Efthymiopoulos *Journal of Innovation and Entrepreneurship* (2019) 8:12
https://doi.org/10.1186/s13731-019-0105-z

Journal of Innovation and Entrepreneurship

RESEARCH Open Access

A cyber-security framework for development, defense and innovation at NATO

Marios Panagiotis Efthymiopoulos[1,2]

Correspondence:
mefthymiopoulos@uclan.ac.uk;
Marios.efthymiopoulos@strategyinternational.org
[1]Senior Visiting Fellow, Law School UCLan Cyprus, Pyla-Larnaka, Cyprus
[2]Strategy International, Larnaka, Cyprus

Abstract

The article is of strategic nature. It projects the importance of cyber-security as policy, while reflecting the need for enhancing constantly NATO's (North Atlantic Treaty Organization) cyber-dimensional strategy, management, and operations. There is a policy need for constant innovation and entrepreneurship in security, one that reflects also NATO's practical needs; its security resilience and business continuity. At a time of strategic challenges and policy recommendations, the production of this article is timely. It examines NATOs Heads of States and Governments decision of the Brussels Summit meeting on Cyber Security that was held in July 2018. The article proposes a framework of strategic re-alignment, with a stronger eye toward practical innovation and entrepreneurship; practicality in operational management, while enhancing political cooperation and tactical/strategic preparation for field operations. The aim, design, and setting of this article explicitly and methodologically evaluates NATO's security and cyber-security options to come for the near future. The article integrates and proposes a new design for a new format of collective defense. The article considers cyber-defense as key tool for current and future operational and network centric operations. The article enables us to comprehend better the Alliance' global and regional needs the framework of current and future defense, requesting at the same time for a holistic approach to innovation and entrepreneurship, while new geostrategic and geo-economic challenges emerge.

Keywords: Strategy, Cyber-security, Innovation, Entrepreneurship, Management, Business resilience, Collective defense, Military, Network-centric operations, NATO

Introduction

Cyber-security is a method of e-protection. It is a framework policy of and for defense when reflective to a political-military alliance such as NATO (North Atlantic Treaty Organization). At the level of the NATO alliance, cyber-security is adopted and adapted as central policy by the Heads of States and Governments, representing members of the Alliance. Private institutions/organizations that are leaders in creativity, innovation, and entrepreneurship in cyber-security and defense work along with NATO to create a resilient and robust protection mechanism against electronic threats.

At the level of NATO, cyber-security has become an institutional policy. It reflects elements of security and safety in the virtual world of the internet. It is a procedure. It follows the rule that both individuals and collectives should be protected from malware attacks. Security and safety includes hardware and software protection.

When cyber-security is assessed from the point of view of academic discipline and sciences of security studies and political affairs, cyber-security is defined as a policy framework, a methodology, orientation, and application for all matters relative to the world of the internet when interconnected.

Cyber-security is a discipline of science. It is an interdisciplinary science between IT and other leading sciences from security to business, entrepreneurship, and law, among others. Practically, it defines government and countries' strategic approach on any possible threat while being defensive in nature, through uses of technology and software, while also advanced development tools.

The article is of strategic nature. It projects the importance of cyber-security as policy, while reflecting the need for constantly enhanced methods for NATO's cyber-dimensional operations. Elements and variables related to cyber-security and the necessity to lean toward a grander cyber-security strategy are put forward for consideration. Outcomes and proposals transmit the message for a greater need to hold a joined cyber-security approach, a methodological approach to protect current and future alliance military and civilian infrastructures.

Traditional security affairs require agility and resilience and as such, also at the level of cyber-security and defense. Cyber-security is defined as a method of protectionism from external threats. Cyber-security is an e-dimensional effort to protect infrastructure, of both software and hardware that is "wired" to the world of the internet and therefore our businesses, our governments, and the institutions/organizations that our governments take part in.

Constant research and development (R&D) methods in the fields of electronics, technology, and cyber-security ensure agility and resilience and ensure protection of our lives, making our lives easier and more affordable.

Characteristics of cyber-Security

Cyber-security is a strategy of both preventive and/or pre-emptive action. It allows for technological growth and advancement; it also allows for innovation and entrepreneurship. It introduces us to a new virtual reality that we created and are standing at: the worldwide web, its methods and opportunities, is by now an integrated part of our lives. All elements that we are working with or at professionally or privately at some given time rely or depend on technological advancements that make our life easier and at the same time more complicated while we are in need for constant and enhanced cyber-security protection of our data and also virtual way of life.

Strategically, constant security resilience is of essence. Security as policy is a protection method. Among others, it reflects government policies. In the virtual world, through cyber-security, democracy, development, sustainability, and growth, innovation and entrepreneurship can take place.

Cyber-security is both a strategy and operational framework, a field of operational capacity, an element of cross-disciplinary and trans-disciplinary approach that is fit to all levels of socio-political, economic, engineering, IT, legal, and security-led levels of theoretical approach and practicability uses and issues.

A cyber-security strategy is holistically and politically business oriented; it is entrepreneurial and innovative. Cyber-security in the field of defense is a continued struggle for technological methods of defense development, growth, innovation, democracy, and continuity toward the convergence of a society that is very much depended on technology.

Resilience in cyber-security is reflected in multiple fields. As long as there is a cooperative or global cyber-security strategy. The necessity for a joined cooperative strategic and operational capacity needs to be displayed and pointed out. Safeguarding and enhancing methods and tools of protection against malicious attacks that may involve one or more countries, institutions, businesses, or agencies.

An alliance cyber-security becomes a policy framework for technological continuity, a multinational aspect of cooperative approach that enhances elements of pluralism of Democracy; it will help boost interconnectedness and will boost security efforts to meet all security threats symmetrical and asymmetrical.

National securities and defense strategies rely solely on national cyber-security protection policies and application methods; how cooperation can and will be achieved; information agility and technological advance mechanisms; considering the multidimensional level of threats and challenges. Yet risk analyses and threat analyses are to this extend considered only as national. The article proposes for a joined cooperative approach on Grand Cyber-Security Strategy. A strategy that at an age of interconnectedness and operational creativity will provide an efficient political and military framework to work on, a legal framework that will in turn allow for operational deliverables through a cyber-security command such like the new cyber-security center in Mons Belgium, a decision-taken by Heads of States and Governments, at the recent Brussels NATO Summit of July 2018.

Setting the stage

Cyber-security is yet to be globally, legally, operationally, and strategically defined. The scale of a security perspective is more attractive at this time considering the geostrategic challenges and threats. The possibility of innovation and entrepreneurship in the field is also a tangible reality, due to the necessary research and development methods. More so, the possibility of an open market economy sharing of knowledge and technological skills makes security and cyber-security or defense for that matter more attractive. What lacks in the world wide legal and political framework of operations, exchange of information and protectiveness from new sources or methods that can be deemed as elements of infiltration.

The article's aim is to examine and recommend a global strategic framework for operational capacity and management resilience between allied and cooperative partners in the field of cyber-security. The current article is a follow up of prior scientific publications made in 2014 first and later in 2018, on NATO's cyber-security strategy, presented through a framework of Cyber-Development, Cyber-Democracy, and Cyber-Defense (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018). The aim is to converge diversified information on cyber-security, in a single strategic framework; reflect to the actual practical needs in understanding operations and tactical ability to deliver in multi-complex and dimensional world through management and operational efficiency capabilities. The article requests interoperability of aims and objectives under a global framework of cyber-security; through a strategic framework on cyber-security, global law can be proposed, defined, and adopted by the international community. The strategic framework will define structures that are needed to be put in place on a global scale, when reflecting issues of cyber-security and inclusive for NATO. It will define threats and challenges, as cyber-attacks are real. Cyber-security is not an asymmetrical or hybrid threat, but an existential one. Its destructive capacity can be multi-leveled and can also lead to human casualties. The future of e-safety lays at both a global estimation framework of what constitutes cyber-security and how we react to it; it lays in between cooperation of allies and members of wider alliances, against specified or approximate threats. Yet, its framework of aims and objectives, management, command and control, and operations will be defined and decided by allied parties only such as is the case of NATO.

Operationally, national and cooperative forces need to be continuously agile and technologically advanced. In an asymmetrical world, which is complete with unforeseen challenges and threats, we need forces with flexibility, adaptability, operational and strategic command structure, based on high technologically sophisticated information “coming in,” but also being used while in training or through active operations.

On a theoretical scale, the current article requests a cyber-security strategic framework adoption of resilient adaptability and interoperability policy in the framework of safety and defense. The article considers that understanding the realities of threats is by definition a natural innovation and as we move ahead, we structure and operate a single strategy on cyber-security against a virtual threat from wherever it comes from. Its long-term resilience may be more complex as operational capacity needs to constantly develop and adapt into the convergence of societal structures, and methods; where socio-economic, technological, defense even health, and education issues are affected.

When theory on cyber-security, resilience, and operational capacity will be applied at NATOs level, it will enable allies and members, jointly, to create a true policy and strategy for cyber-security resilience against hybrid virtual threats. The methodology on how to is presented through this current article.

The article’s design is based on cross-disciplinary and interdisciplinary approaches. It combines elements of global security and strategy, national and international law, economic development, and technological research and advancement and most importantly is innovative and entrepreneurial; its understanding will enable us to comprehend global and regional market establishment and convergence, as also economic changes.

The setting of the study required lapse of time to showcase the need and the necessity of the subject. Current output reflects a set of written analyses, rules, and primary experiences. It methodologically acquired sources of information of related necessity and relevance, shaped the understanding, and need to point out for a framework of rules, regulations, management, and operations on cyber-security.

The article and its author frames a specific policy recommendation with regards to the creation of not only a regional alliance (NATO-based scale), Cyber-Security Strategy for the twenty-first century but a global one. The article defines the “dynamism” of cyber-security both as a topic and subject. Cyber-security is a twenty-first century element of policy orientation; a necessity for both collective and individual defense and security resilience.

In specific, a cyber-security strategy for NATO will enhance its innovation and creativity core of operations and methodologies against any kind of virtual threats. It will set standards, policy procedures, and recommendations. NATO's strategy of cyber-security through its new Cyberspace Operations Centre, in Mons (Belgium) as decided in the Brussels Summit of July 2018 (Cyber-Space Operations Center Mons Belgium, 2018) unfolds options and opportunities, innovation, and entrepreneurship in operations efficiency and capabilities application. Current technological advancements and dynamisms through innovation and sustainable futuristic advancement will soon be evident.

Considering the strategic need for cyber-resilience, the current article's characteristic outlines the necessity of a joined strategic positioning of the "willing." It proposes an innovative tactical and operational military and civilian capacity building approach, based on scale of economic and business-led standards, relative similar of alliance standardization, and preparedness agreements. It is a smart-leveled security policy orientation. It will benefit those that seek peaceful cooperation in a digitized and inter-connected world. It applies for those that seek a balanced relationship.

The current article provides a strategic insight information, knowledge, and options for an "ecumenical scale -within the NATO level- cyber-security and defense policy strategy." Reflecting the current and future period of technological agility and advancement as a method also of foresighting or predicting future requirements from strong support and strong defense of the individual and nation infrastructure.

This is an important subject of research with a great and practical impact factor. A recent research-based evaluation on an alliance of nations was put forward bringing international security organizations such as NATO to the forefront of innovation and business-led attention due to the effective creativity on cyber-resilience and specialization; a necessary framework of a possible creation of a global-scale global strategy on cyber-security (Efthymiopoulos, 2013), which however requires a clear understanding of checks and balances between allies and competitors. Considering earlier outcomes of the research, we now value the necessity of cyber-security through strong allies such as at the level of NATO solely, through institutional alignment, in operational security and defense capabilities as was finalized and is yet to be projected in practice in the years to come following the NATO Brussels summit meeting of Heads of States and Government in July 2018.

The issues presented hence forth should give time to the reader to examine, reflect, and comprehend the importance of the subject. This article adds value. It reflects the current status of affairs at NATO and values them as important for future led-operations. Current data presented are based on open sources. Needless to say, this article does not hold any competing interests. The research made for the creation of this article is solely funded and researched by the author for the benefit of specialized research on NATO and cyber-security-led strategic issues. This article is examined, analyzed, and created by the contributor, who is also the sole author. This article puts forward proposals for decision-makers to reflect on a specialized topic, in which the allies seek solutions for a strong viable alliance strategy in cyber-security, reflective to the next steps to be followed following the Brussels Summit of July 2018.

Resilience as methodology: NATO's strategic aim

Resilience is a method. A dedication to the goal. It is therefore an aim. Terminologically is announced in security-led strategies yet also business-led strategies. It holds a completely sound operational aim. To deliver and stick to the requested. It is brand name that defines strategy through which it results to operational capacity that sustains and grows; at the level of NATO, with the capacity to apply in diverse fields of operations adding value, to an already robust policy decision and operational capacity building and actions; at the level of cyber-security policy resilience to the framework is a "strong-hold" policy to deliver a protection mechanism and method.

Resilience's framework acknowledges the will for preparedness so as to counter a possible integrative part of possible emerging crises. It is seen as an innovative strategic management policy procedure and tool. Strategically, it applies to operational capacity building, both civil and military. It is an element of acknowledged standardization of procedures. In the defense sector, when forces are deployed, they need flexible and effective means of countering threats; while in the field of cyber-security, they need agility in operational network centric operations, and constant accurate flow of information.

Strategic resilience in cyber-security requires flexible adaptability to new challenges. Its strategic resilience works as a tool for closeness, mitigation, and/or negotiation; it allows for cooperation among allies or members.

NATO's vigilance and resilience in security-led affairs including cyber-security defines strategic plans and re-assesses risks that will allow us to think entrepreneurial and innovative. For NATO members, Heads of State, and Governments, cyber-security creates a modern administrative and operational format and framework of the alliance at a virtual level that is flexible and e-oriented, reflective to the market needs for security and stability, while augmenting market e-innovation and while adapting to new affordable methods of economic and socio-economic growth. NATO acquires protection mechanisms while its operations and memberships enlarge while operational challenges are upgraded and updated. NATO needs to provide militarily and technologically agile and interoperable forces with added value, through civilian capabilities (NATO's Cyber-Defense Policy, 2011).

Resilience in security-led affairs through innovation and entrepreneurship therefore should be a leveled adaptation process for NATO; a phase to consequently strategize and draw new scenarios for cyber-security among others. This comes through operational result processes of training and experiences, when countered in an effective manner with lessons to be learned constantly in adaptable new circumstances against any forms of cyber-attacks.

Resilience becomes thus a policy orientation for NATO's "Smart Defense" clause. NATO boosts on military innovation and methods of operational support and deliverables and protection mechanisms, while remaining relevant as a political military organization, a regional and global asset value to security and strategy application at a time of vast changes and challenges.

NATO's Smart Defense in security and more so in cyber-security should therefore be resilient, innovative entrepreneurial. It should ensure stability, sustainability and growth, economic, and political. The Atlantic Council of the USA (ACUS) refers to "stability generation" policy (Kramer et al., 2016), adding that NATOs' 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.

In turn, a resilient smart defense in cyber-security 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 and now a center for cyber-security established for e-security led operations, NATO will be able to secure its virtual space, secure and protect its infrastructures, and provide defense and cooperation.

Due to the importance of a resilient policy to collective defense, cyber-defense as policy is now becoming 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 Review, 2016).

NATO's cyber-resilience method

"Future war-like operations will be held in a far more complicated level of military operations" (Efthymiopoulos, 2008a). 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… (Kramer et al., 2016)".

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-defense, 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 twenty-first 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, hybrid or non-hybrid. At the level of cyber-security and cyber-resilience and preparedness, scenarios, of possible attacks and battles, can be anticipated. Along the lines of the new cyber-space operations center, NATO should prepare operational methods for action, whether this is for defense or cooperation for cyber-space.

The use and necessity today of technology is limitless. So is the virtual world of defense and security, where technology and cyber-defense merge. These are the tools for action. Technology plays a key role in a global reach. Yet so does NATO, through the framework of a limitless technology applied in military operations. NATO uses technology to train, prepare, ready, deploy, and operate its forces. Technology for NATO works as tools with which the Alliance protects and defend, yet also is capable to counter-assault, with counter-measures where and when is needed, required, or decided.

Since the adoption of the NATO Cyber-Defense policy (NATO's Cyber-Defense Policy, 2011), NATO trains its military and civilian assets for possible action against possible threats. NATO is constantly training its forces in cyber defense 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 NATO Cyber-Defense Centre for Excellence (CCDCOE) (NATO, n.d.) and now through the Cyberspace Operations center in Mons Belgium. Training and exercises are now anticipated to expand and enlarge. So are multinational operations held through remote areas and locations. NATO is now to get more engaged in the field of cyber-defense, 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 (Hughes, 2009).

NATO Missions, "will continue to require agile and interoperable, well-trained and well-led military forces" (Carayannis, Campbell & Efthymiopoulos, 2014). This new technological and operational environment through cyber-defense 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. On-going 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, the "online" security protection initiative against all possibly known threats.

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

As previously noted, cyber-security capabilities in a smart and resilient way is the "operational goal." NATO members prepare well and also at joint levels. NATO's Smart Defense,[1] a policy framework for defensive tactical advice and operations, used to be the method that among others branded the need for a cyber-security policy. A cyber-resilience of NATO, which was adopted during the Warsaw Summit in July 2016 and reflective to the July NATO summit in 2018, expects allies to take continued actions through standardized procedures of protection effectiveness and also innovative openness and entrepreneurial attraction through NATOs respective institutions, centers of excellence, agencies, and its new cyberspace operations center that is to be inaugurated in Mons Belgium.

What is well known through policy analysis is that NATO military forces should reach to appropriate operational and tactical levels, so as to operate in and around "article and non-article 5 operations" (Sendmeyer, 2010)—meaning not only defensive-clause operations but also in counter-offensive operations (NATO, 2008b). Cyber-protection and cyber-security methods are needed, when defense of allies is associated with possible threats or challenges such as the one of ISIS.

NATO cyber-security 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 (Rehman, 2013). Past events in Estonia showed early on a strong smart cyber-defense "umbrella" which is certainly still needed by 2018, in which agility and resilience needs to be achieved.

There is a need of a resilient cyber-security strategic policy, a methodological and operational approach for a continuously standardized practical operational preparedness so as to constantly be able to counter cyber-attacks of hybrid or non-hybrid nature. Innovative methodology and ideologies are needed to process such a policy approach. There is a need for clear innovation and entrepreneurial understanding of what constitutes cooperation in cyber-security efficiency knowledge acquiring information and cooperation between public-private institutions and agencies.

A strategic cyber-security policy when applied will allow for the 30 member states to counter with more agile ways any emerging crises. This will efficiently manage processes and purposes for operations against any methods of electronic warfare. Interoperability of forces for joint use in cyber-defense is expected to be achieved through an adaptability and standardization process period. NATO should "e-volve" as should Alliance "e-networked" States. NATO should innovate and manage. NATO should administer change on methods of smart resilience in defense through cyber-security policy, strategically and operationally.

Cyber-resilience in cooperative "smart and innovative" security and defense

During the Chicago Summit in 2012, NATOs' policy on "Smart Defense (NATO Chicago Summit, 2012)" was presented in which "…NATO leaders agreed to embrace Smart Defense to ensure that the Alliance can develop, acquire and maintain the capabilities required to achieve the goals of 'NATO Forces 2020… (Carayannis, Campbell & Efthymiopoulos, 2014; Carayannis, Campbell & Efthymiopoulos, 2018)." Following this, during the Wales summit in 2014 (Wales Summit, 2014), 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-defense. The NATO summit in Warsaw in July 2016 exposed the policy or resilience and cyber-resilience in the framework of cooperative defense.

During the year 2018, there was a new security cultural security comprehension; it is considered as multi-leveled and multi-dimensional. In 2018's NATO summit of July, allies evaluated current developments in cyber-security considering challenges, threats, but also opportunities. Evaluated current strategic and geopolitical challenges. They upheld methodological preparedness for network defense and operations and declared under the new NATO command structural reform the setting up of a cyberspace operations center, as part of the adapted command structure. Allies now request for more awareness and openness, innovation methods, and capacity building in cyber-security, considering changes in the market economy, more tangible and operational capacity building through R&D companies. Any decision, considering the changing nature of security and strategic market, should be "business-led" innovative-led, promoting sustainability and growth, market methods to uphold NATO's relevance, while keeping the public informed. The public is keen on understanding the operational usefulness of the alliance, at a time of inside and outside NATO members' landscape threats and challenges.

Defense capacity building for the twentieth century requires a modern way of thinking. It is about encouraging cooperative defense 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. Twenty-first century needs and challenges require agility and compatibility of forces and force command at all levels, including network-centric operations and defense.

NATO forces, force command, technology, and methodological approach in military elements and standards cannot be or remain static. They need to technologically advance, progress methodologically innovate, to accommodate for the increasing need for multi-dimensional ways of security and defense. NATO needs to have interoperable, capable, and well-equipped technologically agile forces considering innovation and entrepreneurial thinking in a period of technological advance.

Planning and budgeting for operations needs to be "smart." Directed funds should now, at a period of specialized or tailored fiscal management, through innovative methods, in which capacity methods will be build. Planning should be effectively applied for practical yet innovative reasons: this includes where operational viability and visibility of forces capacity deliverables that are realized; on a minimum budget level with equalized costs, and enhanced technology and minimum engagement with regards to both time and operations.

Throughout the attempt to achieve a truly cooperative defense, "Smart Defense" stands out on renewing operational and tactical effectiveness; an innovation and business-led orientation for political, tactical, and operational alliance and coordination. It is all about specialization of forces including the element of resilience of forces mainly through technological agility.

Smart defense is prioritized as a method of innovative approach. Reflective toward efficiency and efficacy. Needs to meet NATO forces command and structure as attributed for force resilience 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 defense, through collective efforts; (5) burden sharing; and (6) technological advancements, considering the threats and challenges of the twenty-first century.

2018 was a year of much needed strategic and tactical resilience; smart defense stands out as a request for geo-political capability and capacity building, so as to implement operational preparedness and effectiveness, reflective in operations both on a regional and global scale of operations.

In 2019, the security environment seems politically and militarily hybrid, symmetrical but also asymmetrical, where the cost of human capital is limited, through the optimum use of technology provided. Duplication of operational efforts is limited yet the challenges are still reflective to the volatility of the security environment and threats that we live at.

Member states hold constant joint operational strategic centers of training and operations; on and about among others, ballistic missile defense, intelligence, surveillance, reconnaissance, cyber-defense and security, maintenance of readiness, training and force preparation but also agile deployment bases for effective engagement and now in cyber-security. All aforementioned should be expected to continue work with minimum cost, namely human casualties yet delivering high level of technology operational efficiency and constant preparedness that is both beneficial and practical and of tactical need to succeed against hybrid threats.

Smart defense and more so in the field of cyber-security is NATOs main priority policy. It does however reflect as well on to the tools and mechanisms used to innovated in and for management operations, processes, and tactics. It allows for defense entrepreneurial thinking and application. Constant changes in strategy and policy do request efficient leadership and management skills to operate. And so, should NATO's cyber-resilience strategic policy.

Through a methodological period, such as in the NATO Summit in Brussels of July 2018, NATO will now have to show an enhanced progress report within the second quarter of 2019, assuring current and future abilities also in cyber-security, to counter current and emerging challenges in cyber-space. Defense planning, operations, and lessons learned are therefore a continued process that allows the evolution of NATOs capabilities which always need to be taken into account and more so in the field of cyber-security where the Cyberspace Operations Center will play a key role into it.

Resilience through smart and cooperative innovative defense requires NATOs policy on Cyber-defense to be also effective. As said, it requires decision-making and leadership in this policy context. In the framework of cyber-defense, NATO needs to align supranationalized national capability priorities and standardize processes, 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 leveled agreements need to come forth; NATO should produce a cost-effective projection planning and application for all operational exercise theaters reflecting the real yet also virtual worlds.

Cyber-resilience and methodological specialization through leaders' policy decisions at the level of Heads of States and Governments 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 defense with cyber-resilience: "engagement through policy adaptation"

As fiscal austerity measures are applied and cutbacks are in effect, according to the Chicago Council on Global Affairs, NATO allies have to decide on methods to approach NATOs political agenda decisions. Allies must enhance capacities and capabilities to implement new and innovative methods of tactical management for the benefit of security toward the Alliance space (Chicago Council on Global Affairs, 2012). According to the Atlantic Council, "…The Alliance, given its new strategic landscape, 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 (NATO's Cyber-Defense Policy, 2011)".

Heads of States and Governments do listen and observe, but are not keen in stepping in the extra mile; to therefore consult and call on NATO to hold Summit meetings, to negotiate or mitigate current issues, and to elaborate and concentrate more on economic, political, military and management innovation and efficiency of administrative cooperation in all policy regulated fields of NATO.

A strategic framework policy on "Smart Defense," which is yet to be achieved by 2020, may render a cheaper cost for the total sharing of burden by member states, while attracting more elements or variables where technology can be used to minimize costs. Surely, not all members share the same burden to this day by are reflective to all countries security defenses when it comes to cyberspace.

While a policy on smart defense lowers overall long-term cost, and if burden sharing is actually increased but equaled to lower levels of fiscal sharing, long-term results will show, that in fact, less cost will be achieved and cyber-innovative methods can help mitigate possible costs.

While cyber-security becomes a core, NATO policy for smart defense and resilience attracts attention to stake holders. Through evolving and constant communication and marketing perspectives, social media and workshops, and conferences, cyber-defense 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-security then 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-security 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 defense is being upgraded and developed, cyber-defense "…not a conception but a real-politic issue… (Efthymiopoulos, 2008b)", 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 innovative unity among states (political) yet also business continuity (strategic orientation) about the future of NATO (The entrepreneurial and managerial side of things).

NATO's strategic approach post Warsaw and Brussels of 2017 and 2018 Summits is estimated to reflect a much need realistic plan of operations and engagement in the field of cyber-security and defense. NATO should continue to be 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-security and technological progress within NATO are synonymous. They can therefore be seen as the core of collaboration on smart defense, to be finalized and achieved by 2020 standards. Cyber-security being technologically advanced is resilient to changes and is innovative as a method as it was never been done before at NATO until the date that it was presented to. It does provide adaptable technological architecture and posture, which will be discussed below considering the opportunities but also challenges. It will provide robust deliverables with minimum human capital, fiscal but requests technical deliverables.

With the Internet of Things (IoT), but also challenges such as Darknet and others, cyber-security as a strategy becomes necessary and absolutely important as a business military model, innovation, legal framework, political framework, and economic framework of burden sharing at NATO that will need to be defined, examined, explored, and positioned for, through policy and applicability orientation.

Innovative changes through technology agility and development will simply put pressure to NATO to change. To reflect market needs and security concerns; for NATO to meet the "smartest and easiest way" to operate at a time of financially and socially emerging markets, where non-member states require individual or tailored cooperation and less fiscal implications and human resources with NATO. It will facilitate NATOs expeditionary role for force projector, trainer, and crisis management operator, as an "…active leader in peace and security (NATO, 2016a)" through innovation and methodological approach of entrepreneurship.

Cyber-security liability and NATO: a discussion

NATO's role should be expeditionary not defense led solely. We could state that NATO's role is 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 (Efthymiopoulos, 2008b).

Between the years 2001 and 2018, among others, the Alliance responded through actions such as the following:

1. Invoking article 5 (NATO, 1949), as a consequence of the terror attacks in the USA, on September 11th 2001, claiming its right to defense 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 (NATO, 2002),
3. Agreed to be involved in outer-areas of traditional operations Kosovo (NATO, 1999), Afghanistan in 2001 (Brookings Institution, 2015) onwards via operation International Assistance Force (NATO, 2001a).
4. Supported the creation of the CCDCOE soon after the cyber-security attack in Estonia in 2007.

5. By 2012 at NATOs Chicago summit and confirmed at the Wales Summit of 2014, agreed on a smart defense initiative, that is of qualitative and quantitate value, for among others, agreed into joint interoperability efforts, including efforts to establish a concrete strategy and policy cyber-defense (NATO, 2001a).
6. Warsaw Summit in 2016, reiterated the need to be more resilient, efficient, and innovative through security cooperation
7. By 2018, NATO's Brussels Summit projected the need for fiscal and operational contribution to NATO, considering the needs and innovative policies to be applied, making the Alliance more attractive and more resilient to security needs of the twenty-first century. It further established the importance of sharing and NATO command restructuring. Within this framework, the creation of the cyberspace operations center which is yet to be operational will be evaluated on its short-term deliverables by the second quarter of 2019.
8. Security challenges and threats are evident. Considering the vast changes in cyberspace, the method and location with which NATO will have to operate will be evidently shown in the results following the past NATO Brussels July Summit of 2018 in 2019.

In an emerging globalized world, where complexity may become a 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 (NATO, 2001b) 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 such as cyber-security require NATO to be truly, 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. Our abilities are limitless to point out challenges and face them. We also have the ability to innovate through methodological approaches and security cooperation utilizing the constant upgrade of technology. However, when decisions come to being, this may not be easy.

Lack of sound and constant decision making may affect global financial systems and social structures. Current financial situations in regions and areas, such as in the Balkans or South of Europe, like Greece, Italy, and Portugal among others, affect the larger European Union as a community of union states.

Conflict areas, such as Syria, Iraq, and Afghanistan, do surely provide the impetus for NATO's direct involvement and or cooperation with external allies, yet does not seem to positively affect leadership in taking decisions that are so much needed for the benefit of security resilience and business continuity.

Humanitarian issues, such as 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 defense against 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 innovate, eliminate, distances and borders but also time, NATO should be set to comply with the new "global rules and standards of operational business-minded and political efficiency." 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.

NATOs cyber-resilience experienced 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 unlawful annexation by Russia of Crimea in 2014 (BBC, 2014) and following the disintegrating relations of NATO due to the unlawful act of Russia to Ukraine, the establishment of the USA and then taken over by NATO, of the Missile installation in Romania (Reuters, 2016) and the immediate reaction and accusation of Russia in regard to these developments (New York Times, 2016), the refugee challenges as an outcome on the constant fight against ISIS (US Homeland Security Committee, 2015), but also the phenomenal changes in the financial world (i.e., The Panama Papers (The International Consortium of Investigative Journalists (ICJ), 2016)), 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 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.

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 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 attacks (NATO Review, 2016)"—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-defense 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 of innovation in security in cyberspace

The twenty-first century is characterized by the use of advanced technology. In 2019, technology operates as a tool. Interconnected services through tools like mobile devices provide access through the use of 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 to military policy, through national or NATO command on cyber-security policies, NATO or national armies, use the internet and technology to protect, defend, and secure governments, infrastructures, and people. Therefore, the creation of a cyber-security 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 (Cyber-Policy in Estonia, n.d.).

"…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… (Kramer et al., 2016)."

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" (Kramer et al., 2016).

The NATO's Cooperative Cyber Defense Centre of Excellence in Estonia (CCDCOE), an outcome of the full scale cyber-attack of 2007 (NATO Cooperative Cyber Defense Centre of Excellence, 2016), 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 (National Cyber-Security Framework, 2012) and legal elements (Osula & Rõigas, 2018) and framework for cyber-security and cyber-defense contributes toward 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 (NATO, 2016b)." The NATO Agency will have to be adaptable and innovative 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.

NATO's concept of cyber-defense in 2019

It was NATO's Military Committee decision to adopt a "Cyber-Defense Concept" (Efthymiopoulos, 2008e). The Committee's aim was and still is to deliver business continuity and military resilience. As NATO is a provider of collective defense and as a collective organization in a globalized 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-defense. As technical achievements were delivered, so policy-makers delivered policy results on cyber-defense. 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 Defense in October 2007 of NATO (NATO Defence Ministers Meeting, 2007) 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-defense, named as Cooperative Cyber-Defense Centre of Excellence, CCDCOE (NATO, 2008a). 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-defense 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) (NATO NC3A, 2002) now transformed to the NCIA agency (NATO, 2008a) and the NATO Military Authorities (NMA). The latter authority has implementation as its major task (NATO's Cyber-Defence policy, 2008).

The implementation of NATO's cyber-defense 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" (NATO, 2009a). 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 (NATO, 2008c).

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" and thus the creation of the cyberspace operations center in Mons in Belgium. 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 cooperation 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 coordination of all initial "offering" states to the attempt to establish a cyber-center (under the NATO agreement between states of a voluntary national contribution—VNC), in bringing the NCIRC to a full operational capability (NATO, 2008c).

New and innovative policies were adopted. They were proposed and came to effect (well-known procedure of internal NATO working process) until the adoption of "MoU"; a memorandum of understanding was drafted and proposed to NATO, by a sponsoring state which would establish a center 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 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-defense measures (use of new technology and getting more knowledge on the security environment), in order to enhance cyber-defense posture. Once the third phase was evaluated, the Allied Command Transformation (ACT) decided, to accredit the operational center—in this case the

Cooperative Cyber Defense (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-defense put to the test: the Estonian case of 2007 in 2019

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 center. Today, the Centre of Excellence is yet to welcome more members, the latest ones to join being Greece, Turkey, and Finland (CCDCOE, 2016). (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 center of Tallinn. It was an honorary statue, honoring 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, seven Alliance countries according to the Memorandum of Understanding on the cyber-defense center, 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 center and policy was needed, (2) its operational center would constantly be evaluating and evaluated, and would research on prospective evolutions in technology, malware, and cyber-security (3) that NATO requires resilience when considering the current or future threats and challenges.

The inauguration of its Cooperative Cyber-Defense Centre of Excellence (CCDCOE) in Tallinn Estonia in May 2008, led to a mission, which holds a clear vision 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 cooperative 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 center for NATO in cooperative cyber-defense" (CCDCOE, Training Catalogue, n.d.).

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

- "Legal and policy elements"
- Concepts and strategy

- Tactical environment
- Critical information infrastructure protection (NATO, 2016c)

The Centre's core policy created an outcome of research and policy-orientation, as already analyzed. 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 (Headquarters) 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.

In July 2018 during the Brussels NATO meeting, the Heads of States and Governments agreed to the opening of the cyberspace center as part of the new NATO command structure reform that provides more agility and assurances of operational preparedness, while ensuring force command operations and agility (Efthymiopoulos, 2013). The agreement includes a creation of policy and action reflecting key core issues including a framework policy for the cyberspace operations center of NATO to learn and coordinate in operations how to counter emerging challenges.

Results: NATO innovates with reflection to cyber-security

In terms of cyber-security, the Centre for Excellence in Tallinn continues to portray and project NATOs need for a methodological cyber-resilience policy. At NATO Brussels summit, cyber-security became operational. Therefore, NATOs cyber-defense policy and smart efficient methods while also requested for more interoperability agility and security resilience in the field of cyber-security becomes a core policy.

The attempt as an idea and method to reach out on cyber-security agility of forces for operations is not a new one. On February 6th and 7th 2009, NATO's Science for Peace and Security (SPS) sponsored a workshop. It foresighted the possibility of cyber-security framework. Something we commend through this article: a framework strategy for operational and efficient cyber-security to become a core policy of resilience at NATO. The 2009 workshop titled "Operational Network Intelligence: Today and tomorrow" aimed at adaptation knowledge procedures considering the evolving and fast growing technology. It spoke about innovation and entrepreneurship. It talked about methodological approaches that may bring allies together, while bring cooperative sides together in investment through R&D opportunities.

Its overall purpose therefore was to introduce the possibility of innovation: "rethink present strategies and identify urgent measures to be taken in order to minimize the strategic and economic impacts of cyber-attacks" (NATO, 2009b). This was the level of anticipation at the time; considering future correlation of smart-defense with the policy of cyber-defense at its core. In 2019, innovation seems to be a sound but lone option; a process where through cooperative security and military and technological entrepreneurship NATO can move forward.

In 2019, considering the risk assessments on hybrid threats and challenges (Davis Jr., 2015), the need for better civil awareness and readiness, at a time of much needed cooperative defense, Allies have to decide for a robust long-term planning innovative and entrepreneurial strategy for current and future 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 while making operations to be cost efficient with minimum human casualty numbers.

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 coordination of human factors related to the issues of electronic warfare, operational network, intelligence, and cyber-defense, whether for training, scientific exchange, and or operations (NATO Review, 2015).

NATO is currently using people involved in e-systems, security, IT engineers, researches, officers dealing with network operations and operational centres, as well as professional and academics, among others including military specialists. Specialists in the field on both a strategic and tactical levels should continue to be systematically involved at organized levels of research, sharing, discussion, and exhibition of outcomes, which will in turn enrich the abilities, capabilities, and capacities of rendering current smart-defense and cyber-security as a key and successful resilient and collaborative defense policy to NATO.

Recommendations and proposals

NATO's level of ambition and innovation should be considered through the strategic framework on cyber-security, as we now move ahead with the cyberspace operations center in Mons. There is a need for a clear strategic and resilient policy for cyber-security and defense in operational environments. It should be approached from the perspective of innovation, and business-led resilience. To add, a further 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 also be taken into consideration.

It is proposed that NATO could, on a strategic level do the following:

1. Create a database and share concrete knowledge-based information on security-led affairs in the field of cyber-security and defense within and among member states but also with non-NATO members yet allied in some operational and/or training ways with NATO. This will provide the ability to share knowledge and explore methods of operational efficiency.
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 with external members from around the globe, such as Australia and Brazil and along the lines several Gulf countries that seek more active participation with NATO through the ICI or otherwise independent state such as the United Arab Emirates (NATO and the UAE determined to enhance cooperation, 2016).
3. Allies at upcoming summit in July 2018 should jointly agree on an innovative, business resilient, robust general policy on security and even more so, on a cyber-defense policy,

in which CCDCOE should stand out as a tool for NCIA cooperation methodology for smart defense achievement.

4. NATO should hold a clear budget on cyber-security; what is named as smart budget for defense equally should be innovative; based on the technological necessities that allow lower but shared budgets for the long-term and a policy of cyber-defense that looks operationally viable and globally market-oriented.
5. NATO should reach out for interoperability levels for NATO forces 2020 smart defense standards that are fiscally viable, reflecting the policy, regulations, and strategies of operations and cyber-defense.
6. Through joined cooperation at the level of electronic-warfare prevention, detection and reaction to attacks toward member allied states, the duplication of efforts by nations can and should be avoided. Therefore, clear sharing among security organizations of dues and operations should be taken into account.
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 (UN) for universal discussion and possibly a legally binding adaptation. This can also be achieved as a proposal through the NATO-UN organizations cooperation framework.
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 and innovative application.

Tactically, NATO needs to do the following:

1. Adopt an 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 defense clauses and rules of engagement.
3. An assessment on future warfare should be considered and agreed upon.
4. A foresight and/or future agency, which provides prime information on constantly evolving technology, robotics, genetics, among others; as also optional strategies of innovation and resilience to security approaches.
5. As NATO holds a joined center for warfare, NATO should now enhance its new cyber operations center through a strategy of cyber-resilience in military operational command and control. 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 allies’ 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

The aim of this article was to discuss, examine and analyze, project, and clearly set the importance of cyber-resilience at an Alliance level of 30 at a time of NATOs strategic need for a continued strategic re-evaluation. This article participated through an eye to innovation and entrepreneurship in operations and tactics.

In the July 2018 Summit meeting of NATO allies in Brussels, stated NATOs resilience policy; adopted and completed the creation of the Cyberspace Operations Center in Mons to become an integral part of NATO's modus operandi; it will constitute a methodological and strategic change for NATO. NATO's smart defense and collective defense overall will have to be reexamined by 2020, 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 strategic concept policy on cyber-security and defense, the inauguration of the Centre of Excellence for Cyber-Defense in Tallinn Estonia in 2007, provided an early impetus for future operations that we now are evidently see to be created.

Cyber-security in 2019 is a key priority policy for all nations and NATO. It is innovative but does require a good understanding of management skills and operational efficiency when networked centric, within the framework of the Alliance. Cyber-security is yet to be achieved on a complete operational success, to become a key core policy but eventually will have to be projected into at a time of technological advance and interoperable forces and more so at a time where and when challenges through the virtual space are much more evident.

This article demonstrated the necessity and need of a military strategic framework of a cyber-security policy. One that is innovative and entrepreneurial among allies and partners. The article conceptualized from a strategic and policy concentration. It analyzed the policy needs, the theoretical reflections, and practical issues with reflections on military and civilian-led NATO resilience, smart-defense, cooperative defense, cyber-security, hybrid threats, and crisis management and communication among others. The article 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.

A possible strategy on cyber-security at NATO 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, 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.

Any future decisions made at the level of Heads of State and Government should include the legal element of operation as the cyberspace center is yet to be fully operational. As cyber-threats are borderless, so should NATO work at an operational and capacity building organization that does more to provide effective crisis management solutions through a wide-range of nations cooperation, in innovative ways, along with the support of non-allies but partner members.

The article set the study on future capacity management building on cyber-security, examining and overviewing current administrative decision-training and making, requesting for operational and strategic management innovation and entrepreneurial thinking, limiting fiscal costs, innovating on operations, management, tactics and cooperation, and leveling operational methods in cyber-security considering current and/or future networked operations against challenges and threats.

Endnotes

[1] 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.nato-watch.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

Abbreviations

ACT: Allied Command Transformation; ACUS: Atlantic Council of the USA; CCDCOE: NATO Cyber-Defense Centre for Excellence; HQ: Headquarters; JIW: Journal of Information Warfare; MoU: Memorandum of Understanding; NAC: North Atlantic Council; NATO: North Atlantic Treaty Organization; NC3A: NATO's Consultation Control and Command Agency; NCIA: NATO Communication and Information Agency; NMA: NATO Military Authorities; R&D: Research and Development; SPS: Science for Peace and Security; UN: United Nations

Acknowledgements

I would like to thank the School of Law, at the University of Central Lancashire, (UCLAN) Cyprus campus, for their valuable library but also cooperation and scientific support. I would like to also thank my colleagues at our think tank Strategy International for allowing time to share and exchanges ideas on the related topic. I would finally like to thank the editorial team and the chief editor of the Journal for permitting me to publish in such a timely hour.

Funding

Funding for the research of this article was supported solely by the author.

Availability of data and materials

All data are open sources and available for all to consider. Any further information can be provided on a request by the corresponding author. Please consider referring the author and article when utilizing parts of the published article by Springer.

Author's contributions

The author's academic and research specialization and professional experience includes work at NATO and graduation from the NATO Defense College of its Senior Course program on security and strategy. Currently, an Associate Professor of International Security and Strategy, the author is authoring on cyber-security, strategy, and issues related with innovation and entrepreneurship at defense and security levels. At an earlier period, the author has published peer reviewed articles on relevant issues along the lines which on the current and future challenges of the NATO alliance. This current manuscript is approved and endorsed by the author.

Authors' information

Dr. Marios Panagiotis Efthymiopoulos can be reached out for further clarifications or information. You may find more information about the author his personal professional webpage: https://www.efthymiopoulos.gr.

Competing interests

The author declares that he has no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 1 August 2018 Accepted: 1 April 2019
Published online: 24 June 2019

References

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

Brookings Institution (2015), Blood and hope in Afghanistan: A June 2015 update https://www.brookings.edu/research/blood-and-hope-in-afghanistan-ajune-2015-update/.

Carayannis, Campbell & Efthymiopoulos (2014), Cyber-Development, Cyber-Democracy and Cyber-Defense, Springer 2014 [https://www.springer.com/gp/book/9781493910274].

Carayannis, Campbell & Efthymiopoulos (2018), Handbook on cyber-development, cyber-democracy and cyber-defense, Springer 2018 https://www.springer.com/gp/book/9783319090689.

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, (n.d.) https://ccdcoe.org/sites/default/files/documents/Training_Catalogue_2016.pdf.

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.

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

Cyber-Space Operations Center Mons Belgium, is a decision of the recent Brussels Meeting of NATO members (2018) under the NATO Command Structure Reform. [https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181105_1811-factsheet-key-decisions-summit-en.pdf]

Davis Jr., M. J. R. (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. Accessed 12 May 2016.

Efthymiopoulos, M. P., (2008a), NATO's Security Operations in Electronic Warfare: The Policy of Cyber-Defense and the Alliance New Strategic Concept, Australia. *Journal of Information Warfare*, *8*(3). https://www.jinfowar.com/journal/volume-8-issue-3/nato's-security-operations-electronic-warfare-policy-cyber-defence-alliance's-new-strategic-concept

Efthymiopoulos, M. P. (2008b), 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).

Efthymiopoulos, M. P. (2013). in (Carayannis et al), NATO's Cyber-Security Policy, Chapter in Cyber-Development, Cyber-Democracy and Cyber-Defense. London: New York Published by Springer.

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

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

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

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

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

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

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

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

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

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

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

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

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

NATO (2016a), Operations and Missions: Past and Present, http://www.nato.int/cps/en/natohq/topics_52060.htm. Accessed 4 May 2016.

NATO Communication and Information Agency (NCIA), https://www.ncia.nato.int/Pages/homepage.aspx. Accessed 2 May 2016

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

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

NATO Cooperative Cyber Defense Centre of Excellence, https://ccdcoe.org/. Accessed 1 May 2016.

NATO Cyber-Defence Centre for Excellence, (n.d.) https://www.ccdcoe.org/.

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

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

NATO Review (2015), Hybrid War, Does it Even Exists?. http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-futurewarfare-russia-ukraine/EN/index.htm. Accessed 9 Nov 2018.

NATO Review (2016), Resilience: a core element of collective defence. http://www.nato.int/docu/review/2016/Also-in-2016/nato-defence-cyberresilience/EN/. Accessed 9 Nov 2018.

NATO's Cyber-Defence policy, (2008), Defending Against Cyber-Attacks, Focus Areas: http://www.ccdcoe.org/37.html.

NATO's Cyber-Defense Policy (2011), http://www.nato.int/cps/en/natolive/topics_78170.htm. Accessed 10 Nov 2018.

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. Accessed 26 Apr 2016.

Osula A-M & Rõigas H (Eds.) (2018), International Cyber NormsLegal, Policy & Industry Perspectives, CCDCOE. https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_full_book.pdf. Accessed 11 Jan 2019.

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. Accessed 5 May 2016.

Rehman, S., (2013) 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.

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

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.

The International Consortium of Investigative Journalists (ICJ), https://panamapapers.icij.org/. Accessed 12 May 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. Accessed 5 May 2016.

Wales Summit 4 September 2014, http://www.nato.int/cps/en/natohq/events_112136.htm. Accessed 1 May 2016.