THE FLETCHER SCHOOL
OF LAW AND DIPLOMACY

Tufts
UNIVERSITY

THE CONSTANTINE G. KARAMANLIS CHAIR
IN HELLENIC AND EUROPEAN STUDIES

# NATO Smart Defense and Cyber Resilience

Marios P. Efthymiopoulos

WORKING PAPER 1/2016

May 2016

**THE CONSTANTINE G. KARAMANLIS CHAIR**
**AT THE FLETCHER SCHOOL OF LAW AND DIPLOMACY**

**SHAPING THE FUTURE / HONORING THE PAST**

The Constantine G. Karamanlis Chair in Hellenic and European Studies at The Fletcher School of Law and Diplomacy is committed to promoting Hellenic and European studies in the United States while honoring a towering figure of Greece's recent past.

The Chair's endowment brings academic scholars to The Fletcher School and the Tufts University community, encouraging a renewed focus on modern Greece, Southeastern Europe, the Mediterranean and the European Union, and the crucial role these regions play in world politics. The regular rotation of the holder of the Chair ensures its constant renewal, endows it with new perspectives and subject matters, and has a multiplying effect, as outgoing professors enrich their experience and provide permanent points of contact between their home institutions and Fletcher.

The Chair also forges a strong bond between the Boston area European and Greek communities and members of academia whose interests lie in current Greek and European issues. Through this bond, many opportunities will arise to deconstruct negative stereotypes, overcome obstacles to cooperation, and create innovative ways to move forward, inspiring a more compassionate and peaceful global security.

The Chair was founded at the initiative of the Konstantinos G. Karamanlis Foundation in Athens, led by Ambassador Petros Molyviatis and Minister Ahilleas G. Karamanlis, and then Dean of The Fletcher School, General John Galvin, while its endowment has been supported by many friends of Constantine Karamanlis and the Fletcher and Tufts community.

As funding efforts expand, the endowed Constantine Karamanlis Chair will form the core component of the planned Center for Hellenic and European Studies at The Fletcher School, Tufts University, providing:

- a 1-2 year position for a distinguished scholar
- courses for graduate students at Fletcher and for undergraduates at Tufts University
- lectures for the community at large on Greece, the Balkans, the Mediterranean and the European Union
- Working Papers and conference publications
- roundtable discussions, debates and conferences
- advanced research

## Holders of the Chair:

**Professor Thanos M. Veremis** was the first Karamanlis Chairholder, is Professor Emeritus of Political History at the University of Athens, Greece. He was educated at Boston University and the University of Oxford and has served as a professor and a researcher at universities in Europe and the USA. His many books and articles in English and in Greek have focused on Greek political history and foreign policy, Greek-Turkish relations, Balkan reconstruction, and Southeastern Europe. He served as President of Greece's National Council of Education, 2004-2010.

**Professor George Prevelakis** is Professor of Human and Regional Geography at the University of Paris-Sorbonne, France. He was educated at Athens Technical University and Paris-Sorbonne and has written extensively on geopolitics, Greek geopolitics, the Hellenic Diaspora, the interplay between culture, politics and economics, and the Balkans. He is co-director of the French academic journal Anatoli (CNRS Editions). Currently he is Greece's Ambassador to the OECD.

**Professor Dimitris Keridis** is Professor of International Politics and Deputy Director of the Institute of International Relations at Panteion University, Athens. He was educated at Aristotle University of Thessaloniki and The Fletcher School of Law and Diplomacy and has written extensively in English and in Greek on Greek foreign policy, US foreign policy and the war on terror, Turkey, the Balkans, the effects of disaster diplomacy, EU foreign policy and European security. He is a senior research associate at the Karamanlis Foundation and serves as the Director of Navarino Network (a public policy think-tank in Thessaloniki) and of Olympia Summer Academy.

**Professor Kostas A. Lavdas** is Professor of European Politics and Director of the Center for Political Research and Documentation (KEPET) at the University of Crete, Greece, where he has been a Dean of the Faculty of Social Sciences and a University Vice-Rector. He was educated in Greece, the UK (London School of Economics and

the University of Manchester) and the USA (Massachusetts Institute of Technology) and has served as a professor and a researcher at various universities in Europe and the USA. His many books and his articles in international journals (including The European Journal of Political Research and West European Politics) in English, Greek and German have focused on EU politics and policy, Greek politics, interest groups in comparative political analysis, and applied political theory.

**Dr. Alexandros Yannis** was educated in Greece and Switzerland and has extensive international experience in multilateral diplomacy with the European Union and the United Nations. His experience includes working with the European Union Special Envoy to Somalia (1994-1997), the Special Representative of the United Nations Secretary General in Kosovo (1999-2000) and in the Office of the United Nations High Commissioner for Human Rights in Geneva (2001). Currently he is policy coordinator on global issues and responsible for energy diplomacy in the European External Action Service (EEAS) of the European Union.

**Professor George Mavrogordatos** is Professor in the Department of Political Science at the University of Athens, Greece. He was educated in Greece and the United States and was awarded the Woodrow Wilson Foundation Award of the American Political Science Association ("for the best book published in the United States on government, politics or international affairs") for his dissertation Stillborn Republic in 1984. An Adviser to the Opposition during the debate on the new Greek Constitution, 1975 he founded and edited (with N. P. Diamandouros) Modern Greek Society: A Social Science Newsletter, 1973-1980. He was a member of the National Council for Research and Technology in Greece between 2005-2008.

**Professor Michalis Psalidopoulos** is Professor of the History of Economic Thought at the Department of Economics, University of Athens. He was educated in Athens and Berlin and was a Fulbright Fellow at Duke, a Stanley J. Seeger Fellow at Princeton and a Visiting Research Professor at King's College, London. His research focuses on national traditions in the History of Economics and the relation between economic thought, economic policy and good governance, especially in Southeastern Europe. His most recent book is Economists and Economic policy in Modern Greece (in Greek, 2010). He has also published articles in History of Political Economy, in The European Journal for the History of Economic Thought and in History of Economic Ideas. He is currently involved in a comparative project of economic experiences and policies in Europe's less industrialized countries during the Great Depression. He speaks English, German and French fluently, as well as Greek.

**Professor Kostas A. Lavdas** is Professor of European Politics and Director of the Center for Political Research and Documentation (KEPET) at the University of Crete, Greece, where he has been a Dean of the Faculty of Social Sciences and a University Vice-Rector. He was educated in Greece, the UK (London School of Economics and the University of Manchester) and the USA (Massachusetts Institute of Technology) and has served as a professor and a researcher at various universities in Europe and the USA. His many books and his articles in international journals (including The European Journal of Political Research and West European Politics) in English, Greek and German have focused on EU politics and policy, Greek politics, interest groups in comparative political analysis, and applied political theory. Professor Lavdas became the first returning professor to the Chair in 2014-2016.

## About the Author

Dr. Marios Panagiotis Efthymiopoulos is Assistant Professor of Strategy and Security and Program Coordinator of the MA program at the American University in the Emirates, Dubai, United Arab Emirates.

Dr. Efthymiopoulos is also a member of the Geostrategic Council of the Cyprus Republic and the CEO and Founder of the Think Tank *Strategy International* (Greece).

His former research positions included the Harriman Institute at Columbia University in New York City, the Center for Transatlantic Relations, SAIS, Johns Hopkins University in Washington DC, George Washington University, Business School, EU Center for Excellence, Washington DC, the Woodrow Wilson International Center for Scholars, Washington DC and a research fellowship at the University of South Florida.

He also taught at the department of Social and Political Sciences at the University Of Cyprus, Nicosia Cyprus. Dr. Efthymiopoulos taught at the Hellenic Homeland Office, Joint War College of Greece, NATO Maritime Interdiction Operation and Training Center (NMIOTC), the UN and NATO training corps and the NATO Rapid Deployable Corps Thessaloniki Greece.

He also completed the senior course 105 at the NATO Defense College in Strategic and Security Affairs in Rome, Italy, appointed by the Ministry of Foreign Affairs of Greece. Among others interned at the United Nations Industrial Development Organization (UNIDO) Biotechnology and Biosafety. Prior to this as Political/Financial Analyst, project officer, at the County of Cook Treasurer's Office in Chicago Illinois.

Dr. Marios Panagiotis Efthymiopoulos is a PhD holder from the University of Crete in Political Science with a specialization in Strategic Studies. His Dissertation was on NATO's New Strategic Concept and NATO-Russia Relations. His Master Degree is from the University of Vienna -The Diplomatic Academy of Vienna-in Advanced International Studies (MAIS) (2002-2003). He Holds a BA (Hons) in International Relations & Politics by the University of Lincolnshire and Humberside, (1998-2001), Lincoln, UK.

His Research interests include, among others, Cyber-Defense and Cyber-Security, military affairs, business and development continuity, strategic resilience, projections and global strategies, international organizations, financial security and global and world affairs among others.

He has published two books on strategy and security, one in translation and edited volume on foreign policy and a book on cyber-development Cyber-Democacy and Cyber-Defense, published in July 2014. He is currently a co-editor of the Handbook in Cyber-Development, Cyber-Democracy and Cyber-Defense.

# NATO Smart Defense and Cyber Resilience: A Methodological Approach to Adapting to Emerging Challenges (*)

Dr. Marios Panagiotis Efthymiopoulos

***Assistant Professor of Strategy and Security &***
***Program Coordinator of the MA in Strategy and Security***
***American University in the Emirates***

*Email: marios.panagiotis@aue.ae*

*May 2016*

(*) The views and opinions expressed in this paper are those of the author and do not necessarily represent the views of the Karamanlis Chair and/or The Fletcher School at Tufts University.

# Table of Contents

## Abstract

This paper aims to evaluate NATOs' "Smart Defense"[1] policy in the view of the continuing significance and global roles of the Alliance. Smart Defense being an integrative part of the collective defense of NATO, it is required to respond to existing threats and challenges through the use of new operational and tactical elements, which should include flexibility and the adaptive use of technology.

Current and future strategic threats and challenges require NATO to re-examine policy and operational posture. This includes building on NATOs future strategy, through adaptable policy and procedure. Through NATOs' cyber-defense policy, greater resilience when dealing with threats can be achieved.

A methodological approach will be presented on to how to integrate NATOs collective defense, through cyber-defense policy, to the 21st challenges and threats. NATOs resilience policy, if adopted at the Warsaw Summit in July 2016, will become an integrated part of NATO's Smart Defense and collective defense. It will create a new standardized form of procedure, which will afford flexible strategic and operational forces but also commanding forces, through the use of multi-level and multi-dimensional tools.

***Key Words:*** *NATO, Resilience, Cyber-Resilience, Smart Defense, Cooperative Defense, Hybrid Threats, Warsaw Summit, Standardization, Interoperability.*

[1] NATO's Smart Defense policy: Smart Defence is a cooperative way of thinking about generating the modern defence capabilities that the Alliance needs for the future http://www.nato.int/cps/en/natohq/topics_84268.htm [seen on April 26th 2016].

## Introduction

At NATOs Warsaw Summit in July 2016[2], NATO members are to welcome all possible clauses for cyber-security and cyber-safety procedures, considering challenges and threats, as well as strategic elements for operational capacity building options; in essence allowing for *optimum adaptability in technology, through information resilience* of NATO forces. Technological evolution of NATO means operational and strategic change for the alliance. It is up to NATOs leaders and decision-makers, to decide about the future of NATO and how it is going to be operating strategically and operationally, considering the multidimensional level of threats and challenges. Therefore, in regard to the policy of Cyber-Defense and/or Cyber-security it needs to be decided as to whether they are going to be adopted and or centrally used, as core elements of defense policy. Leaders are yet to show truthful political resilience in decision making at the level of the 28 member states, for NATOs' business and operational continuity, could be at stake.

Operationally, forces need to continue to be agile and technologically advanced at all levels, in an asymmetrical world, which is complete with unforeseen challenges and threats. Currently NATO forces, require a flexible and adaptable operational and strategic command, based on high technologically sophisticated information 'coming in' but also being used while in training or active operations.

Possible operations, require tactically coordinated network-centric, standardized, oriented operational capability and capacity. NATO's current "Smart Defense" policy therefore should be updated. It needs to be automatically adaptable to a new range of e-environment threats. Through 'resilience of forces', a new terminological characteristic, which will become the buzz word, for the next 'operational period' to come, NATO will be adapting to new security challenges.

This paper proposes a tactical military and civilian capacity building approach, based on the strategic needs for resilience in collective defense and/or smart security policies of NATO. Leaders should, through consensus, jointly decide on effective measures for strategic capacity building. New operational and strategic elements need to be procured and applied, considering the technological advances with which modern threats and challenges appear. The policy of resilience and continuity of NATO should be decided so that NATO may continue be relevant as a security organization.

NATOs cyber-defense and cyber-security, is a core policy, which requires the Alliance to become resilient when referring to collective defense. According to "NATO Review", "…NATO's experience and expertise can help partners improve their own capacity for resilience[3]".

[2] NATO Warsaw Summit 8 & 9 July 2016: http://www.msz.gov.pl/en/foreign_policy/nato_2016/ [seen on April 22nd 2016].
[3] NATO Review, NATO Defense and Cyber-Resilience http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/ [assessed April 230th 2016].

This paper provides the reader with updated information on Cyber-Defense policy, Smart Defense and the North Atlantic Alliance considering the forthcoming policy adaptation of resilience as a key methodology for collective defense.

This is a research area which appears to be simultaneously challenging from a scholarly perspective and hugely significant in terms of policy and practice[4]. This paper is an approach to what we can refer to as "NATO's Cyber-resilience policy". It proposes a new strategy in operational and defense capability, built on the necessity to minimize current and future threats, whether these are coming from the North-East, East or South.

We aim to examine current steps taken for a resilient alliance policy. It considers cyber-policy in defense and security, as the most important policy reflecting the need for NATO to adapt to new strategic and operational environments. It looks at the strategic 'lessons learned' to this day, on NATO's cyber-resilience. It recommends strategic and operational management elements, based on the need to hold a flexible and adaptable alliance. The paper finally considers current administrative and fiscal costs, considering cyber-defense and security in a resilient strategic networked environment.

Let us also note that the present paper aims to build on previous research published by the author on NATO Cyber-security[5].

Issues analysed and proposed in this article, are the sole opinion of the author. They are not related in any official way with NATO or any government. They represent ongoing academic research and a proposed analysis that is shaped from primary and secondary sources of information. Current positioning, statements and arguments are based on academic research, experience, judgments and cooperation established in the framework of this current research.

The issues presented hence forth, are for consideration. They solely reflect the operational and tactical levels

## NATO and the Policy of Resilience

Resilience as a terminological and operational factor, will become the newest 'brand' and communication name for the Alliance. Resilience, as a terminological word will create a re-orientation policy for NATO. It will and should reflect all possible crises and strategic management procedures. It should apply to NATO's operational capacity of deployment of forces, through more flexible and effective

[4] Efthymiopulos Marios P (2013), in (Carayannis et all), *NATO's Cyber-Security Policy*, Chapter in Cyber-Development, Cyber-Democracy and Cyber-Defense, London, New York Published by Springer.
[5] Ibid.

means of countering threats. It will be adaptable to mitigation and/or negotiation procedures with non-NATO members and will allow for cooperative members' joined cooperation and training, in consequence, to relative past or currently emerging challenges and threats (i.e., NATO-Russia Relations and NATO-ICI members considering the threat of ISIS and other terror groups).

NATO's resilience will re-define strategic plans and re-assess risks. Heads of State and Governments at NATO should create a 'modern administrative and operational format of the alliance' that is flexible and e-oriented. NATO truly needs to hold agile and technologically advanced forces with added value, through civilian capabilities and social media training and action among others.

Resilience therefore should become also an adaptation process for NATO; a phase to consequently strategize and draw new scenarios. This is in order to operationally process and counter in an effective manner, current, new and upcoming challenges and threats. Resilience is therefore a policy that is being given way from "NATO's Smart Defense" clause. A result and constant request of NATO is to boost change, if it wants to remain relevant and most importantly a global asset value to security and strategy.

The policy of 'resilience', should open way to operational and strategic flexibility. It will be applied at all levels. When strategically managed and operationally approved, resilience will include a further and concrete, development of an "updated" cyber-defense policy for NATO among other policies that will add value to the needs of NATO to counter threats in a multi-dimensional level.

NATO's Smart Defense should be resilient. It should ensure stability. The Atlantic Council of the USA refers to a 'stability generation' policy[6], adding that NATO's collective defense itself should be re-strategized. It should be adaptable to the constantly increasing needs, for a technologically secure and agile environment, in a period of great challenges and threats from outside but also within NATO space.

A resilient smart defense, requires agile network e-centric cyber methods. NATO requires operational capacity steps to be adopted. Through a methodological reasoning and step by step deployment of forces in security and e-security led operations, NATO will be able to secure its e-space, secure its infrastructures but also provide defense and cooperation, as NATO should "confront where we must and cooperate when we can", referring to the NATO-Russia relations, according to Stavridis, the Dean of the Fletcher School at Tufts University.

[6] Franklin D. Kramer, Hans Binnendijk, and Daniel S. Hamilton, (2016), *NATO's New Strategy: Stability Generation, Washington D.C.*, Published by the Atlantic Council of the USA, Brent Scrowcroft Center on International Security.

Due to the importance of a resilient policy to collective defense, cyber-defense as a policy should become a core asset value policy for the Alliance. It should be used as a core element for a renewed flexible, otherwise resilient smart defense policy, for the benefit of collective defense but also cooperative adaptability.

## NATO's Cyber-Resilient Policy

"Future war-like operations will be held in a far more complicated level of military operations"[7]. Current military operational and tactical needs, considering the asymmetrical and multi-dimensional environment, require good and agile capacities and capacity building. Joined forces themselves, require proper command and operations. They require agility but also resilience.

We live in an age "…in which more people have access to highly sophisticated technologies and almost every social, economic or military asset has become 'securitized' or vulnerable to disruption – whether temporary or more lasting – from an outside attacker or even an inside source...In a globalized but also more confrontational and complex world, resilience will remain an ongoing concern for Allies, requiring constant adaptation as new vulnerabilities and threats emerge…[8]".

Operations are conducted today within a complex environment. The use of technology necessitates, accurate 'tools' for possible success. They require interoperability of forces, in a constant adaption environment. The same applies for network-centric oriented operations where cyber-resilience is required.

Technology is therefore used as an asset tool. Its capabilities are used for the success of military operations. Knowledge and good use of technology, and in specific cyber-defence are added values that minimize among others human cost.

When NATO leaders first considered cyber-security as a policy requirement, questions were raised on how to find a smart way and operational way to use technology for its benefit both operationally and strategically in a fast and technologically advancing world.

In 21st century security affairs, NATO forces are required to be well prepared for possible rules of engagement at all levels and dimensions. They should be able to counter symmetrical and asymmetrical battles, threats or challenges. At the level of cyber-resilience preparedness, scenarios, of possible attacks and battles, can be

[7] Efthymiopoulos, M. P., (2008), JIW Vol. 8, Issue 3, (Journal of Information Warfare), *NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defense and the Alliance New Strategic Concept*, Australia, http://www.jinfowar.com/
[8] Ibid 3.

anticipated. There are or should be proposed operational methods for action whether this is for defence or cooperation.

The use and necessity today of technology is limitless to both military and civilian assets. So is the virtual world of defence, where technology and cyber-defence merge. These are the tools for action. Technology plays a key role in a global reach and so does NATO, through the framework of a limitless technology. NATO uses technology for the preparation of its forces, as tools for knowledge as to defend but also to counter-assaults, where counter-measures are needed.

Since the adoption of the NATO Cyber-Defence policy[9], NATO trains its military and civilian assets for possible action against possible threats. NATO is constantly training its forces on Cyber defence. Training can be achieved through national, bilateral even multilateral levels of NATO, through the association of member states, at the level of Centres of Excellence, such as the CCDCOE[10]. Training is anticipated to expand. While NATO gets more engaged in the field of cyber-defence, in both operations and tactics. It is anticipated within the Alliance that NATO is well prepared, both for current and future challenges, countering multiple and multileveled dimensions of cyber-attacks. Yet, it also holds an open option if necessary, to conduct counter-offensives to prevent further escalation of cyber or military actions[11].

NATO Missions, "will continue to require agile and interoperable, well-trained and well-led military forces"[12]. This new technological and operational environment through cyber-defence, provides NATO with a new level of technological possibilities; new tools for use against possible threats but also protective 'cyber-objectives'. Allies have an added policy, mission and value. Ongoing and constant transformation through its Operational and capacity building resilience, aims to reach in updated capabilities and political excellence, in 2016. NATO aims for well-coordinated missions in cooperation with and/or participation with other international organizations, when prompted to react on international threats or challenges. As such, NATO has the ability to continue to be a force and security provided in future potential of, what we may call it, as the 'online' security protection initiative against all possibly known threats.

Now it seeks excellence, in achieving the best smartest way to protect but also counter-attack. By 'nature' NATO exists to prevent and defend member states from attacks.

---

[9] NATO's Cyber-Defense Policy (2011), http://www.nato.int/cps/en/natolive/topics_78170.htm

[10] NATO Cyber-Defence Centre for Excellence, https://www.ccdcoe.org/

[11] Hughes. R. B. (2009) Atlantisch Perspectief,.Ap:2009 Nr. 1/4, *NATO and Cyber-Defense: Mission Accomplished, Netherlands*, Netherlands Atlantic Committee.

[12] Ibid. 1.

Through smart ways and agile training, NATO can counter, most known ways of interface (whether virus or virtual) attacks or spying attempts.

As previously noted, cyber-defence capabilities in a smart and resilient way, is the 'operative goal'. NATO members prepare well and at joint levels. NATO's Smart Defence[13], a policy framework for defence tactical advice and operations, used to be the method that among others branded the need for a cyber-defence policy. Through a possible upcoming Cyber-resilience of NATO, which could be adopted as a policy, among other resilience policies, during the Warsaw Summit in July 2016, NATO will be expected to take preliminary actions through standardized procedures of protection effectiveness. What is well known through policy analysis is that NATO military forces should reach an appropriate level, so as to operate in and around "article and non-article 5 operations"[14]–meaning not only defensive-clause operations but also in counter-offensive operations[15]. Cyber-protection is needed when defence of allies is associated with possible threats or challenges such as the one of ISIS.

This article stresses, that NATO Cyber-Defence policy, should never stop transforming, while technology progresses and threats expand to a new and deeply digitized world of insecurity starting with the case with the cyber-attacks in Estonia in 2007[16]. Past events in Estonia, showed early on, a strong smart cyber-defence 'umbrella' which is certainly needed by 2016, in which agility and resilience needs to be achieved.

There is a need of a resilient policy method approach for continued practical allied update and practical preparation to counter cyber-attacks. Innovative methodology and ideologies are needed to process such a policy approach.

In turn, a preparatory resilience policy applied, will allow for the 28 member states, to be even more agile for defence or crisis management purposes, electronic warfare methods. Interoperability of forces for joint use in Cyber-defence should be achieved through adaptability and standardization processes. NATO should 'e-volve' as should Allied 'e-networked' States. NATO should innovate and manage. NATO should administer change on methods of smart resilience in defence through cyber-defence, strategically and operationally.

---

[13] In the following sub-chapter I include the analysis of a research method to explain the meaning of Smart defense. It was presented at a conference under the name of: "The Shadow Summit of NATO's Washington Summit of 2012", http://www.natowatch.org/node/676 organized on May 14-15, 2012 at The Elliott School of International Affairs, The George Washington University Washington, DC. You can also see live the speech at Cspan on http://www.c-spanvideo.org/mariosefthymiopoulos

[14] Sendmeyer S. A. (Maj), (2010) August, *NATO Strategy & Out-of-Area Operations*, School of Advanced Military Studies, US Army Command & General Staff College, http://www.hsdl.org/?view&did=713508

[15] NATO (2008), *Briefing on Transforming Allied Forces for Current and Future Operations*, NATO Public Diplomacy Division, Brussels.

[16]Scheherazade Rehman, (2013) January, *Estonia's Lessons in Cyber Warfare, US News*, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare

## Cyber-Resilience in Cooperative Defense

During the Chicago Summit, NATOs' policy on "Smart Defense[17]" was presented in which, "…NATO leaders agreed to embrace Smart Defence to ensure that the Alliance can develop, acquire and maintain the capabilities required to achieve the goals of 'NATO Forces 2020…[18]". Following this, during the Wales summit[19] NATO Allies, confirmed and reaffirmed the commitment of all member states to consider the cyber-resilience of each nation to the aims and objectives of the alliance. They affirmed NATO's policy vis a vis the international and inter-connected environment, which are complete with challenges and threats. They also affirmed the raising importance of the element of cyber-security and cyber-defence. The upcoming NATO summit in Warsaw in July 2016, is yet to show the policy or resilience and cyber-resilience in the framework of cooperative defence. At a time of much needed proposal for practical and smart defence, there is a new security culture comprehension, which is now considered as multi-levelled and multi-dimensional.

Defense capacity building for the 20th century requires a modern way of thinking. It is about encouraging cooperative defence at the level of expected outcomes considering global but also regional risk assessments. NATO is still to enhance but also maintaining military capacities and military capabilities.

The new strategic concept of NATO requests the alliance to move forward. 21st century needs and challenges, require agile and compatible forces at all levels, including network-centric operations and defence.

NATO forces cannot be static. They need to technologically advance, progress methodologically, to accommodate the increasing need for multi-dimensional ways of security and defence. NATO needs to have interoperable, capable and well equipped technologically agile forces.

Planning and budgeting for operations needs to be "smart". Directed funds should now, at a period of specialized or tailored fiscal management, build such capacities, in which planning should be effectively applied in practice. This includes where operational viability of forces is realised, on a minimum budget level with equalised costs, and enhanced technology and minimum engagement in regard to both time and operations.

Throughout the attempt to achieve a truly cooperative defence, 'Smart Defence' stands out on renewing operational and tactical effectiveness; operational alliance

[17] NATO Chicago Summit: http://www.chicagonato.org/ May 20 & 21 2012.
[18] Ibid 1.
[19] Wales Summit 4 September 2014, http://www.nato.int/cps/en/natohq/events_112136.htm [seen May 1st 2016].

and coordination. It is all about specialization of forces including the element of resilience of forces mainly through technological agility.

Smart Defence is to soon prioritise to meet the NATO forces command and structure of 2020, through the following steps: 1. Sound strategic structuring and planning, 2. Good operational coordination in exercises and in the field, 3. specialization of force structure, command and operations 4. Achieving collective defence, through collective efforts, 5 burden sharing 6 technological advancements, considering the threats and challenges of the 21st century.

By 2016, in a period of much needed strategic and tactical resilience, smart defence stands out as a request for geo-political capability and capacity, implementation and operational effectiveness, in both the regional and global fields. In environments which are symmetrical but also asymmetrical; with minimum cost possible, through the optimum use of technology provided. While also trying to avoid duplication of efforts, Member states should hold joined operational strategic centres, on and for among others, ballistic missile defence, intelligence, surveillance, reconnaissance, cyber-defence and security, maintenance of readiness, training and force preparation but also agile deployment bases for effective engagement; All aforementioned should be expected to work with minimum cost, casualties and high level of technology preparedness that is both beneficial and practical.

Smart Defence is a priority policy for NATO. And so should Cyber-resilience in the Alliance. Through a methodological period, NATO should continue to be able to counter current and emerging challenges. Defense planning, operations and lessons learned are therefore a continued process of evolution of NATOs capabilities which always need to be taken into account.

Resilience through smart and cooperative defence requires NATOs Cyber-defence effectiveness. It also requires decision-making and leadership in this policy context. In the framework of cyber-defence, NATO needs to align supranationalised national capability priorities and standardize through NATO processes. In the framework of Cyber-Resilience at NATO, policies on standing management of operations need to be agreed upon. Therefore, cooperative and consensus levelled agreements need to come forth; NATO should produce a cost-effective projection planning and application for all operational exercise theatres reflecting the real yet also virtual worlds.

Cyber-Resilience and methodological specialization through leaders' policy decisions at the level of Heads of State and government in operational planning and practically applied, are key components of and for success for the Alliance, considering threat assessments. Resilience with coordinated efforts may lower costs, fiscal, administrative and human, but will require developed technology infrastructure. It will guarantee national engagement of states to NATO policies, when correctly pointed out. Let us not forget that specialization as a key national policy

is and will always remain a form of national interests, which examined changing variables based on geographical interests, strategic sharing of costs, technological information and intelligence sharing or operating in regional or global environments.

## Associating Smart Defence with Cyber-Resilience: "Engagement Through Policy Adaptation"

Not many steps take haven been achieved in the framework of Smart Defence capabilities when resilience is applied. The inability and/or unwillingness of member states, for political and military national engagement has still to be confronted, mainly as fiscal austerity measures are applied and cutbacks are in effect[20]. According to the Atlantic Council, "…The Alliance, given the new strategic landscape it currently finds itself in, requires a new strategy. NATO's current three core tasks—collective defense, crisis management, and cooperative security—are "tasks" but not strategies—they do not identity the full spectrum of ends, ways, and means, and therefore do not tell the Alliance and its members either what to do or the risks involved. NATO has been working diligently but without great clarity or common agreement as to its end goals[21]".

Heads of state and governments however do listen and observe and therefore consult and call on NATO to hold Summit meetings, and to negotiate or mitigate issues such as the upcoming Warsaw Summit of July 2016. In the framework policy 'Smart Defence', which is yet to be achieved by 2020, Smart defence renders cheaper the cost for the total sharing of burden by member states while attracted more to elements or variables where technology is used to minimize costs. Surely, not all members share the same burden to this day, as also the cost differs from state to state and so does as aforementioned national interests.

In a time of austerity measures and political challenges and changes, states are still to realise how cost can be measured, in a smart 'budget and operations' way. While Smart Defence lowers overall long-term cost, and if burden sharing is actually increased but equalled to lower levels of fiscal sharing, long-term results will show, that in fact, less cost will be achieved.

The cost will be equally associated with the value of services provided reflect the needs of strategic management and planning of all 28 member states, which to be fair cannot yet be achieved.

---

[20] Chicago Council on Global Affairs, (2012), Conference: *Smart Defence and the Future of NATO, Can the Alliance Meet the Challenges of the 21st Century*, March 28-30 2012 Chicago Illinois, USA.
[21] Ibid 6, pp.3.

While, national and collective defence remains at the forefront of interests of states, a new 'rapprochement' is needed between member states as threats are now borderless.

Cyber-defence being a key core policy for smart defence and resilience, attracts attention to stake holders. Through evolving and constant communication and marketing perspectives, social media and workshops, conferences, cyber-defence should continue to be promoted and have a clear aim. Reflecting on the needs for a global element of cyber-security against current and emerging challenges, exchange of scientific information and operational processes, promote such ideology, where experts from around the world exchange information and discuss the risk assessments and how to manage.

Cyber-defence, a core policy in Smart Defence itself, works as a 'decree of specialization, which now requires adaptation if not done so already for each member state'; politically, strategically, tactically and operationally but also legally. Cyber-defence policy must and should always be provided as a methodological tool for operational success of NATO against current and emerging threats. It is and will always be a tool for a joint framework of cooperation, globally.

As Smart Defence is being upgraded and developed, Cyber-defence "…not a conception but a real-politic issue…[22]", should remain an element of specialization policy, a key for concrete strategic engagement of all resilient member states. It will emerge to become a policy of unity among states (political) and business continuity (strategic orientation) about the future of NATO.

NATO's strategic approach post Warsaw Summit is estimated to reflect a much need realistic plan of operations and engagement in the field of cyber-security and defence. NATO should continue to be a collective to be a force projector and force protector. It should not limit its role and actions but should allow and seek out enlarged cooperations tailored to the global and regional needs to counter the existing challenges or emerging challenges, considering that as aforementioned challenges are now borderless.

Cyber-defence and technological progress within NATO, can therefore be seen as the core of collaborative smart defence, to be finalized and achieved by 2020 standards. Cyber-Security being technologically advanced is resilient to changes. It does provide adaptable technological architecture and posture which will discuss below considering the opportunities but also challenges. It will provide robust deliverables with minimum human capital, fiscal but requests technical deliverables.

[22] Ibid 4.

With the Internet of all things, cyber-defence and security as a strategy becomes necessary and absolutely important as a legal framework, political framework and economic framework of burden sharing at NATO.

At the same time it will simply 'market' NATO in the 'smartest and easiest way' at a time of financially and socially emerging markets, where non-member states require individual or tailored cooperation with NATO. It will facilitate NATOs expeditionary role for force projector, trainer and crisis management operator, as an "…active leader in peace and security[23]".

## Cyber-Security Liability and NATO

NATO's role is expeditionary. We could state that NATOs role is as a force projector, force planner, force multiplier, force initiator and force applicator. It does apply these 'rules' for the benefit of a safe and secure environment when risk are constantly assessed[24].

Between the years 2001-2016, among others, the Alliance has responded through actions such as the following:

1. Invoking article 5[25], as a consequence of the terror attacks in the USA, on September 11th 2001,claiming its right to defence against external aggression
2. Allied states agreed on an everlasting transformation, political, military, operational and strategic as was approved in during the Prague summit of 2002[26],
3. Agreed to be involved in outer-areas of traditional operations Kosovo[27], Afghanistan in 2001[28] onwards via operation International Assistance Force[29]
4. By 2012 at NATOs Chicago summit and confirmed at the Wales Summit of 2014, agreed on a Smart Defence initiative, that is of qualitative and quantitate value, for among others, agreed into joint interoperability ef-

[23] NATO, (2016), *Operations and Missions: Past and Present*, *http://www.nato.int/cps/en/natohq/topics_52060.htm [seen May 4t] 2016.*
[24] Efthymiopoulos, M. P. (2008), *NATO in the 21st century: The need for a renewed Strategic Concept and the ever Lasting NATO-Russia relations*, Athens, Thessaloniki, Published by Sakkoulas A.E. (in Greek).
[25] NATO (1949), *NATO Treaty: Basic Document of the Treaty*: http://www.nato.int/docu/basictxt/treaty.htm#Art05.
[26] NATO, (2002), Prague Summit, http://www.nato.int/docu/comm/2002/0211-prague/ [assessed May 4th 2016].
[27] NATO (1999), *Operation Allied Force on Kosovo*: http://www.nato.int/issues/kosovo_air/index.html.
[28] **Brookings Institution (2009), *Afghanistan: The Taliban Resurgent and NATO*, Published by Brookings Institution, March 31 2009: http://www.brookings.edu/opinions/2006/1128globalgovernance_riedel.aspx**
[29] NATO (2001), *International Security Assistance Force (ISAF)*: http://www.nato.int/isaf/index.html.

forts, including efforts to establish a concrete strategy and policy Cyber-Defence[30].

In an emerging globalized world, where complexity may become the key characteristic in strategy and security, resilience will become an integrated part of NATOs policy orientation and application. New vulnerabilities and threats continue to emerge. Political pressure will require NATO leaders to take decisions about the organization's future. Yet all agree that NATO is a necessity. As such NATO should become more open, more adaptable and more flexible. With more burden sharing, better smart budgeting, long-term planning and operational application and continued success, NATO should continue be re-branded as an adaptive security organization, that does more to offer security and strategic alignment to truly current but also future challenges and threats, that we may not yet anticipate or think of.

In the not so long past, such similar actions reaffirmed by the Heads of States, included among others, the Treaty of London in 1990 Summit, to the 1994 Summit in Brussels, and in 1999 over its 50th year anniversary Summit in Washington, to the immediate decisions taken in 2001 after the terrorist acts in the USA[31] to its 60th anniversary, which was held in Strasbourg and Kiehl accordingly in April 2009 to the Chicago Summit of 2012 and the Wales Summit of 2014, which added value to the Alliance and Allies reaffirming NATOs long-term necessity but now also strategic resilience to multi-dimensional challenges and threats.

Vulnerabilities and threats considering multidimensional challenges require NATO to be both strategically and operationally agile. It requires NATO to be adaptable to conditions unforeseen.

Considering technological advancements, we are yet to acquaint ourselves, our institutions, governments and international organizations with true phenomena of a new, yet networked global society. In this borderless society, where, electric grids, information or installations failures may have in the past solely affect a country, now affect a region and possibly a larger area. It may also affect global financial systems and social structures. Current financial situations in regions and areas, such as in the South of Europe, like Greece, Italy and Portugal among others, affect the larger European Union as a community of union states.

The Refugee issue and the fear of mass illegal migration, deriving from current wars in Syria, Iraq and other areas such as Afghanistan, affect countries, giving rise to suspicion on cooperative effectiveness, participation in defence against

[30] Ibid 4.

[31] NATO (2001), *Information on immediate NATO reaction*: http://www.nato.int/docu/update/2001/0910/index-e.htm.

threats and challenges. Even more so, when a global society is e-wired, in which education, training, health but also security are part of this 'grid', the threats and challenges are greater.

In this new virtual world of things, where the internet has managed to eliminate, distances and borders but also time, NATO should be set to comply with the new 'global rules'. It should create agile and limitless policies, security basic and specialized military and civilian installation if NATO is to continue to be a crisis management institution.

## NATO Resilience in Crisis Management and Communication

Societal Security, an emerging phenomenon in the field of strategy and security, requires good crisis management skills but also communication effectiveness in both the real and virtual worlds. Business continuity at NATO, requires as foresaid the Alliance, to be resilient; and surely for the purposes of this research paper, the Alliance and allies to be or become cyber-resilient.

By methodological approach, societal vulnerability continues and will always continue to exist, so far and as long as threats are there. Considering the current civil need to be always preparing for a new "cold era", among others, considering the annexation by Russia of Crimea in 2014[32] and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of US and then taken over by NATO, of the Missile installation in Romania[33] and the immediate reaction and accusation of Russia in regard to these developments[34], the refugee challenges as an outcome on the constant fight against ISIS[35], but also the phenomenal changes in the financial world (ie. The Panama Papers[36]), NATO is required to become truly resilient NATO, as should also nations and leaders.

All aforementioned elements are crisis management factors. NATO provides the tools and methodologies, in which the Alliance is requested to reply to strategically and operationally. To mitigating plans for pre-crisis, during crisis and after crises situations. For and during operations, logistics of deployment or information gathering and or training purposes, among others.

---

[32] BBC, (2014), Crimea Profile, http://www.bbc.com/news/world-europe-18287223 [seen May 10 2016]
[33] Reuters, (2016), US activates Romanian Missile Defense http://www.reuters.com/article/us-nato-shield-idUSKCN0Y30JX [seen May 12 2016]
[34] New York Times, "Russia calls new US Missile Defense system a direct threat", http://www.nytimes.com/2016/05/13/world/europe/russia-nato-us-romania-missile-defense.html, [seen May 5th 2016].
[35] US Homeland Security Committee, (2015), *Syrian Refugee flows, Security Risks and Counter-Terrorism Challenges, [seen May 5 2016]*.
[36] The International Consortium of Investigative Journalists (ICJ), https://panamapapers.icij.org/ [seen May 12 2016].

In such similar cases, the legal and political perspectives also on cyber operations should be clear. The success of an operation, lays to effective logistical and operational support. Therefore the legal aspects that come with sharing of information, on how to deploy forces, identify key threats and elements in cyber-space, are important. The Internet has no borders. And threats can be easily infiltrate the national e-space and boundaries. Leaders are welcomed upon to take strong strategic-led decisions.

NATO is to ensure protection of all infrastructure. The Allies should be able to anticipate, identify, mitigate and recover from "hybrid attacks37" - the dimension(s) of simultaneous attacks, while reducing the threat of destabilization and or spreading fear.

In a civic society, it is our responsibility to ensure adequate awareness on cyber-defence and security. To learn about the necessity to protect all infrastructures, NATO's collective defense should be characterized by burden sharing, openness, flexibility and transparency in cooperation and information flow among member states. Through preparedness, strategic and operational awareness, strategic resilience can be achieved. Response time and framework will then allow NATO to counter threats as they emerge.

## Tendencies in the Cyber World

The 21st century is characterised by the use of advanced technology. By 2016, technology is merely a tool, interconnected with services provided through the internet. Our wired-society includes online services such as: banking, communications, security services, shopping, and media-services to name a few, which now take place in cyberspace. These services are by now vulnerable to cyber-attacks. As countries steadily move forward in becoming dependent on technology and wider networks, the security stakes also increase.

Current security risk assessments, consider that there is constant development of cyber-organized crimes that need to be countered. 'Cyber-crimes', are executed by organized groups. Hackers are considered illegal users that know how to get access to personal, classified or other unauthorized information by informal and unaccepted means at all levels and in all places. The use of personal, unauthorized, or private information to get access to other resources such as funds or weapons, is a crime, as is the use of the web to terrorize citizens, states, institutions or organizations.

In terms of applying these issues in military policy, through national or NATO command on cyber-defence policies, NATO or national armies, use the internet

[37] NATO Review, Hybrid War, Does it Even Exists? http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [seen May 2 2016].

and technology to protect, defend and secure governments, infrastructures and people. Therefore, the creation of a Cyber-Defence policy was in fact a necessity, and more importantly, was seen as a necessity that we clearly pointed out following the first truly organized cyber-attacks in Estonia in 2007[38].

"…NATO has now moved on to help Allies improve their cyber resilience by introducing capability targets into the NATO defense planning process and devising a new memorandum of understanding between NATO and individual Allies to establish secure connectivity and arrangements for information-sharing and crisis management…[39]".

As pointed out by NATO Review, Cyber-Resilience is a tendency for building capabilities. Fields include but not limited to network protection infrastructure, awareness and training and education, systems configuration and infrastructure protection among others[40].

The NATO's (CCDCOE) Cooperative Cyber Defense Centre of Excellence in Estonia, an outcome of the full scale cyber-attack of 2007[41], is a supportive element to NATO, through which it achieves, resilience policies and capacity building processes. Through its exercises and conferences CCDCOE raised awareness on the policy of Cyber-Defense. A recent contribution to the national framework[42] and legal elements[43] and framework for cyber-security and cyber-defense contributes towards standardization processes that will be discussed in the Warsaw Summit in July 2016. To allow for resilience in skill building of and about cyber-operators. Cyber-resilience will expand to the appropriate NATO agency, which is the NCIA agency "NATO Communication and Information Agency[44]". The NATO Agency will adapt and standardize procedures, following agreement at the Warsaw Summit of Heads of State and Government and will allow better coordination and collaboration with the market stake holders which hold the already provided infrastructure on cyber-issues and will allow for NATO to align technology global standards.

---

[38] Cyber-Policy in Estonia: http://www.nato.int/cps/en/natolive/75747.htm
[39] Ibid 3.
[40] Ibid 3.
[41] NATO Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/ [May 1st 2016].
[42] National Cyber-Security Framework, (2012) NATO Science for Peace Program, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [seen May 14 2016].
[43] CCDCOE, (2016), International Norms of Cyber-Security, https://ccdcoe.org/international-cyber-norms-analysed-new-book.html [seen May 12] 2016.
[44] NATO Communication and Information Agency (NCIA), https://www.ncia.nato.int/Pages/homepage.aspx [seen May 2nd 2016].

## NATO's Concept of Cyber-Defence

It was NATO's Military Committee decision to adopt a 'Cyber-Defence Concept'[45]. The Committee's aim was and still is to deliver business continuity and military resilience. As NATO is a provider of collective defence and as a collective organization in a globalised and currently unsafe e-world, it needs to be agile. In an environment of insecurity the Alliance' delivers 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 was delivered, so policy-makers delivered policy results on Cyber-Defence. That is why, Allied leaders during the Riga Summit of 2006 acknowledged the need to include these as is stated on its decisions at the Press Communiqué: 1) to protect NATO's operational information systems, and 2) to 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 Norfolk Virginia.

The output of the informal Meeting of the Ministers of Defence in October 2007 of NATO[46], gave way to the inauguration of NATO's Center for Excellence (COE), which at a later stage got accredited to have become the Allied Command Transformation on Cyber-Defence, named as Cooperative Cyber-Defence Centre of Excellence, CCDCOE[47]. It was based, on the Concept and early understanding of cyber-resilience for NATO's future policies in countering challenges and threats, as was 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 accordingly is led by Heads of State and Governments. This is the highest deciding political authority which decides, creates and overviews policy. It also evaluates, considers and adopts NATO's policies and activities with regards to political and military affairs or standing issues on challenges and threats, among others. Below the NAC, is NATO's Consultation Control and Command Agency (NC3A)[48] now transformed to the NCIA agency[49]and the NATO Military Authorities (NMA). The latter authority has implementation as its major task[50].

---

[45] Ibid, 4.
[46] NATO Defence Ministers Meeting (2007), *Informal Meeting of NATO Defence Ministers*: http://www.nato.int/docu/comm/2007/0710-noordwijk/0710-mod.htm.
[47] NATO (2008), *CCDCOE*, URL: from: http://www.ccdcoe.org/11.html
[48] NATO NC3A (2002), *NC3A Agency*, URL: http://www.nc3a.nato.int/Pages/Home.aspx.
[49] Ibid, 44.
[50] NATO's Cyber-Defence policy, (2008d), *Defending Against Cyber-Attacks*, Focus Areas: http://www.ccdcoe.org/37.html

The implementation of NATO's Cyber-Defence policy is considered as the second most important decision by now, once the decisions are taken by the NAC. The 'Concept of Cyber-Defence' "adds practical action programmes, to fit within the overarching policy"[51]. 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[52].

NATO's policy creation and activity is 'encouraged' by Allies. The aim is to adapt the alliance to the new strategic and security environment that is "hybrid". To engage as many as possible governments, industry related market companies and individuals. 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 and market, as to also avoid duplication of efforts and use the necessary global knowledge to achieve interoperability of force action and command also in cyber-space.

Practically, in military policy, implementation or operational areas, NATO has adopted 'three phases of practical activity and cooperation': The initial phase includes a NATO Computer Incident Response Capability (NCIRC). It was established as 'interim operating capability' for NATO to build up on both security risk and manage the element of cyber-threats. Its second phase involved an ever more realistic and pragmatic perspective that required the co-ordination of all initial 'offering' states to the attempt to establish a Cyber-Centre, (under the NATO agreement between states of a voluntary national contribution -VNC), in bringing the NCIRC to a full operational capability[53].

New policies came about. Proposed and came to effect (well-known procedure of internal NATO working process) until the adoption of 'MoU'. A so-called 'Memorandum of Understanding' was drafted and proposed to NATO, by a sponsoring state which would establish a centre for cyber-training, in this case in Estonia.

From that point on, it became an administrative decision of the Allies, that once the aforementioned stages would be put into effect, then a third phase would come into existence: Needless to say, this third phase was a complete implementation and rule based operational procedure that would soon enough bring about into existence NATO's request for technological agility and resilience, which is also yet to be finalized at the Warsaw Summit of July 2016. "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. Once the third phase was

[51] NATO (2009), *A Road Map to the Strategic Concept of NATO*: http://www.nato.int/strategic-concept/index.html
[52] NATO (2008), *NATO Defence Against Cyber Attacks*: http://www.nato.int/issues/cyber_defence/practice.html
[53] Ibid.

evaluated, the Allied Command Transformation (ACT) decided, to accredit the operational centre – in this case the Cooperative Cyber Defence (CCD) COE (Estonia), what is called as a 'Centre of Excellence'-. In turn, this resulted to the inauguration of the CCDCOE by May 2008.

## Cyber-Defence Put to the Test: The Estonian Case of 2007

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. Today the Centre of Excellence is yet to welcome more members, the latest ones to join being Greece, Turkey and Finland[54]. 2) Estonia had already been witness of modern asymmetrical hybrid warfare attacks by 2007. It is estimated that what triggered an attack from inside and outside the country's infrastructure, was the action of Estonians removing the bronze statue of a Red Army soldier, during Soviet times, from the centre of Tallinn. It was an honorary statue, honouring the dead of the Second World War. This matter sparked social outrage between Russian speaking populations. (News Scientist, 2007). It resulted to continuous cyber-attacks on Estonia's e-infrastructure, public and private, military and civilian.

By 2008, 7 Alliance countries according to the Memorandum of Understanding on the cyber-defence centre, supported Estonia to get full operational capability (Germany Italy, Latvia, Lithuania, Slovakia and Spain), which lead to an evolution period. By 2016, NATO Allies, are expected to discuss further and finalize the framework, logistics and operations, elements of cyber-resilience and procedures on the policies, when considering threats and challenges in a changing environment. NATO is yet to decide on the resilience policy, as hybrid warfare is developing, at a time when Smart Defense of NATO nations are expected to achieve the goals and aims which are to be seen by the year 2020.

The cyber-attacks in Estonia of 2007 are still today the biggest and most organized electronic attack, with a duration period of several weeks, provided NATO with a motive and multipurpose task for years to come. NATO's leadership was in fact correct in its judgment that: 1) Such an operational centre and policy was needed 2) Its operational centre would constantly be evaluating and evaluated. Would research on prospective evolutions in technology, malware and cybersecurity 3) that NATO requires resilience when considering the current or future threats and challenges.

The inauguration of its Co-operative Cyber-Defence Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, led to a mission, which holds a clear vision

[54] CCDCOE, (2016), *Greece, Turkey and Finland to join the CCDCOE*, https://ccdcoe.org/greece-turkey-and-finland-join-nato-cooperative-cyber-defence-centre-excellence.html

and statement. It is yet to be 'politically ratified' and adopted as a key core policy by Allies. 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", therefore reflecting on the key core elements to counter hybrid threats and be constantly resilience to strategic requests and needs. The vision is for the CCDCOE to become "a specialized and expertise centre for NATO in cooperative cyber-defence[55].

The domain of the cooperative cyber defense center in the framework of cooperative security within NATO, focusses in the fields of research which include:

- "Legal and Policy elements
- Concepts and Strategy
- Tactical Environment
- Critical Information Infrastructure Protection" [56]

The Centre's core policy created an outcome of research and policy-orientation, as already analysed. It was presented primarily as a first outcome, then accepted by the Supreme Commander Allied Command Transformation (SACT), deriving from a request of NATO HQ (Head Quarters) and by the North Atlantic Council (NAC) level. This included: Doctrine and Concept Development, Awareness and Training, Research and Development Analysis and Lessons learned and finally Consultation. Now we are at the stage of Heads of State agreement as policy and action reflecting key core policy of NATO resilience to counter emerging challenges. Procedure that will be discussed, negotiated and agreed upon by consensus by the Allies in Warsaw.

**NATO Approaches Issues Relevant to Cyber-Security**

For the concept of Cyber-Defence, the Centre for Excellence in Tallinn continues to portray and project NATOs need for a methodological cyber-resilience policy. If agreed, at the upcoming NATOs Warsaw Summit, Cyber-security will become NATOs core policy. It will be an integral part of Smart Defence in the hope to enhance the cooperative defence system.

The ideology and methodology behind the policy recommendations is not a new one. As example by February 6th and 7th 2009, NATO's Science for Peace and Security (SPS), sponsored a workshop. It foresighted a similar argument which we also recommend in our paper, that Cyber-security approach and cyber-defence is and should become a core policy of resilience at NATO.

[55] CCDCOE, Training Catalogue, https://ccdcoe.org/sites/default/files/documents/Training_Catalogue_2016.pdf
[56] Ibid, 41.

The workshop titled 'Operational Network Intelligence: Today and tomorrow' aimed at adaptation knowledge procedures considering the evolving and fast growing technology. Its overall purpose was "to rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber-attacks"[57]. This was the level of anticipation at the time; considering future correlation of Smart-Defence with the policy of Cyber-defence at its core.

Today, considering both the risk assessments on hybrid threats and challenges[58] but also the need for better civil awareness and readiness, at a time of much needed cooperative defence, Allies, have to decide for a robust long-term planning strategy and operations of NATO. Keeping in mind the need for strong success in field operations, including success in and at a multi-dimensional level of operations against all threats.

NATO increasingly recognizes that organized cyber-attacks seek to take advantage of 'gaps' in the 'system social and market matrix'. Therefore it should be a request from member states to examine the increasing need for co-ordination of human factors related to the issues of electronic warfare, operational network, intelligence and Cyber-Defence, whether for training, scientific exchange and or operations.

NATO is currently aiming to involve experts in e-systems, security, IT engineers, researches, officers dealing with network operations and operational centres as well as professionals and academics. Specialists in the field on both strategic and tactical levels should be systematically involved at organized levels of research, sharing, discussion and dissemination of outcomes, which will in turn enrich the abilities, capabilities and capacities of rendering current smart-defence and cyber-defence as a key and successful resilient and collaborative defence policy to NATO.

[57]NATO (2009), *SPS workshop rethinks approaches to cyber security*: http://www.nato.int/docu/update/2009/02-february/e0206a.html

[58] John R. Davis Jr. Major, (2015) Joined Warfare Center, *Continued Evolution of Hybrid Threats*, Three Sword Magazine, 28/2015, http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf [seen may 12 2016].

## Proposals

NATO's level of ambition considering a much needed resilient policy in Cyber-Defence should be decided upon the Warsaw Summit of 2016. Specialized policy against hybrid threats should be adopted. A specialized commitment of Allies to share information and simplify procedures for cooperation with cyber-companies in electronic warfare should increase.

NATO could do more at a strategic level by:

1) Sharing concrete information on security led affairs of Cyber-defence within and among member states but also with non-NATO members.
2) NATO should enhance global cooperation with non-member states in the field of electronic security and safety, as there is an increasing of cooperation level, such as the United Arab Emirates[59].
3) Allies at the upcoming Warsaw summit meeting in July 2016, should jointly agree on a robust and resilient Cyber-Defense Policy; in which CCDCOE should stand out as a tool for NCIA cooperation methodology for smart defence achievement.
4) NATO should hold a clear budget on smart defence, based on the technological necessities that allow lower but shared budgets for the long-term and a policy of cyber-defence that looks operationally viable and globally market-oriented.
5) NATO should reach out for interoperability levels for NATO forces 2020 Smart Defense standards as well for Cyber-Defense.
6) Through joined co-operation at the level of electronic-warfare prevention, detection and reaction to attacks towards member allied states, the duplication of efforts by nations can be avoided.
7) Legally, cyber-resilience can be achieved through clarification of what constitutes an e-crime or e-terrorist attack. It should be clarified if not yet done so and adopted not only by Allies but proposed at the level of the United Nations for universal adaptation.
8) The capability or capacity for NATO to operate at an e-world should be clarified. Under which conditions and under which crisis situations and most importantly with what tools and infrastructures.

It is crucial for NATO to achieve interoperability of force command and structures through a methodological application.

Tactically, NATO needs to do the following:

[59]NATO and the UAE determined to enhance cooperation, (March 2016), http://www.nato.int/cps/en/natohq/news_128753.htm , [seen May 10th 2016].

1. Adopt a operational policy procedure reflecting hybrid threats in a Cyber-environment.
2. Tactically align new policies with regulatory agreements based on NATO regulatory and strategic rules, relating to defence clauses and rules of engagement.
3. An assessment on future warfare should be considered and agreed upon.
4. A foresight agency which provides prime information on constantly evolving technology, robotics and smart attackers should be created.
5. As NATO holds a joined center for warfare so should NATO be proposed to have a cyber-resilient military operational command and control centre on electronic warfare it will apply current rules and regulations, consult the CCDCOE, and provide a time action plan for a hybrid threat assessment accreditation on Cyber-NATO standards.
6. NATO should allow for alliance progress through resilience on all operational levels which involve the creation of interoperable cybernetic command structure and technologically agile forces for all levels of 'analogical and digital' engagement of forces in electronic warfare.
7. NATO should enhance its national protection plan of major infrastructure through a complete and jointly by consensus agreed cooperation of national states.
8. NATO base infrastructures, should be resilient and be constantly ready-protected from possible fraudulent attacks.

## Conclusion

In conclusion, the main aim of this paper was to project the importance of cyber-resilience at a time of NATOs strategic evaluation. The aim was to methodologically approach how to integrate NATOs collective defense, through cyber-defense policy, to the 21st challenges and threats.

In anticipating the outcomes of the upcoming Warsaw summit meeting in July 2016, NATOs resilience policy, if adopted to become an integral part in cyber-defense as well, will constitute a methodological and strategic step forward for NATO. NATO's smart defense and collective defense overall will have to be reexamined to meet the high expected standards of security. It will create a new standardized form of procedures, adaptable to the reality of risk hybrid assessments and threats as analyzed in the paper. NATO will be able to afford flexible strategic and operational forces agile and technologically advanced.

The creation of a concept and later policy of Cyber-Defense, the inauguration of the Centre of Excellence for Cyber-Defence in Tallinn Estonia, provided an early

impetus for future operations but also administrative and operational upgrading in the field of today's smart defence policy a result of the renewed strategic concept.

Cyber-defense is a policy within the framework of NATO. Yet is not a key core policy just yet until the final results of the Warsaw Summit meeting.

This article aimed to show why cyber-defence should become a core policy for resilience at NATO. The article conceptualized from a strategic and policy concentration. It analyzed the policy of smart-defence, cooperative defense, cyber-security, hybrid threats and crisis management and communication among others. It examined strategically overviewing current past current and future events to come. It assessed and concluded that there is a growing necessity for constant protection against current of future challenges and threats which are now multidimensional and as such NATO should be adaptable at all times.

The policy of Cyber-Defence through the prism of Smart Defence allows for a truly and united allied effective engagement; an engagement that should be operationally resilient in military operating environments at all levels. On the way to adapt to the cyber-realities of the internet of all things, NATO should adopt a legal and political framework, a tactical and operational framework in a methodological easily adaptable way that competes the current and future as we referred to hybrid challenges and threats. Any decision made at the level of Heads of State and Government should include the legal element of operation. As Cyber-threats are borderless so should NATO work as an operational and capacity building organization that does more to provide effective crisis management solutions through a wide-range of nations cooperations which are NATO and non-NATO members, when national and supranational security of allies is or may be compromised.

This paper provided the reader with updated information on Cyber-Defense policy, Smart Defense and NATOs expectations for a resilient strategy and made a number of policy recommendations for both strategic and tactical considerations on future capacity management building, administrative decision-training and making, limiting fiscal costs, levelling operational methods in cyber-defense in current or future networked operations.

## References


- NATO's Smart Defense policy: Smart Defence is a cooperative way of thinking about generating the modern defence capabilities that the Alliance needs for the future

http://www.nato.int/cps/en/natohq/topics_84268.htm [seen on April 26th 2016].

- NATO Warsaw Summit 8 & 9 July 2016: http://www.msz.gov.pl/en/foreign_policy/nato_2016/ [seen on April 22nd 2016].

- NATO Review, NATO Defense and Cyber-Resilience http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/ [assessed April 230th 2016].

- Efthymiopulos Marios P (2013), in (Carayannis et all), *NATO's Cyber-Security Policy*, Chapter in Cyber-Development, Cyber-Democracy and Cyber-Defense, London, New York Published by Springer.

- Franklin D. Kramer, Hans Binnendijk, and Daniel S. Hamilton, (2016), NATO's New Strategy: Stability Generation, Washington D.C., Published by the Atlantic Council of the USA, Brent Scrowcroft Center on International Security.

- Efthymiopoulos, M. P., (2008), JIW Vol. 8, Issue 3, (Journal of Information Warfare), *NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defense and the Alliance New Strategic Concept*, Australia, http://www.jinfowar.com/.

- NATO's Cyber-Defense Policy (2011), http://www.nato.int/cps/en/natolive/topics_78170.htm.

- NATO Cyber-Defence Centre for Excellence, https://www.ccdcoe.org/.

- Hughes. R. B. (2009) Atlantisch Perspectief,.Ap:2009 Nr. 1/4, *NATO and Cyber-Defense: Mission Accomplished, Netherlands, Netherlands Atlantic Committee.*

- Sendmeyer S. A. (Maj), (2010) August, *NATO Strategy & Out-of-Area Operations*, School of Advanced Military Studies, US Army Command & General Staff College, http://www.hsdl.org/?view&did=713508.

- NATO (2008), *Briefing on Transforming Allied Forces for Current and Future Operations*, NATO Public Diplomacy Division, Brussels.

- Scheherazade Rehman, (2013) January, *Estonia's Lessons in Cyber Warfare, US News*, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare.

- NATO Chicago Summit: http://www.chicagonato.org/ May 20 & 21 2012.

- Wales Summit 4 September 2014, http://www.nato.int/cps/en/natohq/events_112136.htm [seen May 1st 2016].

- Chicago Council on Global Affairs, (2012), Conference: *Smart Defence and the Future of NATO, Can the Alliance Meet the Challenges of the 21st Century*, March 28-30 2012 Chicago Illinois, USA.

- NATO, (2016), *Operations and Missions: Past and Present, http://www.nato.int/cps/en/natohq/topics_52060.htm [seen May 4t] 2016.*

- Efthymiopoulos, M. P. (2008), *NATO in the 21st century: The need for a renewed Strategic Concept and the ever Lasting NATO-Russia relations*, Athens, Thessaloniki, Published by Sakkoulas A.E. (in Greek).

- NATO (1949), *NATO Treaty: Basic Document of the Treaty*: http://www.nato.int/docu/basictxt/treaty.htm#Art05.

- NATO, (2002), Prague Summit, http://www.nato.int/docu/comm/2002/0211-prague/ [assessed May 4th 2016].

  NATO (1999), *Operation Allied Force on Kosovo*: http://www.nato.int/issues/kosovo_air/index.html.

- Brookings Institution (2009), Afghanistan: The Taliban Resurgent and NATO, Published by Brookings Institution, March 31 2009: http://www.brookings.edu/opinions/2006/1128globalgovernance_riedel.aspx

- NATO (2001), *International Security Assistance Force (ISAF)*: http://www.nato.int/isaf/index.html.

- NATO (2001), *Information on immediate NATO reaction*: http://www.nato.int/docu/update/2001/0910/index-e.htm.

- BBC, (2014), Crimea Profile, http://www.bbc.com/news/world-europe-18287223 [seen May 10 2016].

- Reuters, (2016), US activates Romanian Missile Defense http://www.reuters.com/article/us-nato-shield-idUSKCN0Y30JX [seen May 12 2016].

- New York Times, "Russia calls new US Missile Defense system a direct threat", http://www.nytimes.com/2016/05/13/world/europe/russia-nato-us-romania-missile-defense.html, [seen May 5th 2016].

- US Homeland Security Committee, (2015), *Syrian Refugee flows, Security Risks and Counter-Terrorism Challenges, https://homeland.house.gov/wpcontent/uploads/2015/11/HomelandSecurityCommittee_Syrian_Refugee_Report.pdf [seen May 5 2016]*.

- The International Consortium of Investigative Journalists (ICJ), https://panamapapers.icij.org/ [seen May 12 2016].

- NATO Review, Hybrid War, Does it Even Exists? http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [seen May 2 2016].

- Cyber-Policy in Estonia: http://www.nato.int/cps/en/natolive/75747.htm.

- NATO Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/ [May 1st 2016].

- National Cyber-Security Framework, (2012) NATO Science for Peace Program, https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf [seen May 14 2016].

- CCDCOE, (2016), International Norms of Cyber-Security, https://ccdcoe.org/international-cyber-norms-analysed-new-book.html [seen May 12] 2016.

- NATO Communication and Information Agency (NCIA), https://www.ncia.nato.int/Pages/homepage.aspx [seen May 2nd 2016].

- NATO Defence Ministers Meeting (2007), *Informal Meeting of NATO Defence Ministers*: http://www.nato.int/docu/comm/2007/0710-noordwijk/0710-mod.htm.

- NATO (2008), *CCDCOE*, URL: from: http://www.ccdcoe.org/11.html.

- NATO NC3A (2002), *NC3A Agency*, URL: http://www.nc3a.nato.int/Pages/Home.aspx.

- NATO's Cyber-Defence policy, (2008d), *Defending against cyber-attacks*, Focus Areas: http://www.ccdcoe.org/37.html.

- NATO (2009), *A Road Map to the Strategic Concept of NATO*: http://www.nato.int/strategic-concept/index.html.

- NATO (2008), *NATO Defence Against Cyber Attacks*: http://www.nato.int/issues/cyber_defence/practice.html.

- CCDCOE, (2016), Greece, Turkey and Finland to join the CCDCOE, https://ccdcoe.org/greece-turkey-and-finland-join-nato-cooperative-cyber-defence-centre-excellence.html.

- CCDCOE, Training Catalogue, https://ccdcoe.org/sites/default/files/documents/Training_Catalogue_2016.pdf.

- NATO (2009), *SPS workshop rethinks approaches to cyber security*: http://www.nato.int/docu/update/2009/02-february/e0206a.html.

- John R. Davis Jr. Major, (2015) Joined Warfare Center, "Continued Evolution of Hybrid Threats", Three Sword Magazine, 28/2015, http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf [seen may 12 2016].