

Defending Defence: The Demand for Cybersecurity Expenditures by the Hellenic MOD

Keywords

Cybersecurity, Defence, 2SLS

Abstract

Objectives

This paper approaches the issue of the demand for cybersecurity funds by the Hellenic Department of Defence.

Methods

Following a theoretical background, the paper formulates a demand function for funds required to face cybersecurity threats. Based on this background we estimate a demand function for such funds using the technique of instrumental variables (Two Stage Least Squares).

Results

The findings confirm the heavy reliance of cybersecurity funding on the MoD budget, the frequency of breaches against the system, as well as the spill-over benefits accrued by the EU cyber - defence environment.

Conclusions

The authorities must place emphasis on this relatively new hybrid threat and devote the appropriate resources, both capital and labour, to enhancing the arsenal devoted to the deterrence of such threats. In addition, the paper finds that there is a slow response of the demand for cybersecurity funds to the increased number of threats, a reaction that leaves a lot to be desired. Finally, Greece turns out to be a free rider in the global cybersecurity warfare environment, given that the economic policy uncertainty environment has taken its toll regarding the support of the Hellenic defence sector in the cybersecurity warfare,

Defending Defence: The Demand for Cybersecurity Expenditures by the Hellenic MOD

Vasileios Symeonidis* and George Zombanakis**

Abstract

This paper represents one of the early attempts to approach the issue of the demand for cybersecurity funds by the Hellenic Department of Defence. What we do, in fact, is outline the cybersecurity issue for the Hellenic Defence sector and the problems arising following the increasing cyberattacks in the international environment and the ensuing risk for breaches. We then propose a theoretical background, based on which we formulate a demand for cybersecurity funds required to face such threats. Relying on this background we estimate a demand function for such funds and discuss their degree of responsiveness to changes of its determinants, like the threats facing the Hellenic Defence sector and the funds required to promote and enhance similar efforts. The last part of the paper involves policy implications and conclusions, as well as future research suggestions.

Key Words: Cybersecurity, Defence, 2SLS

*Athens College and the American College of Greece

** Hellenic Navy War College and the American College of Greece

I. Introduction

As it is the case worldwide, the defence sector of Greece is no exception, being a target for cyber threats mainly focusing on national security. In fact, during the past few years several military sectors of the country suffered repeated attacks indicating the need for cybersecurity measures which currently leave a lot to be desired as regards effectiveness. In addition, the country recently faced a series of Distributed Denial of Service attacks (DDoS), targeting the central public sector network, while during the recent past, there has been increased spying activity aiming at NATO and U. S. infrastructure installations in the north of the country. Finally, to make matters worse, a number of local politicians and journalists have complained that the Predator spyware has been used to monitor their professional and personal activities.

It is easy to see, therefore, that such incidents point to several weaknesses within Greece's defence sector, like cybersecurity gaps, state sponsored threats and espionage risks. The purpose of this paper is not to point to how one could treat such weaknesses, because, among other things, such an endeavour required a great deal of technical knowledge which is far beyond our field. What we intend to do, however, is point to the pressing need for cybersecurity funds and given the situation, the determinants which point to the need of such funds and to what extent they affect it.

II. Theoretical Background

We consider that spending on cybersecurity defence is a fraction of the total defence spending of the economy, as this is described in the annual budget provisions. We take it, therefore, that the structure of the function that describes the demand for cybersecurity funds is along the lines proposed by Hartley and Sandler (2001). Thus, we shall assume that the demand for cybersecurity defence spending (CY) can be modelled as a function of the following variables: Total defence expenditure as a percentage of the GDP (DEFGDP), a variable representing security threats, breaches incidents in our case (INCID) and the spill – over benefits resulting from belonging to a group of countries with common interests on this issue, proxied by the worldwide spending on cybersecurity

(SPIL). The international security environment plays a decisive role in such matters and must be taken into consideration, as well (GPRT). These variables are considered as arguments of a utility security function for Greece which is maximised subject to the country's budget constraint. In fact, we assume that the total national defence spending DF is broken down to:

CY = national cyber defence spending and

$REST$ = national non-cyber defence spending.

We also take it that S (national security) strongly depends on the Greek cybersecurity arsenal against breaches (incidents) denoted as $INCID$.

This means that $S = CY - CY^*$

where: CY^* stands for the targeted national cyber defence spending and is given by

$$CY^* = b_0 + b_{1I} * INCID$$

and is treated as an exogenous variable.

What we need to do, therefore, is maximise our anti-cyberwarfare utility denoted as:

$$\begin{aligned} U(S, REST) &= a \cdot \ln(S) + (1 - a) \cdot \ln(REST) \\ U(CY, REST) &= a \cdot \ln(CY - CY^*) + (1 - a) \cdot \ln(REST) \end{aligned}$$

Subject to the budget constraint:

$$DF = p_{REST} \cdot REST + p_{CY} \cdot CY$$

where a = proportion of DF spent on cyber defence spending. The price variables p_{CY} and p_{REST} denote theoretical prices in both cases.

The optimisation setup of the required Lagrange function is given in the Appendix.

III. Variables and Data Issues

Since the issue of Cybersecurity has been classified as a form of hybrid threat only recently, research interest in the area and, consequently, data sources are rather poor before 2010 and refer to annual observations in most cases. To

face the impact which such problems may entail on the degrees of freedom during econometric estimations, we have resorted to transforming our annual observation to quarterly employing the following reasoning:

Q1 Weight: 0.25 During the first quarter of the year, fresh attacks exploit “holiday freeze” vulnerabilities revealing an increase of phishing incidents.¹

Q2 Weight: 0.20 According to “Anti-Phishing Working Group” (APWG) reports this is usually the relatively quitter quarter.²

Q3 Weight: 0.26 The “Check Point” indicates a resurgence of attacks compared to the second quarter.³

Q4 Weight: 0.29 The fourth is consistently the hottest quarter according to the APWG and the Cloudflare Blog.⁴

Applying these coefficients to each annual observation breaks it down to its quarters, following the reasoning outlined above.

Turning to the variables used for the regression estimations and listed in Table 1, the dependent variable is the funds aiming at financing cybersecurity projects (CY), representing a share of the ELKAK⁵ funds. The determinants chosen on the basis of the analysis outlined in section II are the GDP share of the Hellenic defence budget (DEFGDP), the frequency of incidents or breaches (INCID), representing the threat, the global cybersecurity spending (SPIL), included as the spill-over variable and the economic policy uncertainty index (GPRG) to account for the restrictions imposed on the Hellenic defence budget due to the extended financial and economic crisis (2009 to 2019).

¹ docs.apwg.org

² <https://www.nerc.com/comm/RSTC/PAWG/TRD- data Collections Report.pdf>.

³ Check Point Blog. Check Point Software Technologies is a company focusing on IT security,

⁴ docs.apwg.org and The Cloudflare Blog

⁵ Hellenic Defence Innovation Centre

Table 1. Variable Names and Sources

CODE	DATA SERIES	SOURCE
CY	Funds devoted to Cybersecurity	ELKAK funding
DEFGDP	GDP share of Defence funds	Nato Database
INCID	Incidents of Breaches	Enisa
GPRG	Economic Policy Uncertainty Index Fountas et al. (2018)	https://www.policyuncertainty.com/FKT_Monthly.html
SPIL	Worldwide Cybersecurity Spending	Statista

IV. Empirical Results

As earlier pointed out, even after resorting to quarterly data analysis, an empirical consideration of the issue runs the risk of being affected by a low number of degrees of freedom due to the small number of observations, given the lack of reliable, high - frequency data before 2010. Aiming at resolving some of the technical problems arising, we decided to try a Two-Stage Least Squares (2SLS) run since it is particularly useful when dealing with endogeneity issues, in cases in which the independent variables are correlated with the error terms and involve feedback loops within the model⁶.

Table 2. Estimation Results

Dependent Variable: LCY

Method: Two-Stage Least Squares

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-1.152057	2.953494	-0.390066	0.6983
LDEFGDP	2.334076	0.836970	2.788720	0.0076
LINCID	0.969992	0.208149	4.660096	0.0000
LSPIL	-2.766251	1.206582	-2.292634	0.0264
LGPRG (-2)	0.645229	0.284695	2.266390	0.0281
R-squared	0.924248	Mean dependent var		0.883148
Adjusted R-squared	0.914578	S.D. dependent var		1.114215
S.E. of regression	0.325653	Sum squared resid		4.984340
F-statistic	102.3926	Durbin-Watson stat		1.541110

⁶ Despite the restricted degrees of freedom problem, it has turned out that the use of annual data to estimate these equations has led to conclusions similar to those derived using quarterly data. Thus, in terms of a robustness check, we may argue, without loss of generality, that in both cases the elasticity of demand for cybersecurity funds to changes of the budget remains considerably high, as opposed to their elasticity to changes of breaches which is close to unity in both cases. The annual data results are available upon request.

As indicated in Table 2, all variables are statistically significant and bear the expected signs when regressed on the demand for cybersecurity funds. Note that all variables are expressed in log forms (denoted by the prefix L), which facilitates to consider elasticity issues. Focusing first on the total of defence expenditure, this is α variable the changes of which affect cybersecurity funds in a pronounced way, something which is to be expected and reflected in its high elasticity coefficient. In fact, the defence sector is bound to respond to breach threats and devoting considerable funds for its protection is now becoming a top priority. Concentrating, next, on the breach threats per se, we observe that their impact on the demand for cybersecurity funds is close to unity meaning that a given percentage of threats increase is expected to be translated to an equal percentage of rise in the demand for cybersecurity funds. Regarding the remaining independent variables, Greece seems to be a free rider to the battle for cybersecurity, given the negative sign of the spillover variable, to changes of which, however, the behaviour of the dependent variable is substantially elastic. It goes without saying that the economic policy uncertainty combined with a volatile geopolitical environment brings about a strong, however inelastic impact of the cybersecurity funding via the state budget after about six-months. This is to be expected because there is usually a considerable time lag between assessing economic and geopolitical developments and finding the appropriate resources to face them, especially in the EU environment in which the process of decision making faces a substantial number of frictions. Note that in the case of Greece the focus on the economic policy uncertainty plays a major role in determining the demand for cybersecurity funds, as the economy of the country remains still “on probation” after the long economic crisis (2009 to 2019), when channelling budget funds to defence investment purposes was not allowed due to the restrictions imposed by the EU, ECB, and IMF, the institutions responsible for monitoring Greece's austerity measures (Kondylis et al. 2018).

V. Policy Implications and Conclusions

The issue of cybersecurity is relatively new in the economics of conflict and security area and consequently requesting safe conclusions on the issue of the

determinants of demand for the related funds is yet rather premature. There is a couple of issues on which one can safely argue: The first is that the demand for cybersecurity funds is strongly dependent on the defence budget of the country. It follows, therefore, that the authorities must place emphasis on this relatively new hybrid threat and devote the appropriate resources, both capital and labour, to enhancing the arsenal devoted to the deterrence of such threats. More specifically, the high elasticity of cybersecurity funds to the Hellenic defence budget (DEFGDP) indicates the pressing need for training high quality professionals, as well as strengthening the country's infrastructure defences. The second issue to consider is the rather slow response of the demand for cybersecurity funds to the increased number of threats (INCID), with the elasticity coefficient being close to unity. This is a finding which may be anticipated to a certain extent, at least, given the slow pace of reaction of the Greek public sector and the extensive red-tape procedures involved in the issue of public procurement. The next observation based on our research is that Greece turns out to be a free rider in this global warfare environment as the negative sign of the relevant variable (SPIL) indicates. This is a finding which is justified, not just by the usual slow pace of reaction of the public sector authorities and consequently the decision-making process, but mainly because the economic policy uncertainty environment and the consequent lack of funds have taken their toll regarding the support of the Hellenic defence sector in the cybersecurity warfare. It is important to point out that only very recently, following the establishment of the Hellenic Defence Innovation Centre (ELKAK) the cyber security issue has been acknowledged and to some extent, confronted. We are confident that the end of the long-term financial crisis, together with the increasing importance of cybersecurity will convince the Department of Defence to devote more emphasis on aligning with the rest of the EU members in devoting more funds to it, especially regarding R&D expenditure.

In terms of a wrap-up assessment, the defence sector of Greece has embarked on implementing reforms to the right direction. However, such reforms will require more time to produce fruitful results provided that the country catches up with the pace of the rest of the EU countries.

VI. Limitations

The results derived by research in this field are considerably limited by the lack of reliable, high - frequency data before 2010, when the international focus first emphasised on cybersecurity issues. In addition, and despite the shift to modern hybrid warfare threats (Symeonidis and Zombanakis 2025), the administration is notoriously slow in realising, assessing and deciding to confront the problem to its full extent. This has resulted in restricting the number of reliable sources on the subject to a minimum. Given time, however, we feel that these issues will be resolved and the threat of cyberattacks will assume dominant position in the Ministry of Defence priorities.

CONFIDENTIAL:
FOR PEER REVIEW ONLY

VII. Appendix

We assume that the total national defence spending DF is broken down to:

CY = national cyber defence spending

and

$REST$ = national non-cyber defence spending.

We also take it that S (national security) strongly depends on our cybersecurity arsenal against breaches (incidents) denoted as $INCID$.

This means that $S = CY - CY^*$

where: CY^* stands for the targeted national cyber defence spending and is given by

$$CY^* = b_0 + b_{1I}INCID$$

and is treated as an exogenous variable.

We need to maximise our anti-cyberwarfare utility denoted as:

$$\begin{aligned} U(S, REST) &= a \cdot \ln(S) + (1 - a) \cdot \ln(REST) \\ U(CY, REST) &= a \cdot \ln(CY - CY^*) + (1 - a) \cdot \ln(REST) \end{aligned}$$

Subject to the budget constraint:

$$DF = p_{REST} \cdot REST + p_{CY} \cdot CY$$

where a = proportion of DF spent on cyber defence spending.

Therefore, we use the Lagrange multipliers method, and we set up the Lagrange function

$$\begin{aligned} L(CY, REST) &= a \cdot \ln(CY - CY^*) + (1 - a) \cdot \ln(REST) + \lambda \\ &\quad \cdot (DF - p_{REST} \cdot REST - p_{CY} \cdot CY) \end{aligned}$$

First Order Conditions:

$$\frac{\partial L}{\partial CY} = \frac{a}{CY - CY^*} - \lambda \cdot p_{CY} = 0 \Rightarrow \lambda = \frac{a}{p_{CY} \cdot (CY - CY^*)} \quad (1)$$

$$\frac{\partial L}{\partial REST} = \frac{1 - a}{REST} - \lambda \cdot p_{REST} = 0 \Rightarrow \lambda = \frac{1 - a}{p_{REST} \cdot REST} \quad (2)$$

$$\begin{aligned} \frac{\partial L}{\partial \lambda} &= DF - p_{REST} \cdot REST - p_{CY} \cdot CY = 0 \Rightarrow DF \\ &= p_{REST} \cdot REST + p_{CY} \cdot CY \quad (3) \end{aligned}$$

Eliminating λ from (1), (2):

$$\frac{a}{p_{CY} \cdot (CY - CY^*)} = \frac{1 - a}{p_{REST} \cdot REST} \Rightarrow REST = \frac{(1 - a) \cdot p_{CY} \cdot (CY - CY^*)}{a \cdot p_{REST}} \quad (4)$$

Combining (3), (4) we need to solve for the optimum values for the two independent variables, namely CY and $REST$:

$$\begin{aligned} DF &= p_{REST} \cdot \frac{(1 - a) \cdot p_{CY} \cdot (CY - CY^*)}{a \cdot p_{REST}} + p_{CY} \cdot CY \Rightarrow \\ DF &= \frac{(1 - a) \cdot p_{CY} \cdot (CY - CY^*)}{a} + p_{CY} \cdot CY \Rightarrow \\ a \cdot DF &= (1 - a) \cdot p_{CY} \cdot (CY - CY^*) + a \cdot p_{CY} \cdot CY \Rightarrow \\ a \cdot DF &= (1 - a)(p_{CY} \cdot CY - p_{CY} \cdot CY^*) + a \cdot p_{CY} \cdot CY \Rightarrow \\ a \cdot DF &= p_{CY} \cdot CY - p_{CY} \cdot CY^* - a \cdot p_{CY} \cdot CY + a \cdot p_{CY} \cdot CY^* + a \cdot p_{CY} \cdot CY \Rightarrow \\ p_{CY} \cdot CY &= a \cdot DF + p_{CY} \cdot CY^* - a \cdot p_{CY} \cdot CY^* \Rightarrow \\ CY &= \frac{a \cdot DF}{p_{CY}} + CY^* - a \cdot CY^* \Rightarrow \end{aligned}$$

$$\boxed{CY = \frac{a \cdot DF}{p_{CY}} + (1 - a) \cdot CY^*} \quad (5)$$

Combining (4), (5)

$$REST = \frac{(1 - a) \cdot p_{CY}}{a \cdot p_{REST}} \left(\frac{a \cdot DF}{p_{CY}} + CY^* - a \cdot CY^* - CY^* \right) \Rightarrow$$

$$REST = \frac{(1 - a) \cdot p_{CY}}{a \cdot p_{REST}} \left(\frac{a \cdot DF}{p_{CY}} - a \cdot CY^* \right) \Rightarrow$$

$$REST = \frac{(1 - a) \cdot p_{CY}}{p_{REST}} \left(\frac{DF}{p_{CY}} - CY^* \right) \Rightarrow$$

$$REST = \frac{(1 - a)}{p_{REST}} (DF - p_{CY} \cdot CY^*) \Rightarrow$$

$$\boxed{REST = \frac{(1 - a)}{p_{REST}} DF - \frac{(1 - a)}{p_{REST}} p_{CY} \cdot CY^*} \quad (6)$$

Second Order Conditions:

$$\frac{\partial^2 L}{\partial CY^2} = \frac{-a}{(CY - CY^*)^2}, \quad \frac{\partial^2 L}{\partial REST^2} = \frac{-(1-a)}{REST^2}, \quad \frac{\partial^2 L}{\partial CY \partial REST} = 0$$

Constraint:

$$g(CY, REST) = p_{REST} \cdot REST + p_{CY} \cdot CY$$

$$\frac{\partial g}{\partial CY} = p_{CY}, \quad \frac{\partial g}{\partial REST} = p_{REST}$$

We set up the bordered Hessian determinant - if it is positive we have a max:

$$|\bar{H}| = \begin{vmatrix} 0 & -\frac{\partial g}{\partial CY} & -\frac{\partial g}{\partial REST} \\ -\frac{\partial g}{\partial CY} & \frac{\partial^2 L}{\partial CY^2} & \frac{\partial^2 L}{\partial CY \partial REST} \\ -\frac{\partial g}{\partial REST} & \frac{\partial^2 L}{\partial CY \partial REST} & \frac{\partial^2 L}{\partial REST^2} \end{vmatrix} \Rightarrow$$

$$|\bar{H}| = \begin{vmatrix} 0 & -p_{CY} & -p_{REST} \\ -p_{CY} & \frac{-a}{(CY - CY^*)^2} & 0 \\ -p_{REST} & 0 & \frac{-(1-a)}{REST^2} \end{vmatrix} = \frac{a \cdot p_{REST}^2}{(CY - CY^*)^2} + \frac{(1-a) \cdot p_{CY}^2}{REST^2} > 0$$

and we have indeed a maximum.

Therefore:

Optimum values for max:

$$\begin{aligned} CY &= \frac{a \cdot DF}{p_{CY}} + (1-a) \cdot CY^* \\ REST &= \frac{(1-a)}{p_{REST}} DF - \frac{(1-a)}{p_{REST}} p_{CY} \cdot CY^* \end{aligned}$$

Substituting for the exogenous variable $CY^* = b_0 + b_{1I} INCID$

$$\begin{aligned} CY &= \frac{a \cdot DF}{p_{CY}} + (1-a)(b_0 + b_{1I} INCID) \\ REST &= \frac{(1-a)}{p_{REST}} DF - \frac{(1-a)}{p_{REST}} p_{CY}(b_0 + b_{1I} INCID) \end{aligned}$$

It follows, therefore that the demand for cybersecurity-expenditures function depends on the total national defence expenditure (DF), the threat, represented as the cybersecurity breaches (INCID) and the prices p_{CY} . The latter, however, is usually dropped from a standard demand for cybersecurity spending function, as it is rather impossible to determine for a wide variety of reasons which are beyond the scope of the present paper to analyse.

References

Fountas S, Karatasi P. Tsika P. (2018) "Economic Policy Uncertainty in Greece: Measuring Uncertainty for the Greek Macroeconomy", South-Eastern Europe Journal of Economics 1, 79-92.

Hartley K. and T. Sandler (2001), "Handbook of Defence Economics" v. 1.

Kondylis K, Reklos I. and G. A. Zombanakis (2018), "Return to Growth: Does it Mean More on Defence Expenditure?" Nafsivios Hora, Hellenic Naval Cadets Academy, 2018.

Symeonidis V. and Zombanakis G. A. (2025), "Hellenic Air - Space Violations: An Updating Note", Security and Defence Quarterly, Forthcoming.

Table 1. Variable Names and Sources

CODE	DATA SERIES	SOURCE
CY	Funds devoted to Cybersecurity	ELKAK funding
DEFGDP	GDP share of Defence funds	Nato Database
INCID	Incidents of Breaches	Enisa
GPRG	Economic Policy Uncertainty Index Fountas et al. (2018)	https://www.policyuncertainty.com/FKT_Monthly.html
SPIL	Worldwide Cybersecurity Spending	Statista

CONFIDENTIAL:
FOR PEER REVIEW ONLY

Table 2. Estimation Results

Dependent Variable: LCY

Method: Two-Stage Least Squares

Variable	Coefficient	Std. Error	t-Statistic	Prob.
C	-1.152057	2.953494	-0.390066	0.6983
LDEFGDP	2.334076	0.836970	2.788720	0.0076
LINCID	0.969992	0.208149	4.660096	0.0000
LSPIL	-2.766251	1.206582	-2.292634	0.0264
LGPRG (-2)	0.645229	0.284695	2.266390	0.0281
R-squared	0.924248	Mean dependent var		0.883148
Adjusted R-squared	0.914578	S.D. dependent var		1.114215
S.E. of regression	0.325653	Sum squared resid		4.984340
F-statistic	102.3926	Durbin-Watson stat		1.541110

CONFIDENTIAL:
FOR PEER REVIEW ONLY

Manuscript body

[Download source file \(58.56 kB\)](#)

Tables

Table 1 - [Download source file \(14.04 kB\)](#)

Table 2 - [Download source file \(15.72 kB\)](#)

CONFIDENTIAL:
FOR PEER REVIEW ONLY