

NATIONAL DEFENSE AND SECURITY ECONOMICS

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY

—

ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

Economic Dimension of Cyberspace as New Security Threat

Content of Topic

- Introduction
- Basic Concepts
- Cyberspace as a New Security Threat
- Economic Analysis of Cyberspace
- Economic Aspects of Potential Cyber Conflict
- Conclusion

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

INTRODUCTION

Economic Dimension of Cyberspace as New Security Threat

Introduction

- **Main Objective of these lecture is** to explain economic aspect of cyberspace as a new security threat.
- **As partial aims of this lecture, we can see:**
 - definition of cyberspace as security threat,
 - carrying out economic analysis of cyberspace and cyber conflict,
 - demarcation of economic aspects and impact of cyber conflict and
 - description factual examples of executed cyber attacks on national states.

Economic Dimension of Cyberspace as New Security Threat

Introduction

- **Threat of Cyber conflict** is totally up-to-date and vital topic (Cyberspace is number one topic all important political, economic and security discussion).
- **Cyber attack protection** become government, non-profit and for-profit firms care.
- **Cyber attack** can lead to massive financial losses, economic instabilities or even if as a last resort to war.
- **Danger of Cyber conflict** is now a major arena of political, economic, and military contest.

Economic Dimension of Cyberspace as New Security Threat

Introduction

- Despite this potential for harm, little agreement exists on how to respond.
- One problem is the lack of understanding, especially among policymakers, about how interconnected and vulnerable our increasingly sophisticated computer networks are.

Economic Dimension of Cyberspace as New Security Threat

Introduction

- **Beyond this lies a whole host of thorny analytical questions:**
 - What is our ability to track the source of attacks?
 - How susceptible are we to "false flag" attacks where the attackers deliberately seek to "frame" another actor as carrying out an attack?
 - What responsibility should governments bear for attacks carried out by their nationals on foreign governments or entities?
 - How should the responsibility for defending against cyberattacks be apportioned between government and the private sector, between national governments and the international community?
 - Can deterrence work in cyberspace?

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

BASIC CONCEPTS

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

"Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. [...] Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e., cyber security."¹⁶²

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyberspace

the novel 5th space of warfare after land, sea, air, and space, is all of the computer networks in the world and everything they connect and control via cable, fiber-optics or wireless. It is not just the Internet – the open network of networks. From any network on the Internet, one should be able to communicate with any computer connected to any of the Internet's networks. Thus, cyberspace includes the Internet *plus* lots of other networks of computers,¹⁰ including those that are not supposed to be accessible from the Internet.

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyberspace – basic characteristic

- cyberspace is that *it cannot exist without being able to exploit the naturally existing EMS.*
- *cyberspace requires man-made objects to exist*, which again makes **cyber-space unique** when compared to the land, sea, air, and space domain.
- *cyberspace can be constantly replicated*
- ***the cost of entry*** into cyberspace is relatively cheap.
- ***the offense rather than the defense is dominant in cyberspace***, for a number of reasons

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyberspace – basic characteristic

- *the offense rather than the defense is dominant in cyberspace*, for a number of reasons:
 - defences of IT systems and networks **rely on vulnerable protocols** and open architectures, and the prevailing defense philosophy emphasizes **threat detection, not elimination** of the vulnerabilities
 - **attacks** in cyberspace **occur at great speed**, putting defences under great pressure, as an attacker has to be successful only once, whereas the defender has to be successful all the time.
 - **range is no longer** an issue in cyberspace since **attacks can occur from anywhere in the world**.
 - modern society's overwhelming reliance on cyberspace is providing any attacker a **target-rich environment**, resulting in great strain on the defender to successfully defend the domain.

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyber security risks are defined:

- as risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems.

The strategy furthermore exposes the context in which the main cyberspace-related risk vectors exist, in particular:

- cyber espionage and military activities supported by governments,
- the use of the Internet by terrorists, and
- cyber crime.¹⁶³

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyber conflict

- the use of computer power for intelligence gathering or to attack the computer, communication, transportation, and energy networks of states or non-governmental groups.

Dostupné na:

http://resources.sei.cmu.edu/asset_files/TechnicalNote/2010_004_001_152_00.pdf

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyber warfare refers to a massively coordinated digital assault on a government by another, or by large groups of citizens.

- It is the action by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption.
- The term cyber warfare may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent.

Accessible on: <http://definitions.uslegal.com/c/cyber-warfare/>

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyber attack

- is usage concrete forms of electronical means for not only intelligence activity but mainly for assault, infiltration of destruction of computer, communication, transport or power producing network privately or publicly owned.

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Cyberwar

- is conflict that occurs in cyberspace among state actors and represents sort of war, based on destruction enemy by computer systems.
- Impact of the this form of war can take form of tangible and intangible damage from inaccessible websites to material destruction of military and civilian systems, facilities and infrastructures.

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Netwar

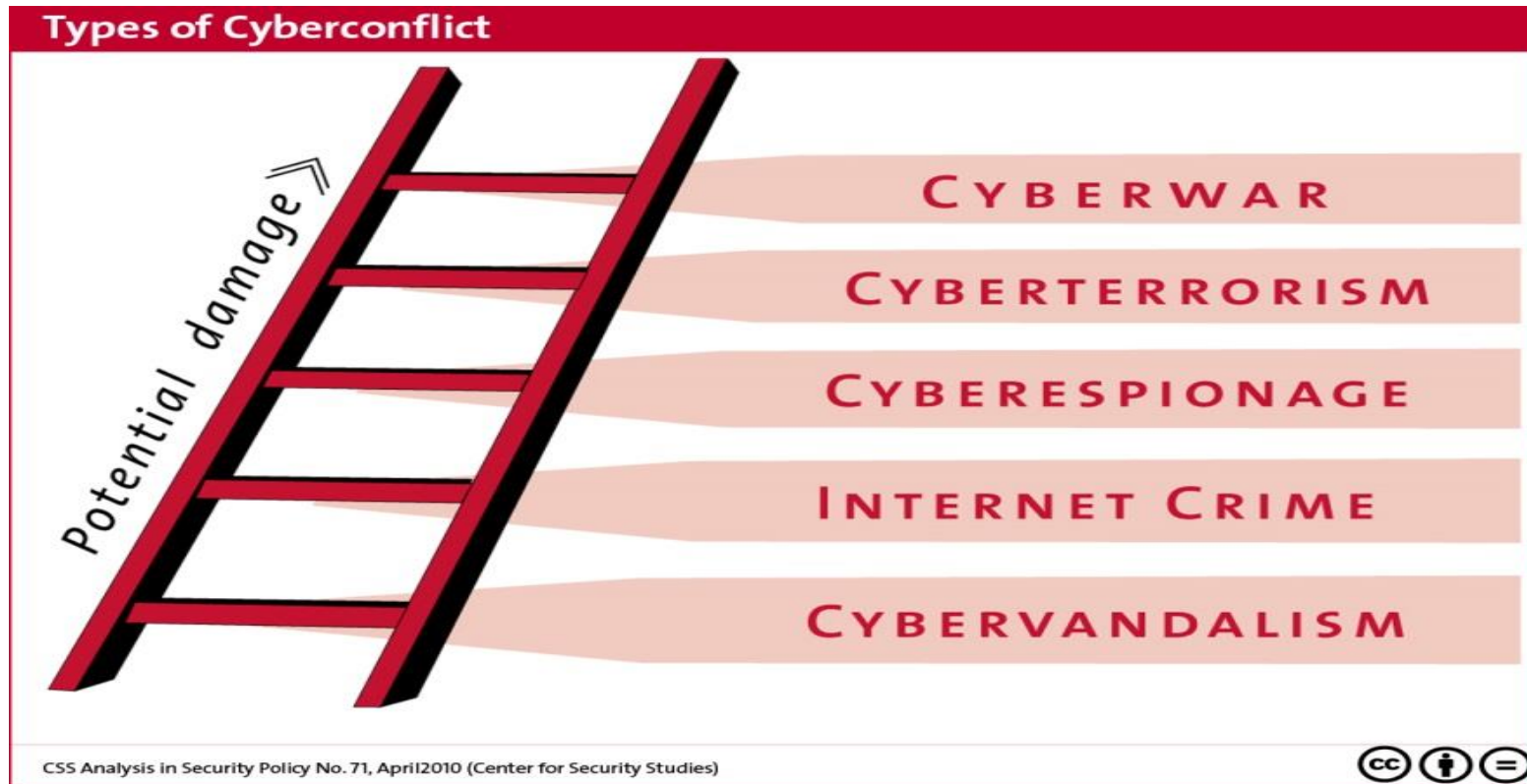
- refers to an emerging mode of conflict (and crime) at societal levels, short of traditional military warfare, in which the protagonists use network forms of organization and related doctrines, strategies, and technologies attuned to the information age.
- These protagonists are likely to consist of dispersed organizations, small groups, and individuals who communicate, coordinate, and conduct their campaigns in an internetted manner, often without a precise central command.
- Thus, netwar differs from modes of conflict and crime in which the protagonists prefer to develop formal, stand-alone, hierarchical organizations, doctrines, and strategies as in past efforts, for example, to build centralized movements along Leninist lines.

ARQUILLA, John., RONFELDT, David. The Advent of Netwar“ .

Economic Dimension of Cyberspace as New Security Threat

Basic Concepts

Classification of cyber conflict



FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

CYBERSPACE AS A NEW SECURITY THREAT



INVESTMENTS IN EDUCATION DEVELOPMENT

Economic Dimension of Cyberspace as New Security Threat

Cyberspace as a New Security Threat

- Cyberspace as a Security Threat for national defense (Armed Forces)
- Cyberspace as a Security Threat for whole society (countrywide context)

Economic Dimension of Cyberspace as New Security Threat

Cyberspace as a New Security Threat

Cyberspace as a Security Threat for national defense (Armed Forces)

- For the top brass, computer technology is both a blessing and a curse. Bombs are guided by GPS satellites; drones are piloted remotely from across the world; fighter planes and warships are now huge data-processing centres; even the ordinary foot-soldier is being wired up. Yet growing connectivity over an insecure internet multiplies the avenues for e-attack; and growing dependence on computers increases the harm they can cause.
- And given that computer chips and software are produced globally, could a foreign power infect high-tech military equipment with computer bugs? “It scares me to death,” says one senior military source. “The destructive potential is so great.”

Economic Dimension of Cyberspace as New Security Threat

Cyberspace as a New Security Threat

Cyberspace as a Security Threat for whole society (countrywide context)

- What will cyberwar look like? In a new book Richard Clarke, a former White House staffer in charge of counter-terrorism and cyber-security, envisages a catastrophic breakdown within 15 minutes. Computer bugs bring down military e-mail systems; oil refineries and pipelines explode; air-traffic-control systems collapse; freight and metro trains derail; financial data are scrambled; the electrical grid goes down in the eastern United States; orbiting satellites spin out of control. Society soon breaks down as food becomes scarce and money runs out. Worst of all, the identity of the attacker may remain a mystery.

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

ECONOMIC ANALYSIS OF CYBERSPACE



INVESTMENTS IN EDUCATION DEVELOPMENT

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

- Levels of economic aspect research of cyberspace as security threat
- Economic principles usefulness for economic analysis of cybernetic security
- Microeconomic analysis of cyber security securing
- Macroeconomic analysis of cyber security securing

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

LEVELS OF ECONOMIC ASPECTS OF CYBERSPACE RESEARCH	
Order	Aim of research
Level 1	Cyber conflict and war as an alternative of conventional warfare
	Cyber conflict and war as an part of conventional warfare
Level 2	Microeconomic analysis of return rate of investment and non-investment expenditures on cyber security securing
	Microeconomic analysis of optimal level of investment on cyber security and defense
Level 3	Microeconomic analysis of costs imposes on society and individuals by cyber war and cyber conflict

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

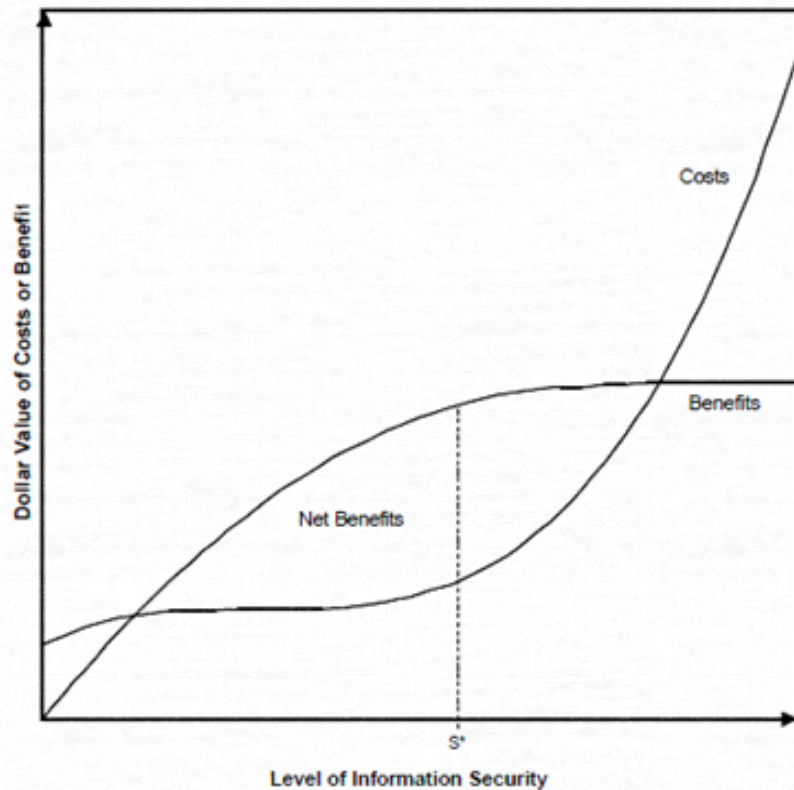
Economic principles usefulness for economic analysis of cyber security

- principle of the marginal opportunity costs,
- principle of expected marginal costs and benefits,
- principle of substitution,
- principle of diminishing returns,
- principle of diminishing benefits.

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

Microeconomic Analysis of Cyber Security providing



Benefits and costs of cyber security providing

Point S^* is place maximum difference between costs and benefits of securing of cyber security .
Mathematically is situation described as:

$$G(S) = B(S) - C(S)$$

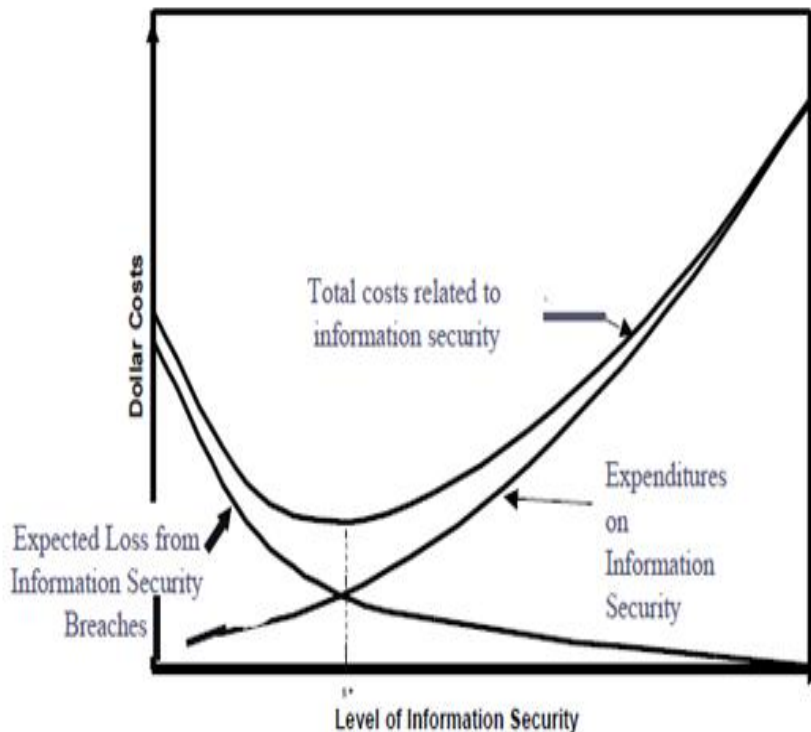
$$\frac{dG}{dS} = \frac{dB}{dS} - \frac{dC}{dS} = 0$$

$$\frac{dB}{dS} = \frac{dC}{dS}$$

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

Microeconomic Analysis of Cyber Security providing



Total costs of cyber security providing. These costs is possible to describe following formula:

$$TC_{CS} = E_{CS} + EL_{CA}$$

where

TC_{CS} total costs of cyber security providing,
 E_{CS} Costs of cyber security providing borne by separate endangered actors,
 EL_{CA} Expected impacts of cyber attack (loss of profit or damage imposed on individuals of societal organizations).

Economic Dimension of Cyberspace as New Security Threat

Economic Analysis of Cyberspace

Macroeconomic Analysis of Cyber Security providing

$$GDP = C + I + G + NX$$

C Expenditure households on consumption

I Private gross homeland investment

G Government Expenditure on purchase of products and services

NX Net export

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

ECONOMIC ASPECTS OF POTENTIAL CYBER CONFLICT

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

- Incentives to not Reveal Information about damages cause by cyber attack
- Classification of cost imposes by cyber conflict

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

Incentives to Not Reveal Information

- Financial market impacts
- Reputation or confidence effects
- Litigation concerns.
- Liability concerns.
- Signal to attackers
- Job security

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

Classification of cost imposes by cyber conflict

- Classification of cyber conflict costs according to its character and impact
- Classification of cyber conflict costs according to ownership character of damaged subject
- Classification of cyber conflict costs according to time character costs (preventive and a eliminative character of costs).

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

Classification of cyber conflict costs according to its character and impact

Typ nákladů		Popis dané kategorie nákladů
Finanční náklady	Civilní	<ul style="list-style-type: none">- ztráty z narušení ekonomického života- ztráty z narušení ekonomické a finanční infrastruktury
	Bezpečnostní (vojenské)	<ul style="list-style-type: none">- zničení techniky a zbraňových systémů- poškození komunikační a energetické infrastruktury
Nefinanční	Civilní	<ul style="list-style-type: none">- ztráta reputace (dobrého jména)- ztráta zájmu o spolupráci (ekonomická, politická kooperace a spojení)- ztráta „morálky“ vlastních lidí (vojáci, policisté, státní zaměstnanci atd.)
	Bezpečnostní (vojenské)	<ul style="list-style-type: none">- ztráta reputace (dobrého jména)- ztráta zájmu o spolupráci (vojenská kooperace a spojení)- ztráta „morálky“ vlastních lidí (vojáci, policisté, státní zaměstnanci atd.)

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

Classification of cyber conflict costs according to ownership character of damaged subject

Typ nákladů		Popis dané kategorie nákladů ²⁷
Soukromé	Jednotlivci	Ztráta soukromých dat Poškození počítačů ²⁸ Odčerpání finančních prostředků z účtů ²⁹
	Firmy	Ztráta firemních dat Poškození firemních sítí a počítačů Ztráta firemního know-how (duševního vlastnictví) Odliv zákazníků, ztráta obchodních partnerů Ztráta finančních prostředků ^{30,31,32}
Veřejné	Stát	Narušení kritické infrastruktury
		Pokles daňových příjmů
		Ohrožení prestiže státu ³³

Economic Dimension of Cyberspace as New Security Threat

Economic aspects of potential cyber conflict

Classification of cyber conflict costs according to time character costs (preventive and a eliminative character of costs).

Typ nákladů	Popis dané kategorie nákladů ³⁴
Krátkodobé	Náklady související s obnovením napadeného systému do stavu před napadením
	Náklady související s narušením činnosti organizace (ztracená produkce, neodbavení klienti ...)
	Pokles hodnoty nehmotného majetku (duševního vlastnictví) atakovaného během konfliktu
Dlouhodobé	Nárůst nákladů kybernetické bezpečnosti
	Ztráta klientů, obchodních partnerů,
	Dominový efekt provedení kybernetického útoku

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

CONCLUSION

Economic Dimension of Cyberspace as New Security Threat

Conclusion

- Cyber space become real security threat (it is prove empirical and theoretical evidence).
- Crucial problem is determination optimal level expenditures and paied costs of securing sufficient level of cyber security and defense.

Economic Dimension of Cyberspace as New Security Threat

Conclusion

- The question is what potential damages can impose real cyber attack on society, individuals and firms.
- It is necessary to find efficient way how to face this risk.
- Society have to tolerate acceptable level of private and public costs on securing sufficient level of cyber security and defense.

FUTURE DEVELOPMENT OF ECONOMICS OF DEFENSE AND SECURITY
ECONOMIC DIMENSION OF CYBERSPACE AS NEW SECURITY THREAT

STUDY RESOURCES

Economic Dimension of Cyberspace as New Security Threat

Study Resources

- GORDON, Lawrence A., LOEB Martin P. The Economics of Information Security Investment, 2002
- BAUER, Johannes M., Van EETEN, Michel J. G. Cybersecurity: Stakeholder incentives, externalities, and policy options, 2009.
- CORDES, Joseph J. An Overview of the Economics of Cybersecurity and Cybersecurity Policy, 2011.
- DEPARTMENT OF FINANCE AND SERVICES. A Guide for Government Agencies Calculating Return on Security Investment, 2012.
- CHIRCA, Alexandra. An Empirical Study Regarding the Cost-Benefit Analysis of Open Source Software for Information Security, 2010.

THANK YOU FOR YOUR ATTENTION !!!

IN CASE OF QUESTIONS, CONTACT ME ON

Dipl. Eng. **Aleš OLEJNÍČEK**, Ph.D.
Department of **ECONOMICS**
Section of **NATIONAL DEFENSE**
ECONOMICS
Office **K-65/100**
Phone number: **+420973443153**



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ