed in a host of networks, most notably the Internet. It has become increasingly apparent that we can no longer go about our daily business without being affected by news, rumours, commercials and our friends´ updates of their latest interests in various network groups, all brought to us via our tablets and smartphones. Due to the almost instant nature of Internet-based media the traditional forms of communication are dragging behind and perhaps are a slowly dying breed. This relatively new, immaterial kingdom where some people might spend even most of their cognitive presence during their day has been claimed to be a new domain of its own, the cyber domain.

Psychological operations are operations with the intent of affecting people. As no audience is homogeneous, it has for long been customary for marketing businesses and those responsible for psychological operations to segment the audience in to various groups of people. These groups have their own characteristics, opinions, interests and thus different and unique ways of influencing them. In the field of psychological operations this segmentation is called Target Audience Analysis (TAA).

Target Audience Analysis, as described in the U.S. Army Field Manual FM 3-05.301 is by definition a “detailed, systematic examination of psychological operations (PSYOP) -relevant information to select target audiences that can accomplish a given supporting psychological operations objective” (FM 3-05.301, 5-1). In other words, target audience analysis is a process with the intent of finding a group of people that could and should be affected in order to accomplish a certain psychological operations’ task.

The purpose of this thesis is to study the means of conducting a TAA in the cyber domain. The intent is to find a useful, practical process that covers the vital elements of the process and is applicable in various networks. Almost synonymous to the TAA is the customer segmentation process used for marketing purposes. The main difference is that while for marketing purposes the desired group of people is preferably as large as possible, the target audience of a psychological operation might consist of a single individual.

The composition of this thesis is as follows: Chapter 1 introduces the subject and its theoretical basis. Chapter 2 analyses the characteristics of cyber domain and its' possibilities, caveats and restrictions. The main focus of this work is in chapter 3 where the target audience analysis is addressed. The conclusions of this thesis are presented in chapter 4.

1.2 DEFINITION OF MAIN CONCEPTS

Cyber domain is defined in the Finnish cyber security strategy (2013) as follows:

> [It is] an environment consisting of one or more networked information systems with the intent of processing information (data) in electronic format. It is characteristic of the environment to use electronic devices and electromagnetic spectrum to store, modify and transmit information via communication networks. Included in the environment are the physical structures necessary for the use of data and information. Use of information means collecting, saving, restructuring, using, transmitting, yielding, maintaining, changing, combining, protecting, removing, erasing and other procedures targeted at information (data). (Kyberturvallisuusstrategia 2013, translation by author.)

This definition covers the nature and boundaries of the cyber domain as addressed in this study. Although almost any communication network bears the trademarks of before mentioned cyber domain, the most referred to in this work is the Internet.

Psychological operations (PSYOP) are "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behaviour of foreign governments, organizations, groups, and individuals" (JP 3-13.2, GL 8). Some countries prefer not to use this type of direct approach to influence operations and prefer to use terms such as strategic communication or army support operations. In this study, however, this definition is valid and is thus used throughout the text.

Psychological operations objective (PO) is "a statement of a measurable response that reflects the desired attitude or behaviour change of a selected foreign target audience as a result of Psychological Operations" (FM 3-05.301, Glossary 17). In other words, once the decision of launching a psychological operation has been made, a definite target must be set. In psychological operations this target typically is to alter either the behaviour or the attitude of a certain individual or groups of people. In order to avoid vague and possibly ineffective targets, there must be some way of measuring whether or not the desired effect takes place.

Supportive psychological operations objective (SPO) is "the specific behavioural or attitudinal response desired from the target audience as a result of PSYOP. The SPO is what PSYOP will do to get the target audience to achieve psychological operations objectives [PO]" (FM 3-05.301, 4-10). Once the psychological operations objective (PO) has been set, the more practical approaches of how to achieve this objective are considered. These more straightforward and detailed targets that converge to achieve the PO are the supportive psychological operations objectives.

Target audience is "an individual or group selected for influence or attack by means of psychological operations" (JP 3-13.2, 1-2). As defined, target audience is the group of people that has been selected to be influenced. The composition of the TA has no definite rules, a TA might be connected (or separated) by geographical boundaries, profession, age or preferences of interest of the individuals, or simply by topology of a computer network.

Target Audience Analysis (TAA) is a "detailed, systematic examination of PSYOP-relevant information to select target audiences that can accomplish a given supporting psychological operations objective" (FM 3-05.301, 5-1). In other words, during target audience analysis the conductors of PSYOP search through the available groups of people to choose those to influence via the SPO's. Finding an effective target audience often requires rigorous work, suitable tools and lots of data. In marketing the same process is often called customer segmentation.

Weak signals are tiny changes or marks that possibly indicate major events. Hiltunen (2010, 104) defines weak signals as follows:

> "[Weak signals are] indicators of possible changes. They are not synonyms for emerging issues. While emerging issues refer to an event or clusters of events, weak signals are signals or these events. In practice these signals can be for example articles in scien-

> tific journals, or notes in a diary of a researcher, blog or microblog posts, rumors and visual observations. The strength of the signal can be measured by its visibility of amount of them. Weak signals have low visibility, and they appear in very few channels."

1.3 PREVIOUS STUDIES

The Finnish National Defence University has recently published quite a many volumes concerning cyber warfare and information operations. Closely linked to this thesis are theses by Kimmo Pispa *Psykologiset operaatiot ja joukkokäyttäytymien internetissä* (2013) and Saara Jantunen *Strategic communication: practice, ideology and dissonance* (2013).

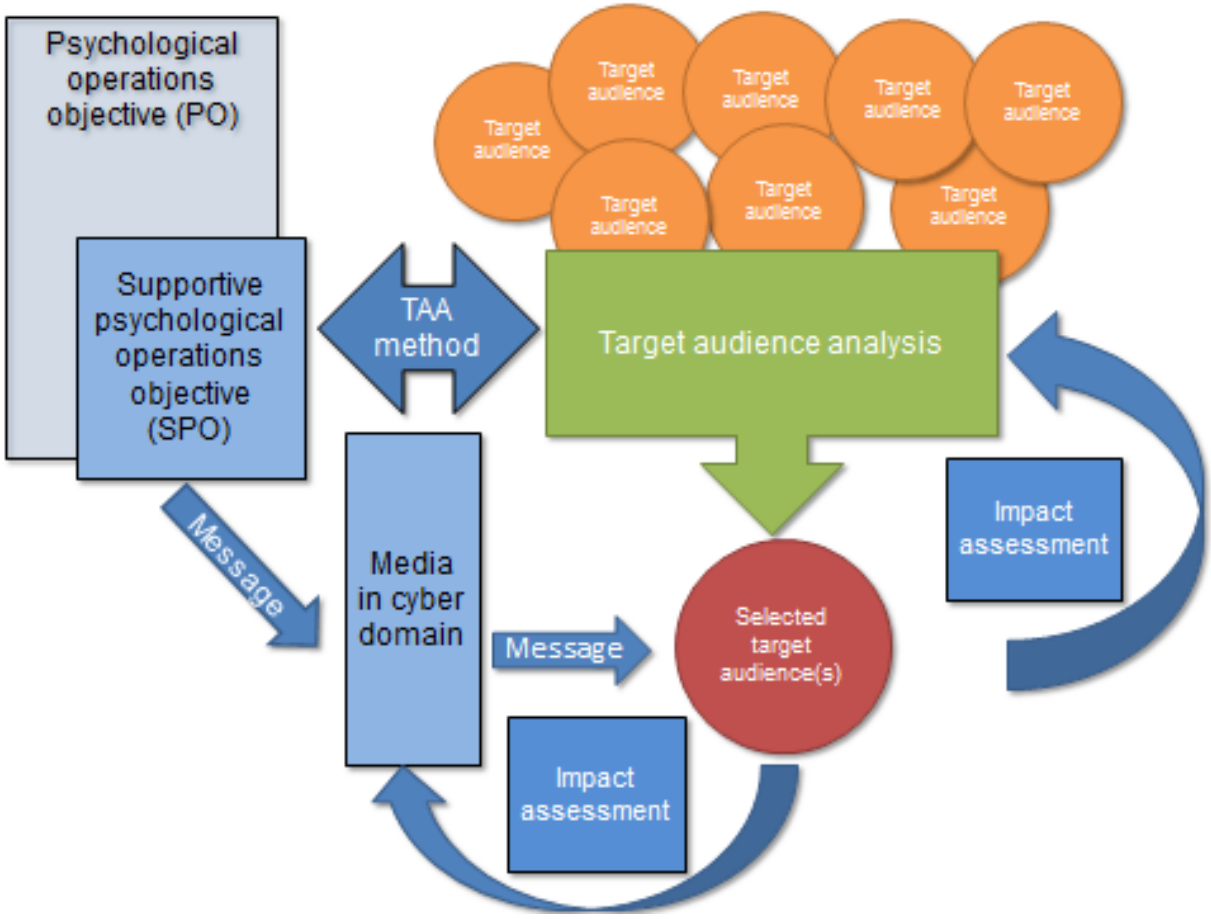
Sakari Soini analyzes social media in his thesis *Puolustusvoimien maineenhallinta sosiaalisessa mediassa* (2013). Another interesting examination of the "social battlespace" can be found in Teemu Nurmela´s work *The social battlespace of stabilization operations – action amongst the people* (2010), in which the subject is viewed from the military perspective of the desired end result. A more practical approach to psychological operations can be found in the thesis of Teemu Saressaro, *Israelin strategisen kommunikaation järjestelyt ja toteutus Cast Lead- operaatiossa* (2013).

A more overall view of cyber defence can be obtained from publications by National Defence University, such as *The Fog of Cyber Defence* (2013), edited by Jari Rantapelkonen and Mirva Salminen, *Cyber Warfare* (2013), edited by Jouko Vankka and *Verkostoavusteinen puolustus* 2030 (2009), edited by Torsti Sirén.

Many studies have recently been conducted in the field of strategic communication and psychological operations. Research concerning social psychology and communication via different media is also numerous, including many textbooks written on the subject. Target audience analysis is covered briefly in U.S. Army field manuals and doctrines, and there are numerous different approaches to audience segmentation offered by commercial marketing companies. Detailed, public coverage of the TAA is scarce, however, even in databases covering scientific studies or articles.

1.4 ORIENTATION AND FRAMEWORK

The orientation of this study is from the viewpoint of a small state. The objective is to find an effective method that does not require large organizations or much personnel. Thus all the elements of the method should be cost-effective and not too time-consuming. The method also must be eligible to be completed with "pen and paper" without computers or network databases.



Picture 1. Thesis framework. Supportive psychological operation´s objective determines the message delivered via media in cyber domain. With the selection and execution of a proper TAA method a suitable target audience is selected as a receiver of the intended message. Impact assessment is later performed to analyze the effectiveness of both the TAA and delivered message.

Psychological operations are a field of information warfare, and target audience analysis is one of the methods used during the planning phase of these operations. As described in the U.S. Army field manual 3-05.30, PSYOP process consist of seven phases of which the TAA is the second, partly overlapping with the first. (FM 3-05.30, 6-2)

Typically psychological operations support the commander's mission via a specific psychological operations objective (PO). Once the PO has been set, more specific supportive psycho-

logical operations objectives are developed. To find the most effective target audience for the reception of the message and thus achieving the SPO, a target audience analysis is conducted. (FM 3-05.30, 6-2)

1.5 RESEARCH QUESTIONS AND METHODS

The goal of this thesis is to find an effective target audience analysis process to be used in the cyber domain by a small nation (i.e. a small team of experts). The intent is to find a useful, practical process that covers the most vital parts of TAA without the need for a massive organization.

The main research question is: "How to conduct a target audience analysis in cyber domain?" The additional research questions are:

1. What is the most effective procedure for conducting a target audience analysis, i.e. what are the main factors to cover in the process?
2. What possibilities and restrictions does the cyber domain offer to this process?

The initial part of the research was conducted by a survey of open-ended questionnaires, sent to both domestic and international operators in the field of psychological operations and market analysis. The purpose of the survey was to gather source material about the operators' TAA methods and their views about the cyber domain. These methods were then to be analyzed in order to find the essential parts of the TAA process via a cluster analysis. During this part of the research it was found that most of the contacted operators either were not willing to participate in the study or did not have a systematic method to be analyzed in this work.

As neither the purpose nor the range of this study allow an entirely new method to be created, it was decided to continue with a theory-based content analysis of the U.S. Army Field Manual FM 3-05.301, which offers a complete method for a target audience analysis. Although updated versions of field manuals concerning psychological operations have been published, they do not include a revision of the method itself and thus the selected manual is still relevant.

According to Tuomi and Sarajärvi (2009, 112-113), in a theory-based content analysis "classification of material is based on an existing orientation of a theory or a system of definitions". Analysis is driven by a theme or a framework. As the first phase of a theory-based content analysis, an analysis framework is constructed. This framework can be strict or loose, and can

include different classifications and categories. It also can be structured, allowing the theory or framework to be tested (as in this work) in a new environment by selecting from the source material only those items that fit the analysis framework. (Tuomi & Sarajärvi, 2009, 112-113, translation by author.)

Content analysis can be seen both as analyzing or as laying out the findings of the source material and can be conducted either inductively or deductively. The objective is to create a "verbal and definite" description of the studied phenomenon, based on logical inference and interpretation of the source material. During the process, the source material is fragmented, conceptualized and reconstructed in a new way to create a coherent structure. (Tuomi & Sarajärvi, 2009, 107-108, translation by author.)

In the more down-to-earth approach of Jennifer Mason (1996, 180), the before mentioned "theory comes first" –view is seen as a more deductive method, in which theory is first presented and then modified (or falsified) by empirical research.

Järvinen and Järvinen (2011, 64) define the content analysis method simply as follows: "Construct the codification chart, code the text, count the frequencies or percentages, test the hypotheses." The view of the content analysis is quite brief and presented as a more mathematical, quantitative rather than a qualitative method. In line with this view, Hirsijärvi, Remes and Sajavaara (1996, 153,157) see content analysis as one of many methods of conducting qualitative research, with close association to language and communication studies.

The FM 3-05.301 is used as a base theory in this study because it includes the concepts and classifications that suit the framework of this study well. It also presents a public, thorough method of conducting a target audience analysis. As found out during the first part of conducting this study, most such procedures are either classified (not applicable to be used as sources in this study) or not sufficiently detailed to be used as a theory.

The selected field manual is also suitable for the intended use of "updating" the TAA procedure to fit the modern cyber domain, because it's focus is on the psychological aspects, not on the technical proceedings. Its concepts and classifications suit the framework of this study without the need to conceptualize further psychological or sociological phenomena. This also enables the method presented in the theory to stand the test of time, although some aspects (as shown by this study) are contested by recent studies in the field of both psychology and sociology.

1.6 SURVEY

Open-ended questionnaires were sent to both military and commercial operators in Finland and abroad, 8 in total. The questionnaire was sent both in English and in Finnish, and the participant was able to choose the preferred language for answering. Open-ended questionnaire was chosen as means of gathering data in order to not confine the participant's views of the cyber domain to the preliminary knowledge of the author. In addition, it was suspected that the participants would employ numerous and fundamentally different TAA methods. Too narrow definition of the TAA could have left some of the data out, perhaps deemed to be out of context by the participants. Only 3 operators eventually answered the questionnaire, which is listed as appendix 1.

The answers were received from the following operators in the field:

- The Finnish Defence Forces Defence Command Public information division
- Pohjoisranta Burson-Marsteller Ltd.
- National Defence University Behavioral Sciences Department

The Defence Command Public information division was chosen because it is an operator in the field of the Finnish Defence Forces´ strategic communication. Pohjoisranta Burson-Marsteller Ltd. was chosen to obtain a commercial view of conducting TAA in cyber domain. The company was selected because of its co-operation with the National Defence University, which helped the author to establish contact. National Defence University Behavioral Sciences Department was chosen in order to apply the practices and experience of the psychologists of the department, in an attempt to add more depth in the field of psychology.

The different participants´ answers are referred to as follows: PA refers to participant A, Q1 refers to the questionnaire´s question number 1.

2. CYBER DOMAIN

This study will not address the technical characteristics of the cyber domain, i.e. the practical technological means and restrictions of said means to conduct a target audience analysis and the possible future uses of data collected. Instead, two main areas of interest are viewed: the nature of the cyber domain itself and the prospects of international law worth considering while conducting operations in an international domain which, by its very nature, knows little national boundaries.

2.1 CHARACTERISTICS OF THE CYBER DOMAIN

The different aspects of the nature of the cyber domain were addressed in question 4 of the questionnaire. Question 4a asks specifically: "What are the main differences in the use of the cyber domain compared to "traditional media"? PA lists these as follows: "1) faster ways to spread information/disinformation, 2) less control, 3) specific target groups can be located, 4) identity secrecy, 5) vulnerability to cyper attacks". PA also adds that: "I believe that in future conflicts the cyper domain will have tremendous effect on outcomes of conflicts… I believe that in operations such as Fallujah, integration between traditional media and cyper domains are already happening." (PA, Q4a.)

PC (Q4a, translation by author) lists the differences as follows:

- an environment of multiple operators
- technical environment
- easy to use, direct communicational affect without media "in-between"
- risky in its own way
- not globally equal, mainly a matter of the Northern hemisphere
- allows new actors an opportunity to be heard
- creates new information (for instance the tweets from Syria = situational picture)
- an opportunity for communal services (such as Wikipedia)

PB (Q4a, translation by author) suffices to note that: "Cyber domain is faster, but also difficult to predict."

Concerning the opportunities granted by cyber domain PA (Q4b) notes that: "cyper domains such as SOME (social media) information and disinformation can be spread rapidly and with-

out control of authorities. Traditional media is often under control or is harnessed to serve certain political view or agenda; where as social media is not."

PA further notices that in the cyber domain and social media it is easier to both locate potential target groups and deliver focused messages to these groups. As potential main cyber domain targets in future conflicts PA lists adolescents and young adults, as they use internet (social media and chats) more than traditional media to get information. (PA, Q4b.) Adolescent and young adults are also more prone than adults to believe this type of information to be true. PA is concerned about the fact that most of these sites are not controlled by proper authorities and thus it is easy [for cyber criminals] to find potential victims from these channels. (PA, Q4b.)

PC (Q4b, translation by author) finds that all participants in the cyber domain (everyone with network access) can have their voice heard. The cyber domain also provides fresh sources for news for the media and information for everybody, although it´s quality is uncertain and confirmed information may be difficult to recognize (PC, Q4b, translation by author). PB (Q4B, translation by author) lists the ease of analyzing weak signals in cyber domain as an opportunity, although reliability remains a challenge.

Of threats and caveats lurking within the cyber domain, PC notes the following: "No one checks and verifies, [thus] concept of information alters and degenerates. Security risks are big. The entire cyber domain is vulnerable to damage – most probably we haven´t seen the worst yet. [There is] a risk of intentional disinformation and rumors." (PC, Q4c, translation by author.) PB (Q4c) mentions only the reliability of information as possible caveat.

Question 4d addresses the main changes taking place in the near future concerning target audiences and their reachability in the cyber domain. PB predicts that target audiences will be smaller in size and more fragmented. In addition, mobile services will also play a part. (PB, Q4d.) PC (Q4d, translation by author) foresees "the scattering of target audiences, who constantly move from one [Internet] service to another. People may have a service account, but they are not reachable via that service." PC also notes that this is a new challenge to communication; "One should open new channels and upkeep the same information in multiple places". PC also expects the ease of use [of different services] to became a demand by the users. (PC, Q4d, translation by author).

An observation from the real world of military operations is provided by Nurmela (2010) in his thesis on the social battlespace in stabilization operations. Nurmela (2010) sees that in such operations the focus should be more on social battlespace consisting of five dimensions, of which the information dimension is where this battle takes place. Although using different terminology, the view provided by Nurmela is very much in line with those of the participants:

> "The fact that modern technology provides commercial off-the-shelf – and most of all, affordable – global means of communication, the information dimension flow within the battlespace will usually become impossible to control. Technology can network actors that reside in different physical environments, but who still share the same lifeworld, idealism or cause. This may include relatives, friends, members of groups, supporters, compatriots, brothers in arms, etc. Ultimately, a virtual lifeworld may become more valued than a lifeworld oriented to the physical world. These aspects may shade the meaning of citizenship, nationality, ethnicity and other social standings." (Nurmela 2010, 81.)

As a conclusion it can be stated that the technical composition stated by the Finnish Cyber Security Strategy (2013) is very much in line with the definitions of the participants. As to the other characteristics, there seems to be a number of mutually agreed observations about the cyber domain. They are as follows:

- fast (in terms of information flow)
- vast (in terms of possible contacts)
- fragmented
- uncontrollable
- ambivalent in information reliability (lots of data available, but it's reliability is questionable and difficult to verify)
- rich in opportunities (previously inaccessible operators can now have their voices heard)

2.2 LEGAL MATTERS

Considering both the execution of a TAA in the cyber domain and the possible future applications of collected data, (for instance in the form of a cyber-attack) legal considerations cannot be unchecked. The cyber domain, especially the Internet, is often viewed as a lawless entity, where information flows freely from a server to another with no legal or international borders.

Albeit many wishing this to be so, this is not entirely true. First, when used mainly as a medium, the use of Internet plays no role whatsoever on the legality of, for instance, selling stolen goods. The act is criminal whether you sell it directly from your store shelf or from your Internet store.

Second, most countries have come to understand the ever growing importance of the cyber domain in both politics (domestic and international) and economics. In order to control and protect their own interests, many countries either apply domestic restrictions on the use of the Internet or try to enforce international co-operation to apply ”law and order” to the cyber domain. One such example is described by Fidler (15, 15) in his article concerning approach of the Obama administration to the cyber domain. He sees the need for “a rule of law” in the Internet as the objective of the current US government. This can be applied via two approaches – clarifying the applicability of current international laws or creating new ones. (Fidler 15, 15.) As potential causes of future disagreements, Fidler (15, 15) points out that the US agenda suggest these laws should be applied universally and enforce democratic practices in all user countries, which may not be in the best interests of some countries currently limiting their citizens’ access to the Internet.

A concrete example of this ongoing struggle can be found by observing the conventions of the International Telecommunication Union (ITU). In his article concerning the revision of the ITU regulations due to take place in 2015, Fidler (17, 6) describes the difficulties observed between the international treaty members. In 2003 China suggested a more diverse approach to the current state of matters with the United States as the solo “maintenance operator” of the Internet, including a proposal for an international Internet treaty. So far, no consensus has been reached. The latest of the ITU conventions, WCIT-12, ended with 89 countries, including China, Iran and Russia signing the revised, multilateral approach. Refusing to sign were 55 countries, including Australia, Canada, EU countries, Japan and the United States. (Fidler, 17, 6.)

With a somewhat narrower focus, concerning the possible gathering of data to perform an effective TAA, a view to the laws affecting cyber espionage has its place here. Another article by Fidler covers the controversy faced by acts of intelligence gathering in the cyber domain, pointing out the *de facto* lack of international laws prohibiting such matters. Although time and again news or assumptions of government-operated espionage emerge, it is generally internationally accepted that spying on each another is something all governments do. Despite some attempts by, for instance, the Obama administration, it remains unlikely that effective

international laws would govern the intelligence gathering of data in cyber domain at least in the foreseeable future. (Fidler, 17, 10.)

For the time being it can thus be concluded that for the purposes of TAA in the cyber domain, no international law prohibits gathering data of the persons that linger online. This can be seen, for example, in the way many international commercial operators gather various levels of data about the users of their services. It is important to note, however, that as per national laws, there is a multitude of laws concerning user privacy and collection of data. These laws are case-specific and often require legal advice prior the execution of TAA process.

Once open hostilities between states break out, different laws take place. This thesis addresses the current state of international law and the terms of armed conflict with no interest in the starter of hostilities. In his article considering the applicability of international law to hostilities conducted in the cyber domain, Schmitt (84, 369) states that the nature of cyber warfare does not exclude the prospects of legal consideration. Martens Clause (the internationally accepted principle of protecting civilians and combatants even in situations not specifically covered in *Lex scripta*) itself is enough to cover any absence of law. (Schmitt, 84, 369.)

Schmitt (84, 373–375) also concludes that one should not see to the actors but to the consequences of actions in determining whether armed conflict (the main subject of Geneva Conventions) takes place. The use of biological or chemical weapons, for instance, with the absence of kinetic weapons fall under the legislation of international law. It is the intended end result of injury, death, damage or destruction that bear the trademark of armed conflict, not the means themselves. (Schmitt, 84, 373–375.) An apparent allegory to cyber warfare can be found here – it can easily be argued that conducting a cyber-attack with the intention of, for instance, disturbing the landing procedures of an aircraft is a hostile attack, i.e. an act of armed conflict.

Herein lies a very thin line – at which point of a consequence of actions one independent act itself can be considered hostile? If TAA is conducted with the intention of eventually causing injury or damage – is it by itself a hostile act? A typical viewpoint with kinetic weapons would be that the employment of weapons to the front line, defining targets and preparing the weapon to fire – all actions short of actually firing the weapon do not fall within the definition of a hostile act. The acquisition of target information, however, might be considered hostile or not, depending on the means of gathering the necessary data (whether the data was collected by the use of armed reconnaissance forces in the defender's territory or by the use of pub-

lished geographic material). Using this allegory it can be argued that the conduct of a TAA itself is not a hostile act *per se*, as long as injury or damage was not caused during and because of the TAA process.

Another point is the targeting of attacks in cyber domain. Although cyber or information attacks fall outside the main focus of this thesis, they are relevant as TAA is typically conducted in order to find suitable targets for an operation. Influencing the TA might require some type of cyber-attack to achieve the SPO. Should the operation not be executable due to legal restrictions, the TAA will be a waste of time. Additionally, as referred to in the previous chapter, the cyber domain by its nature is very uncontrollable. Once a hostile act has been launched, there is typically no meaningful ways to control the carnage or take back the action taken. Hence the need for a view to the targeting practices' legality in the terms of international law.

Considering targeting processes (of which TAA is part of) Schmitt (84, 377–379) refers to the Geneva Convention Additional Protocols that seek to protect civilian lives and property in the battlefield. The protocols prohibit the targeting of civilians as main targets of a military operation. They do not, however, outright ban an operation in which collateral damage (i.e. civilian casualties) is possible. Instead, the commander of any operation must consider the possible military advantages gained by the intended operations versus the expected negative outcome against civilians (SPR, Additional Protocol I, art 52-57, 157–158).

To complicate the matter, civilians might be working for the armed forces without directly taking part in the hostilities. Such personnel as the civilian technicians maintaining a military organization's computer centers may be difficult to judge whether or not they belong to the armed forces. It should be pointed out that these personnel might also be very suitable targets for psychological operations. The armed personnel and operators themselves typically are under daily security scrutiny, but the contracted civilians might be less so. Would it be permitted by the international law to attack these personnel to affect the military capabilities of such a computer center?

Schmitt (84, 379–381) draws the line to the intended end result of death, injury, damage or destruction, both ways. If the civilians directly take part in the actual hostilities of armed forces, they are legitimate targets whether or not they wear a uniform. Likewise, it is not permitted to attack these civilians directly in order take out a hostile military's computer center. This matter checked, Schmitt however points out that psychological operations directed

against civilians are permitted as long as their aim is not to terrorize the people. (Schmitt, 84, 379–381.)

One important aspect to remember can be found in the Additional Protocol I of the Geneva Convention treaties which states that ”In the study, development, acquisition or adoption of new weapons, means or methods of warfare, a High Contracting Party is under obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol of by any other rule of international law applicable to the High Contracting Party” (SPR, Additional Protocol I, Art 36, 149). In no way it is thus possible to conduct any operations in the cyber domain without first addressing the relevant considerations about the actions´ legality.

Finally, as psychological operations typically support the mission of a military commander, operation-specific restrictions and rules must also be taken into consideration. In addition to the before mentioned list, FM 3-05.30 (1-13) offers the following:

- treaties in force, such as status of forces agreement (SOFA) with the host countries
- other statutory constrains, such as postal or propaganda regulations
- operation-specific rules of engagement (ROE)
- communication agreements (local, host nations’ or international)

From the point of view of a small state it can be argued that in the case of any intended hostilities it is imperative to stay within the legal means of warfare as per international treaties. A state, a High Contracting Party of the Geneva convention treaties has to carefully study the expected outcome of its own operations in the cyber domain and conclude whether or not such actions fall within the umbrella of armed conflict. Thus any operation conducted in cyber domain should be counseled by legal advisors prior to their execution, including that of gathering information via TAA.

3. TARGET AUDIENCE ANALYSIS

To provide a military view to what this chapter tries to accomplish, the conclusions about target audiences of the thesis on the Israeli operation Cast Lead by Saressalo (2013) are useful. Saressalo (2013) reminds that a target audience is the group of people whose minds are to be affected, and both individuals and groups of individuals can form a target audience. These TA's are not similar and inside a large TA also the individuals themselves vary. Thus the messages (or lines of persuasion) must be tailored for each target audience. (Saressalo 2013, 83.)

One important aspect provided by Saressalo (2013) is that the message by itself is not as important as the way it is viewed and understood by the TA. Thus knowing the TA's culture, practices and social structures is important. He also makes the important remark that the message intended to be received by the TA will most probably be read by other audiences as well. (Saressalo 2013, 83.) Considering the latter, in cyber domain this may be especially true, as the flow of information from one TA to another is one of the main characteristics defining this environment. With these objectives in mind the practical methods of conducting the target audience analysis are addressed in this chapter.

Finally, it should be kept in mind that in the Finnish Defence Forces there is a recognized need for an effective, structural method of TAA. PA (Q1) states that: "Even though TAA is not required in my current task, I found it most important single issue when evaluating success of influence operations. Influence operations I have studied (mostly PSYOPS) there are two things that are still not appreciated and understood enough. One is TAA and second is MOE (measurement of effectiveness)." PA also states that: "In those cases where MOE has been properly conducted, one thing has often predicted the failure of the operation, the failure to conduct TAA or failure to use the information of TAA" (PA, Q1). As noted earlier, the same need can be seen from P3´s answer to question 3 considering the most important part of TAA methods (P3, Q3).

3.1 DIFFERENT METHODS AND THEIR APPLICABILITY

The original purpose of this thesis was to compare systematically the different methods used by the various operators in the field, in order to find out the common integrative elements amongst the methods. This, however, proved challenging as no applicable descriptions of TAA methods were granted by the participants. Either very basic methods (such as surveys or

interviews with no structural processes) were used (PA, Q1) or the method was tailored ad hoc, based mainly on the experience and skill of the makers of the TAA (PB, Q1). Covered in this chapter are the answers received from the participants concerning the methodology of target audience analysis.

PB (Q1, translation by author) lists the methods used as follows:

- regression analysis (to find the links between groups)
- secondary analyses, in which collected data is viewed from a perspective of resolving a certain problem or theme
- division of data by target groups or archetypes
- micro-targeting, in order to find the groups in which the intended affection is most needed

Of the use of pre-analysis methods in order to choose the proper analysis method, only one of the participants stated that pre-analysis was used if deemed necessary (PC, Q1b), others typically do not use this method (PA, PB, Q1b).

Concerning the reliability of different methods, PB (Q2) states that by focusing on relevant questions with enough participants, generalized answers can be found. Challenges arise from the representativeness of the sample when using network-based questionnaires, in addition to the variations of the activity of between different participant groups. When using social media, the width and depth of different opinions is a problem. (PB, Q2.) PC (Q2) notes that it is quite easy to learn to know your audience depending on its areas of appreciation (what it reads and "clicks"). PC (Q2) also finds the collected information´s reliability hard to estimate, as most of it is qualitative and difficult to verify.

When asked to find the most essential parts of the methods used, PB finds them hard to define. PB notes, however, that searching for weak signals, for instance, in the social media or collecting user/download statistics of a web service could be these. (PB, Q3, translation by author.) PC (Q3, translation by author) states that: "In reality it is based on hunch. If only that could be systemized…" PC adds that more analytic approaches could be purchased [from commercial operators], for example, by using services that further analyze the statistic between the chains of observation.

As can be concluded, the execution of a TAA, as seen by the participants, depends heavily on the expertise and experience of the operators themselves. The method used is selected *ad hoc*, with only one operator using pre-analysis to help in the selection of the most proper method.

A totally different approach to the process, presented here as an alternative and perhaps the shape of things to come, is to use computers to perform the audience targeting. In their study, Abrahams, Coupey, Zhong, Barkhi and Manasantivongs (2012, 2777–2780) used a neural network classifier to segment both semantic and sentiment content of advertisements targeted at industry groups presenting different media channels. The system used dictionaries for both the semantic and sentiment analysis, with a predetermined scoring and tagging system to allow computerized classification. (Abrahams, Coupey, Zhong, Barkhi & Manasantivongs 2012, 2777–2780.)

The test results vary among different industries, but as the researchers point out, the neural network used in the process outperformed a random model classification result by 100-300% (Abrahams, Coupey, Zhong, Barkhi & Manasantivongs 2012, 2777). In addition, the method also enabled the researches to find out differences and typical characteristics of each industry (media channel) type. From the TAA point of view the results present a potentially useful way of conducting either the whole process or a preliminary analysis of the media to be used. At least this type of classification processes help the selection of possible target audiences.

The use of computers allow massive amounts of data to be used and are probably at least partly utilized routinely in the future TAA processes. In the cyber domain this probably is especially so. As the researchers of the before mentioned study point out, in Internet media textual content is easy to retrieve (and use) for this type of automatic segmentation (Abrahams, Coupey, Zhong, Barkhi & Manasantivongs 2012, 2786).

The orientation of this work was to find a process to be used by a small nation, i.e. a small team with no computer-aided processes and thus the computerized operations are not addressed any further. It has to be noted, however, that if the budgetary circumstances would allow purchase or even development of this type of segmentation (or TAA) software, it would allow a small team to access and process large amounts of data. Such force-multiplier software will most probably be available in the near future and is a valid target for further research.

3.2 ANALYSIS OF THE TAA METHOD IN CYBER DOMAIN

The target audience analysis procedure described in FM 3-05.301 offers a complete and thorough view of the TAA process and is used as a base theory in this study. The analysis consists of 10 steps. As defined in the manual, it seeks the answers to the following questions (FM 3-05.301, 5-1):

- What TAs will be most effective in accomplishing the desired behavioural or attitudinal response?
- What lines of persuasion will influence the TA to achieve the objective?
- What media will effectively carry the chosen line of persuasion?
- What events will indicate success or failure of the PSYOP effort?

In this chapter the applicability of the TAA procedure is analyzed for its applicability in the cyber domain. Those parts of the method that are found to apply equally well for all media types are more briefly addressed. Some parts (such as step 2, Target audience selection) are more thoroughfully contested against the nature of the cyber domain and new scientific studies.

3.2.1 **HEADER DATA**

Header data (step one) is a crucial part of any thorough process. The necessary information for later reference, the purpose of the TAA process, environmental factors and all assumptions should be listed here. It is suggested that all the operators of a nation's armed forces, for instance, use the same format. This helps both to systemise and later correlate the data used.

This step of the process remains the same whether or not the TAA takes place within traditional media or cyber domain, although the volatile nature of the latter require careful notes of what networks and sites were addressed and when. A popular site, for instance, might suddenly go offline and thus all information stored in it could be lost.

3.2.2 **TARGET AUDIENCE SELECTION**

Target audience selection (step two) is a crucial part of the process. FM 3-05.301 (5-2) states that: "To select an appropriate TA, it first must be broken into a homogenous group of people with similar characteristics and vulnerabilities with the ability to achieve the desired behav-

ioural or attitudinal change." The main aim of this step is to find clearly defined target groups that can be affected (by their vulnerabilities) and can carry out the intended supportive objective (SPO). This is done by dividing the people to *primary and secondary groups*, *categories*, by finding *aggregates*, *centers of gravity* or *key communicators*. (FM 3-05.301, 5-2.)

In the cyber domain the **primary groups** (families, friends etc.) as defined in the process might not be a good selection. The method itself finds them not ideal as they typically are too small to have the desired effect and receive information from each other, shunning information outside the group. (FM 3-05.301, 5-2–5-3.) In terms of cyber domain it is also quite obvious that the primal requirement for a target group, homogeneity, does not necessarily exist. Amongst family members, for instance, there typically are big differences in the use of networked services, such as news, social networks etc. This is especially true in countries where networked services are not readily available, where you have to, for instance, go to an Internet café to gain access. Social groups and friends might better fulfil the homogeneity requirement, but in comparison to other groups that exists in the Internet their sizes are relatively small and thus are not of primary interest as a target group.

According to FM 3-05.301 (5-3), people form **secondary groups** to "achieve some goal or purpose". These groups are seen as the best types of target audiences, as: "they have a common goal or goals that PSYOP personnel can use as vulnerabilities. Secondary groups readily receive information from outside sources. This type of TA best meets the definition of a TA because they generally have similar conditions and vulnerabilities and are usually large enough to have some power to accomplish the objective." (FM 3-05.301, 5-3.)

In the cyber domain finding such groups can be relatively easy. It could even be said that the cyber domain is a natural habitat of such groups. Election or environmental campaigns typically have their own network sites, with usually a linked forum where people can share their opinions and ideas. As these groups usually try to gain influence by making their voice heard, these network sites typically are not restricted to members only, or require only a brief registration to become a member.

It can be assumed that by its very nature a psychological operation is linked to a political or otherwise commonly known event. In the modern world it can also be assumed that a forum or forums with a suitable target audience already exists prior the conduction of the TAA. Closed network societies serve this purpose equally well, as long as they are formed on the

basis of secondary groups and are accessible in some way. In conclusion, finding secondary groups appears to be a feasible selection in the cyber domain.

Categories, "people who share specific demographic characteristics", as defined in FM 3-05.301 (5-3) are a multi-faceted entity. As can be obtained from the participants' answers (PA, Q4a, PB-PC, Q4c) viewed in chapter 2, the anonymity and the lack of verification make it hard to target specific people by this means of categorization in the social networks or other sites that are open to everybody. The persons accessing these networks might not be using their own name or state their age, profession and other demographic characteristics truthfully, making the targeting of groups such as "male lawyers, aged 35-50" or "female Christians with academic degree" difficult.

On the other hand, accessing, for instance, profession or religion-specific social networks will make this categorization more effective. This effect is further strengthened if access to a closed network is available via a person belonging to the group or by some other means. Accessing closed networks is advantageous at least in three ways:

- persons inside these networks are less likely to lie about their personal data (as this would quite easily be found out by co-workers attending the same network)
- people specific to the intended category belong by the nature of the closed network to the intended category
- persons in the network are more likely to accept information from the members of the same category than from people outside their category

It should be noted that this is an opportunity especially granted by the use of cyber domain. Other media, such as magazines are typically edited and controlled. In a hostile environment spreading messages that counter the views of the editor might be difficult.

Finding **aggregates**, "collections of people identified solely by a common geographic area" is deemed unfruitful by FM 3-05.301. They "rarely if ever make a good TA since they almost never share common conditions and vulnerabilities". (FM 3-05.301, 5-3). In cyber domain this can be seen to be even more so, as members of network societies seldom form a geographic entity. It is unlikely that the members of one part of a city, for instance, would share common values and use same networks, in addition to sharing same vulnerabilities.

In some circumstances (such as targeting people concerned with pollution of a local river) a geographic identification factor can be found. Another example could be members of ethnic

or religious groups living in a certain area of a city. In these cases, however, other means of segmentation (such as categories or secondary groups) will probably be more effective.

FM 3-05.301 (5-4) states that: "**centers of gravity** are individuals or small groups who have a large degree of power over others". They are very good target audiences with possibly tremendous impact if they can be affected by psychological operations. However, according to the field manual this typically is not so as their susceptibility is low. (FM 3-05.301, 5-4.) Assessing small groups or individuals in the cyber domain directly can be difficult, apart from using their e-mail or personal sites as means of communication.

The differences of the applicability of cyber domain vs. other media in the terms of affecting the centers of gravity are hard to define and very case-dependent. It seems unlikely to affect centers of gravity via cyber domain only. It is more likely that affecting a large group (such as a secondary group) directly can achieve the indirect goal of affecting a center of gravity. A political figure, for instance, can be affected by an apparent change in the "public opinion" of a people. In some cases delivering verifiable new information via the cyber domain can also affect these groups. In these cases, however, it seems unlikely that the form of media itself plays an important part.

Key communicators are "individuals to whom members of a TA turn to for information, opinion, or interpretation of information" (FM 3-05.301, 5-4). According to the field manual, using these individuals can add credibility to the intended [SPO] message but can seldom be directly affected (FM 3-05.301, 5-4). Viewed from the perspective of cyber domain, the characteristics of these persons by means of affecting them appear at first glance to be those that of the centers of gravity – no apparent differences between using either the cyber domain or traditional media are visible. Some key communicators (Pope Francis, for example) already use the cyber domain very effectively. Nevertheless, there is no effective difference between the traditional media and the cyber domain in this case, as these persons already are well-known and can use the traditional media to present their views as well.

In the cyber domain, however, new types of key communicators exist. One such example are the bloggers and vloggers (video bloggers), persons that share their views about politics, economics etc. and who can rise from anonymity to a key communicator status in a matter of weeks, if not days. In the traditional media these persons (such as famous news anchors, columnists, experts etc.) exist as well, but they often gain their audiences by the willing ac-

ceptance of the editor or producer. As such, their views can be seen to reflect that of the shareholders of the media enterprises.

This new type of a key communicator might be a very effective target audience. As noted by PC (Q4a, translation by author), the cyber domain "allows new actors an opportunity to be heard". Some actors gain the weight to their message via their expertise, some with their popularity only. It can be assumed that at least some of these persons are vulnerable to the messages of the psychological operation without the interest or means to verify the message. As noted by PA (Q4a), adolescents and young adults are more prone than adults to believe information from social media and chats to be true. A popular icon could present such a TA, especially if the person has risen to popularity via some other means than by his or her expertise in the political or commercial arena, for example.

It should be noted, however, that many of these new type of key communicators rise to publicity via a reference to them in the traditional or commercial Internet media. This idea is reflected by Pispa (2013, 71–73) in his thesis, in which he states that "according to studies, mass media affects what people have an opinion on, the type of these opinions and how people react to phenomena". In other words, a communicator shunned by media is not a very good communicator. Especially in those areas where the access or use of Internet is constrained by authorities these persons might not gain the favourable audience to their opinions simply because they are not known to the public and hence might not present a successful target audience.

A different approach to key communicators is presented by Shakarian, Shakarian and Ruef (2013) in their book "Introduction to Cyber Warfare". Addressing the "tipping model" first introduced by Thomas Schelling (1978), Shakarian et al. have concluded that a *social cascade* (introduction and propagation of a new trend through an entire network) might require only 1% of the network's population to originally adopt the new trend (assuming members adopt the trend if their friends do). These persons are the key nodes of the network topology. (Shakarian et al. 2013, 178–180.) Depending on the intended message, it may thus sometimes be more effective to find this type of "seed sets" (as defined by Shakarian et al.) within a network, rather than targeting individuals or "super nodes".

An effective way of finding these persons is by the use of computer algorithms. As suggested by the book, this type of computer software is already being acquired by at least Russia and

the USA (although in the USA the project was cancelled due to privacy concerns) (Shakarian et al. 2013, 180).

As the function of these seed sets from the perspective of TA selection is similar to that of key communicators, no new categorization for this type of key nodes of ”seed sets” is suggested in this study. Instead, the category of key communicators is defined as including these persons of threshold value in a network.

A more fruitful comparison can be made between the segmentation groups mentioned in the FM 3-05.301 and those existing in (cyber domain) social media as defined by Soini (2013) in his thesis. He finds four types of networking groups.

Group consist of at least two people. To function they need mutually agreed upon goals, are aware of their own and others' membership and interact with each other. Groups commonly have public or unconscious rules, procedures and norms, violation of which may lead to sanctions. (Soini 2013, 37, translation by author.) In comparison to the field manual segmentation, some aspects of both primary and secondary groups can be found here, with perhaps more commonality with the secondary group (via the commonly agreed-on goals).

It can be concluded that this type of group would make a good TA, as the common rules and norms emphasize the TA requirement of a homogeneous entity. It also can be expected that as the entity has been created in the cyber domain, it can also be affected there. To make an effective TA, however, the group has a common failing with the primary group described in the field manual – its size. If all the members know each other, it means that the group cannot be very large, and unless being a center of gravity it might not be able to carry the intended mission. Thus it is suggested that the larger version, network society is used as a segmentation group instead.

A **Swarm** is made up of people that take part in an action without forming a group. The main idea of a swarm is to produce collective intelligence (swarm intelligence) that exceeds that of a single expert. Examples of this swarm intelligence are the search algorithms of Google, creation and updates of Wikipedia and Open Source –type programs. (Soini 2013, 38, translation by author.)

To be effective, a swarm must be (Soini 2013, 38, translation by author):

- multiform, consisting of people with different background, education or view of the World
- independent within the group, i.e. the opinions of the members of the groups must not depend on the opinions of the others
- diverse, with people using their own or local information

As one example of the utilization of swarms, Soini (2013, 39) presents *crowdsourcing*, giving a task to a previously undefined group of people by an open invitation. An "invitation" to attack Estonian network sites during the Bronze Soldier incident is one example of utilizing a swarm. Presented by Pispa (2013, 84) in his thesis, he points out that for the cyber-attacks (the end result, perhaps, of a successful psychological operation) a specific target audience was selected: the youth of Russian minority in Estonia.

If there was a psychological operation (this is disputed), the target audience bears both the trademarks of a secondary group (of the field manual) and swarm (as defined by Soini). The TA assembled to achieve a common task, had the mass and means to affect, had similar vulnerabilities and were willing to accept information (the narrative of the "oppressive Estonian state" and means of successful cyber-attack) from an outside source (the social networks addressing the issue). From the attacker's point of view the target audience selection was a clear success.

Another swarm phenomenon, *produsage* (from words production and usage) bears the idea of users not only consuming but also refining the content (and information) of a network. As examples Soini (2013, 39, translation by author) list the wiki-phenomena, YouTube video blogs and Open Source –programs.

Networks (of people) are held together by a common social objective of interest. As listed by Soini (2013, 40–41), they are typically relatively stable and consist of more than tens of members. Unlike in the previously addressed group, not all members are known by everybody else, although all members are aware of being a member of a common network. The relationships between members are mainly due to belonging to the network, and there is a loose feeling of community. (Soini 2013, 40–41, translation by author.)

From the perspective of the TAA, Soini (2013, 40–41, translation by author) addresses a very interesting phenomenon, a so called *scale-free network* rule. This rule states that amongst a random group of single units (or nodes) in the cyber domain a network consisting of connec-

tions by some measurable rule can by established. In this network some nodes have significantly more connections than other, and some, so called *super nodes* have exponentially more connections than others. These super nodes are very scarce. (Soini 2013, 40–41, translation by author.)

The similarity between super nodes and key communicators is apparent, although these two phenomena may have different origins. As previously described, key communicators are those persons whose opinions other people respect. This may or may not have anything to do with how many connections in the cyber domain this person might have. The end result from the TAA point of view is nevertheless the same – via accessing these persons a potentially great number of people can be accessed. At least the risk of losing all the potential audiences beyond a single super node in the cyber domain is too big so as not trying to identify these persons. So as not to create too many segmentation rules it is suggested that the categorization term ”key communicators” should be seen in wider perspective as ”those whose input is accessed and/or respected by a large number of people”.

Although it would be tempting to compare centers of gravity to these super nodes as well, there is an important difference. As described by the field manual, centers of gravity have a degree of power over others. By definition, this power is acquired by means other than just popularity (or number of connections in the cyber domain). As such it is suggested that the center of gravity –segmentation is left as it is, a type of its own. (This does not mean that a center of gravity could not simultaneously be a key communicator or a super node as well.) However, from the perspective of making a TAA, network (of people) appears to be a useful segmentation tool, at least more proper in the cyber domain than finding aggregates, for instance.

As described by Soini (2013, 43–44), **network societies** (of people) are held together by a common interest. In this they resemble a large group. Network societies differ, according to Soini, from the network in the way the members interact with each other. Compared to members of a network, the interaction between members it often more active, there are social connections of many levels, integral hierarchy and norms in the society. In addition, there is a relatively strong feeling of community. The members of the network society may connect with each other using multiple social network sites (Soini 2013, 43–44, translation by author.)

From the TAA point of view it has to be addressed whether networks and network societies are different from each other enough to be segmented as separate entities for a selection of a

TA. Considering the later steps of the TAA process, some aspects such as conditions or lines of persuasion can be seen to require elements in which these two groups differ. For instance a network society with potentially multiple levels of social contacts is more likely to have similar orientations compared to a network with a common social object only. Likewise a line of persuasion based on this social object only may be more effective among a network than a network society with possibly more diverse range of reactions. As such it is suggested that these entities are listed as separate rules of segmentation.

Another example of the selection of target audience is presented by Blasius and Mühligen (2009) in their article "Identifying audience segments applying the ´social space´ approach". Originally presented by Bourdieu (1984), the social space approach focuses on three dimensions; economic, social and cultural capital (Blasius & Mühligen, 2009, 73). In their research, Blasius and Mühligen constructed a "social space", a diagram of persons' lifestyle choices of clothing, food, celebrities and movies among the before mentioned three axes. In their study they demonstrated that consumer choices of soft drinks are correlated with the social space they had created. In other means, people who liked Pepsi Cola could be found in a certain segment of the social space, whereas consumers of Red Bull inhabited another area. (Blasius & Mühligen, 2009, 83–85.)

For marketing purposes, these findings are useful. If the people who like a certain movie star or film director also make certain lifestyle choices, the advertising of a new soft drink, for instance, can be focused on the films which' audiences are more likely to enjoy the product. From the TAA point of view the question, however, is whether or not the social space approach is applicable in the TAA process.

To begin with, let us be reminded that according to FM 3-05.301 "To select an appropriate TA, it first must be broken into a homogenous group of people with similar characteristics and vulnerabilities with the ability to achieve the desired behavioural or attitudinal change" (FM 3-05.301, 5-2). The social space approach clearly enables the first part. There is no theoretical limit to the number of people inhabiting the social space (although large numbers effectively require the use of computers), and by selecting applicable axes almost any group of people can be clustered into homogeneous (by means of the selected axes) groups.

On the contrary, however, it can be argued that the most important underlying potential for the target audience to take action is the motivation of the people affected. If the persons belonging to the affected group are not motivated to act on basis of new information, that audi-

ence is not suitable, even if other aspects would get a high ranking in the process. The social space approach clearly is applicable for marketing, but whether or not it is applicable for TA selection is not instantly clear. At least it seems safe to assume it could be helpful in the initial part of TA selection as a type of pre-selection method. The susceptibility assessment (estimating whether TA can be influenced or not) is nevertheless done later in the process, during step 7.

The selection of the TA can, of course, be done by whatever means the conductors of the TAA see fit. A multitude of segmentation processes, more or less complex, are available. From the TAA point of view, however, it would seem plausible that at least in an environment as complex as the cyber domain, a simple segmentation into groups along different factorial axes is not enough. These types of processes may help to organize the groups, but the selection of groups must be done with the accuracy of selecting specific target audiences to be affected. The method of selecting these specific groups amongst the segments of people is a process of its own and begs for further research. It, however, falls out of the range of this study.

A as conclusion of this step, it is suggested that a revised combination of segmentation groups could be used in the cyber domain. These would be:

- swarms
- networks
- network societies
- categories
- centers of gravity
- key communicators

3.2.3 **CONDITIONS**

In step three the conditions affecting the selected target audience are addressed and analyzed. Conditions are events, issues etc. that affect the TA, causing there to be some kind of need for action or change. Characteristic of these conditions is that the TA has little or no control over them. Conditions have three elements (FM 3-05.301, 5-4–5-5):

- stimulus – an event, issue or characteristic that affects the TA
- orientation – the TA’s attitudes, beliefs and values that affect how TA thinks or feels about the stimulus

- behavior – the observable action or lack of action by the TA

The selection of relevant conditions is made by estimating the behavior of the TA. This is done by a six-step process as follows (FM 3-05.301, 5-4–5-6):

- identification of the condition (problem) (derived from the SPO)
- selecting research method
- conducting the research
- categorization, in order to assess the relation between TA and SPO
- numbering of conditions (for further reference)
- identification of each condition´s source for later verification of credibility

Concerning the cyber domain it can be noted that from the perspective of the conductors of the TAA in cyber domain the lack of information rarely is an issue. The mass of information about events, current issues and people's opinions and beliefs of them is painstakingly huge. At first glance this can be seen as a positive matter – one has no need to rely on books, magazines, interviews from individuals etc. for information that is possibly both controlled and out of date. The data almost overwhelms the searcher with more and more people waiting in line to tell you how they feel about this very important matter at hand.

As can be obtained from the participants of the questionnaire, the situation nevertheless is far from simple. The stimuli themselves are probably fairly easy to find out, although the bias created by media (as described in 3.3.2) will affect what events and issues are discussed. The orientation of the TA, however, is much harder to resolve. One of the positive facts is that "in the cyber domain everyone with a net access can have their voice heard", as noted by PC (Q4B, translation by author). This allows a more diverse combination of orientations to be considered, compared with that presented only via traditional media. This multitude of voices also allows weak signals, one of the most reliable sources as seen by PB (Q4B, translation by author) to be noted.

How easy is it to find the correct orientation in the end? As noted earlier by PB (Q2), "focusing on relevant questions with enough participants, generalized answers can be found". However, both PB and PC (Q2) find the reliability of the data difficult to verify. In addition, considering potential targets for a psychological operation, for instance in a state run by a dictator, it can be assumed that the amount of malcontent of the people is one of the best kept secrets by the regime.

Once the orientation of the target audience has been figured out, the predicted behavior of the TA has to be estimated. This part of the process has no direct relevance to the media used, as this part is conducted by the makers of the TAA themselves. It must be remembered, however, that the before mentioned rules of behavior in the cyber domain (in contrast to ”real life”) still apply .

Considering the public nature of the cyber domain it can be concluded that this step of the process is both easy and difficult. For the success of the intended operation the prediction of the behavior of the target audience is vital. Lots of information to base the analysis on can be found, but at the same time its relevance is hard to estimate. One has to conclude that to this part of the process the method itself offers no final answer – it is up to the makers of the analysis and their experience and expertise to judge the reliability of the data.

3.2.4 **VULNERABILITIES**

As stated in FM 3-05.301 step four (5-6), “vulnerabilities are the needs that arise from the conditions of a TA, which they will strive to satisfy or benefit from once they are satisfied.” The key work here is “strive”, whether it is a need, a want or a desire that is the goal of the TA. For the latter part of this chapter the term “need” is used to define the before mentioned triad of goal of ambition.

Vulnerability selection is done by a five-step process (FM 3-05.301, 5-6–5-9):

- identification of needs
- categorization and prioritization of needs
- identification of needs conflicts
- determination between the need and the supportive objective
- examination of each vulnerability

The process lists two types of needs – biological (physiological) and social. Biological needs are similar among all human societies, whereas social needs vary from one culture to another. According to the method, the possibility achieving the acknowledged needs will be the motivation for the TA to alter its behaviour. (FM 3-05.301, 5-6.) As the most widely known explanation of need satisfaction, the FM 3-05.301 (5-6) presents the Maslow hierarchy of needs. Presented in the field manual is the original model with 5 levels.

A recent critique to the Maslow´s hierarchy of needs, especially concerning its´ applicability in cyber domain was published by Ruthledge (2013). She states that none of the famous needs of the hierarchy can be fulfilled without social connection. This idea is even further strengthened by the ever-increasing connectedness and complexity of our modern life. She argues that: "As such, observed behavior is not necessarily reflective of what we are unconsciously driven to do to satisfy our needs." The point is that observed behavior might not be directly connected to motivation but to means instead. As a concrete example Ruthledge views the Arab Spring – social media (Facebook and Twitter) did not cause them, but their existence connected people and "inspired them to act on existing motivations and goals". She points out that despite the recent technological leaps the human brain with its needs still remains the same. (Ruthledge 2013.)

It is easy to agree with this view. At least in the modern societies (in which people have an access to social media in cyber domain) we are all increasingly co-dependent on each other. Even the most basic needs (in accordance to Maslow´s hierarchy) of food and shelter depend on mutual trust of the currency used to pay rent and grocery bills, and on the logistic chains of supply. Should we no longer trust each other in terms of these basic functions, the everyday life in our society would crumble in the matter of days. Conscious or not, the need for social co-operation is a relevant factor of survival in modern societies.

Another possibility presented in FM 3-05.301 (5-7) to address the needs of the TA is a bit modified version of the Maslow's hierarchy. The needs are divided to critical, short-term and long-term needs. Critical needs are needs of immediate safety, whereas short-term needs focus on the lack of proper environment for healthy life. Long-term needs focus on Maslowian needs of self-esteem and self-actualization and aim to create a stable and healthy environment. In most cases it would seem that this triad would be more usable than the Maslow's hierarchy in those cases where the makers of the TAA are not experienced psychologist with deeper understanding of the underlying machinations of human needs. (FM 3-05.301, 5-7.)

As to the conduction of this step in the cyber domain, it can be concluded that while the needs of the TA are essential to the TAA *per se*, in the cyber domain the assessment of TA's needs is ambivalent. Information is in excess, but its relevance to the real needs of the TA is hard to estimate. From the author's view this part of the process might well be the one that needs most data from other sources (such as long-time strategic or cultural studies).

One detail not to be forgotten, though, that the interactive nature of the cyber domain offers one unique capability. One does not always need to estimate the needs of the TA – in a proper network site, for instance, you can simply ask the TA what it needs and desires. Some network sites (such as Pinterest) exist solely for this purpose.

3.2.5 **LINES OF PERSUASION**

Lines of persuasion (step five) are arguments that are by definition: "used to exploit, minimize, or create vulnerabilities. A line of persuasion is a detailed, thorough, and concise argument that will persuade the TA to behave or believe in the desired manner." A line of persuasion is created via four steps (FM 3-05.301, 5-9):

- articulation of the main argument
- identification of supporting arguments
- determination of suitable appeal
- determination of the most effective technique

The field manual presents numerous examples of appeals, techniques and their suggested uses to choose from. The natural question is: "What type of influence is the most effective one?" In an interesting study, Nolan, Schultz, Wesely, Goldstein and Griskevicius (2008) state that normative social influence (witnessing the actions of another people) is a powerful yet underdetected force, perhaps even the most powerful one. In two studies the researchers observed both the subjects' change in the nature conserving behavior and their awareness of the normative influence targeted at them. As a result, it was found that "the strongest predictor of energy conservation was the belief that other people are doing it ($r = .45$, $p < .01$), despite the fact that it was rated as the least important motivating factor." (Nolan et. al, 2008, 916)

Another powerful finding in the study was the observation of the actual change in the behavior (not just the change of opinion). The researchers were able to measure the actual change of energy consumption in relation to the different "lines of persuasion" or appeals targeted at subject households. (In addition to normative appeal, appeals such as protecting the environment, benefiting the society and saving money were used.) As shown in the study, the normative appeal had the strongest effect on actual behavior, not just on the opinions of people. (Nolan et. al, 2008. 917–921.) As the purpose of any psychological operation typically is to alter the behavior (rather than just opinions) of the TA, this is an important finding.

Considering these factors it seems that the cyber domain with its anonymity and fast spreading of information is almost the perfect platform for normative appeals. As previously noted by PC (Q4c, translation by author), "No one checks and verifies, concept of information alters and degenerates". With no verifiable knowledge of who actually is behind the comments of a network site, for instance, it seems plausible to assume that barraging a popular site with arguments in favor of the intended behavior can be effective. In a way, from the perspective of the normative influence, the quality of the arguments is sometimes perhaps thus secondary to their quantity.

An interesting point is also made in the discussion part of the study, suggesting an alternative explanation for the results. Nolan et al. (2008, 921) find that: "By going beyond environmental protection and social responsibility, normative messages reach a new population of individuals who might not otherwise have a reason to conserve". From the TAA point of view this comment is interesting, as it suggest that a normative line of persuasion can affect the target audiences not influenced by other means. It can thus be suggested that normative lines of persuasion should be included even if other lines of persuasion are assumed to be more effective.

One opportunity granted by the site structure of the cyber domain is that via a thorough examination of the threads of a network site the "climate" of the site can be estimated. If the main body of the participants, for instance, seem to be young adults with an individualistic attitude, *legitimacy* (laws, institutions, tradition) appeals may be counterproductive. *In-group-out-group* (us vs. them) or *bandwagon* appeals (peer pressure) may in this case be more effective. (FM 3-05.301, 5-6–5-9). This reflects the view of PA (Q4a), that in cyber domain "specific target groups can be located".

It can be concluded that the cyber domain as an environment does not by itself affect the lines of persuasion. The argument is the same whether you read it from a newspaper or on a network site. The package it comes from, however, matters more than previously estimated. Thus, even if the argument itself might not differ whether presented in television, newspaper or Internet, the cyber environmental factors must be considered. If the TA is in the cyber domain, the lines of persuasion must be constructed in a way that fits the "packaging" of the cyber domain.

3.2.6 **SYMBOLS**

Symbols (step six) are visual, audio or audiovisual means used to convey, reinforce or enhance a line of persuasion (FM 3-05.301, 5-13). From the very first glance to any network site the importance of the symbols is made clear: company or group logos (if there is one) are situated in the front page of almost every site and typically follows the user throughout the entire visit to the site. Graphic images typically also make any message easier to understand. According to FM 3-05.301 (5-13), symbols must have the following characteristics:

- they must be recognized by the TA
- they must be meaningful to the TA
- they must be appropriate for the selected line of persuasion

How important symbols are in conveying intended messages? A logo, representing a company or a brand is a symbol. In a study addressing the importance of brand logos, performed by Park, Eisingerich, Pol and Park it was found that: "Since logos visually represent what the brand is and what it stands for, they have the potential to serve as a focal point of connection for customers by communicating and reinforcing a brand's core values. In other words, a brand's logo can be a critical tool for conveying associations between the brand and the self, which in turn helps people see the brand as part of themselves." (Park et al. 2012, 182)

Yet the symbol itself is not enough. The target audience must recognize the "brand" the symbol presents for it to be useful, be that brand a nation, an organization or perhaps an abstract idea such as peace or democracy. In the same study Park et al. (2012, 185) found that the mere familiarity of the logo is not a significant factor in creating customer commitment. In contrast: "commitment is significantly associated with each of the three suggested logo benefits: facilitating brand self-associations, representing the functional benefits of a brand and providing aesthetic appeal". (Park et al. 201, 185.)

From the TAA perspective this means that for the symbol to be effective the TA must know what it stands for. The symbol doesn't naturally need to represent the organization behind the line of persuasion, but it must be in line with the intended effect. The before mentioned logo benefits of self-association and representing the functional benefits of a brand could be used to encourage people to support peaceful elections, for instance, by using well-known symbols of peace and prosperity among the lines of persuasion.

In conveying the intended line of persuasion, a visual symbol is more effective than just a brand name presented in a more visual format. Park et al. (2012, 186) state that: "[their study's] findings indicate that brands with symbols as logos are more effective at providing self-identity/expressiveness benefits than logos that consist purely of brand names. They are also more successful at communicating the functional benefits of a brand than brand name-based logos are".

What type of symbols to use? A recent study on brand logos by Walsh, Winterich and Mittal (2012) suggest that if "customers", or in this case the target audience, favour the "brand" behind the line of persuasion, it is best to use familiar symbols (or logos) without changing them. In their study of brand logo changes it was found that those consumers strongly committed to a brand valued the brand more negatively after the logo was altered. Alternatively, those not very committed to the brand tend to view the brand more positively once the logo has been changed (Walsch et. al.2010, 80–81.)

Although not a primary objective of their study, Walsch et al. (2010, 83) also tested one feature of the logo – its roundedness. In summarizing their and other similar studies, they note that: "A common finding in several studies is the significance of shape. Specifically, roundedness was a key factor of logos perceived to be natural, friendly and harmonious. The apparent significance of this design feature has prompted numerous firms to opt for more curved styles of logo and practitioners believe this particular trend will persist. For sharp or pointed shapes, vigour, strength and robustness are more common associations." (Walsch et al. 2010, 83.)

In choosing the symbols to be used within the line of persuasion, it can thus be suggested that if the target audience is likely to view the suggested message favourably, in other words conveying feelings of familiarity and presenting the target audiences' own opinions and views, a traditional, unchanged logo or symbol should be used. If, however, the TA is likely to view the message in a more unfavourable terms, it might be useful to alternate the symbol a bit while keeping it still recognizable. If the symbol is to be altered, for an intended friendly, coercive line of persuasion it might be useful to apply round variations to the symbol. For an ultimatum-type, more offensive message, sharp and strong angles are suggested.

As to the relevance of this step in the cyber domain, it can be concluded that symbols are effective in all the media that displays visual content. The cyber domain differs not from the others in this regard, although it has to be noted that the use of symbols in the Internet is

commonplace and one symbol might easily be lost among the others. In addition, it must be kept in mind that the symbol itself is not meaningful, the emotions and conceptions associated with it are.

3.2.7 **SUSCEPTIBILITY**

During step seven, the previously crafted lines of persuasion are ranked for their assumed effectiveness, i.e. the "degree to which the TA can be influenced to respond in a manner that will help accomplish the PSYOP mission, or simply put, how well a vulnerability can be manipulated". FM 3-05.301 (5-13) suggests using ratings between 1 and 10, 10 meaning that the influence is estimated to be very high. This is the case with most critical needs. As noted by the field manual, events and circumstances will change the value and thus this step should be re-evaluated after significant changes in the aspects affecting the TA. (FM 3-05.301, 5-13.)

To add insight into the effectiveness evaluation the aspect of the regulatory fit theory should be considered. In a work summarizing the contemporary knowledge of regulatory fit in 2006, Avnet and Higgins find that: "Regulatory fit theory proposes that regulatory fit occurs when the strategic manner in which a choice or a decision is made sustains the decision maker's current goal orientation, and this regulatory fit affects the value that he or she assigns to this choice or decision outcome." (Avnet et al. 2006, 2.)

How does this apply to the TAA process? Avnet et al. (2006, 6) hit the spot with their note that: "Regulatory fit suggests that people have more confidence in their reactions to a message and its content when they engage the message in a manner that sustains their orientation than when they do not. This effect of fit occurs regardless of whether their reactions to the message are positive or negative, that is, regardless of whether the message and its content are relevant or irrelevant to the recipient's needs and goals." (Avnet et al. 2006, 6.)

To estimate the effectiveness of a line of persuasion it is thus useful to try to estimate whether the selected lines of persuasion are in line or in contrast with the regulatory fit of the selected TA, as an effective line of persuasion *per se* might lose its effectiveness if presented in a non-effective way. For instance, if the TA is more afraid of losing its current status (loss aversion) than gaining new influence over others, a line of persuasion promising new power or wealth might not be effective. In this case, an argument suggesting ways to avoid losses (of current status) would probably be more effective.

The research of Avnet et al. (2006, 14) also suggests there to be a difference between effective arguments whether the TA is promotion or prevention oriented. For chronically promotion oriented people, the use of feelings (instead of reasoning) appeared to make the decision more favorable (in the test performed it raised the monetary value of the test object). In contrast, appealing to reason seemed to be more effective with prevention oriented people. (Avnet et al. 2006, 14.) Even if the orientation of the TA in the current case is not known, it might be useful to bear in mind these results. For instance, if the argument is intended to help the TA to prevent losing its current standing, the message may be more effective if the argument appeals to reason rather than to emotional values.

The regulatory fit theory is not the only concept available to assess the decision making process. It was chosen to be presented here as an example of relatively new psychological research available to be used in the making of the TAA. Other concepts are excluded from this study, but should be addressed if the TAA process is (as suggested) to be completely revised.

The cyber domain differences from other media in at least in the way these before mentioned ratings can be tested. The vastness of the everyday interaction in the cyber domain makes it possible for the conductor of the TAA to "test" an uncertain rating by writing a suitable comment in the network site where members of the TA visit. A quick analysis of the reaction (or lack of it) can then be used to have some idea of the effectiveness of the line of persuasion.

Another opportunity, granted of course that the makers of the TAA have the resources, is to gather long-time data of the reactions and behavior of the TA. This will enable to look for similarities between earlier cases and the one attempted. Most network sites have a long history of discussions and this makes it possible to gather these similarities even if the data gathering itself would not have happened earlier.

Once again, this step in the cyber domain is ambivalent. Some TAs' (those active in the discussion groups etc.) reactions will be easier to estimate that others'. Nevertheless, as noted before, the unique opportunity offered by the cyber domain is the very fast "reaction time" of the TA, which allows different lines of persuasion to be tested simultaneously. In addition, unlike in the traditional media, ineffective or counterproductive arguments can be corrected if found unsuitable for the task.

3.2.8 **ACCESSIBILITY**

Step eight seeks to answer the question: "what mix of media will effectively carry the developed lines of persuasion and appropriate symbols to the TA?" (FM 3-05.301, 5-13). As this is a relevant part of the process concerning the cyber domain, it is analysed here more thoroughly. The answer is found in seven steps as follows (FM 3-05.301, 5-14–5-17):

- determine how the TA receives information
- assess the TA´s usage of media
- answer the question: "Why does the TA access the medium?"
- assess the involvement of the TA in accessing the media
- find whether the media is accessed alone or with others
- summarize the media usage of the TA
- summarize the media sources available

All steps described above apply to the cyber domain as well, although the definition of media in the manual (due to its publication year) is a bit outdated. Describing the media of the time, the manual lists radio (AM and FM), television and newspapers or magazines as the media types to be used. Nevertheless, the steps listed above are still useful in the modern cyber domain as well, as far as internet radio stations, internet-based TV and digital versions of newspapers and magazines are concerned.

The major update to the before mentioned list are the contemporary, much more interactive mediums of the cyber domain, such as discussion sites, Internet community sites and services, as well as modern types of communication. Considering accessibility, the relevant question about TA might not be "accessible or not" but rather "which avenue or avenues of access to choose?" Thus, a bit broader definition of accessibility might serve the process of TAA better. As defined in FM 3-05.301 (5-13), the accessibility step searches for media that "will effectively carry the developed lines of persuasion and appropriate symbols to the TA". A comment on the TA's network site (amongst hundreds or thousands of others) will access the TA, but not effectively.

To revise the accessibility step to be more relevant in the cyber domain it is thus suggested to rewrite the question as follows: "What type of interaction will effectively carry the developed lines of persuasion and appropriate symbols to the TA in the cyber domain?"

One example of engaging access (in the before mentioned context) is the famous case of Robin Sage, as presented by Lisko (2010). In the Robin Sage case, Thomas Ryan was able during his 28-day experiment in 2010 to obtain 300 contacts on LinkedIn, over 100 connections on Facebook, and about 150 followers on Twitter. Among the contacts were high-ranking military officers and politicians, and "Sage" also received job offers. As the factors behind the success of the fake personality, the gender and attractiveness of "Sage" as well as her impressive education and career are listed. (Lisko, 2010.)

The previous example is not a valid sample of what might happen in the real world, as Ryan initially targeted persons he knew well and whose trust he could more easily gain. Additionally, once the fake identity of Robin Sage was discovered by certain members of the community, Ryan contacted them and asked them not to reveal the secret. (Lisko, 2010.) From the TAA point of view, however, this case is a good example of how a TA can be accessed. It also presents the unique opportunity granted by the cyber domain. In addition to PSYOP operators contacting TA's, the TA's can also play the initiative part by contacting the PSYOP operators, replacing the traditional "one-way" presentation of one's own message with that of an active discussion between members. The benefit of the TA being the active partner of this interaction is that the initial threshold of interaction is lower.

Like the step 2, this step differs a lot from traditional media. The cyber domain offers a unique capability, that of two-way interaction between the operators and the TA. Instead of just presenting information to the TA, the TA can be more engaged in the influence process by its own interest. In other words, instead of trying to make your message heard in the noisy environment, the cyber domain allows an operator to make itself interesting in the eyes of the TA, thus enabling the initial steps of the interaction to take place in a favorable way. If the TA contacts (or "clicks") the operators' message by its own accord, the initial resistance typically directed towards new phenomena has already been overcome.

3.2.9 **EFFECTIVENESS**

During step nine the effectiveness of the selected target audience is rated using the already familial range of 1-10. According to the field manual: "effectiveness is the actual ability of a TA to carry out the desired behavioural or attitudinal change". For this the TA must have "power, control, or authority" and it must not be too restricted so as not to be effective. (FM 3-05.301, 5-17.)

Considering the cyber domain, perhaps the most profound restriction is that of access to the network itself. Quite clearly, all TA's outside the network cannot be reached and thus are not to be further considered in this step. Of those that have the access, the restrictions listed in the field manual can be seen to apply. The nature of the cyber domain itself adds some more restrictions, such as the inability to effectively use the network because, for instance, due to lack of technical skills.

As to the differences between the cyber domain and traditional media concerning this step, it can be concluded that the step itself does not differ much depending on the environment it is conducted in. When considering the TA in the cyber domain, however, one additional aspect has to be estimated – that of the TA's influence in the cyber domain itself. Although estimated to be of similar level of authority by themselves, TA's may vary dramatically in the way they behave and affect others in the cyber domain.

3.2.10 **IMPACT INDICATORS**

As described in FM 3-05.301 step ten (5-17), impact indicators are "those events that aid in determining the success of the PSYOP effort". The importance of this step was emphasized by PA (Q1) in his statement that: "…two things that are still not appreciated and understood enough. One is TAA and second is MOE (measurement of effectiveness)".

Impact indicators are addressed in a later section in FM 3-05.301 (7-12) and are defined as being either *positive* (favorable to the intended PSYOP effect) or *negative* (unfavorable). Both can have a *direct* or *indirect* orientation. Direct indicators show the actual behavior of the TA, whereas indirect show a possible effect without direct causal relevance to the PSYOP operation. (FM 3-05.301, 7-12.)

Once again, in the cyber domain at least some results can be very quickly assessed. A new ad campaign, for instance, might spark a heated discussion within hours, if not minutes. Assessing the number of people viewing the site and the general climate of the conversations a quick analysis of the immediate effect can be conducted. In this, however, one must still keep a clear vision of the intended target audience. If the intention was to target the voters of the next election, the discussions taking place in sites mostly populated by adolescents bear no fruit to this analysis.

4. CONCLUSIONS

4.1 TARGET AUDIENCE ANALYSIS

There is not one single, all-conclusive method for selecting a target audience in the cyber domain, but rather a multitude of approaches. This is especially true if the segmentation processes used by marketing companies are included in this definition. Some (perhaps more experienced) operators currently use a variety of (sometimes ad hoc) methods, tailored to the task at hand. However, in the The Finnish Defence Forces there is a common agreement on the need for one detailed procedure that would cover at least the most important aspects of TAA and would be readily available, helping to synchronize the efforts of different operators. The solution suggested by this thesis is to use the TAA procedure detailed in the US Army Field Manual 3-05.301.

The TAA procedure detailed in the FM 3-05.301 is still relevant and applicable to be used in the cyber domain despite is relatively "old age" (it was published in 2003). The manual offers a detailed and thorough procedure that addresses various aspects of the TAA process. Some parts of the process can, however, be updated due to both technical changes in the environment of the cyber domain and to latest achievements in the field of psychology. The most important parts to be updated as found in this thesis are the selection of target audiences (step 2 of the process) and the accessibility assessment (step 8).

The categorization of the target audiences (chapter 3.2.2.) as described in the FM is not directly applicable in the cyber domain. A new segmentation mix is suggested in chapter 3.2.2, based on the original model and some new studies in the field of network societies. The temporal, fast-pace environment of the TA existing in the cyber domain with volatile topologies makes some of the original segmentations (such as aggregates) obsolete.

The accessibility assessment (3.3.8) still applies to "traditional" media converted into digital form. It lacks, however, the modern interactive nature of the cyber domain and its network sites. The question relevant in the cyber domain is not "is there an access" but rather "which ways of access to use?" Additionally, the target audience can hardly be viewed as a passive listener, viewer or reader of the modern media. As the TA in the cyber domain consists of active members (even the access of the cyber domain itself requires action), the meaning of accessibility has to be viewed in a broader perspective of not only presenting the message but also engaging the TA in to interaction with it.

4.2 POSSIBILITIES AND CAVEATS OF CYBER DOMAIN

In conclusion, the cyber domain is a volatile environment. As found in this study, it is "fast and vast", allowing a piece of information to spread out to far reaches of the globe within seconds. In such, it offers opportunities previously unheard of. Vast number of target audiences can be accessed by a network in an interaction that allows both learning to know the target audience and sending it messages that it accepts and feels as if its own.

This interaction even allows the target audience to initiate contact by its own accord, provided the subject is of some type of interest to it. These contacts, however, may as well became counterproductive, as the flow of information within the networks is not controllable. The message can be distorted, removed from its original context and spread as fast and far as the original message. The message can thus "spill over" and eventually end up making more damage than the original benefits.

The cyber domain consists of immeasurable amounts of data, the reliability of which is difficult to verify. This ambivalence works both for and against the makers of TAA. Information about almost any TA is readily available, and helps to assess the needs, values and other important aspects of the intended TA. The caveat, however, is that this data may sometimes lead to misconceptions or false estimations. The one important matter to understand about the nature of the cyber domain is that you must look for what is not there. In some cases an overwhelming majority of the information might point to a certain direction, but this might be a result of a small overactive minority. The action based on this information might run aground because of the resistance of the de facto majority of the passive members of the population.

Considering the legality of TAA in the cyber domain, for the time being no internationally accepted "cyber domain laws" exist. As per the gathering of data to be used for an effective TAA, no legally binding international counter-espionage laws hinder the use of whatever means of information gathering takes place. Domestic and national laws naturally have to be carefully observed, preferably with legal advisors, prior execution of such operations.

During hostilities between nations, from a legal standpoint, the conduction of TAA in cyber domain is not by itself an act of armed conflict *per se* as defined in the articles of the Geneva Convention treaties. The practical application of the process might, however, brake both domestic and international laws. Concerning the legality of intended action as an act of war, the end result of possible death, injury, damage or destruction is the matter that draws the line.

Once the TAA is complete and the actual operation executed, the Geneva Convention treaties concerning the protection of civilian life and property are in effect. No difference is made between cyber and "physical" attacks if the end results fall within the Geneva treaties. Thus it is not the means but consequences to be carefully observed before even starting the first, intelligence gathering part of an operation.

4.3 FINAL THOUGHTS

In estimating the reliability of this study it can be concluded that the source material used is valid, though probably not conclusive. The material used in this study, consisting mainly of published sources and scientific studies have by their nature undergone a more or less thorough scientific scrutiny and validation. By its public nature, this work lacks the more detailed and tested target audience analysis methods constructed by both military and commercial operators in the cyber domain. This does not, however, make the findings of this work less relevant. It just points to the fact that as the cyber domain is still shaping and growing in its importance, new information offers an edge over a competitor and is therefore not something easily parted with.

The operators of the Finnish Defence Forces find that there should be an common, effective method for conducting a TAA in the cyber domain. As currently such a structured and commonly agreed upon method does not exist, it is suggested that the method described in the FM 3-05.301 (with the suggested alterations of this thesis) should be further tested and revised as a basis for a common model. This would help the co-operation of different operators in the field and would probably further encourage revisions and improvements of this method.

Another suggestion for research is to study the automated segmentation processes provided by neural networks or more simplistic segmentation software. The question is whether a computer-assisted process would be a force multiplier (allowing lots of data to be processed) or just create too much uncomprehensible data to be useful in selecting specific TA's. In the near future these types of programs might be commonplace, but the question is whether or not the software available today is cost-effective.

SOURCES

1. UNPUBLISHED SOURCES

Participant A, answer to questionnaire. In authors possession.

Participant B, answer to questionnaire. In authors possession.

Participant C, answer to questionnaire. In authors possession.

Suomen Punainen Risti 2013. Geneven sopimukset ja muita sodan oikeussääntöjä. Course material from the course "Training of international Geneva Convention treaties to the personnel of Finnish Defence Forces".

2. PUBLISHED SOURCES

2.1. LITERATURE

Hirsijärvi, Sirkka, Remes, Pirkko, Sajavaara, Paula. 1997. Tutki ja kirjoita. Kirjayhtymä Oy. Gummerus Kirjapaino Oy, Jyväskylä 2005. ISBN 951-26-5113-0

Järvinen, Petteri, Järvinen, Annikki. 2011. Tutkimustyön metodeista. Opinpajan kirja. Tampere. 2011. ISBN 978-952-99233-4-2

Shakarian, Paulo, Shakarian, Jana, Ruef, Andrew. 2013. Introduction to Cyber Warfare. A Multidisciplinary Approach. Elsevier Inc. 2013. ISBN: 978-0-12407-814-7

Tuomi, Jouni, Sarajärvi, Anneli. 2009. Laadullinen tutkimus ja sisällönanalyysi. Kustannusosakeyhtiö Tammi. Hansaprint Oy, Vantaa 2013. ISBN 978-951-31-5369-4

2.2 THESES

Hiltunen, E. 2010. Weak Signals in Organizational Futures Learning. Helsinki School of Economics. 2010. ISBN 978-952-60-1039-7

Nurmela, T. 2010. The social battlespace of stabilization operations – action amongst the people. Finnish National Defence University, Department of Tactics and Operational Art. Series 1No 1/2010.

Pispa, Kimmo. 2013. Psykologiset operaatiot ja joukkokäyttäytyminen internetissä. Senior Staff Officers´ course thesis. Finnish National Defence University. 2013.

Saressalo, T. 2013. Israelin strategisen kommunikaation järjestelyt ja toteutus Cast Lead – operaatiossa. Senior Staff Officers´ course thesis. Finnish National Defence University. 2013.

Soini, S. 2013. Puolustusvoimien maineenhallinta sosiaalisessa mediassa. Senior Staff Officers´ course thesis. Finnish National Defence University. 2013.

2.3 ARTICLES

Abrahams, Alan S, Coupey, Eloise, Zhong, Eva X, Barkhi, Reza, Manasantivongs, Pete S. 2013. Audience targeting by B-to-B advertisement classification: A neural network approach. Expert systems with applications. Vol. 40 (2013) 2777-2791. <http://dx.doi.org/10.1016/j.eswa.2012.10.068> March 17, 2014

Avnet, T, Higgins E.T, 2006. How Regulatory Fit Affects Value in Consumer Choices and Opinions. Journal of Marketing Research: February 2006, Vol. 43, No. 1, pp. 1-10. <http://journals.ama.org/doi/abs/10.1509/jmkr.43.1.1> February 22, 2014

Blasius, Jörg, Mühlichen, Andreas. 2009. Identifying social segments applying the "social space" approach. Poetics vol. 38. Issue 1, February 2010. doi:10.1016/j.poetic.2009.10.003

Fidler, David P. 2013. Controversies Involving Government Acquisition of Trade Secrets through Cyber Technologies. American Society of International Law. Insights, vol 17, issue 10. <http://www.asil.org/insights/volume/17/issue/10/economic-cyber-espionage-and-international-law-controversies-involving>. January 7, 2014

Fidler, David P. 2013. The Controversy Concerning Revision of the International Telecommunication Regulations. American Society of International Law. Insights, vol 17, issue 6. <http://www.asil.org/insights/volume/17/issue/6/internet-governance-and-international-law-controversy-concerning-revision>. January 7, 2014

Fidler, David P. 2013. The Obama Administration's International Strategy for Cyberspace. American Society of International Law. Insights, vol 15, issue 15. <http://www.asil.org/insights/volume/15/issue/15/international-law-and-future-cyberspace-obama-administration>. January 7, 2014

Lisko, Tim. The Robin Sage Experiment: Interview with Omachonu Ogali. Privacy Wonk blogspot. 6.9.2010. <http://www.privacywonk.net/2010/09/the-robin-sage-experiment-interview-with-ogali-om.php> February 25, 2014

Mason, Jennifer. 1996. Qualitative researching. SAGE Publications Ltd, London, California, New Delhi 2002. ISBN 0-7619-7428-8

Nolan, Jessica M, Schultz, P. Wesely, Cialdini, Robert B, Goldstein, Noah J, Griskevicius, Vladas. 2008. Normative Social Influence is Underdetected. Personality and Social Psychology Bulletin 2008; 34; 913. Sage publications 2008. <http://psp.sagepub.com/content/34/7/913.abstract> February 22, 2014

Park, C. Whan, Eisingerich, Andreas B, Pol, Gratiana, Park, Jason Whan. 2012. The role of brand logos in firm performance. Journal of Business Research, vol. 66. (2013). <http://dx.doi.org/10.1016/j.jbusres.2012.07.011> March 3, 2014

Ruthledge, P. 2011. Social Networks: What Maslow Misses. Positively Media 8.11.2011. <http://www.psychologytoday.com/blog/positively-media/201111/social-networks-what-maslow-misses-0> January 15, 2014

Schmitt, Michael N. 2002. Wired warfare: Computer network attack and *jus in Bello*. RICR Juin IRRC june 2002 VOL 84 nro 846

Walsh, Michael F, Winterich Karen P, Mittal, Vikas. 2010. Do logo redesigns help or hurt your brand. The role of brand commitment. Journal of Product & Brand Management, vol. 19, number 2, 2010. <http://ssrn.com/abstract=1998809> March 7, 2014

2.4 OTHER

USA Joint Publication 3-05-301. 2003. Psychological Operations Tactics, Techniques and Procedures. <https://www.fas.org/irp/doddir/army/fm3-05-301.pdf >. October 1, 2013

USA Joint Publication 3-05.30. 2005. Psychological Operations. <http://www.fas.org/irp/doddir/army/fm3-05-30.pdf>. October 2, 2013

USA Joint Publication 3-13.2 2010. Psychological Operations. 07 January 2010. <http://www.fas.org/irp/doddir/dod/jp3-13-2.pdf>. January 18, 2014

Valtioneuvosto. 2013. Suomen kyberturvallisuusstrategia. Valtioneuvoston periaatepäätös 24.1.2013. <http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/49-suomen-kyberturvallisuusstrategia-ja-taustamuistio>. October 5, 2013

3. APPLICATIONS

Pinterest. <https://www.pinterest.com/> March 19, 2014

Wikipedia. <https://www.wikipedia.org> March 19, 2014

APPENDICES

APPENDIX 1

Survey questions

1) Which or what type of target audience analysis method do you use?
   a) Is the same process applicable for all instances or do you use different methods or vary the basic method case-to-case?
   b) If you change or vary the method, is there a pre-analysis made in order to effectively use a proper method?
   c) How is the method conducted in practice?
2) How reliable in your opinion is the method you use?
   a) What are the strengths of the method used?
   b) What liabilities are there in the method?
   c) How do you test the reliability of the method?
3) What are the most essential parts of your method, i.e. if you were forced to make a quick analysis very hastily, which part or parts of the process would you mostly rely on?
4) What characterizes the cyber domain?
   a) What are the main differences in the use of the cyber domain compared to "traditional media"?
   b) What opportunities are granted by its use?
   c) What threats or caveats are there?
   d) What are the main changes taking place in the near future concerning target audiences and their reachability in the cyber domain?
5) How are you going to refine or update your process in the future?
6) Any other ideas or points concerning the subject?

Kysely

1) Mitä tai minkä tyyppistä kohdeyleisöanalyysimenetelmää käytätte?
   a) Voidaanko samaa menetelmää käyttää kaikissa tapauksissa, vai vaihdetaanko tai varioidaanko perusmenetelmää tilannekohtaisesti?
   b) Jos menetelmää varioidaan tai käytetään eri menetelmiä, tehdäänkö ennen analyysia esianalyysi, jonka perusteella menetelmä valitaan?
   c) Miten analyysi tapahtuu käytännössä?
2) Miten luotettava mielestänne käyttämänne menetelmä on?
   a) Mitkä ovat menetelmän vahvuudet?
   b) Mitä haasteita menetelmässä on?
   c) Miten menetelmän luotettavuus testataan?
3) Mitkä ovat menetelmänne tärkeimmät osuudet, ts. jos analyysi jouduttaisiin tekemään erittäin nopeasti, mihin analyysin osuuteen luottaisitte eniten?
4) Miten luonnehditte kybertilaa ts. tietoverkkoja?
   a) Mitkä ovat kybertilan ja "perinteisen median" tärkeimmät erot?
   b) Mitä mahdollisuuksia kybertila tarjoaa?
   c) Mitä uhkia tai sudenkuoppia kybertilassa on?
   d) Mitkä ovat lähitulevaisuuden tärkeimmät kohdeyleisössä ja niiden tavoitettavuudessa tapahtuvat muutokset kybertilassa?
5) Miten aiotte tulevaisuudessa parantaa tai kehittää menetelmäänne tulevaisuudessa?
6) Mitä muita ideoita tai ajatuksia tulee mieleen aiheen tiimoilta?

APPENDIX 2

TAA CHECKLIST

This is a short checklist for conducting a target audience analysis in the cyber domain. Some of the appropriate revisions suggested by thesis are added.

STEP 1 HEADER DATA

Write down header data, including information about the operation, date and makers of the TAA as well as the psychological operation's objective (PO) and it's supportive objectives (SPO). This data should be uniformly formatted, standardized for all operators within the organization.

STEP 2 TARGET AUDIENCE SELECTION

Select target audience. The effective audiences of the cyber domain can be found within the following groups:

- swarms (people connected by a network with a common goal but without knowledge of each other, for example makers of Wikipedia)
- networks (people aware of their membership of a network but not necessarily of each other, for instance members of a discussion group)
- network societies (people held together by a common interest, such as a hobby or an event, for example members of a sports club)
- categories (demographic qualities, such as education, profession, age or gender)
- centers of gravity (those with degree of power over others)
- key communicators (respected or popular persons, well known (and connected) bloggers, threshold personnel of a network etc.)

If necessary, use pre-selection methods such as segmenting people among relevant axes to create homogeneous groups.

STEP 3 ASSESSMENT OF TA'S CONDITIONS

Assess and analyze the conditions that affect the selected target audience. Conditions consist of three elements:

- stimulus – an event, issue or characteristic that affects the TA
- orientation – the TA's attitudes, beliefs and values that affect how TA thinks or feels about the stimulus
- behavior – the observable action or lack of action by the TA

Select relevant conditions by estimating the behavior of the TA. This is done by a six-step process as follows:

- identify the condition (derived from the SPO)
- select the assessment method
- conduct the assessment
- find and categorize the relation between TA and SPO
- number the conditions for further reference in step 4
- identify each condition´s source for later verification of credibility

STEP 4 LISTING TA'S VULNERABILITIES

Combine steps 2 and 3 by listing TA´s vulnerabilities. Vulnerabilities are the TA's needs, wants and desires that arise from the conditions assessed during step 3.

Vulnerability selection is done as follows:

- identify the TA's needs
- categorize and prioritize the needs
- identify needs conflicts
- determine the connection between the need and the SPO
- examine and list each vulnerability

STEP 5 SELECTING LINES OF PERSUASION

Select lines of persuasion. Numerous appeal types are available, and each target audience is more vulnerable to certain arguments than others. Normative appeals, "this is how everyone else behaves or thinks" are both effective and underdetected by the target audience. The use of normative appeals may also affect target audiences not affected by other lines of persuasion and should thus be considered as a part of every persuasion attempt.

STEP 6 SELECTION OF SYMBOLS

Select symbols to be used with the line of persuasion. Symbols must have the following characteristics:

- they must be recognized by the TA
- they must be meaningful to the TA
- they must be appropriate for the selected line of persuasion

In addition, the following should be considered:

- If the TA is expected to respond to the lines of persuasion and the ideals or organizations they present favorably, traditional and well-known symbols should be used
- It the TA is expected to be more hostile, the symbol or symbols used should be varied in appearance to alter the response of the TA as follows:
    - if the intended message should be seen as friendly and familiar, round shapes should be used
    - if the intended message is threatening, sharp angles and straight lines should be used
- In conveying the intended line of persuasion, a visual symbol on its own is more effective than the organizations name with symbol

STEP 7 SUSCEPTIBILITY RANKING

Rank each line of persuasion for its assumed effectiveness. Give a numerical value between 1 and 10, with 1 for those evaluated to be the least effective and 10 for the most effective. The question to answer is: "To which degree the TA can be influenced to respond in a manner that will help accomplish the PSYOP mission?"

STEP 8 ACCESSIBLITY ASSESSMENT

Assess the accessibility of the TA by answering the question:" What type of interaction will effectively carry the developed lines of persuasion and appropriate symbols to the TA in the cyber domain?"

This interaction can take the form of traditional "one-way" presentation of one's own message or that of an active discussion between members. The unique opportunity granted by the cyber domain is that in addition to PSYOP operators contacting TA's, the TA's can also play the active part by contacting the PSYOP operators, helping to lower the initial threshold of suspicion directed towards strangers.

In addition to assessing the active members of the network, it is important to assess whether these members present a representative percentage of the TA. In other words, if a message or interaction is targeted towards a specific TA, it is important to find out whether the whole TA or just those found to be active in the network will eventually be accessed.

STEP 9 EFFECTIVENESS RANKING

Rank the assumed effectiveness of the TA by answering the question: "What is the actual ability of the TA to carry out the desired behavioural or attitudinal change?" Use number from 1 to 10, 10 for the most effective TA.

STEP 10 LISTING IMPACT INDICATORS

List the impact indicators, i.e. the events that should be followed to determine if the intended change is actually taking place. Some indicators are direct, some have to be assessed indirectly. Impact indicators can be both positive and negative.