Journal of Computations & Modelling, vol.4, no.1, 2014, 1-10
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2014

Challenges and Objectives for the National Cyber-Security Strategy Beyond 2020

Col. **Dimitrios Choupis**, Phd, GRC A[1]

Abstract.

While the prediction of cyberspace future landscape is quite difficult, Greece must seek to define the potential threats and understand the forces that are formulating the national, regional but also the global future of Cyberspace in order to modulate influence and adapt to these changes. As we look toward 2020 and beyond, it is crystal clear that there are significant challenges, issues and functions that might need to be taken under consideration. However, in order Greece to form an effective cyber defense strategy, a significant number of future challenges need, to be taken into account. Till now independent practical steps and incoherent cyber defense initiatives are under implementation. The majority of NATO nations but also a significant number of non-NATO nations developed their own national strategies in order to establish an efficient and effective response mechanism and roadmap for the future. The answer for Greece to all these future requirements, is a comprehensive mid-term strategic framework, through which the nation will guide its activities and will react to all changes and advances in technology, in order to actively meet both the threats and opportunities. Greece requires an "early warning-early response" cyber defense strategy in order to articulate the framework to 2020. The goal must be to keep technological efficiency and effectiveness in close cooperation and coordination with our allies and other critical stakeholders, in order the nation to be able to respond faster than vulnerabilities and threats will be exploited. Through this roadmap Greece will meet its vision for a safe, secure and resilient cyberspace and will establish a strong foundation for all efforts in the future full of challenges complex cyberspace environment.

Keywords: Cybersecurity, strategy, cyber-defense, cyber space, cyber terrorism

[1] Hellenic Army Staff
E-mail: dimchoupis@yahoo.gr

1 Introduction

Greece has already recognized the significance of the cyber threats that face the country mainly since the cyber attacks on Estonia in 2007. Afterwards, Greece has began establishing a limited number of initiatives in order to improve national ability to prevent, deter, defend against and recover cyber attacks, which are rapidly evolving both in frequency and sophistication. Despite these initiatives there is no relative national policy on Cyber Defense which provides a solid foundation from which all relevant national stakeholders can take work forward on cyber security. Following this roadmap, the nation improved its ability to defend its own networks but there is no implementation of a coordinated approach to cyber defense that encompasses planning objectives and capability development aspects for nation's own structures and nation's local authorities and public sector's services, in a coherent response mechanism in the event of a cyber attack. As we look toward 2020 and beyond, it is crystal clear that there are significant challenges, issues and functions that might need to be taken under consideration in close coordination with our allies. However, the answer to these future requirements, is a comprehensive mid-term strategic framework, through which the nation will guide its activities and will react to all changes and advances in technology, in order to actively meet both the threats and opportunities.

2 NATO and EU Cyber Defense Policy and Action Plan Overview

2.1 NATO

On 8 Jun 2011, NATO Defense Ministers approved a revised NATO policy on Cyber Defense, in order to provide a solid foundation methodology which Allies can take work forward on cyber security. The document itself clarifies NATO's priorities and NATO's efforts in cyber defense, including which networks to protect and the way this can be achieved. The document is coupled with an implementation tool (an Action Plan) which represents a detailed living document (continuously updated), with specific tasks and activities. Through this framework, NATO will ensure that it is at the forefront of developments in cyber space and maintains the proper flexibility to meet the issues and challenges posed by cyber threats. More briefly, NATO's

Cyber Defense Policy set out the “What” and Cyber Defense Action Plan details the “How” it will be achieved.

All NATO structures ([1]), including NATO’s agencies and bodies abroad, will be under centralized protection. New cyber defense minimum military requirements will be applied, either in national networks that are connected to NATO or process NATO information, in order to meet the objective for a secure infrastructure. Additionally, this policy will integrate cyber defense considerations into NATO structures and planning procedures. Moreover, it will focus on prevention, resilience and defense of critical cyber assets of NATO and Allies. Last but not least, NATO will provide, if needed, coordinated assistance for an ally or allies to achieve the minimum level of requirements for cyber defense and also to reduce vulnerabilities of their national critical infrastructures, including a situation in which they are victims of a cyber attack.

Principle cyber defense initiatives and a significant number of practical steps are under implementation. In a multilevel approach, different NATO organizational elements, bodies and committees are responsible for implementation of the planning of capabilities and assisting Allies. It is indicative, that a NATO Computer Incident Response Capability (NCIR) will be established by the end of 2012, including the dispatch of a Rapid Reaction Team (RRT) ([2]), in a role of NATO’s “cyber warriors”. Moreover, NATO’s Cooperative Cyber Defense Centre of Excellence (CCDCoE) ([3]) in close cooperation with Allies, is encouraged to provide expertise, support and research and training, also in parallel with NATO’s existing schools.

2.2 European Union

European Union is in close cooperation with NATO, with regards all the cyberdefence initiatives in order to establish a comprehensive approach also in this crucial area. Research and innovation for cyber defence and combating cyber-crime is an issue that concerns the European Defence Agency (EDA), the European Commission, and the European Space Agency (ESA) and all similar EU organizational entities. Many of the underlying technologies are the same for civil and military applications so this subject is also a crucial initiative for ESDP also. Consequently, a certain degree of coordination between civil and defence research is under implementation and a significant number of projects are also on the execution phase also. Last but not least many joint workshops to shape the research and innovation agenda in the areas of cyber defence and the fight against cyber-crime and terrorism was therefore organized.

3 Greece Moving Towards 2020 Cyber Space Challenges

While the prediction of cyberspace future landscape is quite difficult, Greece must seek to define the potential threats and understand the forces that are formulating the national future of Cyberspace in order to lead influence and adapt to these changes. However, in order for Greece to form an effective cyber defense strategy, a significant number of future challenges need, to be taken into account. These challenges are outlined below:

- The aggregation of data in national and more generic global **network cloud computing** ([4]), combined with remote and distributed management, will create additional security challenges and will complicate today's traditional techniques. It is indicative that this network cloud, more or less, will be an "internet of things" and the threat actors could probably use highly available on-line tools to hack key infrastructure in this cloud-based computing operational environment.
- The "on-line user based" concept, also in nation's cloud network, will expand in order to include many and smart **mobile platforms and devices**, capable of using the web exchanging (collaboration), or transfer sensitive classified information without the need of intervention (virtualization). This technologically advanced "mobile network", can expose Greece's sensitive data and processes to threat actors. "Botnets" ([5]) one of today's most potent IT threat, will evolve dramatically and they will incorporate more and more, these internet-enabled devices.
- Cyber attacks will be increasingly sophisticated, undetectable by the existing antivirus solutions. No single organization in a national basis but also through the Alliance (NATO), could respond effectively, in a real time basis, without a comprehensive and synchronized strategy. This **cyber exploitation** will have as prerequisite for our nation, an advanced situational awareness and incident response and also to professionalize its workforce, in order to succeed.

- This network centric infrastructure with increased integration, collaboration and virtualization, in parallel with Commercial off the Shelf (COTS) equipment, will increase agility in both hardware and software systems. From users' point of view, **new software operating systems and tools** will be applied and this will also affect the cyber security risk. The cybercriminals will create malicious software less effectively for a big variety of software platforms or they will continue to focus primarily to devices and platforms which include "traditional operating systems". This "post-Windows" cyberspace environment will be also for Greece, a new technological challenge in its global role.
- **Globalization of the information** in the commercial marketplace and its close relation with national , EU's but also NATO's procurement supply chain will provide increased opportunities for those to intent on harming Greece, by penetrating the acquisition chain, in order to gain unauthorized access to data, alter data or interrupt communications. As an effect, a great exposure of risk level also in this area will be posed.
- **Strong international collaboration** will be established beyond strict geographic boundaries. This "web-interrelation" between EU's, NATO and other inter-organizational bodies globally but also with not-state actors will grow exponentially the volume of cyber attacks. This new reality in combination with the development of cheap cellular-mobile internet based communications (e.g. mobile spam) will offer a fundamental shift to Greece's cyber vulnerability.
- The integrated nature of cyberspace between the national military and civilian operations and activities will also complicate national role to prevent and manage "**collateral damage**" or "**side effects**" ([6]) consequences in national networks by execution of an offensive cyber attack operation by a NATO's nation , another national cyber-entity or by another cyber actor. This will create a new type of threat ("collateral cyber casualties") because the high level of integration between the networks.
- Acceptable norms of behavior and appropriate **legal frameworks** will be unclear in a national but also n intra-alliance level ([7]). This lack of non existence of law agreements or standardization security procedures will be remain a continuous and dynamic process for Greece and its national entities, because of the "unpredictable" illegal behavior of the cyber criminals.

- Significant real-time requirements and extremely complex cyber security **risk management and threat tracking** software application tools, will be in use on a 24/7 basis in order to minimize the probability of having incidents in the national's networks. This rigorous, multilevel and comprehensive predictive analysis and response to virtual threats will be adapted also to these networks.
- An exploitation and evolution of **Research and Development** projects on the cyber defense area will be implemented, not only within national, NATO and EU bodies, but mainly in other developed allient nations, the private sector and academia. On the other hand, threat actors including the non state cyber criminals ([8]), will also invest in this area, mainly with the help of members of the younger generation, who are capable of writing malicious code for the new platforms.

4 Tracking the Future through NATO's 2020 Cyberdefense Strategy Project

To help Greece as nation and member of different alliances and partners to lead the nation's future efforts to address effectively and efficiently cyber threats, complex challenges and insecurity, a certain number of recommendations/initiatives, are proposed through this paper ([9]) and they are summarized below:

- Greece should adopt a **comprehensive cyber security strategy** to meet our national vision and to achieve the future goals for a safe, secure and resilient cyber environment. This "early warning-early response" strategy is the medium to long term planning process, through which the nation in coordination with NATO will plan its future, to a 5 to 10 years resource plan. Through this strategy, Greece will prioritize activities, set milestones and track progress, in building cyber defense warning capabilities with performance metrics to measure the progress. In parallel, an updated network centric security baseline plan, a cyber intelligence plan and a cyber defense risk management plan must be implemented and run, in order for the Alliance to ensure the integrity of the classified and also unclassified networks and the data they contain. The implemented initiatives should be included in this strategy's goals and objectives, in order for Greece, simultaneously and coherently, to face, current but mainly future, challenges and threats in cooperation with its member existing cyber security strategies.

- Despite the increasing calls for fiscal austerity, **significant growth of cyber security resources** must be endorsed, from an investment point of view, for the upcoming years. This must be depicted clearly in our national strategy goals and objectives. These funds must be focused on R&D projects, software tools, recruitment of personnel and consultants and, last but not least, training and testing facilities. Moreover, a significant amount of indirect cost must also be included for development of new or upgrading the existing network architectures, for implementation of new "leap ahead" high risk projects in cooperation with private sector and NATO's subject agencies and finally for spending resources to recover the network after a possible cyber attack. An indicative minimum amount of 25% of IT and communications budgets should be focused on cyber security. In any case all the previous initiatives, must be combined with an "out of the box thinking" 12-18 months acquisition process and a "secure and transparent partnership roadmap with industry", far away from the existing national bureaucratic acquisition policy. This is a prerequisite, in order for Greece to respond effectively to the future complex global marketplace, to provide a nation-wide data integrity in the future computing cloud and to standardize the access control and policy de-conflictions, in coordination with its members states, partners, agencies and related industry companies.

- Greece should create a **24/7 cross-alliance cyber defense operating network**, through which headquarters and alliance bodies, agencies and "partner-companies" will provide cyber response services for Greece ,connected with relevant NATO's bodies and other national cyber-centers (under bilateral agreements) and will share in real-time information regards cyber threats. This live inter-alliance internet network information with member nations cyber ops centers and other cyber-defense partners should be exchanged under an pre-approved, trusted and real-time response mechanism, to enhance situational awareness and collaboration against cyber threats. This is will be enforced also through information sharing procedures from cyber counterintelligence actors, by deploying an instruction detection system of sensors and software tools across national and Alliance's networks, in order to identify and track unauthorized users attempt to gain access to networks. In this new cyber oriented network, related initiatives like the implementation of a new on-line information assurance policy, the development of a new cyber centric C4ISR target architecture , the acquisition of new network software tools and the activation of a "cyber-warriors" real-time response cell in all core critical infrastructures, need to be taken into consideration.

- No single individual national entity or organization, including NATO, is aware of all cyber related R&D activities. **Collaboration and coordination in R&D activities** is the answer and the key, for Greece in order to respond effectively to future cyber threats. It is this initiative, which will develop and establish a coherent approach with regards national sponsored, EU and NATO nations sponsored and "cyber-partner companies" sponsored classified and unclassified projects. Through this process, Greece will identify research gaps, will prioritize funding and will redirect effort and responsibilities in order to avoid duplications and to get full value for strategic investment. Moreover, Greece must develop and endure a **technologically skilled and cyber-savvy workforce** through education and training and maintain an effective pipeline of future skilled employees, similar to 1970's effort to secure NATO infrastructures and classified networks, in order to meet the Cold War's challenges. Through this dynamic R&D approach, Greece in cooperation with NATO's member governments and NATO's R&D Agencies, will be always one level above and one step in front of the future cyber threats and challenges and will ensure technological superiority and scientific advantage.
- Greece in close cooperation with EU and NATO should create a cyber **security legislation and audit mechanism**, in line with the relevant strategies of other NATO nations ([10]) in order to address crucial cyber defense issues through transparent security processes, norms and standards. Through this process member state governments will agree on the legal elements of a cyber attack that would elevate national responses and also a possible national offensive in order to safe cyber commons. Greece's cyber defense tasked personnel and authorities will conduct and monitor an audit, in order to address which actors including nations, national organizations, private sector and non-state actors share the "common approved legal cyber security environment". It is crystal clear, that in this future complex cyber security environment, only approved procedures ("rules of cyber engagement") are needed. These standardization mechanisms must include shared security interests, national but also inter-alliance collective actions, nations and individuals role regarding concepts like "the need to share" and "the responsibility to protect" cyber commons. This national **legal engagement with a variety of international actors**

and stakeholders will produce new cyber security standardization agreements, codes of conduct and international standards for companies dealing with cyber security. This legally oriented interaction must be planned among all national levels but also through the Alliance, other members intra-governmental ministries, nations EU's and NATO's partners and the private sector also. As a result, Greece will enhance legal effectiveness and transparency on the cyber security collective but also shared responsibility.

5 Conclusion

Despite the productive efforts and significant progress Greece, must do much more to outpace all the above future threats and challenges in cyber space. As the world's premier collective entity, Greece has a responsibility to take all adequate measures to protect efficiently and effectively national networks and provide assistance to national entities and inter-allies when needed. Greece requires an "early warning-early response" cyber defense strategy in order to articulate the framework to 2020.The goal must be to keep also in future, technological superiority in close cooperation and coordination with other nations, in order to be able to respond faster than vulnerabilities and threats will be exploited. Through this roadmap the nation will meet its vision for a safe, secure and resilient cyberspace and will establish a strong foundation for all efforts in the future full of challenges complex cyberspace environment.

References

[1] *Web-page*, "NATO and the cyber defence", www.nato.int/cps/en/nato/reltopics_78/70.html

[2] *News*,13-3-2012, http://www.nato.int/cps/en/natolive/news_85161.html

[3] *Web-page*, http://www.ccdcoe.org

[4] *Article*, ''Cyber crime outlook 2020", Kaspersky Lab, 24-2-2011, Moscow, http://www.securelist.com/en/analysis/204792165/Cybercrime_Outlook_2020_From_Kaspersky_Lab

[5] Conference report -publication , "Emerging Cyber threats 2012", GTCSS,Tbilisi

[6] *Project Study*, ‘America’s Cyber Future”,Center for a new American Security, June 2011, Kristin M. Lord and Travis Sharp

[7] *Nato Defence College Research Paper N.76-May 2012* , “Five years after Estonia’s cyber attacks: Lessons Learned for NATO”, Vincent Joubert

[8] *Article*, “Europolice to lead international Cyber Security Protection Alliance consultation into the future of Cyber crime ”, 19-7-2012, (London and the Hague)

[9] *NATO nations cyber security strategies ,as reference, listed below:*

USA: “Department of Defence Strategy for operating in Cyberspace”,
http://www.defense.gov/news/d20110714cyber.pdf

EU: “Proposal on a European Strategy for Internet Security”,
http://ec.europa.eu/governance/impact/planned_ia/docs/2012_infso_003_european_internet_security_strategy_en.pdf

GBR: “The UK Cyber Security Strategy”,
http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

CAN: “Canada’s cyber security Strategy”,
http://www.publicsafety.gc.ca/prg/ns/cbr/_fl/ccss-scc-eng.pdf

DEU: “Cyber Security Strategy for Germany”, http://www.cio.bund.de/SharedDocs

NLD: “The Defence Cyber Strategy”,
http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf

JPN: “Information Security Strategy for Protecting the Nation”,
http://www.nisc.go.jp/eng/pdf/New_Strategy_English.pdf

RUS: “Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space”,
http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf

FRA: “Informations systems Defence and Security.France’s Strategy”,
http://www.ccdcoe.org/328.html

[10] *Webpage*, CCD COE ,National Strategies and Policies, 28 Oct 2012, http://www.ccdcoe.org/328.html