Challenging NATO's Security Operations in Electronic Warfare: the Policy of Cyber-Defence: the Case of Greece.

Dr. Marios Panagiotis Efthymiopoulos

Biography: PhD University of Crete, Faculty of Social and Political Sciences, Department of Political Sciences, former academic envoy of the Greek Foreign Ministry at the NATO Defense College, Rome Italy, author of the book: NATO in the 21st century: NATOs need for a new security concept and the ever enlarging NATO-Russia relations.

marios.efthymiopoulos@strategyinternational.org

Abstract: NATO is evolving. It is changing. It is estimated that in the 2010 summit meeting in Portugal, Allied member-states will hold, as requested at the Kiehl-Strasbourg summit of 2009, a first evaluation on the need for renewed Strategic Concept. In terms of 21st century asymmetrical warfare, as part of the current security dogma, NATO requires to be technologically updated. This entails NATO to continue its effort to change. The results that shall occur in this subject shall be portrayed to the effort made on the renewed security concept. NATO is steadily unfolding its policy of Cyber-Defence. NATO needs to be operationally ready to counter all attacks of assymetrical warfare, whether from the inside or the outside of its operational sphere of influence. The aim of this paper to provide the reader with the necessary information to firstly learn what has been done up to this date, in relations to NATO's operational preparations and in relations to its Cyber-Defence policy. In a second part, this paper examines and evaluates current policy decisions, as to understand whether a) NATO will actually take a major step into becoming involved into a new form of self-defensive or offensive assymetrical warfare b) whether a political-military organisation of international members, such as NATO can actually afford working together. C) Whether the unfolding of Cyber-Defence policy will be implemented in NATO's operational environments, as to counter new phenomena of terrorism via the web. An explanation on network preparations and operations shall be made. At the same time an explanation shall be provided, why should the internet be so important to NATO's network centric operations and why does NATO need a Cyber-Defence policy. In practical terms, the case study of Greece is examined. What is Greece's policy objectives vis a vis NATO policy of Cyber-Defense? What has been done by Greece in creating the necessary steps to both take an initiative at NATO and at the same time initiate a national policy of implementation of the possible outcomes decided by NATO Heads of States? This paper is part of the author's wider topics of research made on NATO and its policies in the 21st century.

Keywords: *NATO Cyber Defence Concept, NATO Cyber-Defence Centre of Excellence, North Atlantic Council, Transformation, Greece's policy on Cyber-defence.*

1. Introduction

It is said, that future war-like operations will be held in a far more complicated than the current one, military operational environments, where battles will be dealt at multiple levels and multiple dimensions. Missions, according to NATO, in all fields "will continue to require agile and interoperable, well-trained and well-led military forces"[i]; assuming that these military forces shall be in greater need than today, if NATO decides to take part (as ordered by a viable and robust renewed Security Concept, -that is currently considered) at "offensive – first to be engaged- operations of all kinds, if need be, but also in defensive-clause operations".

In the following paper we argue that NATO's new electronic security operational preparation that is unfolding should be challenged, as there is an increasing need to adopt new methods and actions, as to counter both, current and new, symmetrical and asymmetrical threats. Accordingly the result of possible new methods and actions to counter the ever emerging

challenges should be applied at a renewed Security Concept, to come. A proposal for a renewed and viable concept of security for NATO is expected to be proposed at the Portugal Summit of 2010. The outcome is a decision made by Heads of States at the Stratsbourg-Kiehl Summit in April 2009.

This paper shall examine the evolving challenges of the North-Atlantic Organisations' security operations and preparations at the fields of Electronic Warfare and in specific Cyber-Defence.

The aforementioned subject will be portrayed and examined. It is the purpose of the paper to draw the reader's attention, to portray and understand how the future of, what and how, when and in what other dimension, shall military operations be, according to NATO decisions, as accepted by the North Altlantic Council (NAC). This paper argees that the argument that -most future, defensive or offensive battles shall also occur in an asymmetric level-, as was the case with the cyber-attacks in Estonia in 2007. Therefore a policy of Cyber-Defence but also a general preparation for electronic warfare, which includes network-centric operational interoperability of forces preparation, is in need at NATO to exist and to evolve for the sake of the Allied 'e-networked' states, against all traditional but also non-traditional forms of attacks.

The outcome of this paper's analysis shall be a variety of proposals, which will be put forward for consideration. At the same time these proposals shall be combined with any efforts made by the Greek Government to apply this new policy both at a national or supranational level. What are if any, the proposals that are in preparation by the Greek State to NATO's objectives on a renewed security concept and in specific NATO's policy of Cyber-Defence?

What should be noted is that the opinions mentioned in the current paper reflect solely the opinions of the author. They do not reflect any countries' or the North Atlantic Organisations' policies or actions. Current arguments are solely based on personal academic research, judgments and working experience from NATO.

A variety of issues in this case study needs to be addressed. The issues for consideration reflect the operational and tactical levels of what NATO needs to be. The Alliance is currently renewing and evaluating its transformation process that was initiated after the Prague Summit in November 2002[ii].

2. Establishing NATO's new symmetrical and asymmetrical security environment.

Latest research has shown that NATO's policies and its security environment has been assessed[iii]. At the same research, it is mentioned that -in a post-2001 terrorist attacks in the USA- era, the Alliance has 1) invoked article 5[iv], claiming its right to defense against external aggression 2) Allied states agreed on an ever lasting transformation, politically, militarily, operationally and strategically in Prague 2002, 3) agreed to be involved in outer-areas of its traditional (26 member states) area i.e. Kosovo 1999[v], Afghanistan 2001[vi] onwards via operation International Assistance Force (ISAF)[vii], 4) now challenged its current operational planning and decision procedure and agreed to examine and be engaged at new forms of

military preparation, for preventive or offensive purposes i.e. Decisions of the Allied Defence Ministers October 2007[viii].

Considering aforementioned political decisions, one important issue is that has been agreed by all member-states is that NATO is a necessity[ix]. NATO is in fact, "required, requested, but now also retained". By introducing the 3 (R)s in this paper, we establish what the Heads of States decided over and over again, from the Treaty of London during the beginning of the 1990s Summit, to its 1994 Summit in Brussels, to its 1999 over its 50th year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA[x] and finally to its 60th anniversary, which was held in Strasbourg and Kiehl (in specific Baden-Baden) accordingly in April 2009: NATO was created for a long-term and thus it is here to remain. NATO today is evovling. NATO's administrative, operational and tactical current form is considered as "the purest form of a true military-political alliance that brings and binds together countries that hold the same supranational interests, in terms of security, in all fields related, such as military, political, financial, sociological and environmental security"[xi].

Politically, militarily, administratively, by consensus decision-making process of the Allied states, it was considered in 2002, due to the constantly challenging security environment that NATO is required to change. Its current 2001 Strategic Dogma is under evaluation and consideration as it is now widely challenged by member-states. Some say, it is no longer viable. Others consider NATO's 2001 Security Concept would be the basis for collective member-states negotiations, as an opportunity for restructuring a renewed Strategic Concept; One that will portray all needs but also challenges; A Concept that will clarify policies, operational needs and doings, both at tactical and operational levels; a concept that will provide with the necessary financial but also legal clauses, which are now needed. The outcome for a renewed Concept of Security was portrayed at NATO Heads of State Summit in Strasbourg-Kiehl in April 3rd and 4th 2009[xii].

NATO is in need for a renewed Security Concept. The Alliance should be able to deliver better and robust outcomes in the 21st century security challenges. 10 years within the 21st century, it is the result of the authors recent research outcome[xiii] that NATO should continue to transform in order to operate within the limits of its political decisions (that should be widened), according to its own 'rules of engagement' (NATO's military doctrine). Therefore a renewed legal and political plan of operation and co-operation, for which NATO was in fact challenged and criticized, meaning over its ability to prepare and deliver actual military results, is in need. These aforementioned issues were also the reasons why the NATO Prague Summit of November 2002 came about. It resulted to the policy of transformation. Two major operational camps were created: 1) the Allied Command Transformation (ACT –USA-) and 2) the Allied Command Operations (ACO –Belgium-). In the following Summits, NATO's Istanbul (2004), Riga (2006) and Bucharest Summits (2008), accordingly, delivered concrete and practical results after thorough evaluation of the current and ongoing changes within the Structure the administration, the military and political preparation. NATO's leaders believe that the Alliance has today the ability to operate in a largely different security environment that is no longer limited only to symmetrical threats or geographical areas but also to an environment of asymmetrical threats as well as unstable areas of interest. The Alliance's readiness for prevetion against any or all assymmetrical attacks includes: Radiological, Biological, Chemical attacks, all forms of terrorists attacks. NATO has also the capability and capacity to counter-fight any opponents by military men-led operations supported by components of land and sea power in an out of controlled area operation via its NRF (NATO

Reaction Forces) force, i.e. Afghanistan. It is also capable of support led, peace-keeping, or peace-making operations i.e. Darfur or Somalia.

3. The trend for an e-security world.

Within the framework for a renewed security dogma, to be proposed[xiv], NATO leaders have to acknowledge the need to establish a policy that is linked to the general technological trends. This opinion, motive-wise, was certainly sustained post-2007 case of cyber-attacks in Estonia. The outcome was the creation of a cyber-defence centre according to the decision made by the Allied Command Transformation, in Norfolk Virginia USA.

It is believed that the 21st century shall be the century where all things will be dealt by constant creations and use of advanced technology. Of course technology has long-lasting history that dates back to the use by the Phoenicians, the Ancient Greeks and the Chinese. At the 21st century however, technology is referred to as the use of computers and their means such as the (World Wide Web). Unfortunately, our so-called wired-society that includes online services such as: banking, communications, shopping, media-services etc, take place in cyberspace and therefore are eligible to cyber-attacks. The fact that countries do steadily move forward in becoming dependent on computers and networked e-world, network security is becoming increasingly needed. E-world assurance of information is therefore needed, as to increase the security level of countries, meaning peapole, institutions and businesses.

Current security risk assessments consider that for the development of an e-secure world, organized crimes, made via the use of the web, should be countered. 'Cyber-crimes', are nowadays done by organized small groups. 'Hackers', are considered eligible to criminal justice judgements, by accessing to personal, classified or other unauthorized information by informal and unaccepted ways. The use of personal, unauthorized, or private information to get access to other resources such as funds is a crime, as is a crime the use of the web to terrorize citizens, states, institutions or organizations.

In terms of applying these issues in military policy, for which this paper is concerned with, the web and its service operations, are now widely used by national or multinational armies, by organizations such as NATO. Their technology invented is thus used as to become engaged at e-level networked centric operational preparation for assymetrical warfare and counter-warfare operations, where decided. As aforementioned above, cyber-space shall be used as a form of battleground and counter-battles in future conflicts. At the same time the thought only of hackers: 1) having access to sensitive information on military weaponry and possible use against any possible public, government or multinational organization, 2) using the web for cyber-attacks, makes the creation of a Cyber-Defence policy necessary.

Below, we will explain NATO's newest policy issue, a decision-made by the Heads of States and Governments as published at the Bucharest Summit of 2008 and the request of the ACT, which, since the Prague Summit in November 2002, deals with the ever ongoing NATO transformation, to seek solutions for the constant and emerging challenges against cyber-attacks.

4. NATO's Concept of Cyber-Defence:

NATO's Military Committee has recently decided on what has come to be called as a "Cyber-Defence Concept". The Committee's aim is to deliver practical results that will point out: 1) the necessity of NATO as a collective organization in a globalised and currently unsafe e-world 2) the Alliance' ability to deliver new policy results, taking into perspective new forms of asymmetrical threats such as cyber-attacks.

Historically, the 2002 Prague Summit first marked NATO's tasking authority committee with regards to all activities that should be held in relations to Cyber-Defence. As technical achievements were delivered, so did policy-makers, deliver policy results on Cyber-defence. That is why, Allied leaders during the Riga Summit of 2006 acknowledged the need to include as is stated on its decisions at the Press Communique: 1) protect NATO's operational information systems 2) protect its allied countries from any e-, or in other words cyber-attacks by new forms and means developed by NATO's Allied Command Transformation (ACT).

In turn, the October 2007 outcomes of NATO, at the level of Allied Defence Ministers[xv], gave way to the inauguration of NATO's centre of excellence (COE) [xvi] by the Allied Command Transformation[xvii] on Cyber-Defence, in Estonia –Tallinn[xviii]-. It is based, on the aforementioned Concept on Cyber-Defence, as agreed by NATO's Military Committee.

The central and final decision-making role over the policy of Cyber-Defence however is the North Atlantic Council (NAC), which is the highest deciding political authority, as we foretold. It considers NATO's policies and activities in regards to the subject politically and militarily. Below the NAC, is NATO's Consultation Control and Command Agency (NC3A)[xix] and the NATO Military Authorities (NMA). This latest authority, takes part mostly on the implementation as its task[xx].

The implementation of NATO's Cyber-Defence policy is considered as the second most important decision of countering criminals and terrorists, as the decisions are taken by the NAC. The "Concept of Cyber-Defence" "adds practical action programmes to fit within the overarching policy"[xxi]. The 'Cyber-Defence Management Authority' that is tasked upon its policy concept "brings together the key actors in NATO's Cyber-Defence activities". Its aim is to manage and support all NATO communication and information networked systems and individually allies upon request[xxii].

NATO's policy activity is encouraged by the Alliance, to the engagement of as many as possible, if not all governments, member-states of the Alliance, but also industries relating with these subject matters. In accordance to its best practice policy, NATO considers that its 'operational forum' can and should be considered as the best joint operational co-operation between states, as to also avoid duplication of efforts.

Practically or otherwise said in military policy implementation, operationally, as is mentioned by NATO, there are "three phases of practical activity" as how this policy came about: In its initial phase a "NATO Computer Incident Response Capability (NCIRC)" was established as well as its "interim operating capability". Its second phase involved an ever more realistic-pragmatistic perspective, that required the co-ordination of all initial 'offering' states (under the NATO agreement between states of a voluntary national contribution -VNC-), in bringing the NCIRC to a full operational capability[xxiii].

New policies came about after being proposed and then coming to effect (well-known procedure of internal NATO working process). A so-called 'Memorandum of Understanding' is drafted and proposed to NATO by the sponsoring state, in this case Estonia, prior to any of the above-mentioned phases of practical activity. From that point on it is the administrative decision of the Alliance, that once the aforementioned stages are put into effect, then a third phase comes into turn. Needless to say, this third phase may also be the most important. "It consists of incorporating -lessons learned- from the prior two phases as using new and latest Cyber-Defence measures (use of new technology and getting more knowledge on the security environment), in order to "enhance Cyber-Defence posture"[xxiv]. Once the third phase has been evaluated, then the Allied Command Transformation (ACT) decides whether to declare the operational centre –in this case the Cooperative Cyber Defence (CCD) COE (Estonia)[xxv], what is called as a "Centre of Excellence"[xxvi]. The outsome in May 2008, was that the centre of CCD was declared by NATO Allied Command Transformation as a 'Centre of Excellence' (CCDCOE).

5. Cyber-Defence put into the test: The Estonian Case.

The Centre of Excellence in Tallinn was primarily supported for two reasons: 1) It was already scheduled by the time of its inauguration as an idea. Estonia would have been the host country for such an operational centre. It had proposed as a newcomer to the Alliance to establish the first operational international military centre ever, in NATO's history as an Ally. 2) Estonia had already been witness of modern asymmetrical warfare attacks in 2007. This came as a result of Estonians removing the bronze statue of a Red Army soldier from the centre of Tallinn an honorary statue honouring the dead of the Second World War. This matter sparked social outrage between the 60-65% of its Russian Speaking, Russian native population and the Estonian Government[xxvii]. It resulted to continuous cyber-attacks on Estonia's e-infrastructure public or private, military or civilian. One year later in 2008, 7 countries according to the memorandum of understanding, helped Estonia get full operational capability (Germany Italy, Latvia, Lithuania, Slovakia and Spain), which lead to its current status. Current Status includes also the possibility of evolving as the US in interested in Joining; Turkey and Greece are in the middle of initiating an evaluation of their needs on whether or not to join this centre.

The cyber-attacks in Estonia, with a duration period of several weeks, in 2007, provided nonetheless NATO with a motive. NATO was in fact right on its judgment that: 1) Such an operational centre was in fact needed 2) Its operational centre, it was decided, that it should constantly be evaluating current and prospective evolutions in warfare and more specifically in Cyber-Defence.

Therefore, for this positive, for NATO, development on the matter of electronic warfare, the centre looks like that it will become the leading operational centre against any cyber-attacks.

Since the inauguration of its Co-operative Cyber-Defence Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, the 30 men group operational centre, initiated a mission and a vision statement. Its raison d' être as stated is "to enhance the co-operative Cyber-Defence capability of NATO and NATO nations, thus improving the Alliance's interoperability in the field of cooperative Cyber-Defence". Its vision is to be "a primary source of subject matter expertise for NATO in cooperative cyber-defence related matters"[xxviii].

Core policy-creating by research and policy-presenting areas, are presented primarily at the Supreme Commander Allied Command Transformation (SACT), by a request of NATO HQ (Head Quarters) and by the North Atlantic Council (NAC) level. This includes:

- "Doctrine and concept development
- Awareness and training
- Research and development
- Analysis and lessons learned
- Consultation"[xxix].

6. NATO approaches issues relevant to cyber-security

For the concept of Cyber-Defence to be successful, the Centre for Excellence in Tallinn, should continue to portray NATOs need for the creation of a permanent, of major importance core policy. On the 6th and 7th February 2009, NATO's Science for Peace and Security (SPS) sponsored a workshop entitled "Operational Network Intelligence: Today and Tomorrow". Its overall purpose as stated was "to rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber attacks" [xxx].

NATO increasingly recognizes that organized cyber-attacks seek to take advantage as is stated "modern society's dependence on sophisticated technology in order to inflict serious damage on economies and national security"[xxxi].

NATO is also of firm belief that there is an increasing need for the co-ordination of the human factors related to the issues of electronic warfare, operational network, intelligence and Cyber-Defence. Said that, NATO implies that all people involved such as systems and security engineers, researches, officers dealing with network operations and operational centers should be systematically involved at organized levels of discussion, under the form of academic research. In turn, at this point the paper proposes that this research could, if applicable, be put under the central command and authority of the Estonian Cyber-Defense Centre with simoultaneous presentation of its outcomes to the political and military Commitees of NATO and under the auspices of the Secretary General of NATO.

It is also important to stress that NATO's level of ambition on the policy of Cyber-Defence and at the general policy of electronic warfare should increase. Current Academic research should co-ordinate itself with practical work made at NATOs military operational levels. Said that, NATO should and could do more on this matter by:

1) Applying the outcomes both from the Centre of Excellence but also from the SPS at both tactical but also operational levels of NATO main forces.

2) Applying Tallinn's coordinated efforts outcomes on Cyber-Defence in its operational military centers that deal with the use of interoperable forces and network centric operations in warlike engagement operation.

3) The Allies involved at the Cyber-Defense centre should consider inviting more Allied member states to join, under the NATO co-operation form of 'Voluntary National Contribution (VNC)[xxxii], looking to a positive outcome that will be offered by the Centre of Excellence on Cyber-Defence, in Tallinn Estonia.

4) By joint co-operation at the level of electronic-warfare prevention, detection and reacti onto attacks to member allied states, duplication of policy can be avoided.

The NATO Summit Meeting in April 2009, proposed two major issues: 1) The intention for a renewed Security Concept and 2) a policy-creation for negotiations amongst states, as well as evaluation and policy implementation agenda for the renewed Security Concept. While NATO creates, a political and military agenda for a successful renewed and viable dogma for security, a new policy-implementation and operational-strategic framework on the Cyber-Defence Concept, should also be drafted and then requested under the framework of the renewed Security Concept. Once accepted is should be included at the as aforementioned renewed NATO Security Concept. In turn, for this matter this paper proposes:

1) New policies relating to practical operational and tactical guidelines on how to achieve full operational security in electronic warfare to be drafted as included at the Security Concept.

2) At the same time as network-centric warfare has not established its legal status of engagement, the NAC or ACT should provide with the necessary decisions to allow the CCDCOE to evaluate and propose a legal guideline for the proper legal protection but also operation within the framework of the wider NATO legal operative environment.

3) Tallinn's CCDCOE, should be supported by the creation of a purely military NATO operational centre on electronic warfare (NATOCEW) that will deal only with the application of current CCDCOE research, towards the successful and interoperable engagement of NATO forces. It will be able to co-operate with other leading nations and possibly non-Allied members that do support wider policies such as the fight against terrorism.

4) Within the evolving strategy of NATO on Cyber-Defence, the CCDCOE should propose more Nations to get involved into the subject matter. Political support is there. The former Secretary-General Jaap de Hoop Scheffer (at that time still current) insisted on supporting its creation. Accordingly, at NATO's summit communiqué in Bucharest in April 2008, NATO reaffirmed its readiness to "provide a capability to assist allied nations, upon request, to counter a cyber attack"[xxxiii]. In 2008 the US forces command stated that it would not be involved at this level of operational research. However by February 2009, the CCDCOE was informed that the US would become an offering nation under the VNC (Voluntary National Contribution) clause, at the NATO effort made for a joint co-operation on Cyber-defense. At the same time, Turkey expressed its willingness to be involved at the operational research of the CCDCOE[xxxiv]. As of the end of 2008, the CCDCOE holds also the recognition of an international organization, which offers the centre's ability to choose its partners but to also widen it perspectives depending on its current needs and allocation of funds[xxxv].

7. Greece's case on NATO policy of Cyber-Defence

Although Greece has not yet joined Tallin's Centre of Excellence against cyber-defence, Latest developments, following the NATO summit on 2009, resulted to a joint consultations and proposals workshop meeting of high level experts of NATO and General Armed Forces Staff of Greece in Athens between the 12th and 15th May 2009[xxxvi]. This was the 11th NATO workshop on cyber-defence. It was hosted by Greece General Armed Forces and sponsored by NATO's NCIRC (NATO Computer Incident and Response Capability).

The aim was to present and provide an update on NATO's cyber-defence policy and management aspects, NATO's policy on cyber-defence operations, on its capability but also project deployment. The aim was to initiate a discussion at the military level with the creation of syndicate committees and to result to a positive outcome for both NATO and Greece on how to deal and to this effect, examine the possibility of Greece joining the Center of Excellence of NATO and international organisation, in Tallinn.

Greece's is still far from joining a cyber-defence centre and even more joining in Tallin's centre of Cyber-defence. This abovementioned cyber-defence workshop that took place in Athens in May 2009 was therefore considered essential in presenting the causes, the needs and the burdens that Greece would be asked to include in its military but also political agenda if agreed to join. The first results are therefore yet to be presented once they are made officially publisized. In the meantime, Greece's policy of cyber-defence as NATO military objectives are portrayed, do not formally apply to Greece's current and formal military objectives.

Greece is in the middle of re-allocating its military priorities in terms of symmetrical and assymetrical threats as is ordered by its national military dogma. What ever the decision will be, shall be a policy of full integration on the perspective under the policy of NATO interoperability of forces. As the Minister of Defence stated in his speech at the NATO council on 8th February 2008, and one year prior to the n April 2009 NATO summit, several issues where discussed as well as the policy of Greece vis a vis NATO's cyber-defence[xxxvii]. The combination of a workshop in Athens one year later in May 2009 headed by the General Armed Forces of Greece and NATO, simoultaneously leads us to the initial outcome that Greece is planning both at the national but also NATO levels to apply an interoperable policy of a joint effort on the matter of cyber-defence, avoiding any possibilities of duplication of efforts as is also the statement made by NATO Secretary-General.

At the operational level the decision of the Greek Prime-Minister to apply more national forces under the ISAF and NATO commands in Afghanistan and in specific in Herat, entails that in the effort of operational success network forces should be interoperable but also protected from any e-threats.

It is therefore the authors' assumption that Greece sooner or later shall be involved at a military level at the tactical preparation and authorization of NATO to conduct simoultaneous and joint operations at a defensive level against possible and world cyber-attacks.

Concluding Remarks:

In conclusion to this paper, the main aim was to portray a recently new but important issue that has been decided by NATO Allies, to develop a policy in regards to electronic warfare and in specific Cyber-Defence. The creation of a Concept of Cyber-Defense and the inauguration of the Centre of Excellence for Cyber-Defence in Tallinn Estonia, according to the decision of the SACT at Norfolk Virginia, NATO is now challenging its current form of Strategic Dogma that has been there since 2001. It is of importance to stress that NATO Allies do widely accept now that a renewed Security Concept that portrays all challenges of the 21 century, is necessary. Within this renewed Concept, we estimate that the policy of Cyber-Defence and overall the policy of electronic warfare shall be mentioned. The question

is what and how the final decisions shall be made; whether the actual current players on this policy shall increase for an effective engagement in practical military operating environments; will other allies such as Greece decide to offer their co-operation under any form such as the VNC or otherwise instructed or decided, as was recently done by the USA and intended to be done by Turkey to the CCDCOE? Will the CCDCOE finally reach its full operational pick? Not withstanding the fact that a legal procedure still needs to be drafted as to evaluate and establish the legal scale and the wideness of operations that it should reflect.

During the course of this paper we estimated that current developments shall lead the CCDCOE to a full operational capability. It will offer robust results, in support of current military man-handled operations. Nonetheless, what is needed to be clarified is NATO's intention for this current centre to offer its outcomes to the effort made by military operational centres such as the 'NATO Deployable Coprs' in Greece, in order to reach at an electronic level but also the levels of the military, interoperability of forces.

It is thus the outcome and proposal of this paper that this centre continues its efforts to become fully operational: Once all administrative decisions have been taken for its smooth operation and once all member allies such as Greece are in full co-operation amongst each other upon this matter, then the centre, should establish a strategic and tactical plan of operation and co-operation in the field of electronic warfare.

This plan shall be in support to current preparations of military man-made operations under NATO forces, such as the preparation of the NRF. Although the latest has become into full operational capability (Riga summit 2006), the NRF is still located at its preparatory and rotating (country-wise preparation) basis levels, where interoperability is yet to be accomplished.

By portraying such a subject we believe that there is a collective interest for NATO members. This subject relates directly not only to security matters to a third party such as states but rather to the well-operational environment of NATO forces, as are offered by the Allied States.

Greece is in the middle of a decision-making process that is not yet to become official as current risk assessments are been made. Greece has just recently embarked on examing the possibility of joining NATO's policy of cyber-defence, according also to the 'guide' of NATO's policy of interoperability of forces command and operation. The results are yet to be presented and then be evaluated. According to Greece's responsibilities to NATO, its military heads of Armed forces shall consider both possibilities positive or negative from this policy evolution on cyber-defence. If Agreed to join then Greece will do the outmost to take initiatives for the best co-operation at the level of NATO co-operation.

NATO is consider to represent the military moral values and the ethics of a collective supranational alliance that works for the collective interests, which are to defend democratic values, the rule of law and the respect of human rights. That is why NATO changes and that is also why NATO is required to change, to evolve, to develop and to expand current or new policies such as matters of Cyber-Defence.

NATO is needed. It is a provider of security in all fields. A preliminary assessment and a critique on NATO's policies were made. During the course of this paper we examined and analysed the policy of Cyber-Defence and the case of Greece. We proposed new practical,

administrative, political ways of expanding NATOs operational environment symmetrical or assymetricall, in constantly changing security environment.

Bibliography:

NATO's Alllied Command Operation (ACO)-Allied Command Transformation (ACT) (2004), *Strategic Vision: The Military Challenge By NATO' s Strategic Commanders*, NATO Unclassified. Norfolk ACT.

NATO DEFENCE COLLEGE (NDC) Occasional Paper (2005), *Security Strategies and their Implications for NATO's Strategic Concept.*

B. Bot (2005), *Transatlantic Relations: Europe must exercise both soft and hard power*, European Affairs spring Vol.5 No.2 pp30-36.

NATO DEFENCE COLLEGE (NDC) Occasional Paper (2005), *Security Strategies and their Implications for NATO's Strategic Concept*, Research Branch Rome November Issue 2005.

Brig.Gen. Phillips, T.R. (ed.) (1985) *Roots of Strategy*, Stackpole Books, Mechanicsburg PA (USA), pp13-65.

Necas P. (2004) *"Beyond Tradition: A New Strategic Concept for NATO?", (ed) by Peter Faber,* Research Paper NATO Defense College, No. 11, pp1-7.

Binnendijk H. & Kugler R.L. (2003) *Dual Track Transformation for the Atlantic Alliance,* Defense Horizons, Publication of the Center for Technology and National Security Policy National Defense University

Dufourcq J. (ed), (2004), *After Istanbul: A Preliminary Assesment*, NATO Defense College, Research Branch NATO, Rome, pp5-71.

Efthymiopoulos M & Demergis J (2006) *NATO's war on terror and the electronic medium* , Last accessed 20/05/2009 19:18 pm

NATO, (1999) *"The Alliance's Strategic Concept"*, North Atlantic Alliance Organisation.

NATO, (2003) *"The Prague Summit and NATO's Transformation"*, North Atlantic Treaty Organisation, pp1-109.

NATO, (2004), *"Istanbul Summit, A Reader's Guide"*, North Atlantic Treaty Organisation, pp5-136.

NATO, (2000), *NATO in the 21st Century*, North Atlantic Treaty Diplomacy and Public Division Publications, Brussels.

NATO (2006), *NATO Review Riga Summit Special*, Brussels, Published by NATO Public Diplomacy Division.

NATO DEFENCE COLLEGE (NDC) (2004), *Beyond Tradition: New Alliance's strategic concepts*, Rome, Published by NATO Defense College Rome.

NATO (2004), *Istanbul Summit Reader's guide*, Brussels, Published by NATO's Public Diplomacy Division.

NATO's Nations (2004), *War on Terror*, Bonn, Published by Monch Publishing Group, Vol.49 No. 1/2004.

NATO (2004), *Enhancing security and extending stability through NATO enlargement*, Brussels, Published by the NATO Public Diplomacy Division.

NATO (2008), Bucharest Summit meeting, Brussels, Published by NATO Public Diplomacy Division.

---

[i] Periodical: "Briefing on Transforming Allied Forces for Current and Future Operations, NATO Public Diplomacy Division", 2008.

[ii] Prague Summit Declaration: http://www.nato.int/docu/pr/2002/p02-127e.htm, Novermber 2002.

[iii] Efthymiopoulos Marios P. (2008), "NATO in the 21st century: The need for a renewed security concept and the ever increasing NATO-Russia relations, Athens, Thessaloniki, Published by Sakkoulas A.E. (in Greek).

[iv] Invoking Article 5 of the North Atlantic Treaty: http://www.nato.int/docu/basictxt/treaty.htm#Art05

[v] Operation Allied Force on Kosovo: http://www.nato.int/issues/kosovo_air/index.html

[vi] Afghanistan: The Taliban Resurgent and NATO, Brookings Institution March 31 2009: http://www.brookings.edu/opinions/2006/1128globalgovernance_riedel.aspx

[vii] International Security Assistance Force (ISAF) website: http://www.nato.int/isaf/index.html

[viii] For more information on the evolution of NATO's policy on cyber-defence see: http://www.nato.int/issues/cyber_defence/index.html

[ix] Ibid 2.

[x] NATO updates for information on immediate NATO reaction see: http://www.nato.int/docu/update/2001/0910/index-e.htm

[xi] Ibid 2. pp 8.

[xii] NATO Declaration on the Decisions of Heads of States, NATO Summit Strasbourg-Kiehl April 2009 http://www.nato.int/cps/en/natolive/news_52837.htm?mode=pressrelease

[xiii] Efthymiopoulos M.P. (2008), NATO's policies in the 21st century: the need for a renewed security concept and the ever enlarging NATO-Russia Relations, Athens-Thessaloniki, Published by Sakkoulas Publications (in Greek).

[xiv] NATO secretary General meets with President Obama 25 March 2009: http://www.nato.int/docu/update/2009/03-march/e0325b.html

[xv] Informal meeting of NATO Defence Ministers October 2007: http://www.nato.int/docu/comm/2007/0710-noordwijk/0710-mod.htm

[xvi] What is a Centre of Excellence (COE)? 4 December 2003, the concept for Centres of Excellence was published. "This concept defines what a COE is, explains the applying principles, talks about accreditation, relationships and also includes guidelines on legal arrangements between the Strategic Commands and sponsoring nations…". For more NATO information on COE see http://www.act.nato.int/news.asp?storyid=342

[xvii] The Allied Command Transformation vision statement and objectives http://www.act.nato.int/content.asp?pageid=200

[xviii] NATO opens new Centre of Excellence on cyber-defence: http://www.nato.int/docu/update/2008/05-may/e0514a.html

[xix] NC3A Agency official website: http://www.nc3a.nato.int/Pages/Home.aspx

[xx] For basic information on the topic of NATO's cyber-defence policy see: "Defending against cyber-attacks http://www.nato.int/issues/cyber_defence/index.html

[xxi] Ibid.

[xxii] Defending against cyber attacks: http://www.nato.int/issues/cyber_defence/practice.html

[xxiii] Ibid.

[xxiv] Ibib 15.

[xxv] Cooperative Cyber Defence (CCD) COE (Estonia): http://transnet.act.nato.int/WISE/TNCC/CentresofE/CCD

[xxvi] Centres of Excellence (COEs), are funded nationally or multi-nationally and are consistent with NATO efforts. For more see the ACT website on Centres of Excellence at: http://www.act.nato.int/content.asp?pageid=335.
[xxvii] See News Scientist: http://www.newscientist.com/article/dn13904-nato-to-give-estonia-cyber-defences.html or Ibid 2.
[xxviii] CCDCOE website at: http://www.ccdcoe.org/11.html
[xxix] Core areas of the CCDCOE http://www.ccdcoe.org/37.html
[xxx] SPS workshop rethinks approaches to cyber security: http://www.nato.int/docu/update/2009/02-february/e0206a.html
[xxxi] Ibid.
[xxxii] VNC is a form of National Contribution under the rules of national policy for a specific period of Time under the auspices of a Government of Foreign or Defense Ministries.
[xxxiii]NATO creates cyber-defense centre in Estonia, May 15 2008: http://www.jamestown.org/single/?no_cache=1&tx_ttnews[tt_news]=33636
[xxxiv] History and way ahead of the CCDCOE: http://www.ccdcoe.org/12.html
[xxxv] Ibid.
[xxxvi] 11th NATO CYBER DEFENCE WORKSHOP 12-15 May 2009, Athens, Greece hosted by NATO and HNDGS www.geetha.mil.gr/media/11cyber/4.Agenda.doc
[xxxvii] Greek Defence Minister to the NATO Council: http://www.greekembassy.org/Embassy/content/en/Article.aspx?office=1&folder=19&article=22812