Rhizomatic Target Audiences of the Cyber Domain

M Sartonen[1], A-M Huhtinen[1], M Lehto[2]

[1]*Finnish National Defence University*
Helsinki, Finland
E-mail: miika.sartonen@gmail.com; aki.huhtinen@mil.fi

[2]*University of Jyväskylä*
Jyväskylä, Finland
E-mail: martti.lehto@jyu.fi

Abstract: *Target Audience Analysis (TAA) is a process of finding suitable target audiences for psychological operations (PSYOPS). Typically, a TAA is a one-way process with some kind of a feedback system. The cyber domain presents a challenge to this type of sequential, linear process by refusing to stay still while the process is being executed, possibly leading to results from yesterday's data in an environment that no longer exists today. Another challenge is that identifiable human beings—the traditional targets of PSYOPS—are not the only inhabitants of the cyber domain. Physical devices, nicknames, IP addresses, networks, and a vast amount of data populate this environment, in which there are no human beings, only their presentations and behavioural residue in a multitude of forms. The authors argue that while the psychological theories behind influence operations still form the basis for PSYOPS as a whole, a re-thinking of methods is necessary for the cyber domain. To conceptualize the cyber domain as a platform for influence operations, the authors suggest a five-layer structure based on Martin C. Libicki's model. In each of these five layers, the target audiences are present in different forms. Thus, all information between humans is filtered through all of the layers with their own rules and causalities. In order to be successful in any influence attempt, one must understand and utilize the characteristics of each layer. The authors also propose that the rhizome theory is the most effective theoretical approach for understanding the complex interactions within the cyber domain.*

Keywords: *Cyber Domain, Psychological Operations, Rhizome, Social Media, Target Audience*

Introduction

Many contemporary crises, from the Ukraine to the Middle East, illustrate the reality that this is an age of information warfare, whether the fact is acknowledged or not. The Internet has connected the world, both for pleasure and pain. Most stay away from the physical battlefields, but no one can avoid entering the area of information warfare every day. According to Munro (2005, 2009), information and communication networks can be used as tools for productive purposes and for innovation. However, such networks can also be used as weapons for destructive and defensive purposes, which have been characterized by the term 'information

warfare'. Information technologies and communications networks are both the weapons and the targets of information warfare operations.

The doctrine of information warfare was first given systematic formulation by researchers at the RAND Corporation and now forms a significant part of the Pentagon's Revolution in Military Affairs (RMA). The researchers have made a distinction between two general forms of information warfare, 'cyber wars' and 'net wars'; the former pertain to high-technology attacks and the latter to broader social uses of information warfare, including conflicts other than war. Under this doctrine, there is a blurring of the traditional boundaries between what is military and non-military. Today, this revolution of military affairs poses a challenge to the traditionally educated security authorities in the world's security organisations, especially when working with social media (King 2011).

Cyber is not a synonym for technology. It is a political notion anchored in the convergence of technologies (such as radios, telephones, computers, satellites, and cable) within the physical world in societies, individuals, companies, nation states, and non-governmental organizations. Due to the growing importance of Information and Communications Technologies (ICTs) in the information age, the cyber domain is simultaneously global and local, 'bad' and 'good', presenting both possibilities and threats (The International Institute for Strategic Studies 2015). The cyber domain is everywhere; and, even though it cannot be seen or touched, it is fundamentally important to everyone. No matter what one's role in society is—citizen, CEO, or military leader—the ability to use the cyber domain provides both incredible opportunities and risks. A better understanding of the rhizomatic cyber domain will give everyone better capabilities to effectively utilize the benefits of the digital age.

The cyber domain and information operations are primarily used as terms in the military and security field, and refer to offensive and defensive activities as well as cyber strategies and policies of the nation states. However, nation states or public security organizations do not own the cyber domain. A variety of defensive cyber operations are conducted as daily business across multiple sectors of societies, such as private-sector finance and telecommunication operators, as well as retail industries. Several organisations in the private sector also perform offensive cyber operations in the form of industrial espionage. The most important activities, however, are those conducted by civil societies in order to join political and public discussion via social media (Lemieux 2015). Currently, information in the cyber domain, in general, does not 'want' to be free but more asymmetrically controlled by rhizome networks (Doctorow 2014).

The existence of the cyber domain, which can be interpreted as a new global digital 'meshwork', challenges both authorities and citizens with several questions. To what extent should technical or regulatory structures be introduced by governments to determine the extent of different actors' abilities to share and control information? How far should information surveillance go in order to protect the public interest? Can grassroots activism movements have an effect on a society if nothing is private? When automated search technologies limit the scope and diversity of information available based on search habits, language, and geographical location, can the results provided by search engines really be trusted (International Federation of Library Associations and Institutions 2015)?

The cyber domain is complex, hard to visualize and—to many people—an esoteric concept that they do not need to comprehend. The best way to approach the cyber domain is to understand that it adds a new dimension to both economic competition and politically driven conflict. The existence of the cyber domain requires a fundamental change in strategic approach and thinking. To the average civilian or military leader, this is a difficult premise to accept because the 'experts' have been advocating that the cyber domain can only be understood by the most technically advanced. The experts are focused on the cyber domain's technical dimension and do not give enough space to the leaders for effective strategic-level decision-making. The rhizomatic cyber domain calls for a more comprehensive knowledge and understanding of all its elements and processes.

This paper joins the discussion on perception management in the cyber domain. First, the concept and importance of Target Audiences (TA) within psychological operations are discussed. Second, a five-layer structure as a framework for better understanding the cyber domain is suggested. Third, the concept of the rhizome as a possible theoretical approach to the complex interactions of the active target audiences in the cyber domain is introduced. Finally, the researchers suggest that, in the cyber domain, the concept of a TA may need to be expanded and perhaps completely rewritten, without preconditions and strict restrictions about the nature and volume of the TA.

Target Audience Analysis

During the early investigation into influence operations in the post World War I era, researchers found that it was not possible to create uniform messages that would affect all recipients in the same way. Rather, message recipients consisted of multiple target audiences, each perceiving the message in their own way based on factors such as demography, selective perception, attitudes, and other social and mental factors. As a result, the intended outcome would seldom be the type of stimuli/response effect suggested by the contemporary behaviouristic approach (Jowett & O'Donnell 2012).

From a military perspective, these influence operations have been typically referred to as psychological operations (PSYOPS). The U.S. Army Field Manual 3-05.301, which offers a detailed procedure for conducting a Target Audience Analysis (TAA), dictates that TAA is a "detailed, systematic examination of PSYOP-relevant information to select target audiences that can accomplish a given supporting psychological operation's objective" (U.S. Joint Publication 2003). Target audiences must essentially have the following characteristics: they must be reachable for them to be influenced; they must be prone to the influence effort by having specific needs to be fulfilled; their change of attitude must lead to a change in behaviour; and finally their change in behaviour must have significance in the larger population (the overall target audience of the PSYOPS) to justify the effort (U.S. Joint Publication 2003). (While there are newer definitions of PSYOPS, the definition given in this field manual is particularly suitable to the present discussion because it includes a detailed TAA procedure.)

The process described in the FM 3-05.301 essentially presents a one-time process, although the effectiveness is measured afterwards, allowing for corrections to the persuasion effort to be made. The question asked is does the TAA in the cyber domain differ from the TAA processes conducted in other media? The answer seems to be 'yes', although the FM 3-05.301 model is

still practical and useful in many cases. The nature of the cyber domain, however, enables the TA to be approached in ways exceeding those of traditional media and, thus, in the authors' view, requires a different approach, harnessing new powers granted by the digital environment.

What are these new powers? The cyber domain is a vast meta-channel that enables the fast, reciprocal exchange of information between new and traditional media types. For instance, a news service may use its agenda setting function to attract its followers to a certain blog by providing a link within an article. Likewise, a popular person's single comment on a blog or a Social Networking Site (SNS) may incite heated discussion among followers, which in turn may be reflected on a news channel. The digital domain is not only vast; it is also fast. Breaking news may take only minutes to spread across the globe, and to change opinions and attitudes of the target audience. A well-placed piece of information may transform an indifferent audience into a favourable or hostile one within hours, if not minutes.

Other important characteristics of the cyber domain are its reciprocity and equality; a transformation of audiences from passive information consumers/receivers into active information producers is now apparent. The active nature of the audience makes it not only the target of influence (influencee) but also an influencer. This characteristic capability of creating new phenomena, trends, and opinions is not available *en masse* in traditional media. As anyone can post a comment or create a site for presenting his or her ideas, the gatekeeper function of the media may at first seem to have diminished or to be totally absent. What is often forgotten, however, is that the various search engines that help find relevant information among millions of web pages have algorithms that may not always have the best interests of the researcher in mind. Unlike the traditional gatekeepers, such as magazine editors, these gatekeepers stay out of sight and, thus, their existence is often forgotten (Pariser 2011).

These changes in the digital environment play to the hands of the digitally agile—organisations with means to observe and react to sudden changes in the information and emotional atmosphere of the cyber domain. To achieve the necessary situational awareness, the arduous work of reading and collecting newspaper and journal articles, listening to radio, watching TV, and meeting people in order to keep up with the contemporary themes and opinions is increasingly being replaced by software scanning the Internet. This type of software, already commercially available to fit different needs, filters through the digital domain collecting data, opinions, and social connections, and even making its own deductions based on the findings. This approach offers a level of real-time situational awareness previously unavailable.

Because of the reasons mentioned above, traditional means of conducting PSYOPS may not be applicable in the cyber domain. The entirety of the millions of communications taking place every second does not wait for the operators of the TAA to complete their process, observe the effects, and adjust their measures. The TA is a constantly moving, living entity that changes out of immediate view. One possible way forward with PSYOPS is to begin with a new approach. Instead of utilising models more adept with traditional information distribution channels with their more defined sender/gatekeeper/receiver structure, focusing on how the cyber domain processes information is a better way to proceed.

Five-layer cyber domain

Although often used as a synonym for the Internet, the cyber domain is much more. It includes not only hardware, software, data, and information systems, but also social interaction within these networks and the whole infrastructure. The International Telecommunication Union (ITU) uses the term 'cyber domain' to describe the "systems and services connected either directly or indirectly to the [I]nternet, telecommunications and computer networks" (2011). The International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) defines cyber as "the complex environment resulting from the interaction of people, software and services on the [I]nternet by means of technology devices and networks connected to it, which does not exist in any physical form" (2012).

TA models have their origins in the physical world, dealing with groups of real people with different characteristics, such as demography, profession, political views, and socioeconomic status. Within the cyber domain, the different actors' importance must be re-evaluated and reassessed, and the nature of the actors themselves must be rethought. In the world of virtual entities, it is not always the physical members of society that best convey the influence messages. The authors suggest using a new structure to assess the different interaction levels and mechanisms of the cyber domain. This structure applies Libicki's (2007) structure for the cyber domain and includes five layers: physical, syntactic, semantic, service, and cognitive (see **Figure 1**, below).

The **physical** layer contains the physical elements of the communications network. The **syntactic** layer consists of various system control and management software and features that facilitate interaction between the devices connected to the network. The **semantic** layer is the heart of the entire network. It contains the information and datasets in the user's computer terminals, as well as different user-administered functions. The **service** layer contains all of those public and commercial services available in the network. The **cognitive** layer is the user's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created. The cognitive layer can be seen from a larger perspective as the mental layer, including the user's cognitive as well as emotional awareness. Concepts related to emotions, such as trust, acceptance, and experience, are central to emotional awareness (Libicki 2007).

In the physical layer, the target audience is presented as physical networks and devices, where intelligence grows continuously. Numerous applications use different location services not only to provide useful information to users, but also to transform portable devices into tracking devices, enabling constant surveillance. This data tells where the device owner lives, where he or she works, as well as other valuable information, such as indications of hobbies and other lifestyle choices. For instance, the popular fitness applications that give out information about the user's physical condition may be helpful in deciding what type of targeted commercials should be used. Once this information is integrated with the other layers of the cyber domain, the device owner will eventually be given a name and much more information will be added.

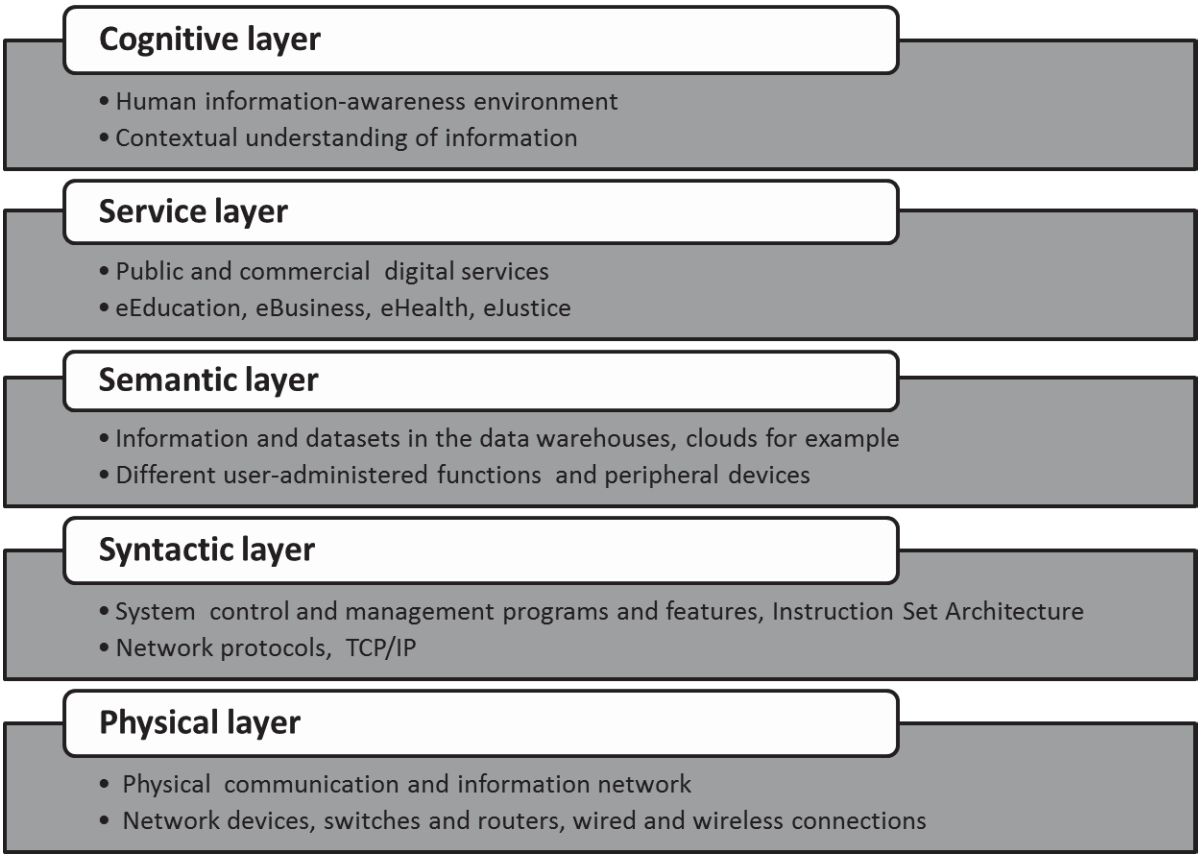

Figure 1: The five layers of the cyber domain

The syntactic layer includes the software that provides the operating commands for the physical devices. In this layer, the TA is presented as Internet Protocol (IP) or e-mail addresses and as user IDs—in other words, as multiple virtual identities that connect people to a certain physical device or service. Today there is a range of software available that allows any user to track and visualize the topology of syntactic layer networks. Someone interested in global distribution of messages can use these tools to find suitable networks and the connections between them.

By following the communications between these virtual identities and networks, it is possible to identify key communicators by their relative position in the global network. A bilingual user, for instance, communicating messages between two different language areas may be essentially important by linking these networks together, even if he or she might not produce any significant content of his or her own in the semantic layer.

The semantic layer involves human interaction with the information generated by computers and the way that information is perceived and interpreted by its user. In this layer, the TA presents itself as data and information, including image, text, and audio files. In a digital society, the smart devices of the physical layer in connection to the diverse information production of the semantic layer allow the TA to be both the user and producer of digital content.

The information stored in the semantic layer has the opportunity to give faces and names to virtual identities, linking these layers together. Other means, such as image recognition software, can be used as additional ways of creating links between people or for finding useful information for marketing or even criminal purposes. People may not be aware of all of the risks connected to storing sensitive information in virtual hard drives. Despite their best efforts, respectable enterprises can be subject to cyber-attacks and can have user information stolen.

In the service layer, the TA is presented as different networks of various social media, such as Facebook, Twitter, or other social networks; distribution lists; subscribers; and so on. Virtual identities enable users to create different networks in which they participate by the identities they have chosen. In different services, the TA can present itself as remarkably variable entities, with different values and motivations driving behaviour. One physical being can act as an authority in one network, while simultaneously being a neglected outsider in another. The importance given to the social media is what makes this layer important. A new piece of information is valued, in part, by its source. Although the information itself is stored in the semantic layer, it is typically ranked in importance by the reliability ranking given by social networks provided by the service layer.

In the cognitive layer, the TA consists of human beings who can be affected by cognitive and psychological means. This layer is the ultimate target of influence operations on the Internet. In the cognitive level, humans exercise processes of knowledge and understanding linked to emotionality and rationality, as well as the ability to make observations and decisions. In the cognitive level, information that has been received is processed. From the viewpoint of PSYOPS, the essential themes concerning the TA are the cognitive processes related to creative thinking, perception, learning, and problem solving. To affect a TA, understanding both individual and group behaviour is imperative because, in the cognitive layer, users, who are rational and emotional beings, define their behaviour and actions based on the information stream that passes through the entire structure of the cyber domain.

From the TA perspective, the cyber domain layers form an entity with each layer having its characteristic rules and causalities. As shown in **Table 1**, below, in each layer the target audience's identifiable identity and its manifestation are different, requiring different approaches and tools.

Cyber domain layers	Manifestation	Identity of the target audience
Cognitive layer	Human being	Rational, emotional identity
Service layer	Network member	Network identity
Semantic layer	Information	Information identity
Syntactic layer	IP-, email-address	Virtual identity
Physical layer	Device	Physical identity

Table 1: The manifestation of the cyber domain layers and identity of the target audience

Starting from the physical layer, within each layer the level of abstraction increases and phenomena get more complicated. In the physical layer, the number of devices is limited, although the Internet of Things is forming into a system of billions of units. Nevertheless, the number of devices an individual person can have is limited. Similarly, in the syntactic layer, the TA will typically have only a limited number of virtual address identities.

The level of complexity rises significantly in the semantic layer, in which the quantity of information is growing rapidly. At the Techonomy Conference in Lake Tahoe on 8 April 2010, Google CEO Eric Schmidt commented that there have been '"5 exabytes of information created between the dawn of civilization through 2003 … but that much information is now created every 2 days, and the pace is increasing. People aren't ready for the technology revolution that's going to happen to them"' (Kirkpatrick 2010).

About 2.5 quintillion (2.5×10^18) bytes of information are created every day, of which, for instance, the New York stock exchange by itself accounts for 1TB. On Facebook, there are 40 billion images (4PB). The flow of data makes the task of finding the essential information ever more challenging. To control this vast amount of data, different types of Big Data analysis tools and algorithms are being developed and are rising to the challenge of controlling the information about target audiences.

In the service layer, both the level of networking and the number of users are also strongly on the rise. In 1996, 0.9 percent of the world's population was using the Internet. Today there are about 3.675 billion users (50.1 percent of population) (Internet World Stats 2016). Every day, more than 200 billion e-mails are sent; and every second, on average, around 6,000 tweets are tweeted on Twitter, which corresponds to more than 350,000 tweets sent per minute, 500 million tweets per day, and around 200 billion tweets per year. Google now processes an average of more than 40,000 search queries every second, which translates to more than 3.5 billion searches per day and 1.2 trillion searches per year worldwide. During its first ten years of operation, Facebook accumulated more than 1.5 billion registered users and more than 1.2 billion monthly active users. There are more than 4.6 billion mobile phone users in the world (Statista 2016).

The digital services of the service layer are implemented in Internet servers. More advanced user applications are available via 'app stores' for those cases in which the local performance of the terminal itself is still practical and thus has value. More and more intelligent algorithms are under development to make services more intuitive. What drives this change is that, in order to be successful as a digital society, states need to create a strong ecosystem of digital services that propagate skillfulness, that ease the acquisition of investments, that develop the infrastructure, and that attract business (Information and Communications Technology 2015).

In accordance with Moore's Law, Diamandis predicts that, in 2025, there will be an acceleration in the rate of change as a world of true abundance nears. In 2025, $1,000 should buy a computer capable of calculating at 10^{16} cycles per second (10,000 trillion cycles per second), the equivalent processing speed of the human brain. The Internet of Everything describes the networked connections between devices, people, processes, and data. By 2025, the IoE will exceed 100 billion connected devices, each with a dozen or more sensors collecting data. This will lead to a trillion-sensor economy driving a data revolution beyond the imagination. With a trillion sensors

gathering data everywhere (autonomous cars, satellite systems, drones, wearables, cameras), someone will be able to know anything he or she wants to know, anytime, anywhere, and he or she will be able to query that data for answers and insights. Many ICT companies are planning to provide global connectivity to every human at speeds exceeding one megabit per second. Billions of dollars of investment will lead to a new generation of displays and user interfaces. Artificial intelligence research will make strides in the next decade. In a decade, it will be normal for someone to give his or her AI access to listen to all of his or her conversations, read his or her emails, and scan his or her biometric data because the advantage and convenience will be so immense (Diamandis 2015).

From the perspective of influencing the TA, the cognitive layer constitutes an entity that differs from the others. The rules of this layer, namely the psychology of human beings, do not change as quickly as they do in the other four layers. What changes, however, is the 'interface' between a human being and the digital environment, forcing a constant adaptation from the human. Today, a soldier who enters a physical battlefield carries a personal terminal which allows him or her to connect to the cyber domain. In many ways, the most important changes today take place in the perception of reality, in how soldiers translate the battlefield.

This five-layered structure forms the PSYOPS area of operations in the cyber domain. When a cognitive being exchanges ideas with another in this environment, the messages are filtered through all of the layers. The powers of sharing, accumulating, and controlling information lie within this mechanism, although very often its existence is not obvious.

Rhizomatic Nature of the Internet

To address theoretically the multitude of interactions taking place simultaneously within the cyber domain, the authors suggest an approach which computer culture theorists have identified as a rhizomatic social condition. The information system network serves as a description of a technical system, but rhizome meshwork describes the wider social, cultural, and political milieu of the richly connected, heterogeneous, and somewhat anarchic cyber domain. The information system network, reduced only to the technical issues, is based on the idea that some kind of hidden authority still lingers, controlling and stabilizing the flow of data as if it were a subway system. The problems with this system-technological thinking are that within this concept everything derives from the main trunk, and there is a hierarchy of dependence. Contrary to this orderly view, the concept of the rhizome presents an attempt to undermine this authority over the network (Coyne 2014). A rhizome has no beginning or end; it is always in the middle. Where one is going, coming from, or heading to are totally useless considerations in the surface of a rhizome (Deleuze & Guattari 1988, p. 25).

The designers of system thinking seem to have great difficulties in disengaging from the metaphor of the tree-structure. The Western tradition of reality is based on the idea of the permanent, unchangeable, and true nature of reality (being). In the empirically-based science disciplines, there exists an attempt to find the first and ultimate point, or to concentrate on the beginning or the end of something, instead of the middle or cross lines of living and chancing situations (becoming) (Chia 1999, p. 214). However, a rhizome 'is' not a system but a becoming meshwork with endless bulbs and tubes. The postmodern reality is not hierarchical and orderly anymore: it counters the spirit of the dialectic. The universe is not necessarily made up of a series

of stages toward technological enlightenment. For the Platonist, everything is just a copy or representation of the original ideal, but there is not an original ideal, because it cannot be proven. It can only be believed as the system of God. The tree of science gives expression to a regime of tracings and puts them in a hierarchical order, but this is only an expression or representation of a possible reality (Coyne 2014). Using these new information technology solutions creates an information bubble. In a way, there is a movement away from the tree of knowledge and toward information meshworks or rhizome networks.

One metaphor to explain the functioning of the cyber domain is the human brain. The nerve cells themselves have a slow lifecycle, but the functionality of the brain and its abilities to quickly process information and to respond to new situations more or less accordingly lie within the connections of nerve cells and the constantly firing messages between them. The brain reacts quickly, not by growing new nerve cells but by changing the messages and connections between the cells. Any new event in the global meshwork creates similar re-structuring. New connections are made, and new messages are sent, re-structuring the global meshwork on a constant basis. One cannot expect to be able to control either the flow of information or the perception of it.

Where is the usefulness of the rhizome in this context? According to Coyne (2014), the circular motion of the rhizomatic interactions can be described benignly, in network terms, as a feedback loop. The rhizomatic process involves backwards and forwards movement, a constant process of revision, and a cycle of understanding that converges on a practical understanding for the moment. The argument this article offers is that, by utilising the concept of the rhizome, it might be more useful to concentrate on the behaviour of the waves, not of the water molecules. In other words, instead of choosing a TA and trying to make it behave in a particular way, it may be more effective to focus solely on the outcome and let Tas change their shape, volume and composition. This means reading the mind of the Internet as a whole and using any means of influence where it will be most effective.

If one thinks of the cyber domain as a rhizomatic entity, the question is: How does one read the ‘mind’ or ‘mind-states’? The way forward lies within the increasing number of social media and other services’ listening tools that scan through the Big Data of the Internet. Only by using this type of sophisticated software will it be possible to have any awareness of the contemporary ‘thoughts’ of the vast global meshwork. Already, some type of profiling exists in all five layers of the cyber domain. The devices of the physical layer, syntactic layer software, and the multitude of services all gather data for different uses. This data, combined with the different tools that analyse a user’s personality and objects of interest based on the user’s behaviour in the Internet, allow the user to be targeted by marketing solutions with previously unprecedented precision. The same type of software can be used for other types of influence efforts as well.

Once the variable mind-states and thoughts of TAs are found, the more traditional psychological and sociological theories of influence can be used. The effectiveness evaluation of these techniques is then made in a real-time fashion by observing the changes in the global or local opinion climate. Any perceived change in the influence attempts can then be reinforced or countered and, once again, the effects can be observed, resulting in a fast-paced feedback mechanism that acknowledges the nature of the cyber domain. Even if some militaries are not willing to execute such operations, at least they can understand the national threats presented by

fast-growing technologies and can prepare adequate defences against them. As with any new weapons, the weapons of information warfare are becoming more common and are increasingly used by non-governmental and criminal organisations as well. With these new weapons, it may be easier than previously thought to turn a nation against itself.

Conclusion

In the cyber domain, human beings and an increasing number of intelligent devices have created a rhizomatic, complex interacting abstract machine, maintaining a continuous feedback loop that constantly creates new ideas. Once a new idea is created, either by a single individual or by the workings of the Internet as a neural network, by a true incident, or by a fabricated event, it collides with other ideas, creating unpredictable results. From the viewpoint of PSYOPS, the cyber domain is an environment in which target audiences can be reached globally and in vast numbers. It poses dire threats but also provides golden opportunities. These opportunities can be utilised by the digitally agile, those with sophisticated algorithms and an understanding of the nature of the digital environment.

In order to understand the cyber domain from the perspective of influence operations, this article suggests using a structure of physical, syntactic, semantic, service, and cognitive layers. Each of the five layers has its own characteristics and provides its own uses and risks. The point of this framework is that human interaction in digital environments passes through all of these layers and, in each one of them, is subject to data mining, analysis, and more or less subtle influence attempts. In order to comprehend the complexity of communications in this environment, it is vital to understand the mechanisms at work within and between each layer.
In conclusion, the researchers make three points in this article:

- TAA is still an essential part of any influence operation, but it needs to be seen in a new way, more in line with the modern information environment.
- In order to be able to conduct successful operations in the cyber domain, a useful framework of how this environment is viewed is needed. For this purpose, a five-layer structure is needed.
- It will not be possible to control the rhizomatic information flow of the cyber domain, and thus a new way of seeing PSYOPS in the digital environment is needed. The use of the rhizome theory is suggested as a theoretical approach so that the global meshwork can be seen as an entity with constantly altering connections and mind- states.

Discussion

This paper is an effort to approach the PSYOPS-related concept of a target audience from the theoretical framework of the rhizome. Further research will need to investigate more closely the nature and complex causalities of the interactions taking place in the rhizomatic cyber domain, and how existence in the cyber domain shapes perception and behaviour. Researchers will also need to seek ways to read the mind-states of the rhizomatic cyber domain by using different algorithms. It is assumed that approaching this task layer-by-layer will make it more

manageable. In addition, different theories, methods, and algorithms will probably be needed for each layer.

Are there limitations to the type of TA analysis suggested? In theory, the Internet is an unlimited network between equal partners; but, in practice, a few important limitations should be considered. First, it is important to acknowledge that not everyone in the world has equal access to the network. Especially when accessing TAs in areas with limited Internet access, the findings may be strongly biased and thus may not present the overall attitudes of the population. This limited access may be a result of limited technological infrastructure and/or some form of censorship applied by governments.

The multitude of languages (and cultural contexts) used on the Internet is another limitation. The increasing number of sophisticated translation software, however, is rising to the challenge of crossing the language barrier. Search programs' selection of SNS programs is yet another limitation. Many publicly available algorithms are limited to the most common SNS programs, such as Facebook, Twitter, and Instagram. Those not involved in these popular networks fall outside the coverage of many analysis tools. Thus, also in the cyber domain, it is important to acknowledge what one does not know, or in this context, what one cannot reach.

References

Chia, R 1999, 'A "rhizomic" model of organizational change and transformation: perspective from a metaphysics of change', *British Journal of Management* vol. 10, pp. 209-27.

Coyne, R 2014, *The net effect: design, the rhizome, and complex philosophy*, CUPUM-ECiD Joint Workshop, viewed 17 December 2015, <http://www.casa.ucl.ac.uk/cupumecid_site/download/Coyne.pdf>.

Deleuze, G & Guattari, F 1988, *A thousand plateaus: capitalism and schizophrenia*, Athlon Press, London, UK.

Diamandis, P 2015, 'The world in 2025: 8 predictions for the next 10 years', viewed 5 January 2016, <http://www.diamandis.com/blog/predicting-the-next-10-years>.

Doctorow, C 2014, *Information doesn't want to be free: laws for the Internet age*, McSweeney's, San Francisco, CA, U.S.A.

Information and Communications Technology (ICT) 2015, Working group report, '21 polkua Kitkattomaan Suomeen [21 paths to frictionless Finland]', Ministry of Employment and Economy, 17 January, Helsinki, Finland.

International Federation of Library Associations and Institutions (IFLA) 2015, *Riding the waves or caught in the tide? insights from the IFLA trend report*, viewed 17 December 2015, <http://trends.ifla.org/files/trends/assets/insights-from-the-ifla-trend-report_v3.pdf >.

International Institute for Strategic Studies (IISS) 2015, *Evolution of the cyber domain: the implications for national and global security*, Routledge, Abingdon, UK.

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 2012, *International Standard ISO/IEC 27032: information technology—security techniques—guidelines for cybersecurity*, ISO/IEC, Geneva, Switzerland.

International Telecommunication Union (ITU) 2011, *ITU National Cybersecurity Strategy Guide*, Geneva, Switzerland.

Internet Live Stats 2016, InternetLiveStats, viewed 8 December 2016, <http://www.internetlivestats.com/>.

Jowett, GS and O'Donnell, V 2012, *Propaganda & persuasion*, Sage Publications, Thousand Oaks, CA, U.S.A.

King, A 2011, *The transformation of Europe's armed forces*, Cambridge University Press, Cambridge, UK.

Kirkpatrick, M 2010, 'Google, privacy and the new explosion of data', Techonomy blog, 4 August, viewed 7 December 2016, <http://techonomy.typepad.com/blog/2010/08/google- privacy-and-the-new-explosion-of-data.html>.

Lemieux, F 2015, 'Trends in cyber operations: an introduction', *Current and emerging trends in cyber operations: policy, strategy and practice*, ed. F Lemieux, Palgrave Macmillan's Studies in Cybercrime and Cybersecurity, New York, NY, U.S.A. pp. 1-16.

Libicki, MC 2007, *Conquest in cyberspace: national security and information warfare*, Cambridge University Press, New York, NY, U.S.A.

Munro, I 2005, *Information warfare in business: strategies of control and resistance in the network society*, Routledge, London, UK.

——2009, 'Defending the network organization: an analysis of information warfare with reference to Heidegger', *Organization*, vol. 17, no. 2, pp. 199-222.

Pariser, E 2011, *The filter bubble: what the Internet is hiding from you*, Penguin Books, London, UK.

Statista 2016, Statista.com, viewed 8 December 2016, <https://www.statista.com>.

U.S. Joint Publication 3-05-301 2003, *Psychological operations tactics, techniques and procedures*, viewed 17 October 2013, <https://www.fas.org/irp/doddir/army/fm3-05-301.pdf>.