CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Pascal Brangetto, Mari Kert-Saint Aubyn

Economic aspects of national cyber security strategies

Project Report

Tallinn 2015

This publication is a product of the NATO Cooperative Cyber Defence Centre of Excellence (the Centre). It does not necessarily reflect the policy or the opinion of the Centre or of NATO. The Centre may not be held responsible for any loss or harm arising from the use of information contained in this publication and is not responsible for the content of the external sources, including external websites referenced in this publication.

Digital or hard copies of this publication may be produced for internal use within NATO and for personal or educational use when for non-profit and non-commercial purpose, provided that copies bear a full citation.

www.ccdcoe.org
publications@ccdcoe.org

Economic Aspects of National Cyber Security Strategies

Project Report

Table of Contents

Summary

Every organisation and government need to know how much is necessary to invest in cybersecurity and how much is enough. Looking at the available literature, it is to be noted that little attention has been given to a fast thriving discipline, namely, the economics of cyber security which provides for some interesting and relevant models to measure the investments made in cybersecurity through cost-benefit tradeoffs

This project report summarises the main findings of a project launched by the NATO CCDCOE in 2014 which stemmed from the analysis of national cyber security strategies (NCSS) and aimed at trying to evaluate the underpinning economic elements for the drafting and adoption of NCSS worldwide. It aimed at addressing the questions from a public policy standpoint and tackled matters such as measuring cost of cyber insecurity, assessing the economic efficiency of a NCSS and economic incentives for all stakeholders involved. This report gives an overview of the basics of economics of cybersecurity and attempts to apply these in the context of NCSSs'. In particular, it looked at the UK's efforts in this area. The general conclusion reached in this report is that there is not enough data currently to measure such costs unless appropriate identification of the roles and responsibilities are appointed within structures, be it governments or private organisations.

1 Project description and methodology

The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), in its 2014 Programme of Work, launched a project that aimed to address the economic aspects of national cyber security strategies (NCSSs). The project's aim was to conduct a study and in order to build on the work that was published in the *National Cyber Security Framework Manual* in 2012 under the auspices of the NATO CCD COE.[1]

For the preparation of the study, a workshop was organised in 2014 in order to discuss the outline and ideas to be developed. Due to lack of interested authors and available data, only a limited study was performed which is included in Annex I of this report. The starting point for this project was to assess to what extent economics have a clear and defining role in the drafting of an NCSS by conducting a study that could serve as a basis for decision making processes in the course of that drafting. There is a clear need for an evaluation framework of such policies that looks at several factors, such as implementation, value for money and efficiency. This research project sought to address these aspects from an economic standpoint.

The project methodology was based on a literature review and desk research using open source materials.

2 Objective of the project and context

The development of NCSSs has been a growing area of interest over the last few years in most developed countries as the issue has gained prominence on the policy-maker's agenda. Addressing the cyber issue has been a long process for states which consider it their responsibility to lead the way in delivering cyber security. As a global policy involving many stakeholders, the economic aspects are key to understanding the motivation of state actors. Cybercrime has been described as the 'largest transfer of wealth in human history'.[2] Such an assertion has the capacity to generate concern among all policy-makers, especially when early estimates of losses were evaluated at $1 trillion every year, roughly 1.4% of the World's GDP. One of the main objectives pursued when securing cyberspace is one nation's ability to sustain and increase its economic activity through the use of information and communication technologies (ICT)[3] such as e-commerce, finance, and e-government. It is considered of the utmost importance that these activities are protected, and that they are perceived as a

[1] Alexander Klimburg (Ed.), NATIONAL CYBER SECURITY FRAMEWORK MANUAL, NATO CCDOCOE Publication, Tallinn 2012.

[2] Josh Rogin, *NSA Chief: Cybercrime constitutes the 'greatest transfer of wealth in history*, FOREIGN POLICY, July 9th 2012, http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history (last accessed November 30th 2015).

[3] As outlined in the *Seoul declaration for the future of the Internet economy*, 18 June 2008, http://www.oecd.org/internet/consumer/40839436.pdf (last accessed November 30th 2015).

common universal goal for all stakeholders in order to achieve the prosperity of societies.[45] Prosperity is a recurrent theme mentioned in NCSSs worldwide. [6]

A policy that is well-balanced, ensuring the continuity of critical infrastructure, resiliency and a stability of the economy while taking into account factors that might lead to an increased competitiveness of its industry, is both key and difficult to achieve.

In order to achieve these goals, most NCSSs focus on a comprehensive approach to the measures that should be implemented in order to respond to threats in cyberspace. [7] The cyber society is considered as a whole, with all types of stakeholders and states providing the instruments that will enable them to carry out their activities without disruption, and also provide a normative environment in order to share the burden of cyber security. States are mandated to provide safeguards in cyberspace in terms of national security, whilst the infrastructure is, for the most part, privately owned. This is where principles of economics surface and start to play a role in policymaking.

The objective of the project was to integrate both the economics of cyber security,[8] which is a fairly new discipline and will be explained in more detail below, and the public policy approach to cyber security, in particular, looking at NCSSs and how economic aspects are implemented within them.[9] These dimensions have seldom been combined, as they seem to be running on parallel tracks. The logic of a top-down approach has been studied thoroughly, as it is generally the way NCSS have been drafted. The question then becomes whether the principles of economics which are usually applied to individual

[4] For an American perspective, see John Dowdy, 'The cyber security threat to U.S. growth and prosperity' in Nicholas Burns and Jonathon Price (Eds.), *Securing cyberspace: A new domain for national security,* 2012, published by the Aspen Institute.

[5] 'While all strategies aim to address cyber security in order to maintain and further develop economic and social prosperity through the continued development of a vibrant Internet economy, the economic aspects of cyber security are gaining increased visibility in several strategies. Some countries highlight that a higher level of cyber security will provide their economy with a competitive advantage as it can give them credibility. They recognise that economic factors play a key role in improving cyber security. [...] Several strategies encourage flexible policies leveraging incentives for markets to better take security into account. Some require better understanding of the incentive structure of market players in relation to cyber security and promote lightweight measures such as encouraging the use of security labels applied to products and services to better inform the market. Several countries set as a key policy objective the development of a stronger cyber security industry sector, including the development of a larger cyber security workforce. They also mention the possible development of a cyber security insurance sector". OECD (2012), *'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy',* OECD Digital Economy Papers, No. 211, OECD Publishing. http://dx.doi.org/10.1787/5k8zq92vdgtl-en (last accessed November 30th 2015).

[6] Alexander Klimburg, *supra* (n1), at 56.

[7] OECD (2012), 'Cybersecurity Policy Making at a Turning Point..., See *supra* (n5).

[8] See Annex I for more information on the description of the economics of cyber security.

[9] See Tyler Moore, *Introducing the Economics of Cybersecurity: Principles and Policy Options*, in Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategic and Developing Options for US policy, National Academy of Sciences, https://cs.brown.edu/courses/csci1800/sources/lec27/Moore.pdf (last accessed November 30th 2015).

organisations can also be adapted and relevant to the NCSSs. Cyber security economics describes and analyses behaviours of the different players (attackers and defenders) of the cyber security market. The role of public policy is to foster socially optimal investments. If the forces of the market were left on their own, there would be an under-investment in security, as free-riding behaviours could arise, resulting in an ill-coordinated effort to thwart cyber threats.

The following research questions were outlined for the project workshop and were meant to guide its content for further research:

RQ1: How is the economy affected by cyber insecurity?

RQ2: At what cost am I ready to protect myself?

RQ3: How is the economic efficiency of an NCSS measured?

RQ4: What do I want to protect and enforce through the implementation of an NCSS?

RQ5: What are the incentives for security for all stakeholders?

3 The study and the workshop

The NATO CCD COE drafted a preliminary outline of the research in order to break down the topic into 4 main categories. These are:

- The stage of maturity of cyber security strategies;
- The intervention of states to correct market failures (the regulatory vs voluntary approach);
- Metrics to assess the efficiency of cyber security strategies; and
- Industrial policy and economic competitiveness – a cyber security industry.

An overview of the general approaches to the economic aspects of an NCSS is attached to this report (Annex I) and provides a useful introduction to the topic for a policy-maker interested in the field. As part of the project, the NATO CCD COE held a thematic workshop in order to gather specialists and an interested audience in order to discuss and present the issues surrounding the economics of cyber security. Annex II of this report includes the main findings of the workshop.

4 Takeaway points of the project

Lack of accurate and available information. Metrics used internally within an organisation or from external resources are difficult to quantify. Problems arise due to the difficulties of estimating losses that may never occur, and the availability of good data (crime rates, cost of damage, effectiveness of countermeasures, etc.). Estimates can often be biased by our perception, and the calculation of risk can easily be manipulated in order to fit the needs of the users to justify a decision.[10] Finding accurate data on incidents is another hurdle

[10] ENISA, 'Introduction to Return on Security Investment, Helping CERTs assessing the cost of (lack of) security', December 2012, at 7, https://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport (last accessed November 30th 2015).

to be overcome since many of the organisations suffering from data breaches do not wish to share this information, often due to potential reputational damage. In addition, estimating cost can be a challenge for several reasons: 1) the majority of information is classified; 2) non-classified information flows through many different organisations for various activities; and 3) lack of effective reporting mechanisms.[11]

NCSSs' policies should encourage the collection of data for the purposes of statistics. Current methods use methods such as *a posteriori* evaluation and audits due to lack of data. Implementing the necessary regulation in order to encourage sharing of such data would enable better quantification of the efficiency of NCSSs. An example of such an initiative would be the breach reporting system envisioned in the NIS directive.[12] A better identification of the roles and responsibilities within structures is needed in order to achieve that goal. Collecting such data should be the responsibility of one single body but should be allocated among the different stakeholders, whether government or the private sector.

Lack of cooperation between academics, industries and governments. Better cooperation between the stakeholders, such as academia, government structures and industry, is necessary to enable better quality research. Consequently, the economic toolbox will not provide ready-made solutions (models) but gives great insight to help understand an environment that is normally difficult to grasp.

Cyber security industrial policy should be integrated in the NCSS. In order to quantify and measure the effectiveness of an NCSS it is necessary to gain an understanding of the national industrial cyber fabric. This can be achieved through a mapping exercise to identify potential strengths and weaknesses and so optimise efforts. The UK is one of the few countries that has undertaken such an endeavour. This is especially relevant in the EU due to the tremendous number of small and medium enterprises (SMEs).

'One size fits all' models are not appropriate in the context of an NCSS. The traditional models used in the economics of cyber security should be adapted to the needs of the NCSSs and specifically tailored according to the national industrial capabilities, critical infrastructures, political culture, and social structures.

[11] National Audit Office, 'The UK cyber security strategy: Landscape review', 12 February 2013, https://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf (last accessed November 30th 2015).

[12] COM/2013/048 final, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52013PC0048 (Last accessed January 26th 2016)

Annex I – Economic aspects of national cyber security strategies

The aim of this section is to provide a description of the subject matter and the state-of-play of the economics of cyber security. The purpose of the research was to determine to what extent national cyber security strategies have taken into account the principles of economics, and how relevant the tools available are to crafting an NCSS.

The first section describes what the economics of cyber security are, and gives a summary of the main academic work in the field. The second focuses on analysing the extent to which states have taken these principles and applied them to their national cyber security strategies, and the final part of the report tries to draw out some recommendations and future challenges.

The economics of cyber security has become a fast-moving discipline and has drawn attention to policy-makers. Today, the digital and knowledge-based economy is a powerful engine of developed countries and has become a major driver of economic growth that can account for 8-10 % of the GDP in some countries.[13] According to a McKinsey report, cyberspace accounted for 4% of the world's GDP in 2010. The future of the knowledge-based economies will be determined by whether security and trust will be ensured for all users. Today 'the economic approach to information security focuses on the incentives of these actors and whether these incentives align with a socially optimal level of security'.[14]

The question of how to measure performance in cyber security is still largely unanswered. There have been various attempts at providing a return on investment (RoI) framework for security, a process that often fails because of the difficulty in quantifying the gains with any reliability. The identification of metrics to measure cyber security performance can be a considerable challenge.

One of the main objectives pursued when securing cyberspace is a nation's ability to sustain its economic activity through information and communication technology (ICT). It is considered of the utmost importance that the activities conducted by cyber means (banking, net-retail, services, administration, etc.) are protected and perceived as a common goal for all stakeholders to achieve the prosperity of societies, and this is one of the most recurring objectives pursued in NCSSs worldwide.

The discussion below will combine the principles of the economics of cyber security around national cyber security strategies in order to determine whether and to what extent it is possible to apply them in such contexts.

---

[13] 'The UK cyber security strategy: a landscape review', see *supra* (n11), at 4.

[14] Allan Friedman, *Economic and policy frameworks for cybersecurity risks*, Centre for Technology Innovation at Brookings, 21 July 2011, at 5, https://cs.brown.edu/courses/csci1800/sources/2011_Brookings_Cybersecurity_Friedman.pdf (last accessed November 30th 2015).

1. Economics of cyber security

The economics of cyber security applies principles of economics to the analysis of cyber security problems.[15] It is often thought that information security comes down to technical measures, but Anderson and Moore (2006) have characterised the issue as follows: '*People have realised that security failure is caused at least as often by bad incentives as by bad design*'.[16] This implies that better incentives are needed in order to increase investments in cyber security rather than focusing merely on technical measures.

In general, work in this field includes descriptions of the market, cost-benefit trade-offs by rational market participants, strategic behaviour analysis, market mechanisms, failures, and the economic impact of regulation by governments. Further efforts are dedicated to analysing the financial gains as motivation for cybercrime, modelling cybercrime and cyber security investment decisions, and the problems rising in the insurance sector. Risk management principles are further explored in order to better understand the economic aspects of cyber security.

2. Market challenges for cyber security

Several economic barriers for effective cyber security have been described in the literature and some will be described in this section.

2.1 Externalities

Economists try to determine whether the marketplace invests a socially optimal amount of cyber security. Private network owners do not internalise their cyber risks and when the loss resulting from such a risk affects not only the private network owner but also thousands of other users, it is known as an *externality*.[17] The IT industry can be characterised by many different externalities: network externalities, externalities of insecurity, and interdependent security.[18]

- Network externality. With the increase of the network, the value of it to each of its members grows. An example of this is the rise and dominance of the Windows operating system.
- Insecurity creating negative externalities. The lack of investment in cyber security by one market player can negatively affect the security of the others. Positive externality is the opposite where investment in cyber security by one market player creates increased levels of cyber security for all.

[15] IPACSO, FP7, Deliverable 4.1, State-of-the-art of the Economics of Cyber-security and privacy, at 9, http://ipacso.eu/downloads/public-deliverables.html (last accessed December 16th 2015).
[16] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.477.2090&rep=rep1&type=pdf (last accessed November 30th 2015).
[17] E. Dourado, J. Brito, *Is there a market failure in cyber security?*, MERCATUS ON POLICY, Mercatus Center, George Mason University, No 106, March 2012, at 2, http://mercatus.org/sites/default/files/publication/Cybersecurity_Dourado_WP1205_0.pdf (last accessed November 30th 2015).
[18] T.Moore, *Introducing the Economics of Cybersecurity:Principles and Policy Options*, see *supra* at 9.

- Interdependent security. This occurs where an investment by one market player creates positive externalities for others that in turn may discourage their own investment (free-riding). This occurs often where security depends on the weakest link, and market players not investing enough since others are not doing it either.[19]

On a larger scale, when countries are engaging in efforts to increase their own cyber security, this can also affect others.[20]

A market failure occurs where the market players do not invest enough in security to match the risk, and this is where government intervention becomes crucial.

2.2 Information asymmetry

Information asymmetry can be described as 'economic situations where market players act under conditions of incomplete information'.[21] Today's information systems can be best characterised by overwhelming amounts of data where accuracy and reliability are difficult, if not impossible, to determine. This problem prevails in the estimations of the cost of cybercrime, which are difficult to make due to the lack of data and to underreporting because of fear of reputational damage or fear of exposing systematic vulnerabilities. This means that the market players are likely not investing in the right defences and solutions with the right amounts of money. Ill-informed consumers are more likely to buy snake-oil solutions if they are unaware of the full extent of the threats.[22]

2.3 Incentives

The study of economic incentives gives a better understanding of the market driven behaviour and its relationship with cyber security. There is very little empirical evidence on incentives available[23] that shows the involvement of positive and negative externalities. Companies deciding whether or not to disclose threats and vulnerabilities within their systems can often be motivated to do so through certain legislative incentives, but others can be put off by disclosing threat and vulnerability information due to risks such as damage to reputation and trust, risk of liability, and effect on financial markets. Economic incentives can be described as follows:

> 'an inducement (motivation) that leads to an action or behaviour, which is rendering a (positive) payoff for the actor. Payoffs are outcomes of

[19] *Ibid.* at 9.
[20] 'The United States has made significant investments in reducing its cyber insecurity, some of which –it can be argued –have increased cyber insecurity of other nation states' in Jan Neutze and J. Paul Nicholas Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms, http://journal.georgetown.edu/wp-content/uploads/2015/07/gjia13001_Neutze-CYBER-III.pdf (last accessed November 30th 2015).
[21] IPACSO, FP7, Deliverable 4.1, State-of-the-art of the Economics of Cyber-security and privacy, see *supra* (n15) at 21.
[22] T.Moore, *Introducing the Economics of Cybersecurity:Principles and Policy Options*, see *supra* at 8.
[23] J.M.Bauer, M.J.G. van Eeten, *Cybersecurity: Stakeholder incentives, externalities, and policy options*, TELECOMMUNICATIONS POLICY 33, (2009) 706-719, at 711.

cost-benefit trade-offs. A rational actor seeks the optimal choice by maximizing payoff. In economics, utility functions model cost-benefit trade-offs and therefore represent preferences of actors. Where the outcomes of choices are uncertain, risk or ambiguity are introduced into the decision model'.[24]

Positive payoffs lead to incentives for the actor to perform a certain action, whereas negative payoffs may result in a disincentive and could lead to suboptimal choices. Such trade-offs do not only have to be monetary, but can also result in psychological costs and benefits as described earlier.[25]

Examples of economic incentives were outlined by Bauer and van Eeten (2009),[26] distinguishing them by security-enhancing and security-reducing incentives among the players in the ICT value chain.

3. Quantifying or measuring cyber security

In order to measure whether a certain security measure should be implemented or not, traditional models use a cost-benefit trade analysis which determines whether a certain investment is justifiable and allows the total expected cost of each option to be compared against the total expected benefits to see whether the benefits outweigh the costs, and by how much. Their effectiveness also depends on whether the cost-benefit trade off can be related to the achievement of the intended goal.

However, it is extremely difficult to estimate the cost and the benefit factors in cyber security. A company adopting this model needs to know all the costs, both direct and indirect, and all the benefits involved, and the benefits have to exceed the costs.

The difficulty of quantifying indirect costs is especially acute where the investment in security of a company can indirectly improve the security of another connected company. A quantitative assessment of the benefits of security investment can also prove to be problematic if tangible benefits cannot be estimated. This may result in situations where companies only invest reactively after a large data breach where a business case can easily be made.

4. Return on security investment model

Every organisation needs to decide how much it wishes to invest in cyber security, and how much cyber security is enough. The classic returns on investment (ROI) model is a performance measure used to evaluate the efficiency of an investment or to compare the efficiency of a number of different investments.[27] The formula to calculate ROI is as follows:

[24] IPACSO, FP7, Deliverable 4.1, see *supra* (n15) at 10.
[25] IPACSO, FP7, Deliverable 4.1, see *supra* (n15) at 11.
[26] J. M.Bauer, J.G. van Eeten, Cybersecurity: Stakeholder Incentives, externalities, and policy options, *Telecommunications Policy* 33, at 706-719
[27] See the definition on the following:
http://www.investopedia.com/terms/r/returnoninvestment.asp

$$ROI = \frac{\text{Expected Returns-Cost of investment}}{\text{Cost of investment}}$$

However, this formula is not suitable for security investments, since security does not yield profits; rather, it prevents losses.[28]

A modified ROI calculation can be applied to security investments, hence the term 'return on security investment' (ROSI) which is a key performance indicator that enables organisations to measure the efficiency and effectiveness of spending on IT security by comparing costs, and the preventative and corrective benefits that reduce the probability of losses.[29] It enables an organisation to determine whether it is investing enough in security, whether it is cost-effective, and whether there could be an impact on the organisation's productivity if certain investments in security are not made.

In order to calculate ROSI, one needs to evaluate the amount of potential loss that can be saved by a security investment by comparing the monetary value of the investment with the risk reduction.[30] Quantitative risk assessments are methods for putting a value on risk.

The classic example for quantifying risk is the Annual Loss Expectancy (ALE)[31] which is the total cost of an incident or Single Loss Expectancy (SLE) (both tangible and intangible), multiplied by the probability of the risk or the Annual Rate of Occurrence (ARO) occurring within that year.

ALE= Single Loss Expectancy (SLE) (total cost)*** Annual Rate of Occurrence** (ARO)(probability of risk).

The ROSI model combines the quantitative risk assessment and the cost of implementing security for a specific risk. There are various ROSI models available and no one single model that fits all organisations. Several factors need to be taken into account when assessing which ROSI model should be applied, including the degree of exposure to risk, the nature of vulnerabilities, the type of hazard, the absence or weaknesses of compensating controls, geographic location, type and model of business, critical sectors of the business that depend on IT, and competitor strategy toward IT security.[32] Several explanations of the ROSI model are available (e.g. ENISA, 2012; Sonnenreich, 2006).

The ROSI formula is as follows:

---

[28] Bruce Schneier, https://www.schneier.com/blog/archives/2008/09/security_roi_1.html (last accessed November 30th 2015).
[29] ISACA – *IS Auditing Guideline: G41 Return on Security Investment (ROSI)*, 2010, at 215; http://www.isaca.org/knowledge-center/standards/documents/it-audit-assurance-guidance-1march2010.pdf (last accessed November 30th 2015).
[30] ENISA, ntroduction to Return on Security Investment, see *supra* (n10) at 4.
[31] The Annualised Loss Expectancy (ALE) is the annual monetary loss that can be expected for an asset due to a risk.
[32] ISACA – *IS Auditing Guideline: G41 Return on Security Investment (ROSI)*, see *supra* (n29) at 215.
[32] Ruce Schneier, see *supra*.

$$ROSI = \frac{(ALE * \%risk\ mitigated) - cost\ of\ security}{cost\ of\ security}$$

This formula combines the ALE (monetary loss reduction) and the estimated percentage of effectiveness of a certain security solution with the cost of the investment, in order to determine whether employing a certain solution is cost-effective.

Such calculations are usually based on metrics that have been gathered internally within an organisation or from external resources. Here again is where the problems arise, due to the difficulties of estimating losses that may never occur, and the availability of good data on, for example, crime rates, cost of damage, and effectiveness of countermeasures). Estimations can often be biased by our perception of risk and the calculation can be easily be manipulated in order to fit the needs of the users to justify a decision.[33] Finding accurate data on incidents is another hurdle to be overcome, since many of the organisations suffering data breaches do not wish to share this information, often for reputational reasons. In addition, estimating the cost can be a challenge for several reasons:

1) The majority of the information is classified;

2) Non-classified information flows through many different organisations for various activities; and

3) There is a lack of effective reporting mechanisms.[34]

The complexity of measuring cyber security is illustrated above. Most of these models and formulas are used by the private sector on an organisational level to different extents. The discussion that follows will focus on whether these models and formulas can be applied to a whole nation state.

5. Government intervention

The main discussion in the available literature boils down to whether cyber security is a public or a private good and whether government intervention is necessary and justified to regulate the market. Significant investments have already been made by individuals, businesses and to some extent governments; however, it is clear that cyber security cannot be left only for the private sector to handle. This holds especially true for a nation's critical infrastructure sectors. The situation has allowed some governments to justify intervention through various means – regulatory, supervisory, coordinative, and incentive- and disincentive-based (i.e. financial).

In economic theory, goods are usually seen as public or private. The former can be defined as non-rivalrous and non-exclusive. A non-rivalrous good means that the use of the good by one person does not affect its use by others. A non-

[33] ENISA, *Introduction to Return on Security Investment*, see *supra* (n10) at 7.
[34] National Audit Office, *The UK cyber security strategy: Landscape review*, see *supra* (n11).

exclusive good means that the availability of the good to one person means that it is also available to every other person. The latter, a private good, is a good that cannot be used in a non-rivalrous manner.

There are two problems with the theory of public good: free-riders and assurance. Free-riders typically refrain from contributing to the common good whilst trying to benefit from it. Assurance is the opposite situation where people avoid contributing to the establishment of a public good due to the belief that there will never be enough other contributors, hence one's efforts become fruitless.

Cyber security is usually regarded as having the characteristics of a private good that is sold by private companies on the marketplace to governments, businesses and consumers. However, certain types of cyber security solutions have the characteristics of a public good, such as threat and vulnerability information about new and evolving cyber intrusions. The lack of understanding of the concept of public goods explains the unwillingness to share information, and this is often reflected in legislative and regulatory initiatives.

6. The impact of the economics of cyber security on NCSSs

At least 50 countries worldwide have issued an NCSS in the last decade due to increasing threats in cyberspace. A wave of next generation NCSSs are starting to surface, demonstrating an integrated and comprehensive approach towards cyber security, taking into account economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects. In the EU, several member states have updated their strategies (e.g., Czech Republic,[35] Estonia,[36] Netherlands,[37] France[38]). The overwhelming objectives of these new strategies are to increase economic and social prosperity, and to provide protection against cyber threats. More specifically, partnerships with industry, economic drivers, and incentives are prioritised, including public private partnerships, identification of critical business actors and sectors to the economy, creating cyber insurance, and creating technological independence in cyber security.[39] The state must still determine the proper level of cyber security, and how it can incentivise private actors to invest in a sufficient level of cyber security.

Whereas most companies invest in proactive as well as reactive investment security strategies, it is unclear from the national security strategies whether the

[35] https://ccdcoe.org/sites/default/files/strategy/CZE_NCSS_en.pdf (last accessed November 30th 2015).
[36] https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (last accessed November 30th 2015).
[37] https://ccdcoe.org/cyber-security-strategy-documents.html (last accessed November 30th 2015).
[38] http://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf (last accessed November 30th 2015).
[39] http://www.oecd-ilibrary.org/docserver/download/5k8zq92vdgtl.pdf?expires=1448287495&id=id&accname=guest&checksum=18BBA6F76B1F992D994E9746DE000BC0 (last accessed November 30th 2015).

economic impact has been taken into account, or whether it is done proactively (trying to quantify the risk at the beginning of the strategy) or reactively (evaluating the success of the strategy based on key performance indicators). NCSSs often include policy measures to increase confidence and trust among stakeholders, including citizens and businesses. More awareness campaigns and industrial strategies are being promoted by member states. However, it remains unclear how these policies and their successes are measured, either before or after implementation. Reliable data about such measurements is not readily available and further research into measuring the economic aspects of cyber security strategies is difficult, if not impossible.

7. Metrics to assess the efficiency of cyber security strategies

Given the considerable investments in cyber security from both the private and public sector, it is important to determine how a state (or any other actor) could devise the proper metrics to assess the efficiency of policy measures, and whether the classical ROSI could be applied to NCSSs.

Further research into the topic does not result in a lot of information. A brief OECD survey[40] on the matter yielded some results from various stakeholders. Some of the possible metrics that should be implemented in national strategies are as follows:

- Cost-effectiveness;
- Useful information-sharing;
- complaints;
- Positive and negative impacts on the level of security as measured by breach or other malicious behaviour;
- Costs to business; and
- Economic growth in the use of the internet and the economy.

Some believe that concepts such as fundamental human rights should be included in these metrics, in the form of a human rights compliance checklist or an impact assessment covering this topic. Others would like to measure the level of international participation pre- and post-policy implementation. These recommendations, however, do not address the research question and stay on an abstract level without any practical proposals on how they could be implemented.

Some methods of evaluation of NCSSs have been published by ENISA and give an outline of different options and key performance indicators to measure the efficiency of national cyber security strategies.[41] Evidence-based approaches in cyber security strategies have already been used in the Digital Agenda for

[40] OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy', p 111, http://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf (last accessed November 30th 2015).

[41] ENISA, An evaluation Framework for National Cyber Security Strategies', November 2014. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1 (last accessed November 30th 2015).

Europe and the NIS Directive in order to allow member states to monitor the situation. Member states would be required to submit a report on the results annually to the European Commission, which would then compare the results against the objectives taken up in the Digital Agenda strategy.[42]

Some countries, including the UK[43] and US[44] have conducted financial assessments on whether they have received best value for money in their cyber security investments. Neither of these assessments goes into detail on how and which measurements were used. The UK review acknowledges that it is difficult to measure value for money, but it draws on previous experience in other fields such as counterterrorism. Its approach to measuring value for money is to develop a logical relationship between strategic objectives and strategic benefits, activities under way, deliverables committed, and measurable benefits. These benefits need to be accurate, reliable, credible, and readily available from open sources.[45] The steps for identifying best value for money in the UK strategy include:

- Defining what constitutes success in terms of outputs and outcomes at which time and identifying potential comparative measures of good performance;
- Identification and collection of timely and reliable data and evidence on expenditures through robust processes;
- Developing comparators or benchmarks against which success will be assessed. Benchmarks could include baseline performance before the intervention or strategy, looking at the experiences of other countries and counterfactual scenarios.

The UK National Audit Office also identifies some of the challenges that can turn out to be fundamental obstacles in reaching accurate figures and estimations. Firstly, it recognises that the success of the measurement will be in terms of events not happening – in other words, if events do not happen it is difficult to measure whether the success of the strategy was due to its policy implications or some other reason. Second, it is difficult to determine which parts of the strategy have contributed to the overall success, and the value to be assigned to such success.[46] So far, it seems that only the UK has included the economic concept in the context of their national strategy to such an extent.

The US General Accountability Office (GAO) addresses this cost and resources issue as follows:

> 'While past strategy documents linked certain activities to federal agency budget requests, none have fully addressed cost and resources, including

[42] *Ibid.* at 10.
[43] National Audit Office, '*The UK cyber security strategy: Landscape review*', See *Supra*.
[44] Statement for the Record To the Subcommittee on Terrorism and Homeland Security, Committee on the Judiciary, 'CYBERSECURITY
Continued Efforts Are Needed to Protect Information Systems from Evolving Threats, released November 17th 2009 http://www.gao.gov/new.items/d10230t.pdf (last accessed November 30th 2015).
[45] National Audit Office, '*The UK cyber security strategy: Landscape review*', See *Supra*.
[46] *Ibid.*

> justifying the required investment, which is critical to gaining support for implementation. Specifically, none of the strategy documents provided full assessments of anticipated costs and how resources might be allocated to meet them'[47].

In conclusion, we have seen that current methods use *a posteriori* evaluation and audits due to lack of data. Implementing the necessary regulations to encourage sharing of such data would be a starting point. This would enable better quantification of the efficiency of NCSSs. An example of such an initiative would be the breach reporting system envisioned in the NIS directive. A better identification of the roles and responsibilities within structures is needed in order to achieve such a goal. Collecting such data should be the responsibility of one single body, but should be divided among the different stakeholders, whether government or private sector. The quantification of cyber security policy performance would also be a useful tool to guarantee the oversight of government spending to ensure best value for money.

[47] Testimony Before the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs, U.S. Senate 'A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges' (Statement of Gregory C. Wilshusen, Director Information Security Issues disclosed on March 7th 2013). http://www.gao.gov/assets/660/652817.pdf (last accessed November 30th 2015).

Annex II - Workshop findings

The workshop, organised by the NATO CCD COE and chaired by Prof. Johannes M. Bauer from Michigan State University, brought together 11 experts from the United States, United Kingdom, France, Germany, the Netherlands and Estonia, and took place in Estonia on 17-18 December 2014. The participants presented their views on the economic aspects of cyber security, and introduced their current research in this field. They also engaged in lively discussions during which they exchanged their opinions on the topic.

1. Workshop objectives

Evaluating a public policy, and especially a security policy such as the one implemented through these national cyber security strategies (NCSS), requires assessment of the following:

- Effectiveness – how possible is it to reach an optimal level of cyber security;
- Efficiency – results and resources used; and
- Relevance and impact (are these policies legitimate).

This approach enables the policy-makers to be accountable, and also to decide whether the course is right and should be pursued. Thus, the economic aspects of NCSS are crucial to ensuring its proper implementation. In order to provide a framework for the discussions, certain overarching statements about the economics of cyber security were presented during the introductory remarks.

For anyone investing in cyber security, several inevitable questions arise: 'What do I get for my money? What am I defending against?' We have to realise that the internet looks very different from what people expected 20 years ago. Nowadays, cyber security is a collective asset. Information security is much more than a technical issue; it is also a behavioural and economic issue. We can see a certain parallel in the world of cybercrime, which has become organised, exhibiting features such as division of work and trust-building among cyber criminals.

National cyber security strategies are but one attempt to face the challenge of cyber security. There are two perspectives that need to be taken into consideration; the macro and micro levels. The project will link these two levels, ideally resulting in a book. The workshop is only a first step in the project; it is an experiment to try to bridge the gaps between those two dimensions.

2. Economic aspects of national cyber security strategies

Grand strategies from the past were aimed at 'winning the peace'; the Cold War paradigm changed this into 'containment'. Ours is an era of the end of epochal conflicts. We maintain this legacy and wish to achieve 'cyber peace' through the same mind-set, but the future will be more about resilience. The frequency and intensity of cyber attacks are clear proof that there is no end to history. Atomised risk analysis exacerbates systemic risks, as complex systems tend to organise themselves in the direction of catastrophic shifts. In this context, contingency measures will prove difficult to uphold because the cost-benefit

analysis is usually done ex post. Innovation is driven down because the private sector tries to maximise efficiency with minimum investment in innovation.

In order to provide a practical example during the course of the workshop, the experience of cyber security from the perspective of Estonia was presented. Modern states, including Estonia, are reliant on ICT, and have developed their 'digital way of life' or 'information society', which is a value in itself, and is based on trust. Cyber security's main aim should be to protect this trust.

Since Estonia is a small country, it has a higher per capita cost in providing adequate public services to its citizens. Therefore, it had to look for creative solutions, and developing the information society was a prime opportunity to reduce costs. The new cyber security strategy for 2014-2017 promotes effective coordination with private sector stakeholders, coordinated national defence planning, and preparation for civil emergencies, as well as international multiagency cooperation.

Turning to the cost of cyber security globally, it is difficult to quantify either the losses arising from cyber attacks or the real expenditures on cyber security. The estimates of losses provided by cyber security can sometimes amount to a security racket. It can be easier to find metrics when analysing cyber security expenditures within NATO countries' defence budgets, but even that does not tell us much about the actual effect on cyber security. A comment was also made about the effect of private spending on cyber security.

3. Cyber security as a public policy and the role of government

A cyber security strategy is a political act; it creates expectations and raises awareness among businesses and civil society. However, the implementation of this type of policy comes at a cost. The acceptable level of loss from cyberattacks must be taken into account when drafting a strategy. When addressing cyber security, governments need to answer question about whether competition will do the job, or whether they need to regulate in order to address market failures. The strategies contain a co-regulatory structure, similar to spectrum allocation, and these strategies should define the burden sharing and the efficient alignment of responsibilities by a better allocation of risks. Cyber security is structured in layers with incidents ranging from 'people can die' to 'people can lose trust in e-commerce' that require adapted answers and the involvement of many actors, thus rendering governance of cyber security difficult.

Cyber security is different from security transposed to cyberspace. Enormous volumes of unstructured data, inhumanly short time scales, and strong emergence mean that institutional models based on one-sided liability, arbitrary separation of public and private interest, or a focus on malevolent actors as the source of risk are likely to do more harm than good, because of individual and collective adverse selection and moral hazard, including stable business models based wholly on 'insecurity rents.'

These difficulties stem from the fact that internet governance is a matter that remains to be addressed. The architecture of the internet is more fragmented than it was 15 years ago, but the US government's footprint is still significant. A

large part of the internet addressing system is delegated by the US government to ICANN, enabling the US to take drastic measures. For example they were able to shut down the internet in Iraq in 2003 by wiping the IP addresses, and to take down the Megaupload website in 2012. Currently, ICANN, a US non-profit organisation, still has a say in internet governance, and the internet is regulated by RFCs. The governance structure can thus be described as a horizontal network. During the ITU's World Congress on Information Technology 2012, OECD countries refused the proposal to transfer internet governance from ICANN to the ITU, giving little ground to the multi-stakeholder approach. The omnipresence of the US in the multi-stakeholderism approach is also a complication. There will always be the tension between the 'get it right' and 'get it done' approach. This Wilsonian self-determination may or may not work, as shown in the issues of the adoption of IPv6 v. IPv4, or the SWIFT.

Competition is very important for the internet to thrive and the problem with the internet is how to maintain its openness, an asset both from the civic and economic perspectives. What would qualify as fair governance? There are arguably three new forms of legitimacy that are key to achieving these goals: impartiality, reflexivity, and proximity. Cyber security can be seen as a factor impairing the openness of the internet if the incentives are not aligned and everything turns into a weak link. There is a growing consensus that nations bear increasing responsibility for enhancing cyber security. However, states imitate each other's cyber security strategies and, usually, they are written as broad vision statements; although, for example, the national cyber security strategy of Saudi Arabia is an incredibly detailed 100 pages. These broad visions do not provide many good practices. Hence, managing cyber attacks must be a bottom-up multi-stakeholder endeavour with the active engagement of the private sector. In that perspective, businesses play a vital role in promoting 'cyber peace' by identifying and spreading cyber security best practices such as the burgeoning cyber risk insurance industry. Cyber risk insurance is on the rise, with the market reaching $750 million in 2011.

Thus, a polycentric institutional analysis could be applied to cyberspace, even though remain the problems of fragmentation and gridlock. Nevertheless, lessons can be learned from the sustainability movement; environmental law principles could serve as a model. The notion of Corporate Social Responsibility may re-emerge to play a significant role in cyber security.

Bottom-up and top-down approaches complement each other, but not necessarily in a good way. One must also bear in mind that cyber security is only a cyber artefact, whereas climate change is irreversible. For example, the problem of US cyber security law and policy is the lack of real reform. Cyber security is regulated by executive orders, and the focus is placed on critical infrastructure. Some changes are happening at the level of National Institute Standards (NIST).

4. Metrics to assess the efficiency of cyber security strategies

Measurement, if available, is an important step in the decision-making process in the domain of cyber security. In terms of quantification, the measurement of the ROSI (return on security investment) is one of the most widely used tools. It

is designed to analyse the cost-benefits of security investments. The system of metrics can include various concrete and abstract indicators on the cost and benefit sides. The ISO model and the VeriMetrix measurement model can be mentioned as examples. When considering security investments, many externalities that are involved in the process have to be identified. As a matter of fact, security is interdependent, due to software engineering, interconnected supply chains, information-sharing in online social networks, and the existence of botnets and the nature of the internet.

The question has shifted from 'How much is enough?' (Gordon and Loeb's 2002 model) to 'Where and when to invest?' Uncertainty also plays a key role in the timing of security investments, having an effect on the choice of proactive and reactive protection measures. A question was raised about factoring in reputational risk. In this respect, the EU Network and Information Security (NIS) directive was mentioned as an important effort to reduce the externalities. However, if the rules are stronger, is the compliance better? The whole industry can be affected by an incident, and crisis communication is important.

If data is taken out of context, it is useless; for example, when the rate of cybercrime is correlated to the cyber infrastructure of a particular country. The problem with best-practice measures is that not a single one of them has been properly tested (incident data, attack prediction, situational awareness, security performance metrics, or evaluation). Reputation metrics are based upon anecdotal evidence; metrics themselves can work as security incentives.

An example of a project to develop a reliable reputation metrics for security of services of internet intermediaries was provided. A higher level of cyber security regulation (e.g. the proportion of ISPs participating in the London Action Plan), and a higher level of competition between ISPs in a particular country, are correlated to lower infection rates. A big part of the ISPs' performance in fighting botnets is caused by automation. A question was raised about the relationship between networks' structures and the rate of infection; epidemiological data for Conficker, SIR, and SIS models show that the relationship does not really work this way.

With metrics, states could agree on a common cyber security label, which could actually be good for the security industry due to the protection measures that need to be implemented, and benchmarking. NIS information-sharing processes are untested, which will increase the number of audits required. In the Netherlands, the cyber security issue is centralised by the government, which acts as the clearing-house. The benefit of public private cooperation is to reach a normative approach that mixes performance ratings. Measurement is something for which there is no substitute, and which corrects the discrepancy between the self-image of the ISPs and reality.

5. The cyber security industrial complex

Do we see the emergence of a cyber security industrial complex? Is it comparable to the military-industrial complex that Eisenhower was warning us against during the Cold War? Should we worry?

Companies providing cyber security services are making money, as there is a real market worth billions of dollars. Drawing from older examples, there are some real concerns that governments may not be getting what they need for the money they spend. For example, the US Government spent $1 billion on HP telling the Navy what it did on information architecture overhaul and system integration. This is the problem of the revolving door: it is difficult to trust the expertise when people are worrying more about their future job than about national interest. There is also the apt aphorism about the perfect weapon (for example, the case the B-1 bomber) that has 435 parts – one for each congressional district. A third of billboards on the Washington subway advertise defence industries, including cyber security firms.

The ideas of 'Cyber Pearl Harbor' and 'cyber war' have been around for a while, used or derided by public figures, but they are clearly serving the interests of cyber security companies. For instance, the private sector is interested in the hack-back capability that a company like *Crowdstrike* can provide. They also help them deploy honeynets of their own, assist them in the intelligence gathering effort in order to find out who exactly is the attacker. *Endgame* is probably selling zero-day exploits despite statements to the contrary; there are a number of countries that are buying. Another phenomenon is the porosity between the policy-makers' world and the corporate world. Everyone sits on everyone's board. For example, Richard Perle helped establish *Palantir* in the intelligence community. While, speaking of security rackets, *Tiversa* is a company which scans P2P networks looking for private files and subsequently offer protection for these files.

On another note, can we really frame this issue by declaring 'private good, public bad' – 'innovativeness and efficiency vs. capture and waste'? There can always be the argument in favour of 'blue skies' research that might find an immediate application, but some innovations are generated by the cyber security industry. However, can this be sustainable without massive investment? Brand names are established and it is very hard to enter the market. There have been large-scale IT transformations with mergers, and large corporations can be as bad as public sector.

The cyber security industry is a bonanza for arms producers. In Europe, traditional security companies are expanding into the cyber security market via acquisitions and partnerships (e.g. BAE and Detica). States are investing in cyber security and companies are making use of their long-term good relationship with states. The defence market is characterised as a monopsony and oligopoly, and the Iron Triangle is also at work here. Critical information infrastructures are largely privately owned and states do not have the capabilities to protect them.

The arms market and the cyber security market have several common features: security is a public good; there is a need for trust between the government and the companies providing security; fear is often used as a legitimation of public security policies; and there is an interest in sophisticated tools for both attack and defence. But there are also differences: cyber security is usually not about violence; the structure and composition of the markets are drastically different;

and states have to work with the wider ICT industry to make their products safer by design, rather than only with security companies to fix the problems.

In Europe, the industry is fragmented and there is a redundancy of industrial efforts. The EU should help avoid fragmentation, which is the key goal of the *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*. ENISA proposes a model based on pull by demand, the adoption of common cyber security standards, and R&D funding to accelerate the uptake of EU-centric approaches. Commenting on the previous statements, other workshop participants were more sceptical about the adoption of common standards and more cross-border defence procurement in Europe. Maybe the EU does not want one standard because that would be the US standard.

This workshop proved a great venue for exchange between different specialists in their respective domains applied to the field of cyber security, and was a revitalising experience. However, it was just a first step towards a broader project that would encompass the wide range of topics that were touched on.