Year : 2020

THREE ARTICLES ON THE ECONOMICS OF INFORMATION-SYSTEMS DEFENSE CAPABILITY. Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures

Percia David Dimitri

Percia David Dimitri, 2020, THREE ARTICLES ON THE ECONOMICS OF INFORMATION-SYSTEMS DEFENSE CAPABILITY. Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures

Originally published at : Thesis, University of Lausanne

Posted at the University of Lausanne Open Archive http://serval.unil.ch
Document URN : urn:nbn:ch:serval-BIB_8A0DAC472C8F3

UNIL | Université de Lausanne

FACULTÉ DES HAUTES ÉTUDES COMMERCIALES

DÉPARTEMENT DES SYSTÈMES D'INFORMATION

THREE ARTICLES ON THE ECONOMICS OF INFORMATION-SYSTEMS DEFENSE CAPABILITY

Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures

THÈSE DE DOCTORAT

présentée à la

Faculté des Hautes Études Commerciales
de l'Université de Lausanne

pour l'obtention du grade de

Docteur ès Sciences en systèmes d'information

par

Dimitri PERCIA DAVID

Directeur de thèse

Prof. Dr. Kévin Huguenin

Jury

Prof. Dr. Rafael Lalive, président
Prof. Dr. Stéphanie Missonier, experte interne
Prof. Dr. Steven Furnell, expert externe
Prof. Dr. Jens Grossklags, expert externe

LAUSANNE
2020

UNIL | Université de Lausanne
HEC Lausanne
Le Décanat
Bâtiment Internef
CH-1015 Lausanne

IMPRIMATUR

Sans se prononcer sur les opinions de l'auteur, la Faculté des Hautes Etudes Commerciales de l'Université de Lausanne autorise l'impression de la thèse de Monsieur Dimitri PERCIA DAVID, titulaire d'un bachelor en science politique de l'Université de Lausanne, et d'un master en économie de l'Université de Neuchâtel, en vue de l'obtention du grade de docteur ès Sciences en systèmes d'information.

La thèse est intitulée :

THREE ARTICLES ON THE ECONOMICS OF INFORMATION-SYSTEMSDEFENSECAPABILITY

MATERIAL-, HUMAN-, AND KNOWLEDGE-RESOURCES ACQUISITION FOR CRITICAL INFRASTRUCTURES

Lausanne, le 06 janvier 2020

Le doyen

Jean-Philippe Bonardi

HEC Lausanne
Le Décanat
Tél. +41 21 692 33 40 | Fax +41 21 692 33 05
www.hec.unil.ch | hecdoyen@unil.ch

Members of the PhD Committee

President of the PhD Committee – Prof. Dr. Rafael Lalive
Full Professor at the Faculty of Business and Economics of the University of Lausanne

Supervisor – Prof. Dr. Kévin Huguenin
Assistant Professor at the Faculty of Business and Economics of the University of Lausanne

Internal expert – Prof. Dr. Stéphanie Missonier
Full Professor at the Faculty of Business and Economics of the University of Lausanne

External expert – Prof. Dr. Steven Furnell
Full Professor at the Faculty of Science and Engineering of the University of Plymouth

External expert – Prof. Dr. Jens Grossklags
Full Professor at the Department of Informatics of the Technical University of Munich

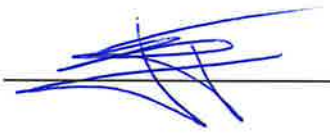
University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Dimitri PERCIA DAVID

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:  Date: 16/12/2019

Prof. Kévin HUGUENIN
Thesis supervisor

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Dimitri PERCIA DAVID

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:  Date: 16/12/2019

Prof. Stéphanie MISSONIER
Internal member of the doctoral committee

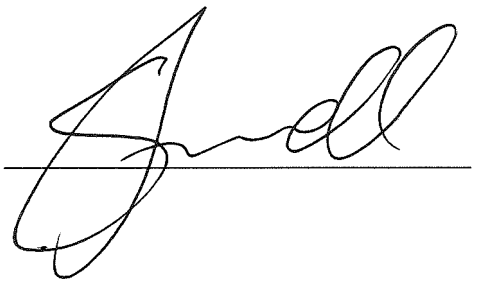
University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Dimitri PERCIA DAVID

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:  Date: 14/12/2019

Prof. Steven FURNELL
External member of the doctoral committee

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Dimitri PERCIA DAVID

and have found it to meet the requirements for a doctoral thesis.
All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature: _____ Date: 18.12.2019

Prof. Jens GROSSKLAGS
External member of the doctoral committee

Declaration

I, Dimitri Percia David, hereby confirm that there are no known conflicts of interest associated with this manuscript and its three articles. In particular, there has been no financial support for this work that could have influenced and/or biased its outcome.

I also confirm that I have given due consideration to the protection of intellectual property associated with this manuscript and its three articles, and that there are no impediments to publication, including the timing of publication, with respect to intellectual property. In so doing, I confirm that I have followed the regulations concerning intellectual property of our institutions and the corresponding scientific journals and conferences.

I further confirm that any aspect of the work covered in this manuscript that has involved human patients has been conducted with the ethical approval of all relevant bodies and that such approvals are acknowledged within the manuscript.

To my mother and my father, Veronica Percia and Anestis David Papadopoulos.

Acknowledgements

First and foremost, I would like to thank my manager at the Military Academy at ETH Zurich, PD Dr. **Marcus Matthias Keupp**, for guiding me from the beginning and throughout the long journey of developing and writing my thesis. Marcus is a great mentor. He funded my research project, supported me, and offered me the best possible working conditions and the necessary freedom to develop my thesis. His expertise in economics, econometrics and strategic management helped me to approach and understand (information-) security issues from a new perspective.

Secondly, I would like to thank my supervisor at the University of Lausanne, Prof. Dr. **Kévin Huguenin**, for taking over the supervision of my PhD thesis. He gave me the opportunity to finalize, considerably enhance, and defend my research by providing relevant, respectful and professional feed-backs. His expertise in information security and privacy constituted a considerable help that enabled to transform my work into a serious scientific research. His numerous relevant feed-backs helped me to elaborate the relevancy of my thesis.

Besides my manager and supervisor, I am deeply grateful to Dr. Brigadier **Peter Stocker** – head of the Military Academy at ETH Zurich –, who provided excellent research conditions. I thank Prof. Dr. **Stéphanie Missonier**, Prof. Dr. **Steven Furnell**, and Prof. Dr. **Jens Grossklags**, for having accepted to sit on my committee; they provided relevant and valuable critics that substantially enhanced the coherence of my manuscript. Also, I would like to thank Prof. Dr. and vice dean **Rafael Lalive** for having accepted to chair my committee, as well as Prof. Dr. **Jacques Duparc**, Prof. Dr. **Olivier Cadot**, Prof. Dr. **Christian Zehnder** and Prof. Dr. **Benoît Garbinato** for their support and advice regarding the internal administration processes of the doctoral school.

During my thesis work, I had the pleasure of working with other great scholars, such as Prof. Dr. **Maximilian Palmié** who supported me with his advanced methodological skills. A special thank goes to **Holly Cogliati-Bauereis** for her outstanding English editing services and **Emérentienne Pasche** for the bibliography, as well as to my beloved sweetheart **Valérie Chaplin-Haederli** for her patience and support during the final process of my PhD.

A sincere thank goes to all my friends who supported me, especially to my best sparring-partner, Dr. **Alain Mermoud**, for his unfailing support during our four years of collaboration.

I am also very grateful to all my colleagues at UNIL who made my journey as an external PhD candidate easier. In particular, I would like to thank my colleagues of the Information Security and Privacy Lab, namely, Dr. **Bertil Chapuis**, and PhD candidates **Noé Zufferey**, **Yamane El Zein**, and **Didier Dupertuis**. Also, I would like to name, among others, Dr. **Thomas Boillat**, Dr. **Hazbi Avdiji**, Dr. **Dina Elikan**, and Dr. **Vaibhav Kulkarni**, as well as PhD candidates **Clément Labadie** and **Martin Fadler**. A special thank goes to Dr. **Mélanie Bosson** and Dr. **Benjamin Rudaz** from the Graduate Campus team. They were of great help in achieving my personal goals at UNIL and beyond.

And last but not the least, I would like to express my gratitude to my family for their support. I will be eternally grateful for the support of all mentioned above.

Abstract

In this thesis, I investigate three aspects related to the acquisition of resources required to build an information-systems defense capability among critical-infrastructure providers.

The operational continuity of critical infrastructures is vital for the functioning of modern societies. Yet, these critical infrastructures are monitored and managed by an interdependent ecosystem of information systems, exposing critical infrastructures to the systemic risk of cascading failures. In such a context of extreme-risk distribution, no private or government (re-)insurer will cover the costs of such failures. As a consequence, critical-infrastructure providers are forced to ensure their operational continuity against these risks, whether the risks are due to deliberate attacks or natural disasters.

Consequently, the operational continuity of critical infrastructures requires an information-systems defense capability – i.e., the ability to prevent, detect and respond to information systems' failure. In order to ensure such a capability, the field of *computer & information security* develops a myriad of technologies. However, scholars and practitioners stress that technical solutions are necessary but still insufficient for ensuring such a defense capability. Incidents are caused by inappropriate organizational design and/or human-behavior aspects, at least as often as by inefficient IT design. Following this logic, information systems are apprehended as socio-technical systems constituted by a nexus of technologies (material resource) and human agents (human, and knowledge resources) who employ such technologies. Building on prior research on *organizational capabilities* and *security economics*, I explore the organizational design and human behavior aspects that are necessary for critical-infrastructure providers to build such an information-systems defense capability. Investigating the case of three specific critical infrastructures and their context, I deconstruct this capability into material, human, and knowledge resources, and I explore how they should be acquired to build such a capability.

In the first article dedicated to material resource, I argue that the swift changes in the technological landscape require novel investment-model assumptions in order to acquire material resources needed for building an information-systems defense capability. Therefore, I adapt the well-known Gordon-Loeb model so that it can integrate the dynamic and discontinuous developments of the technological landscape. This first article helps critical-infrastructure providers to preempt the effect of disruptive technologies on the optimal level of investment in information-systems defense, and provides a framework in order to select and invest in the most effective technologies.

In the second article dedicated to human resource, I argue that an organization must emphasize the recruitment of specialist-knowledge providers in order to build an information-systems defense capability. I adopt an economic approach – based on an opportunity-cost analysis – for attracting new employees in the context of the Swiss Armed Forces, a critical infrastructure that suffers from a deficit of staff for monitoring and managing its information systems.

In the third article dedicated to knowledge resource, I argue that the organization must encourage continuous learning of existing organizational members in order to build an information-systems defense capability. Taking the case of *cyber-risk information sharing* as a means to foster tacit-knowledge acquisition, I propose to investigate why human agents engage in information sharing. I argue that the extent to which an individual engages in information sharing is a function of their individual knowledge-absorption expectation – i.e., the benefit they expect from sharing information.

Policy recommendations for governments and critical-infrastructure providers, and a research agenda for future work are presented in the conclusion.

Résumé

Dans cette thèse, j'examine trois aspects liés à l'acquisition des ressources nécessaires au développement d'une capacité de défense des systèmes d'information, et ce dans le cadre des fournisseurs d'infrastructures critiques.

La continuité opérationnelle des infrastructures critiques est vitale pour le fonctionnement des sociétés modernes. Pourtant, ces infrastructures critiques sont surveillées et gérées par un écosystème interdépendant de systèmes d'information, exposant ainsi les infrastructures critiques au risque systémique de défaillances en cascade. Dans un tel contexte de distribution de risques extrêmes, aucun (ré)assureur privé ou public n'est susceptible de couvrir de telles défaillances. En conséquence, les fournisseurs d'infrastructures critiques sont contraints d'assurer leur continuité opérationnelle face à ces risques, qu'ils soient dus à des attaques délibérées ou à des catastrophes.

Par conséquent, la continuité opérationnelle des infrastructures critiques nécessite une capacité de défense des systèmes d'information, c'est-à-dire la capacité de prévenir, de détecter et de réagir en cas de défaillance des systèmes d'information. Afin d'assurer une telle capacité, le domaine de la sécurité informatique (*computer & information security*) développe une myriade de technologies. Cependant, les chercheurs et les praticiens insistent sur le fait que les solutions techniques sont nécessaires mais encore insuffisantes pour assurer une telle capacité de défense. Les incidents sont causés au moins aussi souvent par une conception organisationnelle inappropriée et/ou des aspects du comportement humain, que par une conception informatique inefficace. Dans cette logique, les systèmes d'information sont appréhendés comme des systèmes socio-techniques constitués d'un ensemble de technologies (ressources matérielles) et d'agents humains (ressources humaines et connaissances) qui utilisent ces technologies. En m'appuyant sur des recherches antérieures basées sur les capacités organisationnelles (*organizational capabilities*) et l'économie de la cyber-sécurité (*security economics*), j'explore les aspects de la conception organisationnelle et du comportement humain qui sont nécessaires aux fournisseurs d'infrastructures critiques pour construire une telle capacité de défense des systèmes d'information. En étudiant le cas de trois infrastructures critiques spécifiques et leur contexte, je déconstruis cette capacité en ressources matérielles, resources humaines et resources de connaissances, et j'explore comment ces resources devraient être acquises pour construire une telle capacité.

Dans le premier article – consacré aux ressources matérielles –, je soutiens que les évolutions rapides dans le domaine technologique exigent de nouvelles hypothèses de modèle d'investissement, et ceci afin d'acquérir les ressources matérielles nécessaires pour construire une capacité de défense des systèmes d'information. J'adapte donc le célèbre modèle de Gordon-Loeb pour qu'il puisse intégrer les développements dynamiques et discontinus du domaine technologique. Ce premier article aide les fournisseurs d'infrastructures critiques à anticiper l'effet des technologies de rupture (*disruptive technologies*) sur le niveau optimal d'investissement dans la défense des systèmes d'information, et fournit un cadre pour sélectionner et investir dans les technologies les plus efficaces.

Dans le deuxième article – consacré aux ressources humaines –, je soutiens qu'une organisation doit mettre l'accent sur le recrutement de fournisseurs de connaissances spécialisées afin de construire une capacité de défense des systèmes d'information. J'adopte une approche économique – fondée sur une analyse des coûts d'opportunité – pour attirer de nouveaux collaborateurs dans le cadre de l'Armée suisse, une infrastructure critique qui souffre d'un déficit de personnel pour la surveillance et la gestion de ses systèmes d'information.

Dans le troisième article – consacré aux ressources de connaissances –, je soutiens que l'organisation doit encourager l'apprentissage continu de ses membres afin de construire une capacité de défense des systèmes d'information. Prenant le cas du partage d'information sur les cyber-risques (*cyber-risk information sharing*) comme moyen de favoriser l'acquisition de connaissances tacites, je propose d'examiner pourquoi les agents humains s'engagent dans le partage d'information. Je soutiens que la mesure dans laquelle une personne s'engage dans le partage d'information est fonction de ses attentes individuelles en matière d'absorption des connaissances, c'est-à-dire les avantages qu'elle attend du partage d'information.

Des recommandations stratégiques à l'intention du gouvernement et des fournisseurs d'infrastructures critiques, ainsi qu'un agenda de recherche pour des travaux futurs sont présentés dans la conclusion.

'Crazy is building the ark after the flood has already come.'

— Howard Stambler

Contents of the Thesis

List of Tables

List of Figures

List of Abbreviations

AFCSO	Armed Forces Command Support Organization (Swiss Armed Forces department)
APG/EO	*Allocations pour perte de gain* (Swiss mandatory insurance for loss of earnings)
APT	Advanced Persistent Threat (cyber-security threat)
ASMZ	*Allgemeine Schweizerische Militärzeitschrift* (Swiss practitioners' magazine, in German)
ATHENA	Critical-Infrastructures Interdependencies Integrator (CIP platform)
BDA	Big-Data Analytics (data-science methodology/trend)
BI	Business Intelligence (business area)
CERT	Computer Emergency Response Team (risk-management and response platform)
CFC	*Certificat fédéral de capacité* (federal certificate of competence, a Swiss diploma category)
CI	Critical Infrastructure (entity)
CI^3	Construction Industry Institute India (CIP platform)
CIMS	Critical-Infrastructure Modeling System (CIP platform)
CIP	Critical-Infrastructure Provider (entity)
CIP/DSS	Critical-Infrastructure Protection Decision Support System (CIP platform)
CIPMA	Critical-Infrastructure Protection Modeling and Analysis (CIP platform)
CISIA	Critical-Infrastructure Simulation by Interdependent Agents (CIP platform)
CLUSIS	*Association Suisse de la Sécurité de l'Information* (Swiss Association for Information Security)
COMM-ASPEN	Agent-Based Simulation Model of the US Economy (CIP platform)
CRITIS	Critical-Information-Infrastructure Security (conference)
CSNet	Cyber-Security In Networking (conference)
(D)DoS	(Distributed) Denial-of-Service Attack (cyber-security threat)
EAR-PILAR	*Procedimiento Informático-Lógico Para el Análisis de Riesgos* (CIP platform)
EMCAS	Electricity Market Complex Adaptive System (CIP platform)
EBIS	Expected Benefits in Information Security (economic term)
ENBIS	Expected Net-Benefits in Information Security (economic term)
FINSIM	Financial System Infrastructure (CIP platform)
FMEA/FMECA	Failure Modes and Effects Analysis (CIP platform)
FTA	Fault Tree Analysis (CIP platform)
GL	Gordon-Loeb (mathematical model)
GOVCERT	Government Computer Emergency Response Team (government's risk management and response platform)
HAZOP	Hazardous Operations (CIP platform)
HR	Hard Rewards (construct of Part III)
HSO	*Höhere Stabsoffiziere* (generals of the SAF)
ICS	Industrial Control System (entity)
ICT	Information and Communication Technology (entity)
IDS	Intrusion-Detection System (cyber-security technology)
IIM	Inoperability Input–Output Model (CIP platform)
ISAC	Information Sharing and Analysis Center (platform)
ISOC	Information Security Operation Center (platform)
IT	Information Technology (entity)
KA	Knowledge Absorption (variable of Part III)
KBV	Knowledge-Based View of the firm (theory)
LNCS	Lecture Notes in Computer Science (Springer publication series)
LUND	Working Methodology (CIP platform, from Lund university)
MARGERIT V2	*Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (CIP platform)
MELANI	*Melde- und Analysestelle Informationssicherung* (Reporting Analysis Center for Information Assurance, Swiss ISAC)
MIA	Methodology for Interdependencies Assessment (CIP platform)
MitM	Man-in-the-Middle Attack (cyber-security threat)
MUNICIPAL	Multi-Network Interdependent Critical-Infrastructure Program for Analysis of Lifelines (CIP platform)
NCO	Non-commissioned officer (rank category in the SAF)
NIST	US National Institute of Standards and Technology (cyber-security policy framework)
NORa	Reciprocal Behavior (construct of Part III)
NSRAM	Network-Security Risk-Assessment Model (CIP platform)
OS	Operating System (system software)
P2C	Power to Coerce (strategic foreign-policy term)
P2P	Peer-to-Peer (network model)
PC	Personal Computer (hardware)
PLC	Programmable-Logic Controller (hardware)
PPP	Public-Private Partnership (entity)
RBV	Resource-Based View of the firm (theory)
RMS+	*Revue Militaire Suisse* (Swiss practitioners' magazine, in French)
R&D	Research and Development (business area)
SAF	Swiss Armed Forces (entity)
SBPF	Security-Breach Probability Function (mathematical term)
SCADA	Supervisory Control and Data Acquisition (specific ICS entity)
S(I)EM	Security (Information) and Event Management (security-management procedures and/or products and/or services)
SIS	Security-Information Sharing (security practice)
STS	Socio-Technical System (entity)
UIS	Urban Infrastructure Suite (CIP platform)
USE	Usefulness Belief (construct of Part III)
VINCI	Virtual Interacting Network Community (CIP platform)
WEIS	Workshop on the Economics of Information Security (conference)
XSS	Cross-Site Scripting (cyber-security threat)

Introduction

'Technological progress has merely provided us with more efficient means for going backwards.'

— Aldous Huxley

Contents of the Introduction

1 Context and Problem Statement

Information systems (IS) have become ubiquitous to the great majority of human activities [244]. Only a few organizations can provide their processes, products and/or services without relying on IS [72, 115]. According to the definition of Baxter & Sommerville [30] and Geels [94], IS are described as socio-technical systems (STS) – i.e., the nexus of humans and information & communication technologies (ICT). Among other functions, IS are used in order to monitor and/or manage the production and distribution of processes, products and/or services of many organizations [30, 94]. When it comes to monitor and/or manage business branches such as operations, research and development (R&D), sales and marketing, productivity, human resources (HR), business intelligence (BI) – to name a few –, IS have become central [231]. For example, the information technology (IT) department of organizations belonging to the financial sector use IS for every kind of activity, should it be for monitoring and/or managing business branches such as accounts payable, accounts receivable, general ledger, budgeting and planning, forecasting and reporting, expense management, funds transfer, investment and portfolio strategies, etc. [199]. Various other sectors such as public health, energy, government administrations, logistics and supply chains, transportation, or even food and agriculture are no exception [228]. Consequently, the functioning and reliability of IS constitute a key criterion for the operational continuity[1] of any modern organization. Therefore, if security incidents disrupt IS, organizations that are dependent to such IS would quickly cease to function [231].

1.1 IS-Security Incidents

Following the cyber-incidents taxonomy of the *NIS Cooperation Group* – established by the 2016 *NIS Directive* of the EU Commission to ensure strategic cyber-security cooperation and the exchange of information among EU Member States – IS-security incidents are classified among five different categories: (1) system failures, i.e., without external causes – e.g., hardware failure, software bug, flaw in a procedure, etc.; (2) natural phenomena – e.g., storm, lightning, solar flare, flood, earthquake, wildfire, etc.; (3) human errors, i.e., the system worked correctly, but was used wrong – e.g., a user mistake, or carelessness affecting security; (4) third-party failures, i.e., the incident is due to a disruption of a third-party service – e.g., power cut, internet outage, etc.; and last but not least (5) malicious actions – e.g., cyber-attack or physical attack, vandalism, sabotage, insider attack, theft, etc. [117].

While the first four categories can be tackled by internal measures and/or procedures of organizations, malicious actions are admittedly more challenging to prevent, detect and contain [241]. Such third parties who attempt to exploit IS vulnerabilities to their own advantage comprise (1) nation-states actors or their proxies (motivated by geopolitical factors), (2) (organized) cyber-criminals (motivated by financial profits), (3) hacktivists (motivated by ideological factors), (4) cyber-terrorists (motivated by ideological violence), (5) thrill-seekers (motivated by self-satisfaction), and (6) insider threats (motivated by discontent against their organization) [86]. All of these parties could attempt to exploit IS vulnerabilities in order to breach IS security, such that they can reach their respective objectives [52]. Therefore, cyber-attacks of third parties threaten the confidentiality, the integrity, and/or the availability, which constitute key principles of IS security [203].

The incidence rate and variety of such IS-security concerns are continuously rising, with attacks becoming more sophisticated and damages taking various forms [52, 241]. Measuring the number of cyber-incidents and their costs is a complex task that is bound to a variety of variables such as criteria selection and researchers measurement of direct or indirect costs (for a systematic study, see [13]). Overall, there is a lack of effective metrics, frameworks and

[1] The term *operational continuity* refers to the ability of a system to continue working despite internal and/or external incidents such as damages, losses or critical events [16].

tools in order to estimate the cost of cyber-attacks on organizations [4]. Yet, whatever could be the actual amount of cyber-incidents and their costs, the magnitude of such incidents is everything but negligible. For instance, according to the *Ponemon Institute*, as of 2018, large organizations with more than 5,000 employees witnessed an average of 145 security breaches, representing an annual increase of 11% compared to 2017, and an increase of 67% for the last five years [235]. Also, according to the computer-security software company *McAfee*, as of 2018, the annual worldwide cost of cyber-crime has reached more than 600 billion US$ – i.e., 0.8% of global GDP [177]. Compared to 2015, such numbers increased by approximately 20% [177]. There is much public and academic coverage of exploitation of IS vulnerabilities leading to security failures and subsequent damages. For instance, the 2014 data breach that affected the American bank *JP Morgan Chase* is believed to have compromised data associated with over 83 million accounts – 76 million households (two out of three households in the US) and 7 million small businesses [262]. This data breach is considered to be one of the most serious intrusions into an American corporation, respectively one of the largest data breaches in history [102, 130, 247]. Another example is *Operation Aurora*, a series of cyber-attacks conducted in 2009 through advanced persistent threats (APT). The primary goal of such coordinated attacks was to gain access to and potentially modify source-code repositories of high-tech, security and defense-contractor organizations such as *Adobe Systems*, *Rackspace*, *Yahoo*, *Northrop Grumman*, *Symantec*, and *Juniper Networks*. Such attacks operated as means of corporate espionage aiming to steal intellectual property, targeting competitive advantages such as know-hows and technology secrets [55]. Another famous example is the 2017 *Equifax Inc.* data breach, by which cyber-criminals had accessed approximately 146 million US consumers' personal data, including credit-card information, leading to financial theft [116]. More recently, in November 2019, a state-sponsored hacking campaign knocked offline more than 2,000 websites in Georgia, including government and court websites containing case materials and personal data [257].

While such losses are certainly significant, they are likely small in comparison to the economic and societal consequences caused by security incidents that affect IS of critical-infrastructure providers (CIP).

1.2 IS-Security Incidents Among CIPs

The aforementioned examples discuss economic and societal losses that are mostly limited to the very organization that suffers an IS-security incident. In the worst-case scenario, these organizations go out of business and disappear from the market, but such organization-specific failures are unlikely to threaten the industry as a whole, the society, or human life itself. However, when it comes to severe IS-security incidents that affect CIPs, these vital issues might be threatened [129].

CIs are defined as organizations delivering goods and/or services that are so vital to the society that any extended disruption and/or failure of them would strongly affect the functioning of the government, national security, economic system, public health and safety, or any combination of the above [6, 53, 132, 242, 250]. Consequently, there is a consensus in the literature that the functioning of modern societies depends – to a large extent – on the operational continuity of CIs (for extensive literature reviews, see [222, 271, 301]). Examples for such CIs are the national power grid, oil and natural gas supply, information, telecommunication, transportation and logistics networks, the electronic banking and payment infrastructure, public health services, government services, police and armed forces[2], water supply systems, and food/agriculture production and distribution [205].

[2]It is often emphasized that one of the most important CI is the armed forces as they are responsible for the security of a society (e.g., [246]).

Whenever a CI fails, significant economic and societal damages follow. For example, when India's national power grid failed in 2012, more than 620 million individuals were left without electricity supply for two days. Consequently, transportation infrastructures such as subways and railways were inoperative, as were traffic lights, resulting in unprecedented traffic jams, and almost the complete telecommunication sector was inoperative. This incident resulted not only in a temporary disruption of economic activity, but it also caused significant societal unrest and riots [65, 284].

Numerous scholars such as Alcaraz et al. [5, 6], Zhu et al. [305], and Van Eeten et al. [286] argue that protecting CIs against disruptions and/or failures cannot be done without proper protection of the management and control systems of CIs [6, 305]. Industrial-control systems (ICS), more specifically their sub-domain of supervisory control and data acquisition (SCADA) systems, progressively and rapidly transited from dedicated solutions towards IP-based integrated frameworks [6, 305]. Therefore, it is no surprise that defending the IS that operate these control and supervisory systems is of the utmost importance. Protecting CIs against IS disruptions and/or failures is therefore highly relevant for policy makers and researchers [301].

Moreover, IS-security incidents among CIPs can cause economic and societal damages that are so large that no commercial insurance firm would be willing to underwrite such risk or provide coverage [98, 134, 190, 294]. This is not only because an important amount of malicious actions/attacks are not discovered and/or under-reported – and thus extracting their risk distribution is difficult, which makes such attacks difficult to model [34, 74, 98, 146] –, but also because CIs are technically and architecturally linked across technology domains, such that, as a whole, they constitute an interdependent *ecosystem*[3] rather than a group of autonomous elements [6, 78, 164, 223]. Due to this interdependency, failures in any particular CI can quickly spread to other networks, such that a cascade of system failures is initiated that makes technical, economic and societal damages grow exponentially [62, 141, 163, 164]. For instance, the consequences of a major power outage in the Netherlands in 2005 were not limited to a regional disruption of electricity supply. Cascading failures caused a subsequent disruption of the Rotterdam subway network, made movable bridges stop halfway such that they blocked road and water routes, and initiated emergency shutdowns of 65 chemical factories, which in turn caused smoke clouds that disrupted highway traffic. It took operators two weeks to return to normal operations [286]. Also, according to some case studies, for temporary and regional disruption alone, economic and societal losses caused by cascading failures are estimated at four to ten billion US$ [134]; also, another practitioners' research estimates the economic and insurance consequences of a severe, yet plausible, cyber-attack against the US power-grid to reach from 240 billion US$ to more than 1 trillion US$ [294]. Moreover, according to a research from the University of Cambridge's Centre for Risk Studies, cyber-incidents of malicious form are able to inflict physical damage on more than 50 generators that supply power to the electrical grid in the Northeastern US including New York City and Washington DC, triggering a wider blackout which could leave 93 million people without power. This same research states that total insured losses are estimated from 20 billion US$ to more than 70 billion US$ across the majority of CI domains [190].

If an intentional attacker can breach the IS security of CIs' operations – or control the system and threaten to do so –, extreme economic and societal damages are expected, putting the whole society as such at risk [129]. As insurance is unavailable [98], CIPs must essentially face such risks alone, and they have no other choice but to deploy effective defensive measures that can neutralize the risk of any such damages [218, 249]. It is therefore no surprise that governments and international organizations continually advise CIPs to

[3]The term *ecosystem* is used as an analogy to natural ecosystems as CIs evolve and adapt to their political and societal environment.

defend their IS against security incidents, up to the point where such defense is considered relevant for national security [214, 215]. For example, in 2017, the *NIST Cybersecurity Framework* was declared mandatory for all CIPs in the US [282]. Member states of the European Union are advised to convert the European Commission's directive 2006/786 – which defines infrastructure-security policies – into national law [57].

However, many CIPs are struggling to produce such defense against IS-security incidents, and there are many examples where the IS security of CIPs has been neglected or compromised. The *Dragonfly* attacks of 2014 and 2015 that targeted CIs of the energy sector in many countries exemplify such an IS-security issue [95]. In the recent years, the energy sector has been targeted by cyber-criminals. Most notably, disruptions to Ukraine's electrical grid in 2015 and 2016 led to power outages affecting more than 230,000 citizens [26]. In 2017, media also reported attempted attacks on the electricity grids in some European countries and on CIPs that manage nuclear facilities in the US [277]. In attacks related to or similar to the *modus operandi* of *Dragonfly*, IS-security issues are mainly due to increasing integration of third-party supplier systems that interact with the CIPs' proprietary architecture. Operating systems (OS) components often come without a graphical user interface, and they have weak or no password protection [142]. As services are outsourced to third-party suppliers, dependabilities and vulnerabilities are also created. In cases related to or similar to *Dragonfly*, CIPs were lured to doppelganger update servers from which they downloaded the code, assuming it would be a regular software update [59]. The case of *Stuxnet* is also illustrative: uncovered in 2010, the *Stuxnet* cyber-attack used a malicious computer worm that targeted SCADA systems [33], causing substantial damage to Iran's nuclear program. Although no country has openly admitted responsibility, the worm is widely understood to be a multination-built cyber-weapon [33]. The *Stuxnet* worm specifically targeted programmable-logic controllers (PLC), which allow the automation of electro-mechanical processes such as those used to control machinery and industrial processes, including centrifuges used for separating nuclear material. Exploiting four *zero-day*[4] vulnerabilities [208], Stuxnet functions by targeting machines using wide-spread OS. The attack reportedly compromised Iranian PLCs, collecting information on industrial systems, and ultimately causing the fast-spinning centrifuges to tear themselves apart [165]. The *Stuxnet*'s conception is not domain-specific and thus it could be tailored as a platform for attacking modern ICS and PLC systems (e.g., in factory assembly lines or power plants), which are currently used in the great majority of Western countries [155]. *Stuxnet* reportedly ruined almost one fifth of Iran's nuclear centrifuges [157]. Targeting ICSs, the worm infected over 200,000 computers and caused more than 1,000 machines to physically degrade [240].

Given that these attacks successfully occur in different contexts, it seems that a general IS-defense problem affects all CIPs. Unless one analyzes what is required to produce IS defense, there can be no understanding of why CIPs fail to produce such defense.

[4] A *zero-day* vulnerability is a computer-software vulnerability that is either unknown to or unaddressed by operators who should be interested in mitigating the vulnerability. *Zero-day* vulnerabilities enable hackers to exploit it in order to adversely affect computer programs, networks, and data [137].

1.3 Requirements for an Effective IS Defense

According to the guideline principles of the *NIST Cyber-Security Framework*[5], the term 'IS defense' designates the ability of any organization to prevent, detect and respond to IS-security incidents [216]. A systematic literature review related to the IS defense for CIPs reveals that, to date, IS research has mainly focused on the development of technologies that are necessary in order provide IS defense. Such technologies are related to two main fields: (1) risk management and (2) operations research [301]. Table i.1 on page 18 provides a structured overview of contributions related to risk-management research and operations research, which model and simulate incidents and hazard maps in order to guide the acquisition and/or production of IS-defense technologies for CIPs.

Yet, approaches related to risk-management research and operations research are necessary but not sufficient when it comes to explaining why CIPs differ among each other as to their capability to defend their IS. If providing IS defense was merely a matter of technology acquisition and/or production, one should expect the incidence rate of IS-security issues to decrease as technologies are acquired and/or produced [38]. Yet, organizations seem to struggle despite the fact that they acquire and/or produce IS-security technologies. To date, extant research provides little evidence that could solve this problem [301].

However, for the last twenty years, scholars and practitioners have been arguing that technology-oriented approaches are useful yet incomplete. For instance, in his seminal article 'Why Information Security is Hard – An Economic Perspective' Ross Anderson [10] argued that IS-defense failures are not only due to technological aspects, but are at least as often due to perverse or misaligned incentives: 'Many, if not most, of the problems can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.' In the same vein, numerous scholars tested the validity of social sciences (economics, sociology, psychology) for explaining, understanding and solving IS-defense challenges and issues [12, 38, 80, 89, 196].

In particular, these contributions recommend to consider that IS are operated by human agents, and that human specialists who operate technological systems are required to produce IS defense. Therefore, human staff and their behavior are relevant components in the production of IS defense. When it comes to providing IS defense, skills, behavior and interactions of operators (human agents) who employ technologies are at least as important as technologies themselves [9, 38, 195]. In particular, human staff might be negligent, and specialists required to operate sophisticated systems might be not numerous enough in order to satisfy the market demand, and they might not always be available at short notice [61, 89, 272]. Thus, it is relevant for CIPs to adopt effective human-resource recruitment to provide IS defense.

Furthermore, research suggests it is not enough to invest in technologies and recruit human specialists as such, but it is also required – for any organization that wants to defend its IS – to absorb specialized knowledge that is not readily or publicly available (e.g., [100, 150, 248, 299]). The production of IS defense is a knowledge-intensive task [32, 147] as highly specialist knowledge is required to combine and deploy resources effectively for organizational defense – for instance, by designing resilient systems architectures and implementing them efficiently [77, 173]. Following this logic, providing IS defense

[5]The *NIST Cyber-Security Framework* provides IS-defense policy guidance for private sector organizations in the US. NIST is used by various other governments such as Japan and Israel. The framework provides 'a high level taxonomy of cyber-security outcomes and a methodology to assess and manage those outcomes'. The first version of NIST was published by the *US National Institute of Standards and Technology* in 2014, originally aimed at CIPs. The framework is being used by a wide range of organizations and helps them to be proactive about risk management [220, 270].

might be associated with the extent to which organizational members (i.e., operators) can absorb specialist knowledge required to combine and deploy resources such as material and human resources. Therefore, when it comes to providing organizational IS defense, specialized knowledge is required to build an IS defense capability. In particular, the IS-defense context often requires sensitive and classified information that is unlikely to be shared or disseminated through public channels [35, 90, 170, 202, 293]. Also, the knowledge required to provide IS defense is expert knowledge and hence is highly tacit – i.e., bound in personal experience [66, 263]. The only way to transfer tacit knowledge is to engage in social interaction [234]. Such tacit knowledge is not only hard to describe objectively (e.g., by documentation in manuals or textbooks), but it can also not readily be transferred among individuals, unless by intense social interaction between sender and recipient [213, 234, 263]. Consequently, it is relevant for CIPs to absorb tacit knowledge in order to acquire and/or produce IS-defense processes, products and/or services.

In the same vein, information-security research emphasizes that economic analysis is a powerful tool whenever one attempts to understand the information security of complex STSs [38, 200]. Economic research, more precisely its sub-field of *organizational theory*, suggests that organizations produce outcomes – such as IS-defense processes, products and/or services – on the basis of rare, valuable, and imperfectly imitable *resources*, both tangible and intangible, which they own, control, or have access to [27, 113]. An organization combines these resources in a purposeful way to produce an organizational capability – defined as the ability to reach a desired outcome [8, 209, 278]. Thus, resources allow an organization to build an organizational capability, which, in turn, is significantly associated with firm performance [239]. When this thinking is applied to the context of CIs, CIPs produce capabilities on the basis of rare, valuable and imperfectly imitable resources that CIPs should acquire, and then combine in order to build an IS-defense capability. Such a capability enables organizations to develop IS-defense processes, products and/or services that can subsequently provide effective IS defense.

According to the organizational capability literature, the three requirements discussed above and related to technologies, human agents and knowledge all constitute resource categories [67, 252, 255, 280]. Applied to the IS domain, these resource categories are defined as the following: *material resources* is related to IT elements such as hardware and software [27, 278], whereas *human resources* is related to human agents who employ, manage and/or monitor such IT elements [264], and *knowledge resources* is related to specialized skills (of human agents and organizations) that are necessary in order to operate IT elements in an effective manner [113, 114, 252, 255, 280]. For instance, Kim et al. [159] propose that an IS capability results from both human-resource and material-resource components. Resources required for IS performance comprise both technological components (infrastructures such as hardware and software) in which the organization has to invest in, and human components (technical and managerial staff) that the organization has to attract and recruit [188, 192]. Furthermore, Joshi et al. [150] and Gold et al. [100] emphasize that IT capability critically depends on a specialist knowledge component (organizational know-how).

Hence, if resources are required to produce a capability, and the three above-mentioned requirements for IS defense constitute resources, then IS defense can be interpreted as an organizational capability that emerges from the acquisition of these resources and, subsequently, the purposeful combination of these same resources. This interpretation of IS defense as an organizational capability not only meets the conception of IS as STSs in which operators (organizational members) and technologies interact [30, 94], it also implies that when organizations struggle to produce IS defense – or cannot prevent IS-defense incidents from happening – their IS-defense capability is ineffective. After all, numerous scholars demonstrated that differences in firm performance and competitive advantage can

be traced to differences in organizational capabilities [119, 239, 266, 300]. Furthermore, as an IS-defense capability is produced from the purposeful combination of the three above resources, this ineffectiveness can be traced to problems with the acquisition and/or the combination of these resources [8, 113, 266, 278].

Therefore, an ineffective IS defense can be traced to two generic problems. (1) The organization has (or has access to) all required resources but fails to orchestrate them. In this case, it is rather an ineffective resources management than a lack of resources endowment that is at the root of IS-defense ineffectiveness. (2) IS ineffectiveness might also be due to problems with resources acquisition itself. Whereas the problem of resources-combination failure presupposes that resources are present at all, the more fundamental problem of resources acquisition deserves to be investigated. More specifically, the focus might be put on a setting where CIPs are unable to acquire the resources required to provide IS defense. This inability might take different forms – e.g., the resource cannot be acquired at all, or not enough resources can be acquired, or only at a lower technological or skill level, etc. In any case, an obstacle is present that reduces IS-defense effectiveness. The problem for any CIP is thus to *acquire* all three resources before even orchestrating them. Consequently, the overarching research question of this thesis is:

> *How can CIPs acquire the material, human, and knowledge resources required to build an effective IS-defense capability?*

2 Research Gaps and Research Questions

Numerous researchers have directly or indirectly investigated some targeted aspects of the above-mentioned resources acquisition, but not necessarily in the domain of IS defense for CIPs. Systematic literature reviews related to the respective three resource categories are available in the end of this chapter (concerning material resources, see Table i.2 on page 19; concerning human resources, see Table i.3 on page 20; concerning knowledge resources, see Table i.4 on page 21). Yet, these systematic literature reviews emphasize relevant research gaps that deserve to be investigated – especially in the context of CIPs. Therefore, the above-mentioned overarching research question is structured into the subsequent three sub-questions that each addresses a particular resource category.

2.1 Part I: Material-Resource Investment

As mentioned above, building an IS-defense capability requires the acquisition of material-resource components [27, 278], which in turn requires investment either for buying technologies from the market, or for developing in-house R&D [104, 254]. As organizations face budget constraints, one of the main challenges is to maximize the efficiency of any monetary investment in order to acquire IS-defense technologies [38, 104, 254] whose operation aims of providing IS defense [22, 104]. While much of the related research focuses on private-sector organizations, the findings also apply to CIPs [206]. Hence, the acquisition of material-resource components that are required in order to build an IS-defense capability for CIPs is essentially a question of investment in technologies [254, 304].

Prior IS research has produced many quantitative models that propose to optimize such investment, as well as recommendations to invest in particular technologies (e.g., [38, 131, 148, 178, 261]). These formal approaches are complemented by less formal practitioner-oriented discussions [22, 267, 292]. Among all of these approaches, the GL model has emerged as the most dominant in IS research [37, 104, 105, 106, 109]. By specifying a security-breach probability function (SBPF) and mobilizing utility-maximization methods, the GL model attempts to determine an optimal investment amount for acquiring IS-defense

technologies (e.g., [29, 107, 176, 189, 295]). Table i.2 on page 19 provides a systematic literature review of this model and its extensions.

However, the model has two significant limitations. As depicted in this systematic literature review, the model and its extensions are essentially based on a static, single-period setting, and they consider a static context of the technological landscape, implying that technological evolution over time cannot be captured [104, 254, 295]. However, the technologies that both attackers and defenders of CIs deploy have become much more dynamic since the GL model was first published. The fast evolution of information technology allows attackers to deploy more dynamic attack patterns, such as polymorphic code[6], adversarial reverse engineering and APTs [7, 182], and the exploitation of *zero-day* vulnerabilities.[7] At the same time, this evolution allows defenders to deploy more powerful analytical methods, such as machine learning, deep learning and other technologies made possible by big-data analytics (BDA)[8], and they can also develop automated defense patterns based on this analysis. Such technological changes might be considered as disruptive – in the sense that they could significantly enhance the efficacy and/or efficiency of IS defense – thus bringing discontinuities in investment. Such discontinuities require dynamic and multi-period investment models [22, 46, 104, 182, 279]. A dynamization of the GL model in this sense would help CIPs to appropriately invest in the face of such technological changes [206]. Yet, to the best of my knowledge, this adaptation has not yet been attempted.

As long as this is not done, CIPs might be unable to adapt their investment policy to such technological changes. As a result, they might invest too little, too much, or invest inefficiently, such that their IS-defense capability might be sub-optimal. Therefore, a first sub-question is:

> *How, if at all, must CIPs adapt current investment models in order to acquire material-resource components required to build an IS-defense capability?*

2.2 Part II: Human-Resource Recruitment

Building an IS-defense capability also requires the acquisition of human-resource components [264]. Many studies confirm that the professional skills of organizational members are a critical input to capability generation and for sustained competitive advantage [8, 113, 114, 185, 297]. Thus, building a specialist IS-defense workforce is highly relevant for innovative responses to security threats and related IS-defense issues [136, 252].

At the same time, the literature is less prolific when it comes to the problem of not finding (enough) qualified professionals that are skilled enough for executing specialized tasks [56]. Much contemporary evidence from both academic research and business practice suggests that there is a significant shortage of IT specialists, particularly in IT security, and particularly for highly-qualified staff. For instance, a 2015 report from *Frost & Sullivan* and

[6] A *polymorphic code* is a code that employs a polymorphic engine in order to mutate while keeping the original algorithm intact. In other terms, the code changes itself each time it runs, but its semantics – the function of the code – will not change [87].

[7] A *zero-day* vulnerability is a computer-software vulnerability that is either unknown to or unaddressed by operators who should be interested in mitigating the vulnerability. *Zero-day* vulnerabilities enable hackers to exploit it in order to adversely affect computer programs, networks, and data [137].

[8] The term *big data* refers to data whose complexity impedes it from being processed (mined, stored, queried and analyzed) through conventional data-processing technologies [168, 182]. The complexity of big data is defined by three attributes: (1) the volume (terabytes, petabytes, or even exabytes (10^{18} bytes); (2) the velocity (referring to the fast-paced data generation); and (3) the variety (referring to the combination of structured and unstructured data) [168, 182]. The field of BDA is related to the extraction of value from big data – i.e., insights that are non-trivial, previously unknown, implicit and potentially useful [182]. BDA extracts patterns of actions, occurrences, and behaviors from big data by fitting statistical models to these patterns through different data-mining techniques (e.g., predictive analytics, cluster analysis, association-rule mining, and prescriptive analytics) [45, 251].

ISC^2 states that the worldwide cybersecurity workforce will have more than 1.5 million unfilled positions by 2020 [230, 302]. Also, a recent survey from *CSIS* concerning IT decision-makers across eight countries found that 82% of employers report a shortage of cyber-security skills, and 71% believe this talent gap causes direct and measurable damage to their organizations [63, 64]. The *Center for Cyber Safety and Education* based in the US states that employers must look to millennials to fill the projected 1.8 million positions that are estimated to be unfilled by 2022 [258]. Researchers also stated that despite increases in IT spending, there is an important imbalance between supply and demand of skilled information-security professionals, which might leave organizations vulnerable to IS-defense incidents such as security breaches and cyber-crimes [43, 219, 253].

These staffing problems can be considered to be even worse when one considers CIPs [41, 158]. Privately owned CIs must compete with other firms in the private sector for skilled personnel [14]. CIPs that operate as part of the public sector might have a limited ability to mitigate bureaucratic inefficiency, to offer entrepreneurial opportunities, or to offer bonus pay for exceptional performance, implying they might be perceived as less prestigious than private sector firms [243].

As the recruitment policy that organizations use to attract human resources is specific to the particular organization [42], focusing the research on a specific case is required. In the case of military organizations, such a recruitment problem is particularly salient and hard to solve. First, military organizations are CIPs themselves as they operate electronic warfare and cyber-defense doctrines that protect government and fight state actors who attempt to compromise national security [135, 152, 283]. Research states that there are several reasons for states to use cyber-warfare. Taking the example of China, researchers argue that the cyber-space is – and will continue to be – a decisive element in China's strategy to ascend in the international system, and this through (1) applying deterrence through infiltration of any given CI, (2) military/technological espionage to gain military knowledge, and (3) industrial espionage to gain economic advantage [135, 152]. Examples of cyber-attacks attributed to China include cyber-intrusions on a US nuclear arms laboratory, attacks on defense ministries and on the US electric grid, as well as on Google, which proved to be a small part of a broader cyber-attack that also targeted the US government [135, 277]. The example of China is by no mean isolated. The great majority of developed nations have structured cyber-defense doctrines [152]. Second, in some cases, military organizations are responsible for the protection and support of civilian CIPs in order to safeguard CIs operations [68, 286]. Finally, many military organizations have significant problems to attract specialists needed for the above activities, particularly so among IT specialists [181]. According to a 2016 US Air Force Research Institute report, job positions in the US cyber-warfare operations are only 46% filled [226]. In Switzerland, the high staff of the armed forces are faced with a similar problem [14]. The same issue also affects the Indian armed forces [265]. Therefore, one might conclude that attracting highly skilled personnel for cyber-defense is a significant problem beyond country-specific contexts or particular military organizations, as private sector organizations represent serious competition when it comes to attract IT personnel.

Table i.3 on page 20 presents an overview of the literature that studies individuals' willingness to enlist in the military. It concentrates on many sociological and psychological factors that might influence this willingness. However, this literature is limited for two reasons. First, specialists are required for IS defense, and they would enter the military sector as officers or warrant officers, and there are few studies on enlistment willingness of specialists. Second, although armed forces worldwide have liberalized service models and increased pay, under-staffing of specialists persists. The military is – by definition – part of the public sector, such that opportunities to compete with the private sector on grounds of monetary or career benefits are limited.

This context is therefore advantageous to study the acquisition of human resources. If this problem of under-staffing persists, then military forces would have problems to produce an IS-defense capability, such that the failure to recruit human specialists can be related to sub-optimal organizational outcomes. However, if the military can mitigate this problem despite the limitations it has being a part of the public sector, obstacles to build an IS-defense capability can be better understood. Moreover, if such solutions work for the military, they are likely to work among civilian CIPs too, as they face fewer restrictions. Hence, while human-resource acquisition can be productively studied in the context of the military, the findings can likely be transferred to other CIPs. Therefore, a second sub-question is:

> *How can CIPs attract the human-resource components required to build an IS-defense capability?*

2.3 Part III: Knowledge-Resource Absorption

Finally, building an IS-defense capability requires the acquisition of organizational knowledge-resource components [185, 264]. The knowledge-based view of the firm suggests that such organizational specialized knowledge is a critical ingredient to any capability production [100, 113, 114].

Organizations improve their capabilities as existing members of the organization absorb knowledge from beyond the boundary of the firm and thus develop new or improve existing skills [185, 264]. Therefore, such knowledge transfer is an important precursor of organizational performance [160, 225].[9] Accordingly, prior research confirms the relevance of such knowledge absorption for capability development [2, 281, 285, 299]. In particular, additional research on knowledge absorption demonstrates that this knowledge absorption allows organizations to produce a better level of IS security with the same investment [90], to reduce duplication of efforts [82], and to increase social welfare [106]. Most notably, the effectiveness of security solutions improves [227, 248]. Table i.4 on page 21 provides an overview of this literature. However, once one considers knowledge absorption in a CI context, there are significant gaps in this literature, and these gaps are problematic as one wants to study the contribution of knowledge absorption to IS defense in CI organizations.

First, knowledge required to build an IS-defense capability is expert knowledge and therefore highly tacit – i.e., bound to the individual and professional experience of the individual that applies it [66, 263]. Such tacit knowledge is not only hard to describe objectively (e.g., by documentation in manuals or textbooks), but it can also not readily be transferred among humans unless by intense social interaction between the sender and the recipient [213]. Still, Table i.4 on page 21 shows that there are no empirical studies of tacit knowledge absorption in a CI context, except a single study that is close to the subject [195]. Therefore, this lack of knowledge-absorption research constitutes an important research gap [289].

Second, given the extreme economic and societal damages that can be caused as a result of insufficient IS defense, both the knowledge about vulnerabilities as well as the knowledge of how to exploit and neutralize these vulnerabilities can be considered to be classified and hard to obtain unless by special, non-public channels. A cyber-security context often requires sensitive and classified information that is unlikely to be shared or disseminated via such channels for security and reputation concerns [35, 90, 124, 202, 293]. Still, a recent overview of the related literature by [170] shows that almost all researches on cyber-security knowledge transfer, exchange, and absorption study a context of knowledge transfer by public databases or discussion forums (e.g., [248, 299]).

[9] One way to ensure knowledge transfer – and thus knowledge absorption – is, for instance, through information sharing (e.g., [195, 248]).

As long as these two problems are not solved, it will be very hard to understand how CIPs can absorb the knowledge required for building an IS-defense capability, what obstacles they face, and how these might be overcome. Therefore, the third sub-question is:

> *How can CIPs succeed at absorbing external knowledge that is required to build an IS-defense capability?*

3 Methodology

In this section, a discussion is provided on how and why each of the three chapters of my thesis contributes to addressing the research gaps and research questions elaborated in the previous sections.

3.1 Research Directions

In the first chapter dedicated to material resource, I argue that the swift changes in the technological landscape require novel investment-model assumptions in order to acquire material resources needed for building an information-systems defense capability. Therefore, I adapt the well-known Gordon-Loeb model so that it can integrate the dynamic and discontinuous developments of the technological landscape. This first chapter helps critical-infrastructure providers to preempt the effect of disruptive technologies on the optimal level of investment in information-systems defense, and provides a framework in order to select and invest in the most effective technologies.

In the second chapter dedicated to human resource, I argue that an organization must emphasize the recruitment of specialist-knowledge providers in order to build an information-systems defense capability. I adopt an economic approach – based on an opportunity-cost analysis – for attracting new employees in the context of the Swiss Armed Forces, a critical infrastructure that suffers from a deficit of staff for monitoring and managing its information systems.

In the third chapter dedicated to knowledge resource, I argue that the organization must encourage continuous learning of existing organizational members in order to build an information-systems defense capability. Taking the case of *cyber-risk information sharing* as a means to foster tacit-knowledge acquisition, I propose to investigate why human agents engage in information sharing. I argue that the extent to which an individual engages in information sharing is a function of their individual knowledge-absorption expectation – i.e., the benefit they expect from sharing information.

3.2 Research Focus

The structure of this thesis implies the study of multiple contexts, all of which relate to decisions that organizations and individuals make as they attempt to acquire resources in order to build an IS-defense capability. This implies the investigation of three specific aspects related to material-, human-, and knowledge-resources acquisition. For each chapter, I study a specific organization that suffers from a specific issue related to resource acquisition.

This approach implies that important choices had to be made. First, the choice of the overarching methodology employed – i.e., the organizational capability approach – represents an important focus. Alternatives to this approach could have been, for instance, based on the use of documented data, such as log-files or incident reports. However, my approach attempts to respond to the call that the understanding of any capability production is incomplete unless the 'black box' of the organization is pried open [278]. I also follow recommendations of [10, 11, 12, 38, 89] who argue that organizations and human action and behavior must be studied in order to reach a deeper understanding of IS security.

Finally, the organizational focus allows me to explore the three resource categories in great detail and rich context, whereas any documented data measurement would involve a higher level of abstraction and hence the loss of much contextual information that is useful to understand any capability production.

Another decision regarding research focus is the use of three different organizational contexts to study the three resource categories. An alternative approach would have been to study all three resource categories in a single organizational context. However, such an approach would entail to study a single organization and the evolution of its IS-defense capability. Thus, the generalizability of the findings would be limited. Further, any profound study of knowledge absorption should involve looking beyond the boundary of the organization and hence study human interaction; else, knowledge absorption could only be studied on the receiving end in the particular organization, and much contextual information about motivations to (not) interact with others in an attempt to absorb information could not be collected. Finally, a single organization might not experience problems with respect to all three obstacles related to resources acquisition I emphasized. For example, an organization might have problems to absorb knowledge but still succeed at investing efficiently and at hiring specialists. This implies that any single organization that experiences all three obstacles at a time (inefficient investment, recruitment problems, knowledge absorption problems) would probably have an insufficient IS-defense capability and would probably also be unwilling to share data about these shortcomings with any researcher (due to reputation concerns). Therefore, I decided to mitigate these risks by studying multiple CIs in various contexts.

3.3 Research Scope

In this thesis, I study three specific problems that are respectively related to material-, human-, and knowledge-resources acquisition. An alternative approach would have been to concentrate on just the acquisition of one resource, exploring this one category in greater detail. However, I have analytically deconstructed an IS-defense capability into three resource categories, so it is consequential to study all of these. The literature surveyed in Section 2 suggests quite unanimously that all three resources are required to produce an IS-defense capability, and I therefore decided to opt for a holistic approach. Further, I argue that as long as an organization merely has only one or any two of these resources, such an organization will experience problems with the production of an IS-defense capability. For example, an organization which invests its funds efficiently for technology acquisition, but fails to recruit specialists and cannot absorb knowledge, will likely fail to produce an IS-defense capability – as such defense cannot be organized on the basis of material investment alone (as I have argued in Section 1.3). By way of analogy, the same applies to any organization that can recruit specialists but fails at both investing efficiently and absorbing knowledge. By the same token, an organization that fails to recruit specialists will be unable to absorb tacit and classified knowledge as recruitment failure implies there will be no organizational members who could absorb this knowledge. An organization that invests efficiently and succeeds at recruiting, but not at absorbing knowledge, will not be able to keep up with contemporary technology evolution and thus implied vulnerabilities, and it might miss out on receiving the most valuable (tacit, classified) type of information.

3.4 Interdisciplinary and Multi-Method Approach

A central idea of this thesis is to transfer theory and analytical concepts from economics into the IS domain in order to contribute to research questions that IS research attempts to address [80]. In doing so, I am following recommendations from the emerging research field of *security economics* (also called *the economics of information security* – e.g., [10, 11,

12, 38, 89]).[10] This implies my methodological approach is interdisciplinary; it combines thinking from IS security, microeconomics, and organizational-capability research. An alternative approach would have been to produce a number of field studies that are specific to the particular research tradition in any of these fields. But then, again, I would have missed out on the opportunity to infuse IS research with thoughts from economics, as there are few studies that span a bridge between these domains [80].

As a result of this interdisciplinary setup, my empirical approach entails the use of multiple methods. An alternative approach would have been to consistently use a single method in all three articles while still studying different contexts and resource categories. For example, as I use formal modeling in the first article of my thesis that studies material-resource investment, I could have specified formal models of specialist staff recruitment and knowledge absorption. But that again would have meant missing out in-depth insights coming from different contexts, as human behavior and knowledge absorption can hardly be captured by formal models [31, 36, 99]. This thesis makes a compromise in this regard as I study human behavior both formally – by assuming rational choice and utility maximization of human agents in my second article – and contextually in my third article as I study knowledge absorption.

The particular methods I chose in each of my articles follow well-established approaches. The first article uses formal modeling as both the original GL model and all subsequent extensions have been specified formally. The second article responds to the call for opportunity-cost analysis to study staffing problems in military organizations as prior research has merely offered sociological and psychological explanations [156, 232, 291]. Finally, the third article is also in tradition with prior approaches that study human intent, belief, behavior, and action. It therefore uses an econometric model to analyze data collected by a psychometric research design. Such designs are also widely used in the IS domain and considered to be highly useful as one studies the interaction of human behavior and ICTs [166, 221, 248, 274, 290].

4 Contributions

In my thesis, I make the following contributions. In Section 2.1, I emphasized the fact that the GL model and its extensions neither consider discontinuous SBPFs – and thus cannot capture potentially disruptive technological changes – nor temporal dynamics, as models are based on a single-period setup [104]. I argued that as long as these two aspects are not integrated into the model, CIPs might invest inappropriately – investing too much or not enough, or investing in the wrong context-specific technologies. As a result, the organization's IS-defense capability might be sub-optimal [104]. Therefore, the first article of this thesis proposes a formal extension of the GL model that introduces these two above-mentioned aspects, namely the discountinuity of any SBPF and temporal dynamics. Specifically, I develop formulae for a multi-period setup, and I relax an important assumption of the GL model by allowing the SBPF to be discontinuous. This revised model helps CIPs to invest more efficiently as they can now consider the effect of disruptive technologies and temporal dynamics. As all CIPs face the same risk structure [301], the proposed extension of the model is generalizable to any CIP. Thus, I contribute to IS-defense capability development by providing a material-resource investment model while avoiding context-specific approaches.

In Section 2.2, I emphasized the fact that few studies consider recruitment problems of IT specialists in the context of CIPs, and that an IS-defense capability would be sub-optimally developed if such IT specialists cannot be attracted and recruited properly [8, 67, 113,

[10] Moreover, such recommendations are aligned with the research agenda of the department of *Defense Economics* at the *Military Academy* of ETH Zurich, where I work as a scientific collaborator.

114, 185, 297]. I exemplified this problem by discussing the case of military organizations, as past research and evidence from business practice suggests that organizations find it difficult to recruit IT specialists [14, 181, 226, 265]. Past research based on sociological and/or psychological factors – that might explain the propensity of individuals to enlist in military organizations – fall short to explain such a lack of personnel. Yet, officers manage and control IS of any armed forces and thus organize and/or lead cyber-defense, but both new candidates and extant personnel are increasingly poached by the private sector [14, 181, 226, 265]. In the case of the Swiss Armed Forces (SAF), a staff deficit persists despite good pay and a general supportive attitude in the population [273]. This organization has been having a persistent recruitment deficit of specialist officers since 2012 (at least) [112]. Hence, this particular organization exemplifies the problems set out in Section 2.2. Due to the lack of scientific explanation for such a recruitment deficit, the second article of my thesis provides an alternative methodological approach based on an opportunity-cost analysis. Such an approach aims to shed some light on specialists' propensity to (not) enlist in a military organization. I operationalize this analysis by using labor-market data from Switzerland and data from the SAF. My opportunity-cost analysis reveals that a career as an IT specialist (who must be an officer in the context of the SAF) is the least attractive of all service alternatives as opportunity costs *vis-à-vis* private-sector employment is prohibitively high. As a result, the SAF have significant problems organizing the defense of their own IS and carrying out their potentially future missions consisting of protecting CIs. Based on my results, I develop recommendations concerning how this staffing problem might be overcome. While the findings were identified in a particular context, they can be generalized to both different armed forces of different countries and to organizations that provide cyber-defense.

In section 2.3, I emphasized the fact that the absorption of tacit and classified knowledge is required for the production of an IS-defense capability [113, 114, 248, 255, 299], and that failing to absorb this knowledge implies failing to produce an IS-defense capability [248, 299]. Still, almost no research has studied human-knowledge absorption in a context where knowledge is tacit and not readily available [170]. Therefore, the third article of this thesis attempts to study such a context. My analysis studies CIP professionals as they exchange and absorb knowledge in the non-public setting of the Switzerland's national Information Sharing and Analysis Center (ISAC).[11] I analyze a unique, restricted and novel dataset collected from these individuals by a survey I helped design and execute (see Section 2.2 of the Appendix on page XXXIX). The results show that human beliefs are associated with individuals' knowledge absorption for producing cyber-security. Resource belief, knowledge-absorption belief, and reciprocity belief are associated with knowledge absorption. To the best of my knowledge, this is the first micro-level empirical study that analyzes knowledge absorption in a private setting, where tacit knowledge is shared and absorbed. I thus contribute to the *security economics* literature by emphasizing that cyber-security is not only a technical issue, but that a proper understanding of knowledge absorption requires the use of econometric and psychometric techniques.

[11] For a general introduction to the concept of an ISAC and illustrative examples, see [236] and [75]. For a detailed description of the Swiss ISAC, its organization and history, see [47].

4.1 List of Publications

1. Percia David, D., Keupp, M. M., & Mermoud, A. (2019). *Knowledge Absorption for Cyber-Security: The Role of Human Beliefs*, Vol. tbd, No. tbd. Computers in Human Behavior (in print).

2. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2019). *To Share or Not to Share: A Behavioral Perspective on Human Participation in Security-Information Sharing*, Vol. 5, No. 1. Journal of Cybersecurity (in print).

3. Percia David, D., Keupp, M. M., Marino, R., & Hofstetter, P. (2019). *The Persistent Deficit of Militia Officers in The Swiss Armed Forces: An Opportunity Cost Explanation*, Vol. 30, No. 1. Defence and Peace Economics (pp. 111-127).

4. Mermoud, A., Keupp, M. M., & Percia David, D. (2019). *Governance Models Preferences for Security-Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection.* In Lectures Notes in Computer Science (pp. 179-190). Springer, Cham.

5. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). *Incentives for Human Agents to Share Security Information: A Model and an Empirical Test.* In Proceedings of the 17th Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria.

6. Percia David, D., Keupp, M. M., Mermoud, A., & Ghernaouti, S. (2016). *Cyber-Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model and Considerations for Critical Infrastructures.* In Lectures Notes in Computer Science (pp. 296-301). Springer, Cham.

7. Mermoud, A., Keupp, M. M., Ghernaouti, S., & Percia David, D. (2016). *Using Incentives to Foster Security-Information Sharing and Cooperation: a General Theory and Application to Critical Infrastructure Protection.* In Lectures Notes in Computer Science (pp. 150-162). Springer, Cham.

Table i.1: **Systematic Literature Review of IS Defense for CIPs**

							Methodologies		
							Risk-Management Research	**Operations Research**	**Capability Research**
Platform [c]	*Availability* [b]	*Modeling Techniques* [d]							
		MAS	SD	RM	RDB	NT	Publication [a]	Publication [a]	Publication
Athena	Limited						[71]		
CI^3	Limited						[58]		
CIMS	Commercial	X					[229]	[229]	
CIP/DSS	Limited		X				[58]	[58]	
CIPMA	Limited		X					[54]	
CISIA	Research	X			X			[224]	
COMM-ASPEN	Development	X					[28]	[28]	
DEW	Limited				X	X	[40]	[40]	
EAR-PILAR	Commercial			X	X		[184]	[184]	
EMCAS	Commercial	X					[58]	[58]	
FINSIM	Research						[85]		
FMEA/FMECA	Commercial			X			[198]	[198]	
Fort Future	Limited	X					[88]	[88]	
FTA	Commercial			X			[81]	[81]	**Research Gap**
GoRAF	Research	X			X		[70]	[70]	
CERT Initiatives	Commercial				X		[50, 51, 307]	[50, 51, 307]	
HAZOP	Commercial			X		X	[127]	[127]	
IIM	Research			X		X	[237]	[237]	
IntePoint Vu	Commercial	X						[17]	
LUND	Research						[149]		
MARGERIT V2	Commercial			X			[187]	[187]	
MIA	Research						[39]		
MUNICIPAL	Research				X		[174]	[174]	
NSRAM	Research				X			[191]	
Risk Maps	Research						[76, 79, 118]		
UIS	Limited	X					[197]	[197]	
VINCI	Research			X				[25]	

[a] The names of the authors have been omitted for readability purposes. Note that most publications cover the two approaches, namely risk-management research or operations research.
[b] Availability of platforms: still under research and/or development, readily available for organizations with commercial purposes, or by a limited/restricted group (usually the military).
[c] A brief description of platforms is presented in the Appendix (Table a.1 on page XXXIII).
[d] Concerning modeling techniques: MAS: multi-agent system; SD: system dynamics; RT: rating matrices; RDB: relational database; NT: network theory.

Table i.2: **Systematic Literature Review of the GL Model and its Extensions**

		Methodologies		
		Microeconomics		**Game Theory**
Temporality [a]	*SBPF* [b]	Theoretical	Empirical	Theoretical
Single-Period Model	Discontinuous	[295]: Willemson (2010) [29]: Baryshnikov (2012)	Research Gap	Research Gap
	Continuous	[295]: Willemson (2010) [189]: Matsuura (2009) [140]: Huang et al. (2008) [217]: Ogut et al. (2005) [141]: Huang et al. (2013) [125]: Hausken (2006) [29]: Baryshnikov (2012) [106]: Gordon et al. (2015) [104]: Gordon & Loeb (2002) [109]: Gordon et al. (2016)	[103]: Gordon & Loeb (2006) [180]: Liu et al. (2006)	[105]: Gordon et al. (2003) [176]: Lelarge (2012)
Multiple-Period Model	Discontinuous	**Research Gap** [c]	Research Gap	Research Gap
	Continuous	Research Gap	Research Gap	Research Gap

[a] The temporality indicates the number of periods the model is built on.
[b] SBPF stands for *security-breach probability function*. A distinction is made between SBPF that are continuous (here: twice-differentiable) and discontinuous (not differentiable).
[c] Whereas Part I suggests two adaptations of the GL model – by implementing a temporal setup and a discontinuity in the SBPF –, the suggested analysis of the optimal level of investment is related to microeconomics as it takes into consideration investment decisions regarding the allocation of resources, namely into disruptive technologies for cyber-security.

Table i.3: **Systematic Literature Review of Military-Enlistment Factors**

Methodologies

Sociology	**Psychology**	**Microeconomics**	
Socio-demographic factors	Intrinsic-, and extrinsic-motivation factors	Opportunity-cost factors	
		Civilian Career vs. Military Career	Conscription Context
[233]: Peuker (2012) [96]: Gibson et al. (2007) [73]: Elder et al. (2003) [97]: Gifford (2006) [161]: Kleykamp (2006) [268]: Smith (2006) [296]: Woodruff et al. (2006) [60]: Council (2003) [24]: Bachman & Segal (2000) [175]: Legree et al. (2000) [204]: Moskos et al. (1999) [20]: Asch et al. (1999) [128]: Heckhausen (1999) [20]: Asch et al. (1999) [23]: Bachman & Segal (1998) [101]: Goldscheider (1998) [260]: Segal et al. (1998) [186]: Mare & Winship (1984) [121]: Haltiner (1996) [172]: Lawrence & Legree (1996) [120]:,Haltiner (1993) [276]: Teachman & Vaughn (1993) [259]: Segal (1989) [269]: Smith et al. (1968)	[275]: Taylor et al. (2015) [298]: Wrzesniewski (2014) [233]: Peuker (2012) [84]: Fiorillo (2011) [210]: Newcomer et al. (2015) [111]: Gorman & Thomas (1991)	[15]: Angrist (1998) [138]: Hosek & Peterson (1985)	**Research Gap**

Table i.4: **Systematic Literature Review of Cyber-Risk Information Sharing**

Approaches					
Impersonal Information Analysis		**Human-involved Information Analysis**			
Methodologies					
Game Theory and Simulation	Log-files Analysis	Associated Factors of the Propensity to Share		Tacit Knowledge Transfer	
Theoretical	Empirical	Theoretical	Empirical	Theoretical	Empirical
[171]: Laube and Böhme (2016) [207]: Naghizadeh & Liu (2016) [107]: Gordon et al. (2015) [169]: Laube & Böhme (2015) [179]: Liu et al. (2011) [11]: Moore et al. (2010) [245]: Romanosky et al. (2010) [19]: Arora et al. (2008) [124]: Hausken (2007) [48]: Cavusoglu et al. (2007) [211]: Nizovtsev & Thursby (2007) [90]: Gal-Or & Ghose (2005) [217]: Ogut et al. (2005) [154]: Kannan & Telang (2005) [105]: Gordon et al. (2003)	[92]: Gay (2017) [1]: Ablon et al. (2016) [288]: Vasek et al. (2016) [183]: Maillart et al. (2017) [167]: Kwon & Johnson (2015) [303]: Zhao et al. (2015) [290]: Wang et al. (2015) [83]: Finifter et al. (2013) [238]: Ransbotham et al. (2012) [287]: Vasek & Moore (2012) [110]: Gordon et al. (2011) [91]: Gatzlaff & McCullough (2010) [108]: Gordon et al. (2010) [201]: Moore & Clayton (2008) [180]: Li & Rao (2006) [153]: Kannan et al. (2007) [3]: Acquisti et al. (2006) [162]: Ko and Dorantes (2006) [145]: Ishiguro et al. (2006) [139]: Hovav and D'Arcy (2004) [49]: Cavusoglu et al. (2004) [44]: Campbell et al. (2003)	[194]: Mermoud et al. (2018) [193]: Mermoud et al. (2017) [245]: Romanosky et al. (2010) [21]: August & Tunca (2008) [18]: Arora et al. (2006)	[196]: Mermoud et al. (2019) [306]: Zibak & Simpson (2019) [248]: Safa & von Solms (2016) [151]: Junger et al. (2017) [93]: Gcaza & von Solms (2017) [126]: Hawr' & Binsawad (2016) [123]: Hassan et al. (2014) [122]: Hassan et al. (2013) [143]: Ibragimova et al. (2012) [179]: Liu et al. (2011) [133]: Herzog et al. (2007) [160]: Kim & Lee (2006) [144]: Im & Baskerville (2005) [256]: Johnson et al. (2002) [69]: Dixon (2000) [212]: Nonaka (1994)	**Research Gap**	**Research Gap**

References

1. Ablon, L., Heaton, P., Lavery, D. & Romanosky, S. *Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information* ISBN: 978-0-8330-9312-7 (RAND Corporation, Santa Monica, USA, 2016).
2. Acklin, C. Design Management Absorption Model: A Framework to Describe and Measure the Absorption Process of Design Knowledge by SMEs with Little or No Prior Design Experience. *Creativity and Innovation Management* **22,** 147–160 (2013).
3. Acquisti, A., Friedman, A. & Telang, R. *Is There a Cost to Privacy Breaches? An Event Study* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'06)* Workshop on the Economics of Information Security (WEIS'06) (University of Cambridge, UK, 2006), 19.
4. Agrafiotis, I., Nurse, J. R., Goldsmith, M., Creese, S. & Upton, D. A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate. *Journal of Cybersecurity* **4,** tyy006 (2018).
5. Alcaraz, C. & Lopez, J. Analysis of Requirements for Critical Control Systems. *International Journal of Critical Infrastructure Protection* **5,** 137–145 (2012).
6. Alcaraz, C. & Zeadally, S. Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection* **8,** 53–66 (2015).
7. Amini, L. *et al. Adaptive Cyber-Security Analytics* tech. rep. US Patent 9,032,521 (2015).
8. Amit, R. & Schoemaker, P. J. Strategic assets and organizational rent. *Strategic Management Journal* **14,** 33–46 (1993).
9. Anderson, R. *Ross Anderson's Home Page* Economics, psychology and criminology of information security. `https://www.cl.cam.ac.uk/~rja14/` (2019).
10. Anderson, R. *Why Information Security is Hard – an Economic Perspective* in *Seventeenth Annual Computer Security Applications Conference* Annual Computer Security Applications Conference (ACSAC) (IEEE, New Orleans, USA, 2001), 358–365. ISBN: 0-7695-1405-7.
11. Anderson, R. & Fuloria, S. in *Economics of Information Security and Privacy* (eds Moore, T., Pym, D. & Ioannidis, C.) 55–66 (Springer, Boston, USA, 2010). ISBN: 978-1-4419-6967-5.
12. Anderson, R. & Moore, T. The Economics of Information Security. *Science* **314,** 610–613 (2006).
13. Anderson, R. *et al.* in *The Economics of Information Security and Privacy* 265–300 (Springer, 2013).
14. Anex, A. L'armée peine à recruter des cyber-spécialistes, plus séduits par Google. *RTS Info* (Oct. 2017).
15. Angrist, D. Estimating the Labor Market Impact of Voluntary Military Service Using Social Security Data on Military Applicants. *Econometrica* **66,** 249–288 (1998).
16. Argenti, J. *Systematic corporate planning* ISBN: 978-0-17-771053-7 (Nelson, London, 1976).
17. Armstrong, M. *IntePoint Vu: Critical Infrastructure Integration Modeling and Simulation* (IntePoint, 2010). `http://intepoint.com/products/index.html`.
18. Arora, A., Caulkins, J. P. & Telang, R. Research Note: Sell First, Fix Later: Impact of Patching on Software Quality. *Management Science* **52,** 465–471 (Mar. 1, 2006).

19. Arora, A., Telang, R. & Xu, H. Optimal Policy for Software Vulnerability Disclosure. *Management Science* **54,** 642–656 (2008).

20. Asch, B. J., Kilburn, M. R. & Kleman, J. A. *Attracting College-Bound Youth into the Military. Toward the Development of New Recruiting Policy Options.* ISBN: 0-8330-2702-6 (RAND Corporation, Santa Monica, USA, 1999).

21. August, T. & Tunca, T. I. Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions. *Information Systems Research* **19,** 48–70 (2008).

22. Azorin, P. Cybersecurity & data privacy trends in 2020. *ITProPortal* (Oct. 2019).

23. Bachman, J. G., Segal, D. R., Freedman-Doan, P. & O'Malley, P. M. Does Enlistment Propensity Predict Accession? High School Seniors' Plans and Subsequent Behavior. *Armed Forces & Society* **25,** 59–80 (1998).

24. Bachman, J. G., Segal, D. R., Freedman-Doan, P. & O'Malley, P. M. Who Chooses Military Service? Correlates of Propensity and Enlistment in the U.S. Armed Forces. *Military Psychology* **12,** 1–30 (2000).

25. Baiardi, F., Sala, G. & Sgandura, D. *Managing Critical Infrastructures through Virtual Network Communities* in *Critical Information Infrastructures Security* International Workshop on Critical Information Infrastructures SecurityCRITIS (Springer, Berlin, Heidelberg, Germany, 2007), 71–82. ISBN: 978-3-540-89173-4.

26. Ball, T. Top 5 critical infrastructure cyber attacks. *Computer Business Review* (July 2017).

27. Barney, J. Firm Resources and Sustained Competitive Advantage. *Journal of Management* **17,** 99–120 (1991).

28. Barton, D. C., Eidson, E. D., Schoenwald, D. A., Cox, R. G. & Reinert, R. K. *COMMASPEN: Simulating Economic Effects of Disruptions in the Telecommunications Infrastructure* SAND2004-0101 (Sandia Labs, 2004). `https://prod-ng.sandia.gov/techlib-noauth/access-control.cgi/2004/040101.pdf`.

29. Baryshnikov, Y. *IT Security Investment and Gordon-Loeb's 1/e rule* in *2012 Workshop on the Ecopnomics of Information Security* Workshop on the Ecopnomics of Information Security (2012).

30. Baxter, G. & Sommerville, I. Socio-technical Systems: From design Methods to Systems Engineering. *Interacting with Computers* **23,** 4–17 (2011).

31. Becker, P. H. Common Pitfalls in Published Grounded Theory Research. *Qualitative Health Research* **3,** 254–260 (1993).

32. Ben-Asher, N. & Gonzalez, C. Effects of Cyber Security Knowledge on Attack Detection. *Computers in Human Behavior* **48,** 51–61 (2015).

33. Bergman, R. & Mazzetti, M. The Secret History of the Push to Strike Iran Hawks in Israel and America Have Spent More than a Decade Agitating for War Against the Islamic Republic's Nuclear Program. Will Trump Finally Deliver? *New York Times* (Sept. 2019).

34. Biener, C., Eling, M. & Wirfs, J. H. Insurability of Cyber Risk: An Empirical Analysis. *The Geneva Papers on Risk and Insurance - Issues and Practice* **40,** 131–158 (2015).

35. Bisogni, F. *Data Breaches and the Dilemmas in Notifying Customers* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'15)* Workshop on the Economics of Information Security (WEIS'15) (Delft, Netherlands, 2015).

36. Blumer, H. Symbolic interactionism. *Contemporary Sociological Theory* **62** (2012).

37. Bodin, L. D., Gordon, L. A., Loeb, M. P. & Wang, A. Cybersecurity Insurance and Risk-Sharing. *Journal of Accounting and Public Policy* **37,** 527–544 (2018).

38. Böhme, R. *The Economics of Information Security and Privacy* ISBN: 978-3-642-39498-0 (Springer, Berlin, Heidelberg, 2013).

39. Bologna, S. *MIA: Methodology for Interdependencies Assessment* (ENEA, Communities, 2010). `http://www.progettoreti.enea.it/mia/`.

40. Broadwater, R. *DEW: Distributed Engineering Workstation* (2006). `/http://www.edd-us.com/S`.

41. Brock, J. L. *Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination* tech. rep. (General Accounting Office – Washington DC, 2000).

42. Budhwar, P. S. & Sparrow, P. R. An Integrative Framework for Understanding Cross-National Human Resource Management Practices. *Human Resource Management Review* **12,** 377–403 (2002).

43. Burrell, N. How Hiring Baby Boomers Can Assist with the Global Cybersecurity Employee Shortage. *International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)* **3,** 1–10 (2019).

44. Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security* **11,** 431–448 (2003).

45. Cardenas, A. A., Manadhata, P. K. & Rajan, S. P. Big Data Analytics for Security. *IEEE Security & Privacy* **11,** 74–76 (2013).

46. Casas, P., Soro, F., Vanerio, J., Settanni, G. & D'Alconzo, A. *Network Security and Anomaly Detection With Big-DAMA, a Big Data Analytics Framework* in *IEEE 6th International Conference on Cloud Networking (CloudNet'17)* IEEE 6th International Conference on Cloud Networking (CloudNet'17) (2017), 1–7.

47. Cavelty, M. D. *Cybersecurity in Switzerland* ISBN: 978-3-319-10620-5 (Springer, Cham, Switzerland, 2014).

48. Cavusoglu, H., Cavusoglu, H. & Raghunathan, S. Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge. *IEEE* **33,** 171–185 (2007).

49. Cavusoglu, H., Mishra, B. & Raghunathan, S. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce* **9,** 70–104 (2004).

50. *Centro de Incidentes del Centro Seguridad de la Informacion del Centro Criptologico Nacional* (CCN, 2011). `http://www.ccn-cert.cni.es/`.

51. *Centro Nacional de Proteccion de Infraestructuras Criticas en Espana.* (CNPIC, 2010). `http://www.cnpic-es.es/cnpic/`.

52. Choo, K.-K. R. The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers & Security* **30,** 719–731 (2011).

53. Church, R. L., Scaparra, M. P. & Middleton, R. S. Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems. *Annals of the Association of American Geographers* **94,** 491–502 (2004).

54. *CIPMA:Critical Infrastructure Protection Modeling and Analysis* (Australian Informatics and Statistics, 2008). `/http://www.csiro.au/partnerships/CIPMA.htmlS`.

55. Clayton, M. Stealing US business secrets: Experts ID two huge cyber 'gangs' in China. *Christian Science Monitor* (Sept. 2012).

56. Cobb, S. *Mind this Gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis* in *Virus Bulletin Conference* (2016), 1–8.

57. Commission, E. *et al. Communication from the Commission: On a European Programme for Critical Infrastructure Protection* 2006.

58. Conzelmann, G. *EMCAS: Electricity Market Complex Adaptive System* (Argonne Labs, 2008). `/http://www.dis.anl.gov/pubs/61084.pdf`.

59. Corporation, S. Dragonfly: Western energy sector targeted by sophisticated attack group. *Outlook Series.* `https://www.symantec.com/blogs/threat-intelligence/dragonfly-energy-sector-cyber-attacks` (2017).

60. Council, N. R. *Attitudes, Aptitudes, and Aspirations of American Youth: Implications for Military Recruitment* (eds Sackett, P. & Mavor, A.) ISBN: 978-0-309-08531-1 (The National Academies Press, Washington, USA, 2003).

61. Cox, J. Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior* **28,** 1849–1858 (2012).

62. Crowther, K. G. & Haimes, Y. Y. Application of the Inoperability Input—Output Model (IIM) for Systemic Risk Assessment and Management of Interdependent Infrastructures. *Systems Engineering* **8,** 323–341 (2005).

63. Crumpler, W. & Lewis, J. A. The Cybersecurity Workforce Gap. *Center for Strategic & International Studies* (Jan. 2019).

64. CSIS. Hacking the Skills Shortage. *McAfee Studies* (July 2016).

65. Daniel, F. India power cut hits millions, among world's worst outages. *Reuters* (July 2012).

66. David, P. A. Knowledge, Property, and the System Dynamics of Technological Change. *The World Bank Economic Review* **6,** 215–248 (1992).

67. Day, G. S. The capabilities of market-driven organizations. *Journal of marketing* **58,** 37–52 (1994).

68. De Bruijne, M. & Van Eeten, M. Systems That Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management* **15,** 18–29 (2007).

69. Dixon, N. M. *Common Knowledge: How Companies Thrive by Sharing What They Know* (Harvard Business School Press, 2000).

70. Donzelli, P. & Setola, R. Identifying and evaluating risks related to enterprise dependencies: a practical goal-driven risk analysis framework. *International Journal of Risk Assessment and Management* **7,** 1120–1137 (2007).

71. Drabble, B., Black, T., Kinzig, C. & Whitted, G. *Ontology based dependency analysis: Understanding the impacts of decisions in a collaborative environment* in *2009 International Symposium on Collaborative Technologies and Systems* 2009 International Symposium on Collaborative Technologies and Systems (IEEE, Baltimore, USA, 2009), 10–17.

72. Druml, N., Genser, A., Krieg, A., Menghin, M. & Hoeller, A. *Solutions for Cyber-Physical Systems Ubiquity* (IGI Global, 2017).

73. Elder Jr., G. H., Johnson, M. K. & Crosnoe, R. in *Handbook of the Life Course* 3–19 (Springer, Boston, USA, 2003). ISBN: 978-0-306-48247-2.

74. Eling, M. & Schnell, W. What Do We Know About Cyber Risk and Cyber Risk Insurance? *The Journal of Risk Finance* **17,** 474–491 (2016).

75. ENISA. *Information Sharing and Analysis Centres (ISACs): Cooperative Models* (European Union Agency for Network and Information Security, Attiki, Greece, 2018).

76. *Enterprise Risk Management — Integrated Framework* (COSO, Committe eof Sponsoring Organizations, Chicago, USA, 2004).

77. Etzioni, A. Cybersecurity in the Private Sector. *Issues in Science and Technology* **28,** 58–62 (2011).

78. Eusgeld, I., Nan, C. & Dietz, S. "System-of-Systems" Approach for Interdependent Critical Infrastructures. *Reliability Engineering & System Safety* **96,** 679–686 (2011).

79. Ezell, S. *Strengthening enterprise risk management for strategic advantage* (ERM, 2010). `http://mgt.ncsu.edu/erm/`.

80. Falco, G. *et al.* Cyber Risk Research Impeded by Disciplinary Barriers. *Science* **366,** 1066–1069 (2019).

81. *FaultTree+: Fault tree analysis* (ISOGRAPH Inc, 2010). `http://www.faulttree.org/`.

82. Feledi, D., Fenz, S. & Lechner, L. Toward Web-based Information Security Knowledge Sharing. *Information Security Technical Report* **17,** 199–209. ISSN: 1363-4127 (2013).

83. Finifter, M., Akhawe, D. & Wagner, D. *An Empirical Study of Vulnerability Rewards Programs* in *Proceedings of the 22nd USENIX Conference on Security* 22nd USENIX Conference on Security (USENIX Association, Berkeley, CA, USA, 2013), 273–288. ISBN: 978-1-931971-03-4.

84. Fiorillo, D. Do Monetary Rewards Crowd Out the Intrinsic Motivation of Volunteers? Some Empirical Evidence for Italian Volunteers: Monetary Rewards and the Motivation of Volunteers. *Annals of Public and Cooperative Economics* **82,** 139–165 (2011).

85. Flaim, S. *FinSim: Financial System Infrastructure* (Los Alamos Labs, 2006). `/http://cnls.lanl.gov/annual26/abstracts.html`.

86. For Cyber-Security, C. C. An Introduction to the Cyber-Threat Environment. *Government of Canada* (June 2018).

87. Forest, E., Schmidt, F. & McIntosh, E. Introduction to the Polymorphic Tracking Code. *KEK report* **3,** 2002 (2002).

88. *Fort Future, in:Applications, M. US Army Corps of Engineers, Engineer Research and Development Center, Construction Engi- neering Research Laboratory* (USACE, 2010). `http://www.erdc.usace.army.mil/pls/erdcpub/docs/erdc/images/ERDCFactSheet_Research_FortFuture.pdf`.

89. Furnell, S. & Clarke, N. Power to the People? The Evolving Recognition of Human Aspects of Security. *Computers & Security* **31,** 983–988 (2012).

90. Gal-Or, E. & Ghose, A. The Economic Incentives for Sharing Security Information. *Information Systems Research* **16,** 186–208 (2005).

91. Gatzlaff, K. M. & McCullough, K. A. The Effect of Data Breaches on Shareholder Wealth. *Risk Management and Insurance Review* **13,** 61–83 (2010).

92. Gay, S. Strategic news bundling and privacy breach disclosures. *Journal of Cybersecurity* **3,** 91–108. ISSN: 2057-2085. `https://academic.oup.com/cybersecurity/article/3/2/91/4775012` (2019) (June 1, 2017).

93. Gcaza, N. & von Solms, R. *Cybersecurity Culture: An ill-defined problem* in *IFIP World Conference on Information Security Education* IFIP World Conference on Information Security Education (WISE'17) (Rome, Italy, 2017), 98–109.

94. Geels, F. W. From Sectoral Systems of Innovation to Socio-technical Systems. *Research Policy* **33,** 897–920 (2004).

95. Genge, B., Kiss, I. & Piroska, H. A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures. *International Journal of Critical Infrastructure Protection* **10** (May 2015).

96. Gibson, J. L., Griepentrog, B. K. & Marsh, S. M. Parental Influence on Youth Propensity to Join the Military. *Journal of Vocational Behavior* **70,** 525–541 (2007).

97. Gifford, B. The Camouflaged Safety Net: The U.S. Armed Forces as Welfare State Institution. *Social Politics: International Studies in Gender, State & Society* **13,** 372–399 (2006).

98. Gillard, S. & Anderhalden, D. in *The Security of Critical Infrastructures* (ed Keupp, M. M.) (Springer Nature (in print), Cham, 2020).

99. Goerger, S. R., McGinnis, M. L. & Darken, R. P. A Validation Methodology for Human Behavior Representation Models. *The Journal of Defense Modeling and Simulation* **2,** 39–51 (2005).

100. Gold, A. H., Malhotra, A. & Segars, A. H. Knowledge management: An organizational capabilities perspective. *Journal of management information systems* **18,** 185–214 (2001).

101. Goldscheider, F. K. & Goldscheider, C. The Effects of Childhood Family Structure on Leaving and Returning Home. *Journal of Marriage and the Family* **60,** 745–756 (1998).

102. Goldstein, M. Hackers' Attack Cracked 10 Financial Firms in Major Assault. *The New York Times* (Oct. 2014).

103. Gordon, L. A. & Loeb, M. P. Budgeting Process for Information Security Expenditures. *Communications of the ACM* **49,** 121–125 (2006).

104. Gordon, L. A. & Loeb, M. P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)* **5,** 438–457 (2002).

105. Gordon, L. A., Loeb, M. P. & Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* **22,** 461–485 (2003).

106. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, L. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* **6,** 24–30 (2015).

107. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* **34,** 509–519 (2015).

108. Gordon, L. A., Loeb, M. P. & Sohail, T. Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly* **34,** 567–594 (2010).

109. Gordon, L. A., Loeb, M. P. & Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security* **7,** 49–59 (2016).

110. Gordon, L. A., Loeb, M. P. & Zhou, L. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* **19,** 33–56 (2011).

111. Gorman, L. & Thomas, G. W. Enlistment Motivations of Army Reservists: Money, Self-Improvement, or Patriotism? *Armed Forces & Society* **17,** 589–599 (1991).

112. Government, S. *Armeeauszählung 2016 [Armed Forces Census 2016]. Operations Staff of the Armed Forces* (Swiss Federal Department of Defense, Bern, Switzerland, 2016).

113. Grant, R. M. Prospering in Dynamically-Competitive Environments: Organizational Capability as Knowledge Integration. *Organization Science* **7,** 359–467 (1996).

114. Grant, R. M. Toward a Knowledge-Based Theory of the Firm. *Strategic Management Journal* **17,** 109–122 (S2 1996).

115. Green, K. C. The Coming Ubiquity of Information Technology. *Change: The Magazine of Higher Learning* **28,** 24–28 (1996).

116. Gressin, S. Equifax data breach. *US Federal Trade Commission* (Sept. 2017).

117. Group, N. C. *Cybersecurity Incident Taxonomy* tech. rep. (European Commission, 2018).

118. *Guıa de los Fundamentos de la Direccion de Proyectos, in: INSTITUTE, P.M., PMBOK3,Philadelphia, PA(EEUU)* (PMI, 2004), 409.

119. Hall, R. A framework linking intangible resources and capabiliites to sustainable competitive advantage. *Strategic Management Journal* **14,** 607–618 (1993).

120. Haltiner, K. W. in *Soldat-ein Berufsbild im Wandel* (eds Klein, P., Kuhlmann, J. & Rohde, H.) Klein, P., Kuhlmann, J., & Rohde, H., 112 (Deutscher Bundeswehr-Verlag, Bonn, Germany, 1993). ISBN: 978-3-559-99000-8.

121. Haltiner, K. W. in *Schweizer Armee heute und in Zukunft: Das Aktuelle Standardwerk über die Schweizerische Landesverteidigung: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse FSK* (ed Carrel, L. F.) 435–447 (Ott-Verlag, Thun, Switzerland, 1996). ISBN: 978-3-7225-6853-9.

122. Hassan, N. H., Ismail, Z. & Maarop, N. *A Conceptual mMdel for Knowledge Sharing Towards Information Security Culture in Healthcare Organization* in *International Conference on Research and Innovation in Information Systems ICRIIS'13* International Conference on Research and Innovation in Information Systems ICRIIS'13 (Kuala Lumpur, Malaysia, 2013), 516–520.

123. Hassan, N. H., Ismail, Z. & Maarop, N. *Understanding Relationship Between Security Culture and Knowledge Management* in *International Conference on Knowledge Management in Organizations* International Conference on Knowledge Management in Organizations KMO'14 (Santiago de Chile, Chile, 2014), 397–402.

124. Hausken, K. Information Sharing Among Firms and Cyber Attacks. *Journal of Accounting and Public Policy* **26,** 639–688 (2007).

125. Hausken, K. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers* **8,** 338–349 (2006).

126. Hawryszkiewycz, I. & Binsawad, M. H. *Classifying Knowledge-Sharing Barriers by Organisational Structure in Order to Find Ways to Remove These Barriers* in *Eighth International Conference on Knowledge and Systems Engineering KSE'16* Eighth International Conference on Knowledge and Systems Engineering KSE'16 (Hanoir, Vietnam, 2016), 73–78.

127. *Hazop+: Hazard and operability study* (ISOGRAPH Inc, 2008). `http://www.isograph-software.com/index.htm`.

128. Heckhausen, J. *Developmental Regulation in Adulthood* ISBN: 978-0-521-58144-8 (Cambridge University Press, Cambridge, USA, 1999).

129. Helbing, D. Globally Networked Risks and how to Respond. *Nature* **497,** 51–59 (2013).

130. Henry, D. JPMorgan hack exposed data of 83 million, among biggest breaches in history. *Reuters* (Oct. 2014).

131. Herath, H. S. & Herath, T. C. Investments in Information Security: A Real Options Perspective With Bayesian Postaudit. *Journal of Management Information Systems* **25,** 337–375 (2008).

132. Herder, P. M. & Thissen, W. A. H. in *Critical Infrastructures State of the Art in Research and Application* (eds Thissen, W. A. H. & Herder, P. M.) 1–8 (Springer, Boston, USA, 2003).

133. Herzog, A., Shahmehri, N. & Duma, C. An Ontology of Information Security. *International Journal of Information Security and Privacy (IJISP)* **1,** 1–23 (2007).

134. Hines, P., Talukdar, S., *et al.* Controlling Cascading Failures With Cooperative Autonomous Agents. *International Journal of Critical Infrastructures* **3,** 192 (2007).

135. Hjortdal, M. China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security* **4,** 1–24 (2011).

136. Hoffman, L., Burley, D. & Toregas, C. Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy* **10,** 33–39 (2012).

137. Holm, H. *Signature-Based Intrusion Detection For Zero-Day Attacks: (Not) a Closed Chapter?* in *47th Hawaii International Conference on System Sciences* 2014 47th Hawaii International Conference on System Sciences (2014), 4895–4904.

138. Hosek, J. R. & Peterson, C. E. *Enlistment Decisions of Young Men.* RAND/R-3238-MIL (Rand corp., Santa Monica, 1985).

139. Hovav, A. & D'Arcy, J. The Impact of Virus Attack Announcements on the Market Value of Firms. *Information Systems Security* **13,** 32–40 (2004).

140. Huang, C., Hu, Q. & Behara, R. S. An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-averse Firm. *International Journal of Production Economics* **114,** 793–804 (2008).

141. Huang, X., Vodenska, I., Havlin, S. & Stanley, H. E. Cascading Failures in Bi-partite Graphs: Model for Systemic Risk Propagation. *Nature* **3,** 1219 (2013).

142. Huq, N., Hilt, S. & Hellberg, N. US Cities Exposed: Industries and ICS. *A shodan-based security study of exposed systems and infrastructure in the US* (2017).

143. Ibragimova, B., Ryan, S. D., Windsor, J. C. & Prybutok, V. R. Understanding the Antecedents of Knowledge Sharing: An Organizational Justice Perspective. *Informing Science* **15,** 183–205 (2012).

144. Im, G. P. & Baskerville, R. L. A Longitudinal Study of Information System Threat Categories: The Enduring Problem of Human Error. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* **36,** 68–79 (2005).

145. Ishiguro, M., Tanaka, H., Matsuura, K. & Murase, I. *The Effect of Information Security Incidents on Corporate Values in the Japanese Stock Market* in *Proceedings of the International Workshop on the Economics of Securing the Information Infrastructure (WEII'06)* International Workshop on the Economics of Securing the Information Infrastructure (WEII'06) (Washington, DC, USA, 2006).

146. Jaffee, D. M. & Russell, T. Catastrophe Insurance, Capital Markets and Uninsurable Risks. *Journal of Risk and Insurance* **64,** 205–230 (1997).

147. Jakobson, G. *Mission Cyber Security Situation Assessment Using Impact Dependency Graphs* in *14th International Conference on Information Fusion* (2011), 1–8.

148. Jerman-Blažič, B. *et al.* Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija* **45,** 276–288 (2012).

149. Johansson, J. *Risk and Vulnerability Analysis of Interdependent Technical Infrastructures: Addressing Socio-Technical Systems* PhD thesis (2010).

150. Joshi, K. D., Chi, L., Datta, A. & Han, S. Changing the Competitive Landscape: Continuous Innovation Through IT-enabled Knowledge capabilities. *Information Systems Research* **21,** 472–495 (2010).

151. Junger, M., Montoya, L. & Overink, F.-J. Priming and Warnings Are Not Effective to Prevent Social Engineering Attacks. *Computers in human behavior* **66,** 75–87 (2017).

152. Junio, T. J. How Probable is Cyber War? Bringing IR Theory Back Into The Cyber Conflict Debate. *Journal of Strategic Studies* **36,** 125–133 (2013).

153. Kannan, K., Rees, J. & Sridhar, S. Market Reactions to Information Security Breach Announcements: An Empirical Analysis. *International Journal of Electronic Commerce* **12,** 69–91 (2007).

154. Kannan, K. & Telang, R. Market for Software Vulnerabilities? Think Again. *Management Science* **51,** 726–740 (2005).

155. Karnouskos, S. *Stuxnet Worm Impact on Industrial Cyber-Physical System Security* in *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society* (2011), 4490–4494.

156. Keller, K., Poutvaara, P. & Wagener, A. Military Draft and Economic Growth in Oecd Countries. *Defence and Peace Economics* **20,** 373–393 (2009).

157. Kelley, M. B. The Stuxnet Attack on Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. *Business Insider* (Nov. 2013).

158. Kessler, G. C. & Ramsay, J. Paradigms for Cybersecurity Education in a Homeland Security Program. *Journal of Homeland Security Education* **2,** 35 (2013).

159. Kim, G., Shin, B. & Kwon, O. Investigating the value of sociomaterialism in conceptualizing IT capability of a firm. *Journal of Management Information Systems* **29,** 327–362 (2012).

160. Kim, S. & Lee, H. The Impact of Organizational Context and Information Technology on Employee Knowledge-Sharing Capabilities. *Public Administration Review* **66,** 370–385 (2006).

161. Kleykamp, M. A. College, Jobs, or the Military? Enlistment During a Time of War. *Social Science Quarterly* **87,** 272–290 (2006).

162. Ko, M. & Dorantes, C. The Impact of Information Security Breaches on Financial Performance of the Breached Firms: an Empirical Investigation. *Journal of Information Technology Management* **17,** 13–22 (2006).

163. Kotzanikolaou, P., Theoharidou, M. & Gritzalis, D. Assessing n-order Dependencies Between Critical Infrastructures. *International Journal of Critical Infrastructures* **9,** 93–110 (2013).

164. Kunreuther, H. & Heal, G. Interdependent Security. *Journal of Risk and Uncertainty* **26,** 231–249 (2003).

165. Kushner, D. The Real Story of Stuxnet. *IEEE Spectrum* (Feb. 2013).

166. Kwahk, K.-Y. & Park, D.-H. The Effects of Network Sharing on Knowledge-sharing Activities and job Performance in Enterprise Social Media Environments. *Computers in Human Behavior* **55,** 826–839 (B 2016).

167. Kwon, J. & Johnson, M. E. *The Market Effect of Healthcare Security: Do Patients Care about Data Breaches?* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'15)* Workshop on the Economics of Information Security (WEIS'15) (2015).

168. Laney, D. 3D Data Management: Controlling Data Volume, Velocity and Variety. *META Group Research Note* **6,** 1 (2001).

169. Laube, S. & Böhme, R. *Mandatory Security Information Sharing with Authorities: Implications on Investments in Internal Controls* in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security - WISCS '15* 22nd ACM Conference on Computer and Communications Security (ACM Press, Denver, USA, 2015), 31–42. ISBN: 978-1-4503-3822-6.

170. Laube, S. & Böhme, R. Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys (CSUR)* **50,** 77 (2017).

171. Laube, S. & Böhme, R. The Economics of Mandatory Security Breach Reporting to Authorities. *Journal of Cybersecurity* **2,** 29–41 (2016).

172. Lawrence, G. H. & Legree, P. J. *Military Enlistment Propensity: A Review of Recent Literature* Final Report (Army Research Institution for the Behavioral and Social Sciences, Alexandria, USA, 1996).

173. Lee, J., Bagheri, B. & Kao, H.-A. A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems. *Manufacturing Letters* **3,** 18–23 (2015).

174. Lee, M. *A Dynamic Systems Simulation Approach to Risk Mitigation for Critical Infrastructure at the United States Military Academy* in *Proceedings of the 19th International Conference of the System Dynamics Society* 19th International Conference of the System Dynamics Society (System Dynamics Society, Atlanta, USA, 2001). ISBN: 978-0-9672914-4-4.

175. Legree, P. J. *et al.* Military Enlistment and Family Dynamics: Youth and Parental Perspectives. *Military Psychology* **12,** 31–49 (2000).

176. Lelarge, M. Coordination in Network Security Games: a Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications* **30,** 2210–2219. ISSN: 0733-8716 (2012).

177. Lewis, J. Economic Impact of Cybercrime – No Slowing Down. *CSIS* **1,** 1–28 (2018).

178. Li, J. & Su, X. *Making Cost Effective Security Decision With Real Option Thinking* in *International Conference on Software Engineering Advances (ICSEA 2007)* (2007), 14–14.

179. Liu, D., Ji, Y. & Mookerjee, V. Knowledge sharing and investment decisions in information security. *Decision Support Systems* **52,** 95–107 (2011).

180. Liu, W., Tanaka, H. & Matsuura, K. *An Empirical Analysis of Security Investment in Countermeasures Based on an Enterprise Survey in Japan* in *5th Annual Workshop on the Economics of Information Security, WEIS 2006* 5th Annual Workshop on the Economics of Information Security, WEIS 2006 (Cambridge, UK, 2006).

181. Lynch, J. Inside the Pentagon's struggle to build a cyber force. *Fifth Domain* (Oct. 2018).

182. Mahmood, T. & Afzal, U. *Security Analytics: Big Data Analytics for Cybersecurity: a Review of Trends, Techniques and Tools* in *2013 2nd National Conference on Information Assurance (NCIA)* 2013 2nd National Conference on Information Assurance (NCIA) (IEEE, Rawalpindi, Pakistan, 2013), 129–134. ISBN: 978-1-4799-1288-9.

183. Maillart, T., Zhao, M., Grossklags, J. & Chuang, J. Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond With Bug Bounty Programs. *Journal of Cybersecurity* **3,** 81–90 (2017).

184. Manas, A. L. H. *PILAR: PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DERIESGOS* (2007). `/http://www.ar-tools.com/index.html?tools/pilar/index.htmlS`.

185. March, J. G. Exploration and Exploitation in Organizational Learning. *Organization Science* **2,** 71–87 (1991).

186. Mare, R. D. & Winship, C. The Paradox of Lessening Racial Inequality and Joblessness Among Black Youth: Enrollment, Enlistment, and Employment, 1964-1981. *American Sociological Review* **49,** 39–55 (1984).

187. *Margerit: Metodologia de analisis y gestion deriesgos de los sistemas de informacion de las administraciones publicas* (CCN Criptologıa, 2010). `http://www.csi.map.es/csi/pg5m20.htm`.

188. Mata, F. J., Fuerst, W. L. & Barney, J. B. Information technology and sustained competitive advantage: A resource-based analysis. *MIS Quarterly* **19,** 487–505 (1995).

189. Matsuura, K. in *Managing Information Risk and the Economics of Security* (ed Johnson, M. E.) 99–119 (Springer, Boston, USA, 2009). ISBN: 978-0-387-09762-6.

190. Maynard, T. & Beecroft, N. Business Blackout: The Insurance Implications of a Cyber-Attack on the US Power Grid. *Society & Security* **1,** 1–65 (2015).

191. McManus, J., Baker, G., Redwine, S. & Riley, P. *NSRAM: Network Security Risk Assessment Model.* (2004). `http://www.jmu.edu/iiia/webdocs/Reports/NSRAMIIIATP04-01.pdf`.

192. Melville, N., Kraemer, K. & Gurbaxani, V. Information Technology and Organizational Performance: an Integrative Model of IT Business Value. *MIS Quarterly* **28,** 283–322 (2004).

193. Mermoud, A., Keupp, M. M., Ghernaouti, S. & David, D. P. *Using Incentives to Foster Security Information Sharing and Cooperation: a General Theory and Application to Critical Infrastructure Protection* in *International Conference on Critical Information Infrastructures Security* (Springer, 2016), 150–162.

194. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M. & Percia David, D. *Incentives for Human Agents to Share Security Information: a Model and an Empirical Test* in. Workshop on The Economics of Information Security (Innsbruck, 2018), 1–22.

195. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M. & Percia David, D. To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing. *Journal of Cybersecurity* **5,** (in print (2019).

196. Mermoud, A., Keupp, M., Huguenin, K., Palmié, M. & Percia David, D. *To Share or Not to Share: a Behavioral Perspective on Human Participation in Security Information Sharing* tech. rep. (HAL, 2019).

197. Michelsen, R. (Los Alamos Labs, 2008). `http://www.nemaweb.org/default.aspx?3435`.

198. Milulak, R. *The Basics of FMEA* (2004). `http://www.fmea-fmeca.com/`.

199. Mocetti, S., Pagnini, M. & Sette, E. Information Technology and Banking Organization. *Journal of Financial Services Research* **51,** 313–338 (2017).

200. Moore, T. & Anderson, R. *Economics and Internet Security: a Survey of Recent Analytical, Empirical and Behavioral Research* Cambridge, 2011.

201. Moore, T. & Clayton, R. *The consequence of non-cooperation in the fight against phishing* in *Proceedings of the Anti-Phishing Working Group eCrime Researchers Summit* Anti-Phishing Working Group eCrime Researchers Summit (IEEE, Atlanta, USA, 2008), 1–14. ISBN: 978-1-4244-2969-1.

202. Moran, T. & Moore, T. *The Phish-Market Protocol: Securely Sharing Attack Data between Competitors* in *Financial Cryptography and Data Security* International Conference on Financial Cryptography and Data Security (Springer, Berlin, Heidelberg, Germany, 2010), 222–237. ISBN: 978-3-642-14577-3.

203. Mosenia, A. & Jha, N. K. A Comprehensive Study of Security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing* **5,** 586–602 (2016).

204. Moskos, C. C., Williams, J. A. & Segal, D. R. *The Postmodern Military: Armed Forces After the Cold War* ISBN: 978-0-19-513329-5 (Oxford University Press, New York, USA, 1999).

205. Moteff, J. & Parfomak, P. *Critical Infrastructure and Key Assets: Definition and Identification* (Library of Congress Washington DC, Congressional Research Service, Washington, DC, 2004).

206. Murphy, H. Companies urged to bolster infrastructure cyber defences. *Financial Times* (Oct. 2019).

207. Naghizadeh, P. & Liu, M. *Inter-temporal Incentives in Security Information Sharing Agreements* in *2016 Information Theory and Applications Workshop (ITA)* 2016 Information Theory and Applications (ITA) (IEEE, La Jolla, USA, 2016), 1–8. ISBN: 978-1-5090-2529-9.

208. Naraine, R. Stuxnet attackers used 4 Windows zero-day exploits. *ZDNet* (Sept. 2010).

209. Nelson, R. R. & Winter, S. G. The Schumpeterian tradeoff revisited. *The American Economic Review* **72,** 114–132 (1982).

210. *Handbook of Practical Program Evaluation* (eds Newcomer, K. E., Hatry, H. P. & Wholey, J. S.) 4th ed. (Jossey-Bass & Pfeiffer Imprints, Wiley, San Francisco, USA, 2015). ISBN: 978-1-119-17138-6.

211. Nizovtsev, D. & Thursby, M. To disclose or not? An analysis of software user behavior. *Information Economics and Policy* **19,** 43–64 (2007).

212. Nonaka, I. A Dynamic Theory of Organizational Knowledge Creation. *Organization science* **5,** 14–37 (1994).

213. Nonaka, I. & Takeuchi, H. *The Knowledge-Creating Company : How Japanese Companies Create the Dynamics of Innovation* 1st ed. ISBN: 978-0-19-509269-1 (Oxford University Press, New York, USA, 1995).

214. Obama, B. *Executive Order (13636) – Improving critical infrastructure cybersecurity* (The White House, Washington, USA, 2013).

215. OECD. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (OECD Publishing, 2012).

216. Of Standards, " I. & Technology". Framework for Improving Critical Infrastructure Cybersecurity. *NIST* (Apr. 2018).

217. Öğüt, H., Memon, N. & Raghunathan, S. *Cyber insurance and IT security investment: Impact of interdependent risk* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'05)* Workshop on the Economics of Information Security (WEIS'05) (Cambridge, USA, 2005).

218. Öğüt, H., Raghunathan, S. & Menon, N. Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis* **31,** 497–512 (2011).

219. Oltsik, J. & Alexander, C. The life and times of cybersecurity professionals. *ESG and ISSA: Research Report* (2017).

220. Otto, G. Workshop Plots Evolution of NIST Cybersecurity Framework. *FedScoop* (Apr. 2016).

221. Ou, C. X. J., Davison, R. M. & Wong, L. H. M. Using Interactive Systems for Knowledge Sharing: the Impact of Individual Contextual Preferences in China. *Information & Management* **53,** 145–156 (2016).

222. Ouyang, M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering & System Safety* **121,** 43–60 (2014).

223. Ouyang, M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering & System Safety* **121,** 43–60 (2014).

224. Panzieri, S., Setola, R. & Ulivi, G. *CISIA:Critical Infrastructure Simulation by Interdependent Agents* (Roma, Italy, 2005). `/http://www.dia.uniroma3.it/panzieri/Articoli/WorldIFAC05-CIIP.pdfS`.

225. Park, B. I. Knowledge Transfer Capacity of Multinational Enterprises and Technology Acquisition in International Joint Ventures. *International Business Review* **20,** 75–87 (2011).

226. Parker, W. Cyber Workforce Retention. *Perspective on Cyber Power* (Oct. 2016).

227. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* **42,** 165–176 (2014).

228. Pearlson, K. E. & Saunders, C. S. *Managing and Using Information Systems: A Strategic Approach* (John Wiley & Sons, 2019).

229. Pederson, P., Dudenhoeffer, D., Hartley, S. & Permann, M. *Critical infrastructure interdependency modeling: a survey of US and international research* (Idaho National Laboratory, Idaho Falls, USA, 2006).

230. Peeler, J., Messer, A. & Hamilton, A. $(ISC)^2$ Study: Workforce Shortfall Due to Hiring Difficulties Despite Rising Salaries, Increased Budgets and High Job Satisfaction Rate. $(ISC)^2$ (Apr. 2015).

231. Peppard, J. & Ward, J. Beyond Strategic Information Systems: Towards an IS Capability. *The Journal of Strategic Information Systems* **13,** 167–194 (2004).

232. Perri, T. Deferments and the Relative Cost of Conscription. *The B.E. Journal of Economic Analysis & Policy* **10,** 103 (2010).

233. Peuker, M. *Motivation of Swiss Army Career Officers: Implications of Generational Characteristics for Attracting and Recruiting Career Officer Candidates* Master's thesis (University of Fribourg, Fribourg, Switzerland, 2012). 20–50.

234. Polanyi, M. Tacit Knowing: Its Bearing on Some Problems of Philosophy. *Reviews of Modern Physics* **34,** 601–616 (1962).

235. Ponemon, L. The Cost of Cybercrime. *Ninth Annual Cost of Cybercrime Study* **9,** 1–42 (2018).

236. Powner, D. A. *Critical Infrastructure Protection Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities: Report to Congressional Requesters.* (DIANE Publishing, 2005).

237. Quarles, L. R. & Haimes, Y. Y. *IIM: Inoperability Input–Output Model* (2007). `http://www.thei3p.org/docs/publications/IIM-factsheet-Feb2007.pdf`.

238. Ransbotham, S., Kane, G. C. & Lurie, N. H. Network Characteristics and the Value of Collaborative User-Generated Content. *Marketing Science* **31,** 369–547 (2012).

239. Ravichandran, T. & Lertwongsatien, C. Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of management information systems* **21,** 237–276 (2005).

240. Ricketts, T. Sheep dip your removable storage devices to reduce the threat of cyber attacks. *Business Insider* (July 2017).

241. Rid, T. & Buchanan, B. Attributing Cyber Attacks. *Journal of Strategic Studies* **38,** 4–37 (2015).

242. Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine* **21,** 11–25 (2001).

243. Ritz, A. & Waldner, C. Competing for Future Leaders: A study of Attractiveness of Public Sector Organizations to Potential Job Applicants. *Review of Public Personnel Administration* **31,** 291–316 (2011).

244. Rockart, J. F. *et al.* The Line Takes the Leadership (1987).

245. Romanosky, S., Sharp, R. & Acquisti, A. *Data Breaches and Identity Theft: When is Mandatory Disclosure Optimal?* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'10)* Workshop on the Economics of Information Security (WEIS'10) (Cambridge, USA, 2010).

246. Rowe, R. Protecting Our Armed Forces Critical Infrastructure: Prioritize Patriot. *IEM* (Sept. 2019).

247. Rushe, D. JP Morgan Chase reveals massive data breach affecting 76m households. *The Guardian* (Oct. 2014).

248. Safa, N. S. & Von Solms, R. An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior* **57,** 442–451 (2016).

249. Sahebjamnia, N., Torabi, S. A. & Mansouri, S. A. Integrated Business Continuity and Disaster Recovery Planning: Towards Organizational Resilience. *European Journal of Operational Research* **242,** 261–273 (2015).

250. Santos, J. R., Haimes, Y. Y. & Lian, C. A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies: Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. *Risk Analysis* **27,** 1283–1297 (2007).

251. Sathi, A. *Big Data Analytics: Disruptive Technologies for Changing the Game* ISBN: 978-1-58347-380-1 (Mc Press, Boise, USA, 2012).

252. Scarbrough, H. Knowledge Management, HRM and the Innovation Process. *International Journal of Manpower* **24,** 501–516 (2003).

253. Schaeffer, D., Olson, P. & Eck, C. An Interdisciplinary Approach to Cybersecurity Curriculum. *Journal of Higher Education Theory and Practice* **17** (2017).

254. Schatz, D. & Bashroush, R. Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers* **19,** 1205–1228 (2017).

255. Schilling, M. A. *Strategic Management of Technological Innovation* 3rd ed. ISBN: 978-0-07-128957-3 (McGraw-Hill Education, New York, USA, 2010).

256. Scholes, K., Johnson, G. & Whittington, R. *Exploring Corporate Strategy* (Financial Times Prentice Hall, 2001).

257. Schwartz, A. Significant Cyber Incidents. *Center for Strategic and International Studies* (Nov. 2019).

258. Seals, T. Cyber-Workforce Shortage to Increase to 1.8 Million Positions by 2022. *InfoSecurity* (Feb. 2017).

259. Segal, D. R. *Recruiting for Uncle Sam: Citizenship and Military Manpower Policy* ISBN: 978-0-7006-0549-1 (University of Kansas Press, Kansas, USA, 1989).

260. Segal, D. R., Burns, T. J., Falk, W. W., Silver, M. P. & Sharda, B. D. The All-Volunteer Force in the 1970s. *Social Science Quarterly* **79,** 390–411 (1998).

261. Shirtz, D. & Elovici, Y. Optimizing Investment Decisions in Selecting Information Security Remedies. *Information Management & Computer Security* **19,** 95–112 (2011).

262. Siegel Bernard, T. Ways to Protect Yourself After the JPMorgan Hacking. *The New York Times* (Oct. 2014).

263. Siesfeld, T., Cefola, J. & Neef, D. *The Economic Impact of Knowledge* (Routledge, 2009).

264. Simon, H. A. Bounded Rationality and Organizational Learning. *Organization Science* **2,** 125–134 (1991).

265. Singh, N. India's new Defence Cyber Agency. *Medianama* (May 2015).

266. Sirmon, D. G., Hitt, M. A., Ireland, R. D. & Gilbert, B. A. Resource orchestration to create competitive advantage: Breadth, depth, and life cycle effects. *Journal of management* **37,** 1390–1412 (2011).

267. Smeraldi, F. & Malacaria, P. *How to spend it: optimal investment for cyber security* in *Proceedings of the 1st International Workshop on Agents and CyberSecurity* (2014), 8.

268. Smith, L. *The Few and the Proud: Marine Corps Drill Instructors in Their Own Words* ISBN: 978-0-393-32992-6 (Norton, New York, USA, 2006).

269. Smith, M. B., Maccoby, E., Lippitt, R., Inkeles, A. & Brim, O. G. *Socialization and Society* (Social Science Research Council (Committee on Socialization and Social Structure), Boston, USA, 1968), 270–320.

270. Snell, E. NIST Cybersecurity Framework Updates, Clarification Underway. *FedScoop* (June 2016).

271. Soomro, Z. A., Shah, M. H. & Ahmed, J. Information Security KManagement Needs More Holistic Approach: A Literature Review. *International Journal of Information Management* **36,** 215–225 (2016).

272. Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. Analysis of end user security behaviors. *Computers & security* **24,** 124–133 (2005).

273. Szvircsev Tresch, T. *et al. Sicherheit 2018: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend* (Center for Security Studies (CSS), ETH Zürich; Militärakademie (MILAK) an der ETH Zürich, Birmensdorf, 2018).

274. Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M. & Rohani, V. A. Evaluation Model for Knowledge Sharing in Information Security Professional Virtual Community. *Computers & Security* **43,** 19–34 (2014).

275. Taylor, J. K., Clerkin, R. M., Ngaruiya, K. M. & Velez, A.-L. K. An Exploratory Study of Public Service Motivation and the Institutional–Occupational Model of the Military. *Armed Forces & Society* **41,** 142–162 (2015).

276. Teachman, J. D., Vaughn, V. R. A. & Segal, M. W. The Selectivity of Military Enlistment. *Journal of Political and Military Sociology* **21,** 287–309 (1993).

277. Team", " R. A. I. Dragonfly: Western energy sector targeted by sophisticated attack group. *Symantec Threat Intelligence* (Oct. 2017).

278. Teece, D. J. A Capability Theory of the Firm: an Economics and (Strategic) Management Perspective. *New Zealand Economic Papers* **53,** 1–43 (2019).

279. Terzi, D. S., Terzi, R. & Sagiroglu, S. *Big Data Analytics for Network Anomaly Detection from Netflow Data* in *International Conference on Computer Science and Engineering (UBMK'17)* International Conference on Computer Science and Engineering (UBMK'17) (2017), 592–597.

280. Tether, B. S. & Tajar, A. Beyond Industry–University Links: Sourcing Knowledge for Innovation from Consultants, Private Research Organisations and the Public Science-Base. *Research Policy* **37,** 1079–1095 (2008).

281. Torkkeli, M. T., Podmetina, D., Yla-Kojola, A.-M. & Vaatanen, J. Knowledge Absorption in an Emerging Economy–the Role of Foreign Investments and Trade Flows in Russia. *International Journal of Business Excellence* **2,** 269–284 (2009).

282. Trump, D. *Presidential Executive Order (13800) – Strengthening the cybersecurity of federal networks and critical infrastructure* (The White House, Washington, USA, 2017).

283. Tyugu, E. *Command and Control of Cyber Weapons* in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (2012), 1–11.

284. Vaidyanathan, R. Hundreds of millions without power in India. *BBC News* (July 2012).

285. Van den Bosch, F. A. J., Volberda, H. W. & de Boer, M. Coevolution of Firm Absorptive Capacity and Knowledge Environment: Organizational Forms and Combinative Capabilities. *Organization Science* **10,** 551–568 (1999).

286. Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., Klaver, M. & Cruz, E. The State and the Threat of Cascading Failure Across Critical Infrastructures: the Implications of Empirical Evidence from Media Incidence Reports. *Public Administration* **89,** 381–400 (2011).

287. Vasek, M. & Moore, T. *Do Malware Reports Expedite Cleanup? An Experimental Study* in *Proceedings of the Workshop on Cyber Secrurity Experimentation and Test (CSET'12)* 5th Workshop on Cyber Security Experimentation and Test (USENIX, Bellevue, USA, 2012).

288. Vasek, M., Weeden, M. & Moore, T. *Measuring the Impact of Sharing Abuse Data with Web Hosting Providers* in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* 2016 ACM on Workshop on Information Sharing and Collaborative Security. event-place: Vienna, Austria (ACM, New York, USA, 2016), 71–80. ISBN: 978-1-4503-4565-1.

289. Wang, S. & Noe, R. A. Knowledge Sharing: a Review and Directions for Future Research. *Human Resource Management Review* **20,** 115–131 (2010).

290. Wang, W.-T. & Hou, Y.-P. Motivations of Employees' Knowledge Sharing Behaviors: A Self-Determination Perspective. *Information and Organization* **25,** 1–26 (2015).

291. Warner, J. T. & Asch, B. J. The Record and Prospects of the All-Volunteer Military in the United States. *Journal of Economic Perspectives* **15,** 169–192 (2001).

292. Weinberger, S. Computer security: Is this the start of cyberwarfare? *Nature News* **474,** 142–145 (2011).

293. Weiss, N. E. *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (Congressional Research Service, Washington, USA, 2014).

294. Whitehead, J. *et al.* Global Risk Dialogue: Industry 4.0, The Next Generation of Corporate Risks. *Allianz Global Corporate & Specialty* **36,** 1–31. `https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/grd/AGCS-GRD-1-2016-EN.pdf` (2016).

295. Willemson, J. *Extending the Gordon and Loeb Model for Information Security Investment* in *2010 International Conference on Availability, Reliability and Security* 2010 International Conference on Availability, Reliability, and Security (ARES) (IEEE, Krakow, Poland, 2010), 258–261. ISBN: 978-1-4244-5879-0.

296. Woodruff, T., Kelty, R. & Segal, D. R. Propensity to Serve and Motivation to Enlist among American Combat Soldiers. *Armed Forces & Society* **32,** 353–366 (2006).

297. Wright, P. M., Dunford, B. B. & Snell, S. A. Human resources and the resource based view of the firm. *Journal of management* **27,** 701–721 (2001).

298. Wrzesniewski, A. *et al.* Multiple Types of Motives Don't Multiply the Motivation of West Point Cadets. *Proceedings of the National Academy of Sciences* **111,** 10990–10995 (2014).

299. Yan, Z., Wang, T., Chen, Y. & Zhang, H. Knowledge Sharing in Online Health Communities: a Social Exchange Theory Perspective. *Information & Management* **53,** 643–653 (2016).

300. Yeoh, P.-L. & Roth, K. An empirical analysis of sustained advantage in the US pharmaceutical industry: Impact of firm resources and capabilities. *Strategic management journal* **20,** 637–653 (1999).

301. Yusta, J. M., Correa, G. J. & Lacal-Arántegui, R. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-art. *Energy Policy* **39,** 6100–6119 (2011).

302. Zadelhoff, M. Cybersecurity has a serious talent shortage: Here's how to fix it. *Harvard Business Review* (May 2017).

303. Zhao, M., Grossklags, J. & Liu, P. *An Empirical Study of Web Vulnerability Discovery Ecosystems* in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security* 22Nd ACM SIGSAC Conference on Computer and Communications Security (ACM, New York, USA, 2015), 1105–1117. ISBN: 978-1-4503-3832-5.

304. Zhou, L., Loeb, M. P., Gordon, L. A. & Lucyshyn, W. Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security* **9,** 720–726 (2018).

305. Zhu, B., Anthony, J. & Shankar, S. *A Taxonomy of Cyber Attacks on SCADA Systems* in *2011 International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing* 2011 International conference on internet of things and 4th international conference on cyber, physical and social computing. IEEE (IEEE, Dalian, 2011), 380–388. ISBN: 978-1-4577-1976-9.

306. Zibak, A. & Simpson, A. *Cyber Threat Information Sharing: Perceived Benefits and Barriers* in *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), 85.

307. Zielstra, A. *GOVCERT: Cybercrime Information Exchange. Cybersecurity and Critical Infrastructure Protection* (Madrid, Spain, 2010). `http://www.govcert.nl/render.html?it=35`.

Part I

Material-Resource Investment

'The joy of disruption comes from accepting that we all live in a temporal state.'

— Jay Samit

Cyber-Security Investment in the Context of Disruptive Technologies

Extension of the Gordon-Loeb Model and Considerations for Critical Infrastructures

Percia David Dimitri[1,2]; Keupp Marcus[2]; Mermoud Alain[1,2]; Ghernaouti Solange[1]

[1] University of Lausanne, Faculty of HEC, Department of Information Systems
[2] ETH Zurich, Military Academy, Department of Defense Economics

Conference paper for *The 11th International Conference on Critical Information Infrastructures Security* (CRITIS), 2016 - Paris, France

- Presented on October 11, 2016;
- Revised and published (post-proceedings) in the Springer *Lecture Notes in Computer Science* (LNCS) on October 29, 2016;
- Published online on November 22, 2017.

N.B.: In order to harmonize some technical notions throughout this thesis, adaptations were implemented.

Abstract

Cyber-security breaches inflict significant costs on organizations. Therefore, the development of an information-systems defense capability through cyber-security investment is a prerequisite. The question of how to determine the optimal amount to invest in cyber-security has been widely investigated in the literature. In this respect, the Gordon-Loeb model and its extensions received wide-scale acceptance. However, such models predominantly rely on restrictive assumptions that are not adapted for analyzing dynamic aspects of cyber-security investment. Yet, understanding such dynamic aspects is a key feature for studying cyber-security investment in the context of a fast-paced and continuously evolving technological landscape. We propose an extension of the Gordon-Loeb model by considering multi-period and relaxing the assumption of a continuous security-breach probability function. Such theoretical adaptations enable to capture dynamic aspects of cyber-security investment such as the advent of a disruptive technology and its consequences on the aforementioned investment. Such a proposed extension of the Gordon-Loeb model gives room for a hypothetical decrease of the optimal level of cyber-security investment, due to a potential technological shift. While we believe our framework should be generalizable across the cyber-security milieu, we illustrate our approach in the context of critical-infrastructure protection, where security-cost reductions related to risk events are of paramount importance as potential losses reach unaffordable proportions. Moreover, despite the fact that some technologies are considered as disruptive and thus promising for critical-infrastructure protection, their effects on cyber-security investment have been discussed little.

Keywords— information systems; security economics; cyber-security investment; Gordon-Loeb model; security analytics.

Contents of Part I

1 Introduction

Cyber-security breaches inflict significant costs on organizations, businesses, and individuals [7, 13, 23]. As a result, operators of information systems (IS) must develop an IS-defense capability. In order to build a capability, investing in material resources is a prerequisite [9, 35, 44]. In the context of cyber-security, such material resources are composed by processes, products and/or services that are related to the security management of IS in general and, among others, to cyber-threats monitoring in particular [2, 4, 31, 38, 41] – e.g., intrusion-detection systems (IDS).

The cyber-security investment issue has received significant academic attention (for an extensive literature review, see [38]), and such a literature is often directly related to practitioners' needs. For instance, as organizations face budget constraints, an important challenge for these same organizations is to maximize the efficiency of any monetary investment in cyber-security processes, products and/or services [12, 21, 38]. Prior IS research has produced many quantitative models that propose to optimize such investment, as well as recommendations to invest in particular technologies or systems (e.g., [12, 25, 27, 30, 40]). These formal approaches are complemented by less formal practitioner-oriented discussions [8, 42, 48]. Among all the available models and approaches, the Gordon-Loeb (GL) model has received wide-scale acceptance [50]. The GL model is based on microeconomics – more precisely on the fundamental economic principle of cost-benefit analysis [21, 22] –, establishing a general setup for determining the optimal level of cyber-security investment. By specifying a security-breach probability function (SBPF), the GL model attempts to determine the above-mentioned optimal investment amount for cyber-security processes, products and/or services (e.g., [10, 21, 22, 29, 49], for an extensive literature review, see Table i.2 on page 19).

However, the GL model framework evades dynamic issues such as perverse economic incentives[1] and the advent of a *disruptive*[2] cyber-security technology [21]. Yet, in the case of the latter, accounting for such dynamic issues could significantly enrich the initial model by giving supplementary time-related insights concerning the potential consequences that disruptive technologies might trigger for cyber-security investment. If conventional cyber-security processes, products and/or services such as IDS are essentially assimilated to the *targeted event-based detection* approach [2, 4, 31, 41], the swift evolution of both the technological landscape and cyber-threats calls for a complementary approach based on *behavior-anomaly detection* [2, 15, 19, 31, 36, 41, 45, 47], and its subsequent (potentially) disruptive technologies.

By extending the original GL model to a multi-period setup, and by relaxing the assumption of a continuously twice-differentiable SBPF, we create room for additional insights on cyber-security investment by delivering a theoretical ground that enables to

[1] For example, externalities arising when the decisions of one party affect those of others [3].

[2] In economic terms, the notion of *disruptive technology* [17] refers to a radically innovative technology that significantly disrupts existing economic structures, markets and value networks, thus displacing established leading products, processes and/or services [17]. Therefore, a *disruptive technology* comes from innovation. However, not all innovations are disruptive, even though they can be revolutionary. For instance, the creation of the first automobiles in the late XIX^{th} century was revolutionary, but not disruptive. The reason is that early automobiles were expensive luxury goods, hence only a small portion of the market share of horse-drawn vehicles was replaced by automobiles. As a result, the market for transportation essentially remained intact until the beginning of the lower-priced Ford Model T (in 1908) [18]. The mass production of automobiles, however, was a disruptive innovation, as it radically displaced the established horse-drawn vehicles, and established automobiles as the type of vehicles that possesses the greater market share [18]. Similarly, the advent of personal computers (PC) in the IT landscape can be considered as a disruption. The multi-purpose functionalities of PCs, as well as their relatively small size, their extended capabilities, and their low price facilitated their spread and individual use. PCs displaced large and costly minicomputers and mainframes, significantly affecting the lives of individuals and the management of organizations.

investigate the effect of a disruptive technology on such investment. In this article, we illustrate the concept of disruptive technologies through the case of big-data analytics[3] (BDA) technologies and their related techniques. To the best of our knowledge, our proposed extension of the GL model is the first approach responding to the need of capturing the aforementioned time-related insights that a disruptive technology might bring on cyber-security investment.

The remainder of this article is structured as follows. In Section 2, we contextualize this research by emphasizing the evolution of cyber-threats monitoring approaches and their potential disruptive technologies. In Section 3, we present an extension of the GL model and we provide related propositions in order to create room for capturing the consequences of disruptive technologies on cyber-security investment. In Section 4, we suggest that our framework can be applied by critical-infrastructure providers (CIP) in order to help them optimize their investment in IS defense technologies. In the last section, we discuss limitations and future work.

2 Cyber-Threat Monitoring Approaches

Cyber-threat monitoring approaches can be divided in two broad classes: (1) *targeted event-based detection* and (2) *behavior-anomaly detection* [2, 31, 41]. Both approaches aim to detect suspicious events (i.e., related to security concerns such as data breaches) through IDS [41]. However, technologies related to (2) are rapidly evolving and could disrupt the cyber-security market [31] and the investment in these technologies.

2.1 The *Targeted Event-Based Detection* Approach

For the past three decades, scholars, practitioners, and organizations have been developing numerous conventional technical means to increase cyber-security by using signature-detection measures and encryption techniques [4, 6]. However, the success of such conventional approaches has been limited [4, 6, 12, 16].

The *targeted event-based detection* approach essentially relies on signature-detection measures in which an identifier is attributed to a known threat[4] (i.e., a threat that had been witnessed in the past), so that this threat can be subsequently identified [2, 4, 31, 41]. Examples of *targeted event-based detection* include network-IDS, access-control mechanisms, firewalls and pattern-based antivirus engines [2, 4, 31, 41]. For instance, a signature-detection technology such as an anti-virus scanner might detect a unique pre-established pattern of code that is contained in a file. If that specific pattern (i.e., signature) is discovered, the file will be flagged in order to warn the end-user that their file is infected. [4, 31]. Yet, such an approach is becoming more and more ineffective, as the swift evolution of cyber-threats is becoming more sophisticated [2, 4, 15, 31, 47]. Over the last decade, cyber-crimes have rapidly increased because hackers have developed new procedures to circumvent IS security to gain unauthorized and illegal access to the system [31]. For

[3] In this article, the term *big data* refers to data whose complexity impedes it from being processed (mined, stored, queried and analyzed) through conventional data-processing technologies [28, 31]. The complexity of big data is defined by three attributes: (1) the volume (terabytes, petabytes, or even exabytes (10^{18} bytes); (2) the velocity (referring to the fast-paced data generation); and (3) the variety (referring to the combination of structured and unstructured data) [28, 31]. The field of BDA is related to the extraction of value from big data – i.e., insights that are non-trivial, previously unknown, implicit and potentially useful [31]. BDA extracts patterns of actions, occurrences, and behaviors from big data by fitting statistical models to these patterns through different data-mining techniques (e.g., predictive analytics, cluster analysis, association-rule mining, and prescriptive analytics) [14, 37].

[4] Common cyber-risks include malware (spyware, ransomware, viruses, worms, etc.), phishing, man-in-the-middle attacks (MitM), (distributed) denial-of-service attacks ((D)DoS), malicious SQL injections, cross-site scripting (XSS), credential reuse, and brute-force attacks.

instance, as malware spread from one system to the next, hackers employ *polymorphic code*[5] techniques in order to (automatically) rapidly modify the pattern [20], thus evading and circumventing existing detection mechanisms.[6] Consequently, such a *targeted event-based detection* would be ineffective because of the lag that exists between the development of signatures and the rapid expansion of cyber-threats [31]. Moreover, *zero-day*[7] vulnerabilities cannot be caught with such an approach.

Therefore, an important limiting factor of the *targeted event-based detection* approach is that it is intrinsically reactive in nature [2, 4, 31]. Attributing a signature to a cyber-threat is always preceded by a cyber-incident, which implies that signatures are unable to identify unknown and/or emerging threats. As a consequence, signature-detection measures can be rendered almost ineffective by hackers [15, 31, 47]. Such a scenario is even amplified in the era of extended digitization and big data [31, 41]. The reasons are that (1) the swift development of computer networks (e.g., the extensive use of cloud and mobile computing) in the past decades generated new channels that expose data to cyber-attack, thus increasing the pool of systems to be attacked hence amplifying numerous security issues related to intrusions on computer and network systems [31, 41]; (2), up to multiple exabytes of information are being transferred daily, usually impeding the process of the entire set of security information, e.g., network logs, access records, etc. [31]; (3) the velocity of data generation makes any type of data processing difficult through conventional computer hardware and software architectures [31]; (4) the complexity of data also impedes security information from being processed by conventional computers, e.g., data come from diverse sources, it is stored in different formats and on different IT. Hence, the damage done by cyber-threats could be identified only after an attack, giving hackers more efficient possibilities to access networks, to hide their presence and to inflict damage [16, 31].

2.2 The *Behavior-Anomaly Detection* Approach

In order to address the drawbacks of the *targeted event-based detection* approach, research & development has been focused on a *behavior-anomaly detection* approach [15, 16, 19, 31, 36, 41, 45, 47]. Such an approach aims to detect suspicious/unusual events through the extraction of patterns, by using behavior anomalies and/or deviations from behaviors (actions, occurrences) of entities and/or users of a network, rather than patterns of code as in the case of the *targeted event-based detection* [15, 16, 19, 31, 36, 41, 45, 47]. The *targeted event-based detection* approach is predominantly based on *security analytics*[8] and aims to provide dynamic detection of cyber-threats through techniques derived from BDA by fitting statistical models on these patterns through different techniques (e.g., predictive analytics, cluster analysis, association-rule mining, and prescriptive analytics) [14, 37] used for network forensics, traffic clustering and alert correlation [2]. Some examples have been developed by [19, 36, 45].

Complementing the *targeted event-based detection* approach by using signature-detection measures, such a *behavior-anomaly detection* approach is envisioned to foster cyber-threats

[5] A *polymorphic code* is a code that employs a polymorphic engine in order to mutate while keeping the original algorithm intact. In other terms, the code changes itself each time it runs, but its semantics – the function of the code – will not change [20].

[6] Additional techniques such as, sandbox resistance, fast fluxing, adversarial reverse engineering, social-engineering attacks, spoofing, and advanced persistent threats (APT) are continuously evolving and spreading [2, 31].

[7] A *zero-day* vulnerability is a computer-software vulnerability that is either unknown to or unaddressed by operators who should be interested in mitigating the vulnerability. *Zero-day* vulnerabilities enable hackers to exploit it in order to adversely affect computer programs, networks, and data [26].

[8] The field of *security analytics* aims to detect suspicious events by extracting patterns related to behavioral anomalies and/or deviations from behaviors (actions, occurrences) of entities and/or users of a network. In other words, *security analytics* methods aim to distinguish patterns generated by legitimate users from patterns generated by suspicious and/or malicious users [16, 31].

monitoring by increasing its productivity [16, 31]. Examples of *security analytics* applications are the development of *security information and event management* (SIEM). SIEM products and services combine security-information management (SIM) and security-event management (SEM) [11]. SIEM provide real-time analysis of information-security alerts generated by applications and network hardware. SIEM are sold as managed services, as software, or as appliances [11]. These products and services are also used to log security data and to generate reports for compliance purposes. SIEM products and services are widely used within *information-security operation centers* (ISOC) – also called *fusion centers* – of organizations. The open-threat exchange platform called *AlienVault OTX* is an example of SIEM products and services.[9]

Cyber-security technologies related to the *behavior-anomaly detection* approach – and more precisely related to *security analytics* – are susceptible to disrupting the cyber-security market [19, 31, 36, 45, 47]. However, the dynamic (i.e., time related) consequences of such disruptive technologies on cyber-security investment cannot be analyzed through the existing GL model and its extensions. They rely on restrictive assumptions that are not adapted for analyzing dynamic aspects of cyber-security investment [21]. Consequently, a supplementary extension of the GL model is necessary.

3 Extending the Gordon-Loeb Model

By focusing on costs and benefits associated with cyber-security, the GL model states that each organization's objective is to maximize its *expected net-benefits in cyber-security* function ($ENBIS$) [21]. This corresponds to minimizing the total expected cost, equivalent to the addition of the expected loss[10] (vL) due to cyber-security breaches and the expenses (z) in cyber-security processes, products and/or services implemented and/or undertaken in order to counter such breaches [21, 22]. Figure I.1 on page 49 illustrates the maximization of the expected benefits coming from cyber-security expenditures ($EBIS$).[11]

In Section 2, we emphasized that the advent of the *behavior-anomaly detection* approach – triggered by *security analytics* and its use of BDA – is bringing to the fore new cyber-security technologies that have the potential to disrupt the cyber-security market [19, 31, 36, 37, 45, 47] by hypothetically bringing superior returns on investment *vis-à-vis* conventional measures related to the *targeted event-based detection* approach [37]. As a consequence, the $EBIS$ function might shift to the left. Figure I.2 on page 49 illustrates the potential maximization of the $EBIS$ function in the context of BDA. Accordingly:

> ***Proposition 1:*** *If BDA is employed in order to provide cyber-threats monitoring, the $ENBIS$ function will shift to the left due to a greater productivity of BDA compared to conventional technologies.*

Consequently, the optimal level of cyber-security investment will decrease from z^* to z_d^* (c.f.: Figure I.2 on page 49). For the same level of protection, investment in cyber-security will decrease – *ceteris paribus*. Accordingly:

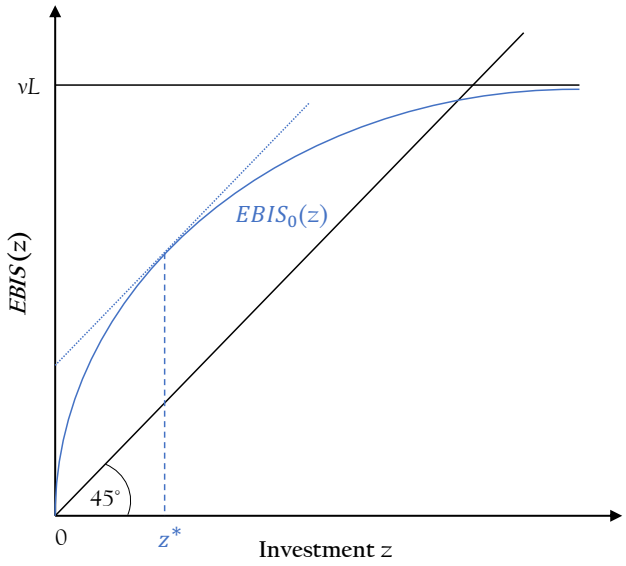
> ***Proposition 2:*** *If BDA is implemented in order to provide cyber-threats monitoring, the $ENBIS$ function will witness a discontinuity in its domain Z due to a greater productivity of BDA compared to conventional technologies.*

[9] `https://www.alienvault.com/`

[10] Wherein v is is the organization's inherent *vulnerability* – defined as the probability that a threat, once realized (i.e., an attack), would be successful – to cyber-security breaches, ($\mathbb{P}$); and L is the potential loss associated with the security breach, (\$). The model description and its assumptions were explained in detail by [21, 22].

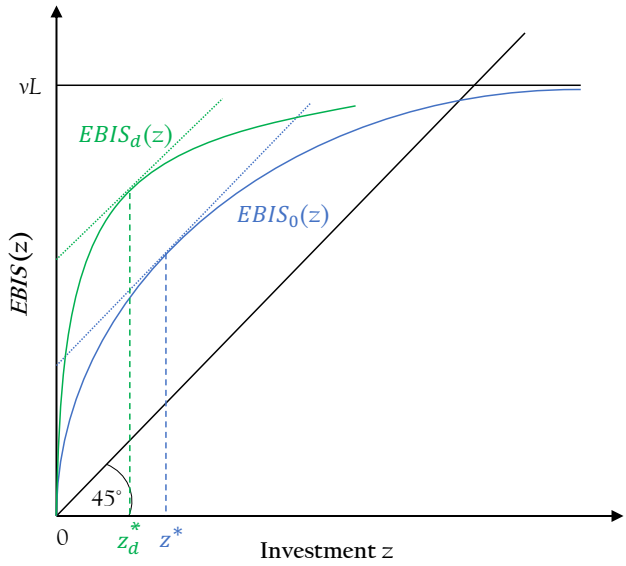
[11] In order to simplify the illustration, figures I.1, I.2 and I.3 on pages 49 and 50 depicts the $EBIS$ function instead of the $ENBIS$ function. The $ENBIS$ function is obtained by subtracting the investment (z) to the $EBIS$ function.

Figure I.1: **Level of Investment in Cyber-Security**



Notes to Figure I.1: The original function of the *expected benefits in cyber-security* ($EBIS_0(z)$) has a domain Z that yields a distribution between zero and the monetary value of the expected loss (vL) in the absence of any cyber-security investment. The monetary value (i.e., costs) of the investment (z), corresponds to the 45° line. The optimal level of cyber-security investment (z^*) is obtained when the difference between benefits and costs is maximized (tangent to $EBIS_0(z)$ – where the marginal benefits are equivalent to the marginal cost of one – yielding a slope of 45°, in blue). *N.B.*: the optimal level of cyber-security investment (z^*) is smaller than the expected loss (vL) in the absence of any investment.

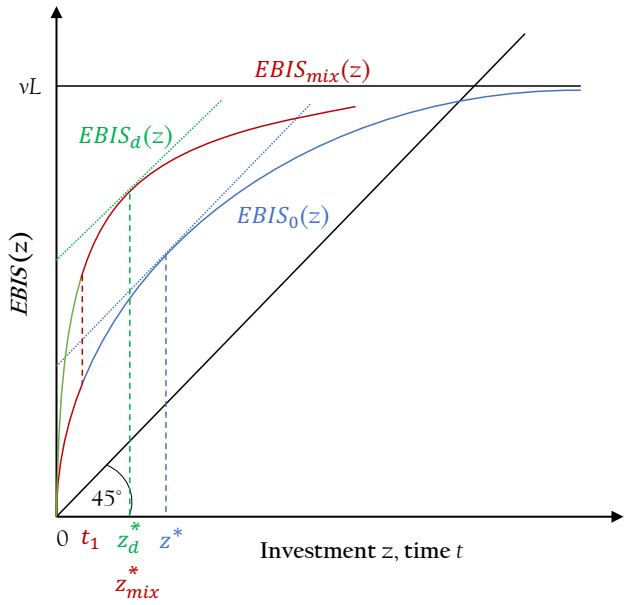
Figure I.2: **Left Shift of the Level of Investment in Cyber-Security**



Notes to Figure I.2: The new function of the *expected benefits in cyber-security* ($EBIS_d(z)$) has also a domain Z that yields a distribution between zero and the monetary value of the expected loss (vL) in the absence of any cyber-security investment. The monetary value (i.e., costs) of the investment (z), also corresponds to the 45° line. Similarly to Figure I.1, the optimal level of cyber-security investment (z_d^*) is obtained when the difference between benefits and costs is maximized (tangent to $EBIS_d(z)$, yielding a slope of 45°, in green). Yet, due to the left shift of the $EBIS$ function (from $EBIS_0(z)$ to $EBIS_d(z)$), the optimal level of cyber- security investment also shifts from z^* to z_d^*.

Figure I.3 on page 50 illustrates such a discontinuity in the $ENBIS$ function described in Proposition 2. Yet, as the implementation of a disruptive technology implicitly triggers a productivity differential over time, we propose to extend the GL model in two distinct but related ways.

Figure I.3: **Left Shift of the Level of Investment in Cyber-Security Over Time**



Notes to Figure I.3: In this graph, the horizontal axis represents both investment (z) and time (t). The red line represents the function of the *expected benefits in cyber-security* over time ($EBIS_{mix}(z)$). The red dashed line represents the discontinuity in the domain Z of the $EBIS_{mix}(z)$ function – due to the implementation of a disruptive technology at time t_1. Without the implementation of a disruptive technology, the function of the *expected benefits in cyber-security* remains $EBIS_0(z)$ (in blue). With the implementation of a disruptive technology from $t = 0$, the function of the *expected benefits in cyber-security* is $EBIS_d(z)$ (in green). The optimal level of cyber-security investment is $z^*_{mix} = z^*_d$.

3.1 A Temporal Setup

First, in order to capture the advent of a disruptive technology and its dynamic consequences on cyber-security investment, a temporal setup has to be implemented. As the GL model was developed for a single-period, it excludes the fundamental temporal dimension for analyzing the technological-shift dynamics induced by efficiency improvements. Hence, the extension of the original single-period model to a multi-period[12] setup might bring significant insight in understanding the dynamic aspects of cyber-security investment that were originally evaded.

Specifically, we adapt the GL model from [21], such as the maximization of the $ENBIS$ function is determined by an antidifference operator of this same function, which has the domain $Z \subseteq \mathbb{R}_{\geq 0}$ (representing the set of investment possibilities, z_i) at the end of the specified time horizon $T \subseteq \mathbb{N}$, wherein each period $i \in [1, n]$. This yields:

[12]Even though there is still an open debate in the field of mathematics about whether time should be considered as continuous or discrete [39], in our proposed extension of the GL model, we consider time as discrete. Such a choice is determined by the fact that any further empirical research that would test our extension will be essentially conditioned by measuring time as a discrete variable. Consequently, the following extension is based on an antidifference instead of an antiderivative.

$$\max_{z_i \in Z} \Delta^{-1} ENBIS(z_i) = \max_{z_i \in Z} \left\{ \sum_{i=1}^{n} [v_i - S_i^I(z_i, v_i)] L_i - z_i \right\} \tag{I.1}$$

wherein for each period $i \in [1, n]$:

- v_i is the organization's *vulnerability*[13] to cyber-security breaches, (probability $\mathbb{P}$);
- S_i^I is the organization's *security-breach probability function* (SBPF), defined as the probability that a cyber-security-breach occurs, (probability $\mathbb{P}$);
- z_i is the organization's investment in cyber-security, (monetary value \$);
- L_i is the potential loss associated with the security breach, (monetary value \$).

3.2 A Discontinuity in the Security-Breach Probability Function

Second, the presumed technological shift induced by the superior productivity of a disruptive technology challenges the assumption of a continuously twice-differentiable security-breach probability function. The original model defines continuously decreasing but positive returns to scale of cyber-security investment. Yet, this continuously twice-differentiable setup leaves no room for a discrete emergence of a technological shift brought by a disruptive and more efficient technology.[14] In such a theoretical framework, the elasticity of the protection of cyber-security processes, products and/or services evades radical technological progress. However, technological progress induced by the implementation of a disruptive technology – such as BDA – could considerably reduce cyber-security investment by bringing suggestively greater returns on investment.[15]

The investor realizes a *Pareto* improvement by either obtaining a higher level of protection for the same investment or by obtaining the same level of protection at a lower cost; because fewer resources, such as time and human labor, can be largely substituted by algorithms, and automation might be used. As a result, with the implementation of BDA, cyber-security investment might be significantly reduced by disruption: BDA would introduce a discontinuity in the security-breach probability function, hence modifying the original GL model assumption of continuity. Accordingly, adapting the security-breach probability function (S^I) from [21], we propose the following security-breach probability

[13] In the original GL model [21], the organization's inherent vulnerability is defined as the probability that a threat, once realized (i.e., an attack), would be successful.

[14] [21] explicitly acknowledge that they 'abstract from reality and assume that postulated functions are sufficiently smooth and well behaved', thus creating favorable conditions for applying basic differential calculus, hence simplifying the optimization problem of the security-investment phenomenon. Although a smooth approximation of the security-investment phenomenon done by [21] is a reasonable first approach, in order to deliver insight concerning the problem of determining an optimal level of cyber-security investment, such an approach lacks realism. As explicitly mentioned by [21]: [...] '*in reality, discrete investment in new security technologies are often necessary to get incremental result. Such a discrete investment results in discontinuities.*'

[15] In BDA, an extremely large, fast paced and complex amount of information can be processed in significantly shortened time frames and at almost zero marginal cost per additional unit of information – once the fixed development and implementation costs of systems and algorithms for investigating threat patterns are invested [43]. Furthermore, the real-time analytics provided by big-data algorithms are likely to neutralize any attacker's information advantage, such that the probability of a cyber-breach should be reduced. For example, an attacker can exploit *zero-day* vulnerabilities by knowing where to attack, whereas the defender does not know, hence has to protect all potential entry spots. As real-time analytics reveals both the time and the position of the attack as it happens, the defender can react precisely on the attacked spot, thus save any unnecessary investment in the protection of spots that are not attacked.

function ($S_i^{I'}$) in order to capture the advent of a disruptive technology by introducing discountinuity through the parameter d_i:

$$S_i^{I'}(z_i, v_i) = \frac{v_i}{(\alpha_i z_i + 1)^{\beta_i + d_i}} \tag{I.2}$$

wherein for each period $i \in [1, n]$:

- $\alpha_i \in \mathbb{R}_{>0}$ and $\beta_i \in \mathbb{R}_{\geq 1}$ represent productivity parameters of a given cyber-security technology at period i (i.e., for a given (z_i, v_i), the security-breach probability function $S_i^{I'}$ is decreasing in both α_i and β_i);[16]
- d_i is a discontinuity parameter at period i, and it is represented by a dummy variable. This dummy takes the value 0 when no disruptive technology is used, and 1 otherwise.

From equation (I.2), equation (I.1) can be rewritten as:

$$\max_{z_i \in Z} \Delta^{-1} ENBIS(z_i) = \max_{z_i \in Z} \left\{ \sum_{i=1}^{n} [v_i - \frac{v_i}{(\alpha_i z_i + 1)^{\beta_i + d_i}}] L_i - z_i \right\} \tag{I.3}$$

Although, in order to extend the original GL model, the multi-period setup and the suggested security-breach probability function ($S_i^{I'}$) constitute the main theoretical contributions, the application of this contribution to a concrete context is necessary in order to exemplify and demonstrate their relevancy, and to empirically test them in a further research.

4 Application for CIPs

A cyber-security breach inflicted on a critical infrastructure (CI) generates massive negative externalities, especially due to the increasing interdependency and to technical interconnectedness of different CIs [1, 22]. As a result, cyber-security issues are the main challenge for CIP [5]. Therefore, the issue of cyber-security investment becomes highly relevant in the context of CIs, and especially so from a social-welfare perspective [22].

In this respect, cyber-security investment is a national security priority for the great majority of governments (e.g., [34]). For example, on February 12, 2013, the administration of US President Barack Obama implemented Executive Order 13636 [33] named *Improving Critical Infrastructure Cybersecurity*. This executive order stated that '*The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats. It is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber-environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties*' [33]. Following this trend, on May 11, 2017, the administration of US President Donald Trump implemented Executive Order 13800 [46], named *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. This executive order stated that '*Effective*

[16] [21] did not specify α and β. These productivity parameters could be, for instance, the relative productivity of a given technology when compared to another (α) and the joint productivity of the same technology when in interaction with a set of already employed technologies in an organization (β).

immediately, each agency head shall use 'The Framework for Improving Critical Infrastructure Cybersecurity' developed by the National Institute of Standards and Technology, or any successor document, to manage the agency's cyber-security risk. Each agency head shall provide a risk management report to the Secretary of Homeland Security and the Director of the Office of Management and Budget within 90 days of the date of this order' [46].

We believe that our suggested extension of the GL model should be generalizable across any kind of cyber-security concerns, yet we illustrate our approach in the context of CIP as security-cost reduction related to risk events are of prior importance because potential losses reach unaffordable dimensions [22]. Despite the fact that BDA is considered a promising method for CIP, its concrete implications have not been discussed much.

More specifically, our extension of the GL model provides a theoretical framework for analyzing the impact of the implementation of any given novel technology on cyber-security investment *over time*. In this respect, by subtracting antidifference operators of $ENBIS$, $\Delta^{-1}ENBIS(z_i)$, at two different specified time-span of same duration, $(A-B)$, a potential decrease in cyber-security investment, Δ_Z, can be analyzed – *ceteris paribus*:

$$\Delta_Z = \left\{\Delta^{-1}ENBIS(z_A)\right\} - \left\{\Delta^{-1}ENBIS(z_B)\right\} \tag{I.4}$$

where $B \subseteq \mathbb{N}$ is a time-span, wherein each period $i_B \in [n, t]$, and in which a given novel technology is implemented; whereas $A \subseteq \mathbb{N}$ is a time-span, wherein each period $i_A \in [1, m]$, and in which no novel technology is implemented. Note that $\sum_{i=n}^{t} i$ and $\sum_{i=1}^{m} i$ must be equal in order to proceed to the comparison.

From equations (I.1) and (I.4), equation (I.5) can be written as:

$$\Delta_Z = \left\{\sum_{i=1}^{m}[v_i - S_i^I(z_i, v_i)]L_i - z_i\right\} - \left\{\sum_{i=n}^{t}[v_i - S_i^I(z_i, v_i)]L_i - z_i\right\} \tag{I.5}$$

From the original equation of [21], equation (I.5) can be rewritten as:

$$\Delta_Z = \left\{\sum_{i=1}^{m}[v_i - \frac{v_i}{(\alpha_i z_i + 1)^{\beta_i}}]L_i - z_i\right\} - \left\{\sum_{i=n}^{t}[v_i - \frac{v_i}{(\alpha_i z_i + 1)^{\beta_i}}]L_i - z_i\right\} \tag{I.6}$$

By controlling for every parameters to remain equal between time-span A and B – except for the domains Z, wherein $Z_A \neq Z_B$ –, an organization can determine if any given novel technology generates a greater $ENBIS$. If it is the case, the organization might consider the novel technology implemented in B as disruptive; inversely, if the $ENBIS$ does not substantially changes, the implemented novel technology cannot be considered as disruptive. Note that even though equation (I.6) can be used for analyzing the differential in cyber-security investment between two time-spans, equation (I.3) remains necessary in order to determine the optimal level of cyber-security investment (z_i) through the maximization of the $ENBIS(z_i)$ function.

The application of our GL model extension to the context of CIP should provide us with a relevant and seminal basis on which our arguments can be formally modeled and simulated. In the case of human-processed information and defense tactics, these issues would probably make the optimal level of protection difficult to attain or even impossible to

finance, as the expected loss would be extreme in the case of cascading failures of CIs; hence the resulting cyber-security investment would also have to reach extreme levels. However, with the effects that the BDA technology (or any similar disruptive technology) could have on investment in cyber-security, the investment needs by CIP could remain at the same level or even decrease, as these novel threats are neutralized by the superior technology that BDA offers.

5 Discussion

In this last section, we present our concluding comments, the policy recommendations resulting from concluding comments, we discuss the limitations of this study and suggest paths for further research.

5.1 Concluding Comments

In this article, we propose an extension of the GL model by adapting its initial theoretical framework in order to capture time-related insights related to the consequences that a disruptive technology can have on cyber-security investment. We propose two important contributions. First, we argue that a single-period model is not adapted to capture dynamic aspects of cyber-security investment such as the advent of a disruptive technology. The extension to a multi-period model is indeed necessary. Second, in the context of the introduction of a discrete disruptive cyber-security technology, the security-breach probability function of the original GL model could not be considered as continuously differentiable. These two arguments enrich the initial model by giving supplementary insight on cyber-security investment. Through our extended $ENBIS$ function, our proposed revision of the GL model captures both the financial consequences on the optimal level of investment and the security productivity of the advent of any given novel (and potentially disruptive) technology. Although we believe that this reasoning is generalizable across a wide range of cyber-security concerns, we illustrate our approach in the context of CIP, for which cyber-security breaches inflict unaffordable social costs that urgently need to be reduced.

5.2 Considerations for Policy Recommendations

First and foremost, our extension of the GL model is intended to be used for determining the optimal level of cyber-security investment through the maximization of the $ENBIS(z_i)$ function. The optimal level of cyber-security investment is obtained when the difference between benefits and costs are maximized – i.e., where the marginal benefits of cyber-security investment are equivalent to the marginal cost of potential losses due to cyber-security threats.

Also, our extension of the GL model provides a theoretical framework in order to analyze the expected net-benefits of the implementation of any given novel technology over time. By subtracting antidifference operators of $ENBIS$ at two different specified time-spans, and by controlling for every parameters to remain equal between two time-spans (except for investment), a potential decrease in cyber-security investment can be analyzed. Throughout our model, an organization can determine if any given novel technology generates a greater $ENBIS$. If it is the case, the organization might consider the novel technology implemented as disruptive; inversely, if the $ENBIS$ does not substantially changes, the implemented novel technology cannot be considered as disruptive.

We presented a dynamic analysis for determining the optimal investment level for IS defense, in the context of potentially disruptive technologies. By conceptualizing a security-breach probability function that includes productivity parameters (α and β) of a given

cyber-security technology, practitioners can calculate the optimal level of investment in IS defense processes, products and/or services, and also select them according to the highest productivity parameters. Although this work remains theoretical, it gives a systematic method for optimizing IS defense investment in the context of potentially disruptive technologies.

5.3 Limitations and Paths for Further Research

Finally, our research design – based on theoretical modeling and utility maximization – has some limitations that future research could help relax.

First, the productivity parameters (α_i and β_i) of a given cyber-security technology are theoretically conceptualized, but not empirically measured. Such an effort could add a substantive benefits in terms of validation/refutation of our propositions. However, researchers might find it difficult to gain access to data as they are substantially difficult to measure and/or to find [32]. A possible solution in order to measure these productivity parameters could be derived from equation I.6, by computing the ratio between Z_B and Z_A. By doing so, a relative measure of productivity between a technology employed in $\Delta^{-1}ENBIS(z_A)$ and a technology employed in $\Delta^{-1}ENBIS(z_B)$ could be extracted.

Second, the term *disruptive technologies* [17] has been qualitatively defined, but not quantitatively delimited. Such a research effort is necessary in order to delimit the dummy variable d_i (that takes the value 0 when no disruptive technology is used, and 1 otherwise). Again, such a quantitative delimitation could be drawn by determining a threshold value in the aforementioned ratio between Z_B and Z_A.

Third, and consequently, this article formally modeled an extension to the GL model, but it did not simulate or empirically test our suggested extension. We decided to leave this operationalization to future research as we wanted to focus on the generalizability of the model. Any simulation or empirical operationalization requires a specification of the above-mentioned productivity parameters α_i and β_i of each technology considered for investment, as well as the specification of the dummy variable d_i for classifying which technologies are considered disruptive (and when). Such choices make the model more specific to particular assumptions about technological and productivity contexts. Hence, we suggest that our model should be operationalized by a series of different simulations and empirical tests, rather than by one illustrative simulation run. Given the fact that specifications of such simulations and/or empirical tests would require multiple cases and thus multiple contexts (and thus multiple articles). Nevertheless, we recommend that future research simulates, tests and develops further the model we proposed here.

Fourth, the security-breach probability function $S_i^{I'}$ that we employed in this work can be replaced by many other families of more complex functions. In this research, we selected the first family of security-breach probability function proposed by [21], namely S^I. However, in reality, adding more families of functions could enrich the analysis (e.g., [29]).

Once the aforementioned points are defined by empirical analyzes and field surveys, further research could propose to simulate a multi-player and multi-period game (e.g., [24]) that models the cyber-security for CIP in the era of disruptive technologies. Such research – by collecting simulated data and quantitatively analyzing them – would contribute to complement the theoretical approach presented in this article, hence test the intuition of our theoretical development.

References

1. Alcaraz, C. & Zeadally, S. Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection* **8,** 53–66 (2015).
2. Amini, L. *et al. Adaptive Cyber-Security Analytics* tech. rep. US Patent 9,032,521 (2015).
3. Anderson, R. *Why Information Security is Hard – an Economic Perspective* in *Seventeenth Annual Computer Security Applications Conference* Annual Computer Security Applications Conference (ACSAC) (IEEE, New Orleans, USA, 2001), 358–365. ISBN: 0-7695-1405-7.
4. Anderson, R. J. *Security Engineering: A Guide to Building Dependable Distributed Systems* (John Wiley & Sons, 2010).
5. Anderson, R. & Fuloria, S. in *Economics of Information Security and Privacy* (eds Moore, T., Pym, D. & Ioannidis, C.) 55–66 (Springer, Boston, USA, 2010). ISBN: 978-1-4419-6967-5.
6. Anderson, R. & Moore, T. The Economics of Information Security. *Science* **314,** 610–613 (2006).
7. Anderson, R. *et al.* in *The Economics of Information Security and Privacy* (ed Böhme, R.) 265–300 (Springer, Berlin, Heidelberg, Germany, 2013). ISBN: 978-3-642-39498-0.
8. Azorin, P. Cybersecurity & data privacy trends in 2020. *ITProPortal* (Oct. 2019).
9. Barney, J. Firm Resources and Sustained Competitive Advantage. *Journal of Management* **17,** 99–120 (1991).
10. Baryshnikov, Y. *IT Security Investment and Gordon-Loeb's 1/e rule* in *2012 Workshop on the Ecopnomics of Information Security* Workshop on the Ecopnomics of Information Security (2012).
11. Bhatt, S., Manadhata, P. K. & Zomlot, L. The Operational Role of Security Information and Event Management Systems. *IEEE security & Privacy* **12,** 35–41 (2014).
12. Böhme, R. *The Economics of Information Security and Privacy* ISBN: 978-3-642-39498-0 (Springer, Berlin, Heidelberg, 2013).
13. Campbell, K., Gordon, L. A., Loeb, M. P. & Zhou, L. The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *Journal of Computer Security* **11,** 431–448 (2003).
14. Cardenas, A. A., Manadhata, P. K. & Rajan, S. P. Big Data Analytics for Security. *IEEE Security & Privacy* **11,** 74–76 (2013).
15. Casas, P., Soro, F., Vanerio, J., Settanni, G. & D'Alconzo, A. *Network Security and Anomaly Detection With Big-DAMA, a Big Data Analytics Framework* in *IEEE 6th International Conference on Cloud Networking (CloudNet'17)* IEEE 6th International Conference on Cloud Networking (CloudNet'17) (2017), 1–7.
16. Chen, H., Chiang, R. H. L. & Storey, V. C. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly* **36,** 1165–1188 (2012).
17. Christensen, C. M., Raynor, M. & McDonald, R. What Is Disruptive Innovation? *Harvard Business Review* **93,** 44–53 (2015).
18. Christensen, C. & Raynor, M. *The Innovator's Solution: Creating and Sustaining Successful Growth* (Harvard Business Review Press, 2013).

19. Cui, B. & He, S. *Anomaly Detection Model Based on Hadoop Platform and Weka Interface* in *10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'16)* 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'16) (2016), 84–89.

20. Forest, E., Schmidt, F. & McIntosh, E. Introduction to the Polymorphic Tracking Code. *KEK report* **3,** 2002 (2002).

21. Gordon, L. A. & Loeb, M. P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)* **5,** 438–457 (2002).

22. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, L. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* **6,** 24–30 (2015).

23. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Richardson, R. 2005 CSI/FBI computer crime and security survey. *Computer Security Journal* **21,** 1 (2005).

24. Grossklags, J., Christin, N. & Chuang, J. *Secure or Insure?: A Game-Theoretic Analysis of Information Security Games* in *Proceeding of the 17th International Conference on World Wide Web* 17th international conference on World Wide Web (ACM Press, Beijing, China, 2008), 209–218. ISBN: 978-1-60558-085-2.

25. Herath, H. S. & Herath, T. C. Investments in Information Security: A Real Options Perspective With Bayesian Postaudit. *Journal of Management Information Systems* **25,** 337–375 (2008).

26. Holm, H. *Signature-Based Intrusion Detection For Zero-Day Attacks: (Not) a Closed Chapter?* in *47th Hawaii International Conference on System Sciences* 2014 47th Hawaii International Conference on System Sciences (2014), 4895–4904.

27. Jerman-Blažič, B. *et al.* Quantitative Model for Economic Analyses of Information Security Investment in an Enterprise Information System. *Organizacija* **45,** 276–288 (2012).

28. Laney, D. 3D Data Management: Controlling Data Volume, Velocity and Variety. *META Group Research Note* **6,** 1 (2001).

29. Lelarge, M. Coordination in Network Security Games: a Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications* **30,** 2210–2219. ISSN: 0733-8716 (2012).

30. Li, J. & Su, X. *Making Cost Effective Security Decision With Real Option Thinking* in *International Conference on Software Engineering Advances (ICSEA 2007)* (2007), 14–14.

31. Mahmood, T. & Afzal, U. *Security Analytics: Big Data Analytics for Cybersecurity: a Review of Trends, Techniques and Tools* in *2013 2nd National Conference on Information Assurance (NCIA)* 2013 2nd National Conference on Information Assurance (NCIA) (IEEE, Rawalpindi, Pakistan, 2013), 129–134. ISBN: 978-1-4799-1288-9.

32. Moore, T., Kenneally, E., Collett, M. & Thapa, P. *Valuing Cybersecurity Research Datasets* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'19)* Workshop on the Economics of Information Security (WEIS'19) (University of Cambridge, UK, 2019), 1–27.

33. Obama, B. *Executive Order (13636) – Improving critical infrastructure cybersecurity* (The White House, Washington, USA, 2013).

34. OECD. *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy* (OECD Publishing, 2012).

35. Penrose, E. *The Theory of the Growth of the Firm* 4th ed. ISBN: 978-0-19-957384-4 (Oxford University Press, Oxford, UK, 2009).

36. Sait, S. Y., Bhandari, A., Khare, S., James, C. & Murthy, H. A. Multi-Level Anomaly Detection: Relevance of Big Data Analytics in Networks. *Sadhana* **40,** 1737–1767 (2015).

37. Sathi, A. *Big Data Analytics: Disruptive Technologies for Changing the Game* ISBN: 978-1-58347-380-1 (Mc Press, Boise, USA, 2012).

38. Schatz, D. & Bashroush, R. Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers* **19,** 1205–1228 (2017).

39. Serfozo, R. F. An Equivalence Between Continuous and Discrete Time Markov Decision Processes. *Operations Research* **27,** 616–620 (1979).

40. Shirtz, D. & Elovici, Y. Optimizing Investment Decisions in Selecting Information Security Remedies. *Information Management & Computer Security* **19,** 95–112 (2011).

41. Singh, J. & Nene, M. J. A Survey on Machine Learning Techniques for Intrusion Detection Systems. *International Journal of Advanced Research in Computer and Communication Engineering* **2,** 4349–4355 (2013).

42. Smeraldi, F. & Malacaria, P. *How to spend it: optimal investment for cyber security* in *Proceedings of the 1st International Workshop on Agents and CyberSecurity* (2014), 8.

43. Sowa, J. F. *Conceptual Structures: Information Processing in Mind and Machine* 1st ed. 481 pp. ISBN: 978-0-201-14472-7 (U.S. Department of Energy Office of Scientific and Technical Information, Boston, USA, 1983).

44. Teece, D. J. A Capability Theory of the Firm: an Economics and (Strategic) Management Perspective. *New Zealand Economic Papers* **53,** 1–43 (2019).

45. Terzi, D. S., Terzi, R. & Sagiroglu, S. *Big Data Analytics for Network Anomaly Detection from Netflow Data* in *International Conference on Computer Science and Engineering (UBMK'17)* International Conference on Computer Science and Engineering (UBMK'17) (2017), 592–597.

46. Trump, D. *Presidential Executive Order (13800) – Strengthening the cybersecurity of federal networks and critical infrastructure* (The White House, Washington, USA, 2017).

47. Wang, Y., Wang, Y., Liu, J. & Huang, Z. *A Network Gene-Based Framework for Detecting Advanced Persistent Threats* in *Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC'14)* Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC'14) (2014), 97–102.

48. Weinberger, S. Computer security: Is this the start of cyberwarfare? *Nature News* **474,** 142–145 (2011).

49. Willemson, J. *Extending the Gordon and Loeb Model for Information Security Investment* in *2010 International Conference on Availability, Reliability and Security* 2010 International Conference on Availability, Reliability, and Security (ARES) (IEEE, Krakow, Poland, 2010), 258–261. ISBN: 978-1-4244-5879-0.

50. Zhou, L., Loeb, M. P., Gordon, L. A. & Lucyshyn, W. Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. *Journal of Information Security* **9,** 720–726 (2018).

Part II

Human-Resource Recruitment

'It's not a faith in technology. It's faith in people.'

— Steve Jobs

The Persistent Deficit of Conscripted Officers in the Swiss Armed Forces

An Opportunity-Cost Explanation

Percia David Dimitri[1,2]; Keupp Marcus[2]; Marino Ricardo[3]; Hofstetter Patrick[4]

[1] University of Lausanne, Faculty of HEC, Department of Information Systems
[2] ETH Zurich, Military Academy, Department of Defense Economics
[3] University of St. Gallen, School of Management, Institute of Technology Management
[4] University of Zurich, Faculty of Economics and Informatics, Chair in HR Management

Journal article published in *Defense and Peace Economics*, vol. 30 (1)

- Submitted on September 30, 2016;
- Revised (minor revisions) and resubmitted on December 11, 2016;
- Accepted on July 8, 2016;
- Published online on July 31, 2017.

N.B.: For the purpose of harmonizing some technical notions throughout this thesis, adaptations were implemented.

Abstract

Despite good pay and a generally supportive attitude from the population, the Swiss Armed Forces – a critical infrastructure of the Swiss government – suffer from a structural deficit of conscripted officers. Yet, these officers are essential for monitoring and managing the information-systems defense of the Swiss Armed Forces. Whereas, prior studies have focused on sociological and psychological studies of intrinsic and extrinsic motivation, volition, and social context to explain the under-staffing in the armed forces, we offer an alternative approach based on opportunity-cost. In this perspective, we model the four service options related to the conscription duty in Switzerland, taking the IT-industry employment as the reference point. We then monetize the not-compensated opportunity-costs of fringe benefits, of leisure, and of IT-industry income. Our results suggest that, in terms of opportunity-cost, serving as a conscripted officer is the least attractive option. This we believe explains the persistent staff deficit. We discuss the implications of these findings for the literature and recruitment policy.

Keywords— security economics; opportunity-cost; military recruitment; Swiss Armed Forces; information-systems defense; critical infrastructure protection.

Contents of Part II

1 Introduction

Critical infrastructures (CI) are commonly defined as organizations that produce and/or deliver goods and/or services that are vital to the society [1]. This implies that any extended disruption and/or failure of any CI would strongly affect the functioning of the government, national security, economic system, public health and safety, or any combination of the above [1, 17, 40, 64, 66]. In the literature, there is a consensus that the functioning of modern societies depends – to a large extent – on the operational continuity of CIs (for extensive literature reviews, see [59, 69]). In this regard, the armed forces constitute a CI as they provide national security and public safety for the society [55].

Among armed forces, managing and monitoring the development, implementation and exploitation of an information-systems (IS) defense requires skilled professionals, who generally endorse an officer[1] function. However, in the case of the Swiss Armed Forces (SAF) – based on a *conscription*[2] architecture –, conscripted-officer positions suffer from a structural deficit. As a consequence, the *Armed Forces Command Support Organisation* (AFCSO) – which is responsible for information and communication technologies (ICT) services and electronic-operations (i.e., anti-cyber attack operations, electronic warfare and cryptology) of the SAF – also suffers from the aforementioned lack of conscripted officers. The AFCSO is responsible to ensure that the SAF can accomplish their missions, guaranteeing the *command and control* under all circumstances: during standard situations, during crises, and during disasters and conflicts. For this purpose, the AFCSO operates an independent communications network, which provides a secure medium for all types of data that are stored in safeguarded computing centers, and are structurally protected against external influences. The command support brigade (CS Bde 41/SCS) composes the AFCSO's military unit, and is composed of 14 battalions (12,000 conscripts). As for other units, the AFCSO needs to fulfill vacant conscripted-officer positions in order to execute its missions.

Almost the entire SAF are composed of citizens who are called upon – by conscription – to serve; as of 2017, the professional personnel constitute less than 2% of the total forces.[3] Consequently, the overwhelming majority of officer positions are filled by citizens who choose to serve as conscripted officers (i.e., non-professional).[4] To receive basic military training, upon entry in the SAF, conscripts first attend boot camp. Then, for the remainder of the time that they are required to serve, they return for annual training; this time – measured by the number of service days – is calculated according to rank, function, and specialty.

Detailed discussions on the philosophy and organization of the Swiss conscription system are available in [38, 49, 71]. Rather than adding to these general discussions, we point to a significant recruitment problem the SAF have experienced since 2010 in their attempt

[1] An officer is a member of an armed forces who holds a position of authority. In the Swiss Armed Forces, officers' ranks are: second lieutenant (OF-1b), first lieutenant (OF-1a), captain (OF-2), major (OF-3), lieutenant colonel (OF-4), colonel (OF-5), brigadier general (OF-6), major general (OF-7), lieutenant general (OF-8), and general (OF-9).

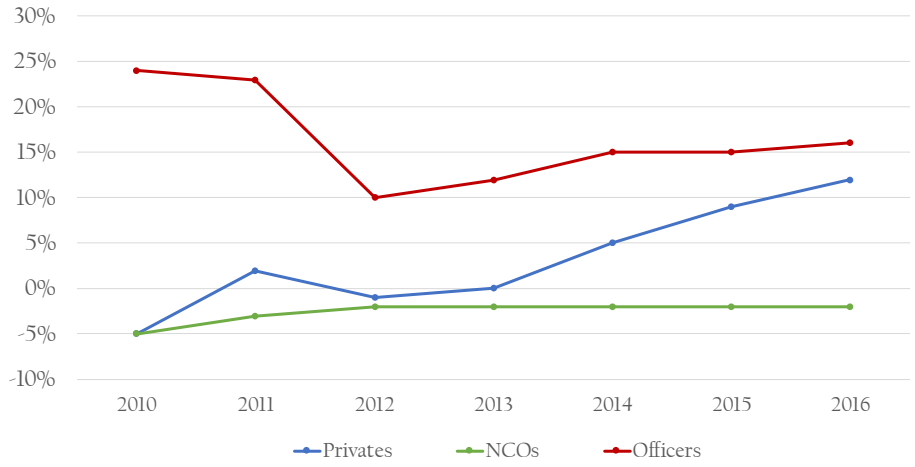
[2] *Conscription* – also called *draft* – is the compulsory enlistment of citizens in a national service (in the context of this research: the military service).

[3] Professional personnel are exclusively hired for basic military training of conscripts (during boot camps), for some highly specialized functions (e.g., jet pilots), or for high staff leadership positions (from the rank of one-star general and upwards).

[4] Conscripts form a personnel pool called *active reserve*. However, the SAF also have a *passive reserve* composed of former conscripts who do not participate in annual training anymore, but who can be called by the SAF if necessary. Hence, the SAF is composed by three categories of personnel pools (the active reserve, the passive reserve, and the professionals). As the deficit of officers is essentially witnessed in the active reserve, only this pool is analyzed in this article.

to recruit personnel for conscripted-officers positions. Under the current system, potential candidates for such positions are identified during boot camp and asked to serve as officers for the remainder of their service.[5] The SAF find it increasingly difficult to fill all officer positions necessary for executing their missions; a significant and persistent conscripted-officers deficit existed since at least 2010. Each year, about 15% of all conscripted-officer positions in the ranks of colonel, lieutenant–colonel, major, and captain cannot be filled. The greatest deficits are witnessed for the ranks of major and captain. The SAF also lack junior conscripted officers (i.e., the ranks of first lieutenant, and second lieutenant). As staff-conscripted officers are recruited exclusively from among junior conscripted officers, recruitment deficits in this group exacerbate the situation. Figure II.1 illustrates the deficit (corresponding numbers are available on Table II.1 on page 82).

Figure II.1: **Structural Deficit of Conscripts** (Required Positions Not Filled)



Notes to Figure II.1: Nominal reduction of conscripted-officer deficit from 2011 onward is due to an armed-forces reform that reduced the number of officer positions (whether filled or not) whereas officer headcount remained almost stable. As a result, the position fill rate nominally improved.

Consequently, existing conscripted officers have to work extra hours, to compensate for the deficit. This is a highly problematic development, as understaffed armed forces lack the leadership capability required to execute their missions [8] – e.g., managing and monitoring the development, implementation and exploitation of an information-systems (IS) defense for ensuring the command and control of the SAF under all conditions. This recruitment problem challenges the recruitment efficiency of the conscription model on which the SAF rely [71].

Psychology and sociology explanations fall short at explaining this structural deficit. Motivational aspects due to low morale or widespread political opposition against conscription in Switzerland are not corroborated by the literature [73]. Since the existence of the recruitment deficit, annually conducted nation-wide polls consistently suggest that Swiss citizens support conscription; they also confirm that the SAF are perceived as useful and necessary [74]. Moreover, in a 2013 referendum, 73.2% of all Swiss citizens voted in favor of the conscription model [23]. The deficit is unlikely to be explained by low pay or irrelevance of military training for subsequent civilian employment. During service executed by conscripts, the Swiss Federation compensates 80% of the conscripts' income earned and pays for fringe benefits. Even if no salary was earned before military service, a minimum compensation is paid. Additionally, the civilian employer can compensate the remaining 20% on a voluntary basis. Conscripts officers on duty are entitled to free

[5] An extensive account of this identification process is provided in Appendix 2 on page XXXVIII.

nation-wide first class public transportation. In 2004 and 2009, the SAF have shortened service duration[6] and introduced additional monetary incentives and fringe benefits for conscripted officers. National trade associations as well as large corporations from all industry sectors publicly stress that a conscripted-officer training is useful for civilian career [2, 26]. It could be argued that the conscripted-officers deficit is related to Switzerland's civilian low unemployment rate.[7] Hence, the conscripted-officers deficit should be inversely proportional to the unemployment rate (such that, when few attractive jobs in the industry are available, the deficit would decrease, and vice versa). However, Swiss unemployment statistics suggest that these two factors are uncorrelated. From 2010 to 2016, unemployment ranged between 2.6% and 4.2% of the eligible workforce (State Secretariat of Economic Affairs 2010–16 [28]). During this time, it remains stable at approximately 3%. In contrast, Table II.1 on page 82 suggests that the conscripted-officers deficit has grown by 60% during the same time-frame. Therefore, the SAF are currently facing the problem that fewer and fewer individuals opt for a conscripted-officer career, despite the monetary incentives and fringe benefits that come with it, and despite a generally favorable reputation.

Extant theory offers little guidance to explain this paradox. Economic studies of military recruitment have modeled the willingness to prefer a military career over a civilian one, suggesting that the former is chosen when its utility exceeds that of the latter [3, 43]. The majority of the literature provides sociological and psychological studies of intrinsic and extrinsic motivation, volition, and social context, looking at how these properties influence an individual's decision to enlist for military service (e.g., [22, 24, 62, 75, 79].[8] Although the aforementioned researches successfully provided relevant insights on factors that attract candidates toward a military career, effects that keep potential candidates away, despite a positive propensity to join, have been studied very little. [8] note that a propensity to join a military organization does not necessarily imply actual involvement. Furthermore, these studies do not differentiate between the recruitment of conscripted officers *vis-à-vis* other ranks. Their results are not readily applicable to a conscription system, where military service does not come as a dichotomous choice between military and civilian life but rather constitutes a temporary yet recurring interruption of an individual's civilian career, the extent of which varies according to the service option chosen.

In this study, we therefore, suggest a novel, opportunity-cost-based explanation: Whenever an individual can choose between two or more mutually exclusive options, the opportunity-cost of an option is the benefit foregone as a consequence of not choosing the other option(s) [13]. Although the literature has repeatedly called for perspectives that model an individual's choice to opt for a military career when presented with service options [9, 27, 36, 37, 54, 68, 71], such perspectives are still notably missing. Although the analysis by [53] is helpful in a conceptual way, it does not analyze individual-level decision-making, while the study by [77] is, to the best of our knowledge, the only contribution where opportunity-cost considerations are at least discussed. The term 'opportunity-cost' is not consistently applied in these contributions, they unanimously highlight the relevance of relative cost-benefit calculations in the face of multiple decision options.

We posit that an individual, in a first step, likely charts the different service options by which the duty to serve (as implied by conscription) can be fulfilled, both within and outside

[6]This was the case for the former SAF development called *Armée XXI*. From January 2019, the new SAF development called *WEA* has, in the contrary, significantly augmented service duration in order to deliver a more complete military training for conscripted non-commissioned officers (NCOs) and conscripted officers. In this article, the new service duration of the WEA is not taken into account as this present study has been done in 2017. However, our framework can easily take into account the new service duration of the WEA in order to actualize the conclusions of this article.

[7]We thank an anonymous reviewer for bringing this point to our attention.

[8]For a detailed review of the literature, see Table i.3 (on page 20) of the introduction of this thesis.

the military organization. In a second step, the individual evaluates the opportunity-cost of each service option and then makes a choice. Using this approach, we respond to studies from Israel [9], the US [68], and Switzerland [71]; they all suggest that the decision for a particular military career is at least partially influenced by individual cost-benefit calculations. Although the relevance of opportunity-cost considerations in a military context has been noted for decades [5, 11, 27, 45, 46, 50, 58, 61, 76], an empirical cost-calculation beyond conceptual discussion is, to the best of our knowledge, still missing in the literature. From an empirical point of view, this article is meant as a first step toward closing this gap.

Our study is set at the individual level. Calculating the opportunity-costs of fringe benefits, as well as the opportunity-cost of leisure and of IT-industry income, we model an individual's choice to opt for a career as a conscripted officer, subject to the relevant service options they have in the Swiss context. These calculations are stratified by three typical archetypes of individuals from whom conscripted officers are recruited. Our findings reveal that the opportunity-cost of a conscripted-officer career *vis-à-vis* other possible service options is excessive, irrespective of the archetype considered. We propose that this significant opportunity-cost disadvantage likely explains the persistent deficit of conscripted officers in the SAF. Finally, we discuss the implications of these findings for the literature and for recruitment policy.

2 Service Options

In this section, we present the four mutually exclusive service options that are available for the individual who has to serve. Also, we discuss the underlying assumption upon which our analysis relies on – i.e., the individual capacity to rationally evaluate the aforementioned service options. Finally, as the service option as an officer is the focus of this research, a brief description of an officer selection criteria is presented in order to compare such a service option among the three remaining service options available for the individual who is subject to conscription.

2.1 Four Mutually Exclusive Options

All physically and mentally fit male Swiss citizens[9] aged between 18 and 34 years are required to serve for a specified number of service days in the SAF as either a *private*,[10] an *NCO*,[11] or an officer. Female citizens are exempt from conscription but can volunteer for all functions. For conscientious objectors, the duty to serve is fulfilled by serving in the civilian service. All service options are conscription based, i.e., in the specific case of the SAF, the individual serves each year for a specified time and then returns to civilian life. All military services imply training in boot camp (consecutive days served, on average 137 service days) followed by annual training that takes between 19 and 28 service days, depending on rank, function, and specialty. Once these days are served, citizens return to civilian life and employment.[12] The same structure applies to the civilian service, where conscientious objectors must partition their service days into at least two-time segments, of

[9] Although foreign nationals and permanent residents together account for 24% of Switzerland's population (as of January 2017), only citizens are eligible to serve in any service option.

[10] A *private* is a soldier of the lowest military rank (equivalent to NATO Rank Grades OR-1 to OR-3 depending on the force served in).

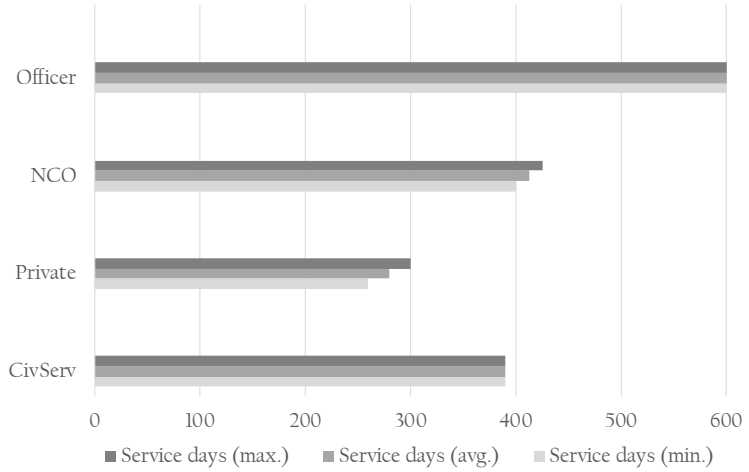
[11] The acronym *NCO* stands for *non-commissioned officer*, and refers to a group of ranks in a military-type hierarchy. It is preceded by the group of non-commissioned men (private). NCOs receive direct orders from officers.

[12] A small fraction of conscripts can serve all of their days consecutively, if certain criteria are met and positions are available. As the overwhelming majority of SAF personnel – and in particular the conscripted officers – serve in the traditional form by annual training, we do not factor the 'at a stretch' service option into the analysis.

which the first comprises 180 days served at a stretch. For any service option, the duty is fulfilled as soon as all days are served.

Whereas, for military service, the particular number of service days depends on rank, function and specialized training and hence varies between individuals, federal regulation defines the number of service days in the civilian service to be 1.5 times the number of days a conscientious objector would have served in the SAF (Federal Law on the Civilian Service – SR 824.0). Since we assume that he[13] would reduce involvement in a military organization to the bare minimum, we use the lower boundary of service days for a private as a basis to calculate the number of service days for the civilian service. To simplify the analysis, the average between the minimum and the maximum number of service days per service option is used as the basis for all subsequent opportunity-cost calculations. Figure II.2 illustrates these service days per service option while Table II.2 on page 82 presents in more detail the four service options: 'Civilian Service [CivServ]', 'Private', 'NCO' and 'Officer', and their respective service-day statistics.[14]

Figure II.2: **Number of Service Days per Service Option**



Before proceeding with the analysis, we must clarify the relevant population for whom this choice is relevant. First, one might argue that the choice between these four service options cannot be made freely, or that some service options entail higher transaction costs than others. However, both effects are unlikely in the case of the SAF. As regards the military functions, with very few isolated cases, neither a conscript nor a volunteer can be forced to become an NCO or an officer if they refuse. Quite the contrary, the individual makes that choice autonomously. For example, a conscript can choose to pursue a military function as an NCO but refuse to become an officer, or they can remain a private for the entirety of service, despite being asked to become an NCO or an officer. Admission to the civilian service is non-bureaucratic and administered by the approval of a simple request. Since 2009, the conscientious objector is no longer required to justify the reasons for his request. Consequently, transaction costs associated with the choice of any service option are unlikely to significantly influence the decision. In practice, the four service options are mutually exclusive. Although, some conscripts object and are assigned to the

[13]Female citizens can volunteer for any military function, but not for the civilian service. Hence, admission to the civilian service is effectively restricted to male citizens, such that it is not a relevant service option for female citizens. However, as only 0.7% of SAF personnel is female (Swiss Federal Department of Defense 2016 [29]) the analysis is unlikely to be significantly influenced by this imbalance.

[14]Under special circumstances, conscripted officers can be required to serve for more than 600 days. As such additional service days would increase opportunity-cost beyond the rates we calculate, our analysis is conservative.

civilian service during and after boot camp, there are very few known cases of privates that objected during their annual training, and no such cases have been reported among NCOs and officers at all [29]. Thus, once an individual has chosen a particular option, they are unlikely to reverse their decision.

2.2 *Rational Choice* Evaluation

We assume that individuals faced with this choice – i.e., who evaluates which service option to choose – are ideologically neutral, such that they equitably evaluate each service option without any reservations. This assumption seems reasonable, as the conscripts or volunteers who ideologically support military organizations are highly unlikely to choose the civilian service, even if opportunity-cost is very low compared to all military service options. Likewise, conscripts opposed to the military for ideological reasons are unlikely to choose any military-service option, even if the opportunity-cost of the most attractive military-service option was lower than that of the civilian service. The analysis is thus conceptually limited to individuals who base their decision on rational (rather than ideological) criteria. Such individuals trade-off the four service options against each other, estimating the opportunity-cost of each service option. Hence, the individual essentially makes an *ex ante* decision, if under *imperfect information*; however, rational decision-making does not necessarily imply the individual must meet the strict normative assumptions of *homo economicus* [25]. An individual can perform rational calculations on the basis of estimates, partial information, social cues, projections, and assumptions [57]. Furthermore, we believe the choice of a service option is likely more ordinal than cardinal in nature, such that the decision is based on relative magnitudes, rather than precise balance, of opportunity-costs.

2.3 Officer Selection Criteria

Serving as a conscripted officer is only open to two subgroups among all conscripts, specifically students (i.e., those who have not yet obtained an academic degree, and those who are in an apprenticeship), and skilled professionals (i.e., those who have been issued a certificate of qualified professional training or a university degree, and who earn a civilian salary). As detailed in Appendix 2 on page XXXVIII, in the process of officer recruitment, a conscript is subject to a number of criteria, hence not all conscripts who would like to choose this service option can. Some of these criteria depend on subjective evaluation: Article 31 of the service regulation 51.013 clearly states that academic studies, an apprenticeship or a skilled professional degree are objective, indispensable, and non-negotiable criteria for admission to an officer career. Hence, only candidates who meet these criteria can freely choose among all four service options.

3 Data and Methods

Categorizing opportunity-costs by using classification criteria is helpful to identity, as exhaustively as possible, an individual's trade-off considerations [56]. Therefore, we propose that total opportunity-cost per service option can be calculated as the global balance of three cost categories: (1) The opportunity-cost of reduced leisure[15], (2) the negative opportunity-cost (i.e., profits) of fringe benefits that are available in the civilian and military service, but not in IT-industry employment, and (3) the opportunity-cost of civilian income not earned during service days. We stratify the analysis of these cost factors across three

[15]Serving in a military organization implies that an individual can no longer freely trade-off work against leisure hours, according to personal preferences, or control their daily routine. As developed in the following subsection related to *Work Leisure Trade-Off*, an individual serving in the SAF will have less time for leisure.

socio-demographic archetypes from which conscripted officers in the SAF can be recruited. The archetype 'student/apprentice' is either a student enrolled in full-time tertiary education and has not yet obtained a degree, or is an apprentice learning a trade before being issued an official certificate of professional training. The archetype 'young professional' has just completed academic studies or an apprenticeship with a first degree or certificate. They have no prior job experience and is earning their first professional salary. Finally, the archetype 'skilled professional' has completed academic studies or professional training and has three years of work experience. As discussions of taxation and social security are beyond our scope, all figures are gross (i.e., before the deduction of any tax and/or social security contributions). Furthermore, our calculations focus on only individuals as such, we do not consider family matters (e.g., opportunity-costs of child care or fringe benefits for spouse support). All monetary values in all tables are in May 2017 current Swiss francs and rounded to the next integer.[16]

3.1 Fringe Benefits

All service options provide an individual with fringe benefits that are not available in civilian employment (daily allowances/soldier's pay and supplements, no expenses for public transport and food, and health insurance subsidies). Figure II.3 on page 73 illustrates these fringes benefits (corresponding numbers are available on Table II.3 on page 83).

Fringe benefits are provided irrespective of socio-demographic background, education, or prior income. Hence, they equally apply to all three archetypes, such that stratification is only required per service options (i.e., according to the number of service days per option). As all of these benefits are earned only while serving and are lost upon return to their civilian life, they constitute opportunity-profits (i.e., negative opportunity-costs). Hence, they are factored into the global opportunity-cost balance with a negative sign. We obtained data on all fringe benefits from the Swiss Federal Office of Statistics [33], the Swiss Federal Department of Defense [32] and from the Administrative Office for the Civilian Service [34]. We then monetized opportunity-profits by calculating average daily rates for each fringe benefit. We then added these to obtain a daily balance and multiplied this balance by the number of service days for the respective service options.

3.2 Work Leisure Trade-Off

Service in a military organization implies that an individual can no longer freely trade-off work against leisure hours, according to personal preferences, or control their daily routine. The extent to which leisure must be sacrificed in the SAF is subject to which of the three military-service options an individual chooses. We therefore structured our calculation as follows. First, we obtained data on the range of median weekly work-hours in the IT-industry sector by using labor-market statistics provided by the Swiss Federal Office of Statistics [30]. Since in Switzerland, work-hours in the civilian service are set according to IT-sector workplace regulations, we assume that the median workweek in the civil service equals the median civilian workweek. Regulatory information and data on the range of hours worked in the SAF were obtained from the service regulation of the SAF, [14], and [42]. We then computed the average of each range to obtain the average daily workload for each service option. Comparing these workloads to civilian employment, we obtained figures on extra hours worked for each service option. We multiplied these by the respective number of service days required to obtain the total of extra hours worked per service option. Figure II.4 on page 74 illustrates these extra hours (corresponding numbers are available on Table II.4 on page 84).

[16] As of May 2017, one Swiss franc is valued at approximately one U.S. dollar in the foreign exchange market.

These extra hours were monetized – i.e., we translated them into their corresponding monetary value [16] – by assuming the value of a marginal unit of leisure is the equivalent of the marginal income that would have been received if the individual had worked instead [7, 18, 44, 60]. However, we modified this classic work leisure trade-off model slightly by assuming a constant, rather than decreasing, return to scale for the work leisure indifference curve. We did this because there is no empirical data that enables us to estimate its concavity and because the work leisure trade-off in Switzerland is restricted by labor market regulations.[17] As we assume constant returns to scale, the work leisure trade-off can be approximated by the median pay per hour. Socioeconomic determinants of median pay per archetype were obtained from the Swiss earnings structured survey conducted by the Swiss Federal Office of Statistics [32], as well as from the 'Salarium' web-based tool.[18]

The opportunity-cost framework provided in this article is intended to be applied to any individual who evaluates their career options. However, as previously mentioned, the focus is put on to the entire pool of the SAF' active reserve, from which conscripts are recruited. Moreover, as our analysis is intended to shed some light on acquiring human resources for building an IS defense capability, the emphasis is put on potential conscripts (specially officers) who will be incorporated into the SAF department *Armed Forces Command Support Organisation* (AFCSO), which is responsible for ICT services and electronic-operations (i.e., anti-cyber-attack operations, electronic warfare and cryptology). Hence, we take into consideration the job categories related to programming, ICT consulting, and general IT activities. This group of professions is clustered by Salarium, and focuses on individuals that are specialized in computer engineering (generally, individuals who have an applied sciences degree). Hence, we decided to use the gross median wage of the aforementioned job categories for the Swiss male citizen (as only 0.7% of total personnel is female). These procedures yielded a median opportunity-cost value of one extra hour of work of 30.10 Swiss francs for the archetype 'student / apprentice', of 42.9 Swiss francs for the archetype 'young professional', and of 56.6 Swiss Francs for the archetypes 'skilled professional'.[19] Multiplying total extra hours by these rates, we obtained opportunity-cost figures stratified by archetypes and service options. Table II.4 on page 84 illustrates these calculus.

3.3 Income not Compensated

An individual who serves in any service option is absent from work during service, hence cannot earn a civilian salary during this time. Therefore, for both the civilian service and all military services, the Swiss Federation, via the Department of the Interior, provides a compensatory income-deficit payment of 80% of the current civilian salary earned. This compensation is paid per calendar day, i.e., also on Saturdays, Sundays, holidays. The information about minimum and maximum payments, as well as conditions that apply per service option, were obtained from the Federal Compensation Office [31]. For each archetype and service option, we analyzed the eligible payments per archetype and calculated averages of their minimum and maximum values. As for NCOs and officers, payments are higher for training than for regular service days, weighted averages were calculated using the percentage distribution data shown in Table II.1 on page 82. We then compared all averages with the median IT-industry sector income that university graduates earn one and three years after graduation, respectively, using data provided by the Swiss Federal Office of

[17] In Switzerland, an individual's weekly workload in the IT-industry sector must not exceed 50 hours (Federal law on work in the industry, crafts and trade – SR 822.11). Note that this regulation does not apply to the SAF. Although a firm can persuade employees to not record hours worked beyond this threshold (e.g., consulting, investment banking), such behavior is not only illegal, but also not representative of the majority of the workforce. We therefore do not consider this effect for our analysis.

[18] `https://www.gate.bfs.admin.ch/salarium/public/index.html`

[19] Further procedural description and auxiliary calculation is available from the corresponding author.

Statistics [35], as well as by the Salarium web-based tool.[20] We used a 365-day reference year to calculate average daily median incomes from these data. Hence, we obtained a daily opportunity-cost rate that monetizes, for each archetype, the daily civilian income not compensated per service option. Finally, to obtain total opportunity-cost, this rate was multiplied by the number of service days per service option. Figure II.5 on page 75 illustrates these calculus (corresponding numbers are available on Table II.5 on page 85).

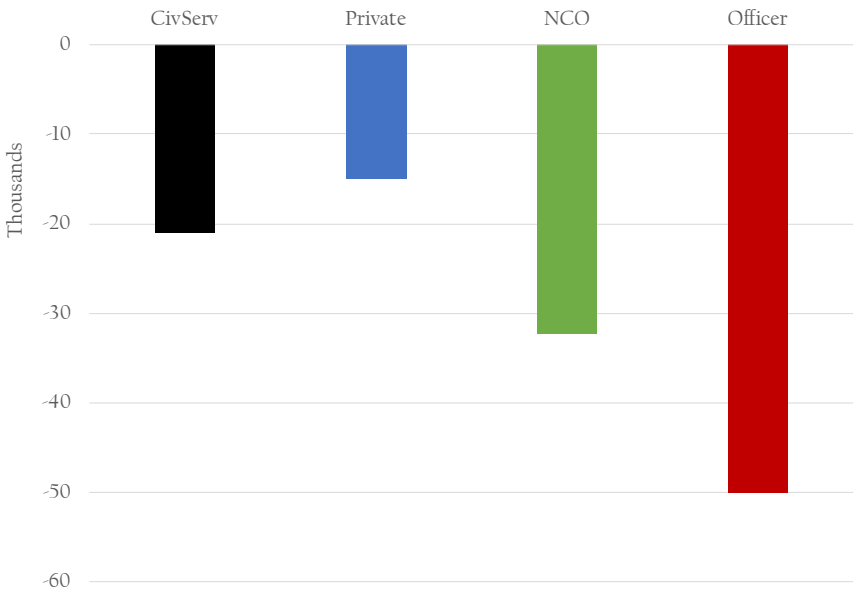
4 Results

In this section, we present four subsections. In the first three subsections, we present the results of our analysis for each type of opportunity-cost previously determined – i.e., for fringe benefits, for leisure, and for income not compensated –, and for each archetype also previously determined. In the last subsection, we present an aggregate opportunity-cost for each type of archetype.

4.1 Opportunity-Cost of Fringe Benefits

The (negative) opportunity-costs of fringe benefits are presented in Figure II.3 (corresponding numbers are available on Table II.3 on page 83). They apply equally to all archetypes as they are earned irrespective of the individual's socio-demographic background and current IT-industry sector income.

Figure II.3: **Total Avg. Opportunity-Cost of Fringe Benefits**



In the civilian service, a daily lump sum allowance of five Swiss francs per service day is paid. Depending on the particular rank, privates receive daily soldier's pay that ranges between 4 and 5 Swiss francs, NCOs between 7 and 11.50 Swiss francs, and officers between 12 and 23 Swiss francs. These ranges yield averages of 4.50, 9.30, and 17.50 Swiss francs, respectively. In addition to this allowance, a daily supplement of 23 Swiss francs is distributed to all NCOs and all officers ranks up to captain (in order to simplify the analysis, we assume that all officers receive this supplement, as the total number of officers with a rank higher than captain is relatively low, compared to the combined number of

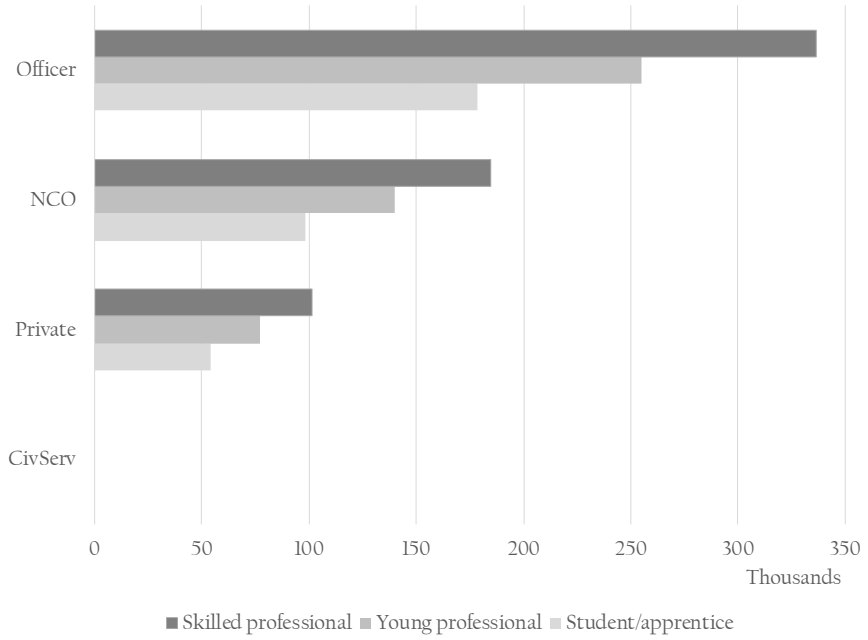
[20] We assume that these salaries are also earned by those without a formal university degree but materially equal professional training that provides them with at least the same, if not a superior, level of productivity.

lieutenants, first lieutenants, and captains). In each service option, these allowances are paid per service day (including weekends and holidays). Furthermore, during weekdays (but not when off duty on weekends or holidays), while traveling in uniform, including private trips made during leave, all soldiers receive free nationwide public transport by train. (if subject to traveling in uniform and presentation of marching orders, privates and NCOs travel in second class, officers in first class). They are also provided with free meals in their respective cantonments or, if travelling, with compensation of expenses. In the civilian service, expenses for travels costs to and from the workplace, as well as meals, are compensated during weekdays. To simplify the analysis, we assume that these fringe benefits have an approximately equal value. Each month a Swiss household spends an average of 827 Swiss francs for transport and an average of 642 Swiss francs for food and non-alcoholic beverages [33]. Assuming a single-person household and a 30-day service month with 22 working days and no holidays, 607 Swiss francs of transport expenses, and 471 Swiss francs of food expenses can be saved during any service, yielding average daily (negative) opportunity-costs of 21 and 16 Swiss francs, respectively, per service day. Finally, in all service options, private-health insurance is paid once 60 consecutive or more service days are served, and this during the entire duration of the respective service option. In practice, this condition is met during boot camp (for all military-service options, 137 service days on average) and the first half of the civilian service (180 service days). Given that a household spends an average of 736 Swiss francs per month on health insurance, and assuming a single-person household and a 30-day service month, we weighted the expenses saved by the quotient of compensated vs. total service days.

4.2 Opportunity-Cost of Leisure

The opportunity-cost of leisure, stratified by archetype and service option, is illustrated in Figure II.4 and presented in Table II.4 on page 84.

Figure II.4: **Opportunity-Cost of Leisure**

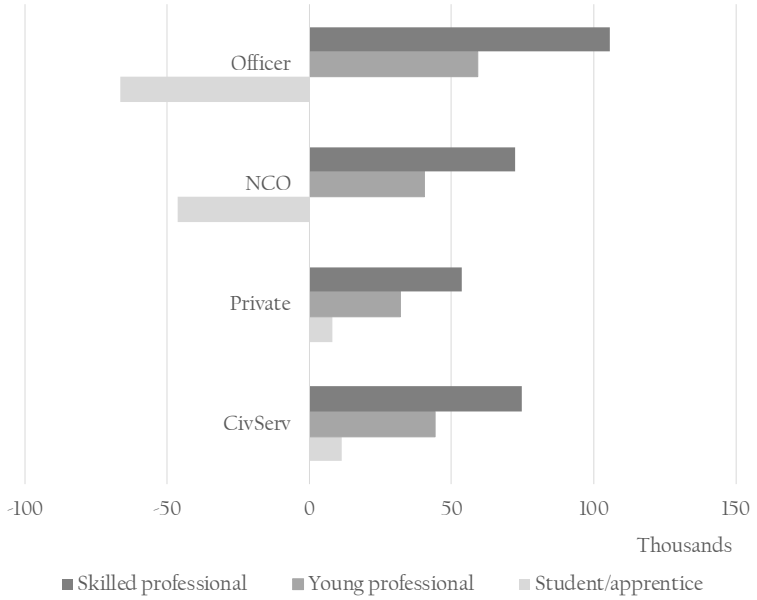


The range of a median workday in the IT-industry sector is between 8.2 and 9 hours, which gives an average of 8.6 hours worked per day. Although this workload corresponds to that of the civilian service (hence, extra hours there are zero, and so is opportunity-cost by consequence), the real workday in all military-service options is significantly longer, and the longest workday is for conscripted officers. Work-hours ranges vary between 12 and 18 hours for privates, between 14 and 19 hours for NCOs, and between 15 and 22 hours for officers. These work-hours correspond to averages of 15, 16.5, and 18.5 hours, respectively. The work-hours for all military-service options account for the fact that many conscripted NCOs and all conscripted officers have only one day off per week and often work additional hours during weekdays and also on weekends. The respective ranges we obtained were already adjusted for these effects.

4.3 Opportunity-Cost of Income Not Compensated

Finally, Figure II.5 and Table II.5 on page 85 presents data on IT-industry sector incomes and the extent to which they are compensated, stratified by archetype and service option.

Figure II.5: **Opportunity-Cost of Income Not Compensated**



Labor-market data suggest that in the IT-industry sector, an average apprentice earns an annual median salary of 12,000 Swiss francs while undergoing professional training. To simplify the analysis, we assume that a student enrolled in tertiary education has a part-time unskilled job yielding the same income. Concerning the aforementioned job categories related to programming, ICT consulting, and general IT activities – individuals that are specialized in computer engineering, generally, who have an applied sciences degree –, the average annual gross median income for young professionals is 88,584 Swiss francs, and 116,760 Swiss francs for skilled professionals with three years of work experience. Assuming a 365-day year, we find that these annual salaries correspond to daily incomes of 33 Swiss francs, 242.7 Swiss francs, and 319.9 Swiss francs, respectively.

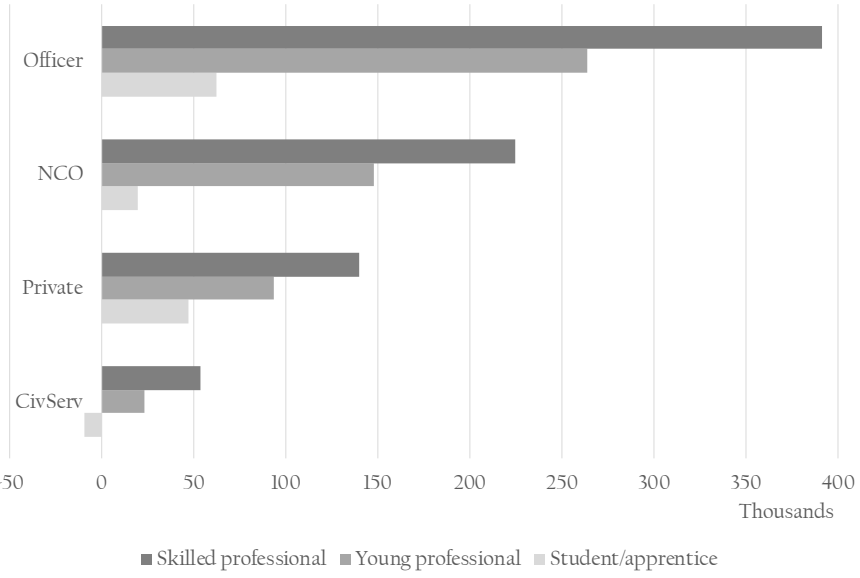
Across all service options, and irrespective of prior IT-industry sector income, the minimum daily compensatory payment is set at 62 Swiss francs, and the maximum is at 196 Swiss francs, thus yielding an average daily compensation of 129 Swiss francs. However,

two exceptions must be considered. First, as the minimum of 62 Swiss francs is applied irrespective of prior IT-industry sector income, the archetype 'student/apprentice' always receives this daily compensation as their daily income of 33 Swiss francs is far below this threshold. For the same reason, students/apprentices cannot receive any compensation beyond this minimum rate, such that it also constitutes the maximum possible compensatory payment. Second, while in training and boot camp, NCOs and officers receive a minimum daily compensation of 111 francs per day, whereas the standard minimum rate of 62 francs per day is applied during all other days. Weighting these data by the percentage distribution data shown in Table II.1 on page 82 gives weighted averages of 145 Swiss francs of daily compensatory payments for NCOs, and 144 Swiss francs of daily compensatory payments for officers. Finally, a daily opportunity-cost is calculated as the difference between daily IT-industry sector income and average daily compensation; this difference is then multiplied by the number of service days per service option. Table II.5 on page 85 illustrates these calculus.

4.4 Aggregated Opportunity-Cost

Figure II.6 and Table II.6 on page 86 summarizes all three opportunity-cost factors into global balances.

Figure II.6: **Aggregated Opportunity-Cost**



If an individual makes a decision about where to serve solely on the basis of opportunity-cost, the civilian service is the optimal choice for all three archetypes. In this service option, students and apprentices actually realize a profit of 9,750 Swiss francs, as the opportunity-cost of leisure is zero, whereas the balance of fringe benefits and compensatory payments exceeds their IT-industry sector income. Moreover, assuming that today's students and apprentices picture themselves to be young and skilled professionals in the future, for them the civilian service is even more attractive as this service option gives them the possibility to serve 'at a stretch', hence they can fulfill their duty to serve long before they would earn professional salaries that are only partly compensated. The effect is analogous for young and skilled professionals, for whom the opportunity-cost of a conscripted-officer post is prohibitively high compared to all other service options. The higher an individual's current or projected IT-industry sector income is, the less that individual would be inclined to choose any military service, especially, a conscripted-officer career.

However, the problem set goes beyond a dichotomous competition between the military and civilian service. If transaction costs for admission to the civilian service were raised to a point where any military service is economically more attractive than conscientious objection, all archetypes would choose to serve as a private and refuse to undergo any further training. If forced to participate in training, all archetypes would refuse to serve as conscripted officers, instead would prefer to serve as an NCO. As a result, all archetypes can in fact serve in the SAF and refuse a relatively unattractive conscripted-officer post.

This finding likely explains the paradoxical effect that, despite the good pay the SAF offer and their generally good reputation among citizens, the conscripted-officer deficit persists. It also explains why there is a greater lack of officers than of privates and NCOs. Moreover, the persistent deficit of conscripted officers might not necessarily be due to the civilian service being more attractive than any other military-service option, rather it is due to the fact that a conscripted-officer career is the least attractive among all military-service options. Even if the opportunity-cost of leisure for conscripted officers were reduced to zero by applying civilian labor-market regulations, the relatively generous fringe benefits would fail to even offset the lack of IT-industry sector income compensation for the young professionals and the skilled professionals archetypes. Only if the opportunity-cost of leisure were to be reduced to zero and income compensation raised to 100%, service as an officer would be more attractive than any other service option.

5 Discussion

In this last section, we present our concluding comments, the policy recommendations resulting from concluding comments, we discuss the limitations of this study and suggest paths for further research.

5.1 Concluding Comments

Using opportunity-cost analysis, we have shown that free-market institutions in the IT-industry sector compete with planned-economy institutions in the public sector, and that the latter often lose this race. Hence, CIs must find novel ways to recruit specialists as fixed-state salaries are rarely competitive. At the time we conducted our study, military units specifically dedicated to cyber-defense did not yet exist as these were only created in 2018. Follow-up studies that could replicate our approach with such specialist troops might be helpful to either refute or corroborate our conclusions.

Our findings have a number of important implications, both for academicians and for policy-makers who are interested in acquiring human resources for building an IS defense capability. To the best of our knowledge, this article constitutes the first attempt to estimate the actual opportunity-cost structure of a complex, multi-option individual decision between service options in the context of armed forces. Hence, our model goes beyond a dichotomous choice between the military and civilian service. In so doing, it responds to calls for such studies, complementing them with an economic perspective eluded by many prior contributions that have instead emphasized socio-demographic, intrinsic and extrinsic motivation factors.

Specifically, with respect to the persistent deficit of conscripted officers in the SAF, we demonstrated that in terms of opportunity-cost, the conscripted-officers positions constitute the least attractive service option. Consequently, we suggest that candidates whose ideological motivation for a conscripted-officer career supersedes opportunity-cost calculations are no longer numerous enough to compensate for those whose decision is, in fact, based on such calculations. Hence, without a corresponding opportunity-cost analysis, studies might overstate an individual's propensity to join armed forces if they are based

only on the analysis of intrinsic and extrinsic incentives.

Consequently, in order to acquire human resources for building an IS defense capability among armed forces, academicians and policy-makers can take into account the following considerations.

5.2 Considerations for Policy Recommendations

The opportunity-cost framework developed in this article can be adapted for any organization that seeks to attract and employ IS defense specialists and/or IS defense managers. By assessing the opportunity-cost that such specialists face whenever they are confronted with choosing an employer among various alternatives, the framework presented helps practitioners to evaluate their competitiveness with competitors hence to shed some light on how competitive they are in terms of hiring conditions. As human resources are an essential component for developing and securing an IS defense capability, such a component is undeniably a building block for ensuring the operational continuity of any given organization/CI.

Specifically for the SAF, the opportunity-cost of the officer-service option is too high with respect to other service options. Without corresponding opportunity-cost analyzes, studies tend to overstate an individual's propensity to join an armed force if they are based on the analysis of intrinsic and extrinsic incentives alone. In the absence of work leisure trade-off considerations, service in the military is less attractive the higher an individual's IT-industry sector income is. If such trends persist, military recruitment will likely face adverse selection problems, as military service will be attractive to only those employed in low-paying industries and/or with a professional education that does not enable them to compete for higher-paying jobs. This might constitute an important drawback as specialized human capital is of prior importance in job categories that are necessary for building an IS defense capability, e.g., computer engineers. In our context, for a conscripted-officer career, the annual break-even salary is 59,220 Swiss francs for a young professional, and is 64,204 Swiss francs for a skilled professional. Although these might seem substantial on a nominal basis, they are in fact 59% and 45% below the median salaries these individuals earn in the IT-industry sector. Consequently, for a conscripted-officer career to become more attractive, the recruitment policy for officers and specialized positions should target potential candidates while they are still students or apprentices, even though they will be undeniably less skilled than individuals that already have a degree.[21] The opportunity-costs of students or apprentices are low and the marginal utility of money is high, as long as they study or undergo professional training. However, as these individuals enter the working world, the opportunity-cost of IT-industry sector income quickly grows to a point where a conscripted-officer career is the least attractive of all available service options.

At the same time, military organizations should caution themselves against the attempt to counter under-staffing by monetary considerations alone, as these could undermine intrinsic motivation [10, 47]. In Switzerland, compensatory pay for income was raised by 14% in 2009, but the conscripted-officer deficit still persists. An opportunity-cost perspective then points to the importance of the opportunity-cost of leisure. In our estimations, such a cost is generated by the excessive workload that comes with a conscripted-officer career, i.e., by a highly disadvantageous work leisure trade-off. In the past, individuals in Switzerland had little choice but to cope with this workload as a civilian service for conscientious objectors was not introduced until 1996, and because military service in a conscripted-officer position was seen as an indispensable requirement for higher management. However, since 1995 elites in Switzerland have gradually become more international, less interconnected,

[21] In order to compensate such a lack of skills, we suggest that the SAF must deliver a state of the art technical training that prioritize essential technical skills related to their *command and control* missions, i.e., anti-cyber attack operations, electronic warfare and cryptology.

and more balanced in terms of gender distribution [2, 15]. Hence, the excessive number of extra hours a conscripted officer must work are less and less implicitly compensated by the expectation of positive job-related externalities. The extent to which (if any) this effect can be compensated monetarily seems questionable. Not only does the globalization of the economy confront potential officer candidates with expatriate competitors, but the value system of today's and tomorrow's professionals is shifting. The workplace attitude of the generation born between 1985 and 2000 ('millennials') puts greater emphasis on the work leisure trade-off and assigns less importance to monetary fringe benefits and status [41]. Hence, this generation would emphasize the opportunity-costs of leisure and be relatively indifferent to increased pay or benefits.

In contrast, non-monetary benefits seem more promising. For example, in the United States, the GI Bill largely waives the cost of studying for a degree once military personnel have completed their duty. This program reached record levels in 2009 with nearly 95% of eligible personnel involved in the program and with 70% of them actually using this program once they left the military [8]. Empirical evidence suggests that spending a fixed budget on recruitment rather than on salary increases is a much more efficient way to win over qualified staff [20].

As suggested in the concluding comments, candidates whose ideological motivation for a conscripted-officer career supersedes opportunity-cost calculations might not be longer numerous enough in order to compensate for whose decision is, in fact, based on such calculations. A solution in order to augment the pool of ideologically motivated potential conscripted-officers could be to augment the recruitment base that is nowadays limited to male citizens. In order to do so, policies that include the conscription duty to female and established foreigners could fill the gap.

Also, once young individuals have joined the armed forces, the structure of the service with academic or professional agendas should carefully be aligned in order to minimize the frustration owing to time conflicts, and should be negotiate with colleges and professional schools for academic equivalents of capabilities created by military training. Furthermore, conscripted-officers training could become more attractive if military capabilities, such as leadership, were valued in the industry [71]. However, the extent to which such incentives reduce perceived opportunity-cost is probably related to the extent to which military training can indeed substitute professional training and education (e.g., an MBA degree). Research suggests that significant conceptual and behavioral gaps between business and military leadership exist, making the transition less than seamless [63, 80].

Finally, military decision-makers should note that the conscripted-officer deficit cannot readily be explained by conscientious objection or the existence of a civilian service. The results we have presented here suggest that a conscripted-officer career is the most unattractive among all military-service options, even in the absence of a civilian service. Compared to privates and NCOs, opportunity-cost for conscripted officers grows exponentially as individuals enter professional life. Hence, applying 'raising rival's costs' tactics [12, 65] by making the civilian service more unattractive *vis-à-vis* the other service options, or by erecting additional barriers for admission, are unlikely to significantly alter the situation because they would only shepherd individuals into the second-best service option, i.e., serving as a private.

5.3 Limitations and Paths for Further Research

Our attempts to monetize opportunity-costs by using socio-demographic, labor market, and benefit data provide empirical contributions that implicitly accept assumptions from economic theory that future research could help relax.

First, an opportunity-cost analysis is framed in neoclassical economic thought; it thus assumes that individuals maximize individual utility and make rational choices [67]. In

the context of our research, this 'homo economicus' assumption might be questionable for two reasons. First, when it comes to making personal career choices, individuals might exhibit bounded, rather than perfect, rationality [25]. Hence, individuals might prefer imprecise estimates, partial information, social cues, projections, and assumptions over precise calculation as they evaluate relative magnitudes of costs [57]. Our analysis could be refined by introducing weights or scaling factors that can take such bounded rationality into account.

Second, we assumed that IT-specialists are ideologically neutral; implying they would evaluate and compare service alternatives inside and outside armed forces organizations as they would consider different career choices in the private sector. However, as both armed forces and many CIPs operate in a public sector and national-security context, individuals might have ideological reservations to enlist. On the other hand, using the reverse argument, a particular type of individuals might enjoy the culture of armed forces and the public-sector context. Such ideological influence would increase the opportunity cost of enlistment for the first type, but reduce it for the second type of individuals. Future research should take this differentiation into account.

Third, although we have collected and analyzed these data in the context of the SAF, we believe our analysis should be generalizable to many other military organizations. For example, researches reported numerous and similar cases of under-staffing in armed forces, e.g., in India [70], the US [39, 48, 52], and Great Britain [19, 21]; both in systems that must rely on a professional model and in those based on conscription model. The problem seems to be more of a general nature and less of a context-specific one. Therefore, an opportunity-cost approach is useful as it can be applied irrespective of cultural and contextual idiosyncrasies. Even in less liberal systems, where free choice between service options is suppressed, individuals can still 'vote with their feet' [6] by emigrating or by bribing officials to be granted exemption from service, e.g., in Russia [51] and Kazakhstan [78]. In other words, even in such systems, the opportunity-cost of not serving in a particular service option (e.g., harassment at work, risk of state prosecution, expenditure for emigration) can be assessed and monetized. Our results can also be generalizable as they likely constitute a lower boundary from a global perspective.

Fourth, additional opportunity-cost factors that are unlikely to materialize in the Swiss context might have to be considered elsewhere in the world – mortality risks, geographic mobility, and effects related to job tenure.[22] Due to the Swiss state doctrines of neutrality and non-involvement in international armed conflicts, the SAF have a defensive and isolationist nature. Switzerland is a member of NATO's partnership for peace since 1994, but does not contribute personnel to NATO missions except for two observers at their headquarters in Brussels. Less than 0.2% of all personnel serve in international, non-combat peacekeeping missions authorized by the United Nations. As a result, the mortality risk is almost nil; over the last twenty years, the few isolated cases of injured and deceased staff were due to either suicide or traffic- and weapon-handling accidents. In contrast, the U.S. Armed Forces witnessed an annual mortality rate of 71.5 per 100,000 staff between 1990 and 2011 (United States Armed Forces Health Surveillance Center [4]). Hence, an individual making a decision on the basis of opportunity-cost would likely factor the cost of increased mortality risk into the equation (e.g., by assuming reduced lifetime income).

Fifth, under the Swiss conscription system, once an individual has passed boot camp, almost all personnel serve in annual training that take between three and four weeks per year. Hence, conscripted personnel very rarely relocate during service days, they rather commute between their home and military sites on weekends. Given the density of transport infrastructures in Switzerland, the small size of the country, and free transport

[22]We thank an anonymous reviewer for drawing our attention to these issues and providing us with valuable arguments.

provided during military service, the financial and temporal opportunity-cost of mobility is low. However, in large territorial states where cross-country travel might take days or requires air travel (e.g., Russia, India, China, Australia, or the US), the opportunity-cost of geographic mobility might be significant. Such costs would have to be added to our estimates. Finally, labor-market research suggests that individuals absent from the civilian working world during military service experience disadvantages because they miss out on the positive external effects of professional networking and might take longer to re-adapt [2, 72]. Furthermore, they could be outwitted by expatriate competitors who have no duty to serve because they do not have citizenship in the said country. As in the SAF, annual training is relatively short, the impact of these adverse effects is limited for individuals living in Switzerland. Yet, in countries with long service times served at a stretch (e.g., Israel), these opportunity-costs can be significant. Hence, the estimates we present in this article might constitute only a lower boundary of the actual total opportunity-cost of any military-service option. Armed forces around the world could therefore take our estimates as a baseline case and factor in these additional costs, according to their specific context. Although we consider the estimation of these cost factors to be beyond the scope of this article, we believe that such an estimation opens up promising paths for future research that could expand our model. Furthermore, our model assumes that the three opportunity-cost factors we study are equally important for the individual's decision. Future work could conceptualize weights by which the relative importance of particular factors for an individual can be modeled.

Finally, our analysis could be refined by the consideration of inter-temporal effects and inflation. Rational individuals could be expected to calculate capital values of global opportunity-cost by discounting future cash flows or their monetized equivalents to the present, by observing both inflation expectations and interest rates.

Table II.1: **Structural Deficit of Conscripts** [a]

	Staff deficit (required positions not filled)		
Swiss Armed Forces census	Privates (%)	NCOs (%)	Officers (%)
2010	−5	−5	24
2011	2	−3	23
2012	−1	−2	10
2013	0	−2	12
2014	5	−2	15
2015	9	−2	15
2016	12	−2	16

[a] Nominal reduction of conscripted-officer deficit from 2011 onward is due to an armed-forces reform that reduced the number of officer positions (whether filled or not) whereas officer headcount remained almost stable. As a result, the position fill rate nominally improved.

Table II.2: **Service Days per Service Option**

	Service Option			
	CivServ	Private	NCO	Officer
Service days (min.)	390	260	400	600
Service days (max.)	390	300	425	600
Service days (avg.)	390	280	413	600
% service days spent in boot camp and training	46%	54%	64%	61%
% service days spent in practical service	54%	46%	36%	39%

Table II.3: **Opportunity-Cost of Fringe Benefits**

	Service Option			
	CivServ	Private	NCO	Officer
Avg. daily allowance/soldier's pay	−5.0	−4.5	−9.3	−17.5
Daily supplement for NCOs and officers			−23.0	−23.0
Free public transport, approx. daily savings	−21.0	−21.0	−21.0	−21.0
Food and subsistence, approx. daily savings	−16.0	−16.0	−16.0	−16.0
Health insurance, weighted avg. daily savings	−12.0	−12.0	−9.0	−6.0
Daily avg. opportunity-cost	−54.0	−53.5	−78.3	−83.5
Service days	390.0	280.0	413.0	600.0
Total avg. opportunity-cost	−21 060.0	−14 980.0	−32 337.9	−50 100.0

Table II.4: **Opportunity-Cost of Leisure**

Archetype considered	**Student/apprentice**			
	CivServ	Private	NCO	Officer
Avg. daily work-hours, industry	8.6	8.6	8.6	8.6
Avg. daily work-hours, service	8.6	15.0	16.5	18.5
Avg. extra-hours per service day	0.0	6.4	7.9	9.9
Service days	390.0	280.0	413.0	600.0
Total extra-hours	0.0	1792.0	3262.7	5940.0
Median opportunity-cost per hour	30.1	30.1	30.1	30.1
Total opportunity-cost of leisure	0.0	53 939.2	98 207.3	178 794.0

Archetype considered	**Young professional**			
	CivServ	Private	NCO	Officer
Avg. daily work-hours, industry	8.6	8.6	8.6	8.6
Avg. daily work-hours, service	8.6	15.0	16.5	18.5
Avg. extra-hours per service day	0.0	6.4	7.9	9.9
Service days	390.0	280.0	413.0	600.0
Total extra hours	0.0	1792.0	3263.0	5940.0
Median opportunity-cost per hour	42.9	42.9	42.9	42.9
Total opportunity-cost of leisure	0.0	76 876.8	139 982.7	254 826.0

Archetype considered	**Skilled professional**			
	CivServ	Private	NCO	Officer
Avg. daily work-hours, industry	8.6	8.6	8.6	8.6
Avg. daily work-hours, service	8.6	15.0	16.5	18.5
Avg. extra-hours per service day	0.0	6.4	7.9	9.9
Service days	390.0	280.0	413.0	600.0
Total extra hours	0.0	1792.0	3263.0	5940.0
Median opportunity-cost per hour	56.6	56.6	56.6	56.6
Total opportunity-cost of leisure	0.0	101 427.2	184 685.8	336 204.0

Table II.5: **Opportunity-Cost of Income Not Compensated**

Archetype considered	**Student/apprentice**			
	CivServ	Private	NCO	Officer
Daily median income	33.0	33.0	33.0	33.0
Daily compensation (min.)	62.0	62.0	62.0	62.0
Daily compensation (max.)	62.0	62.0	196.0	196.0
Daily compensation (avg.)	62.0	62.0	145.0	144.0
Daily avg. opportunity-cost	29.0	29.0	−112.0	−111.0
Nb. of service days	390.0	280.0	413.0	600.0
Total avg. opportunity-cost	11 310.0	8120.0	−46 256.0	−66 600.0

Archetype considered	**Young professional**			
	CivServ	Private	NCO	Officer
Daily median income	242.7	242.7	242.7	242.7
Daily compensation (min.)	62.0	62.0	62.0	62.0
Daily compensation (max.)	196.0	196.0	196.0	196.0
Daily compensation (avg.)	129.0	129.0	145.0	144.0
Daily avg. opportunity-cost	113.7	113.7	97.7	98.7
Nb. of service days	390.0	280.0	413.0	600.0
Total avg. opportunity-cost	44 343.0	31 836.0	40 350.1	59 220.0

Archetype considered	**Skilled professional**			
	CivServ	Private	NCO	Officer
Daily median income	319.9	319.9	319.9	319.9
Daily compensation (min.)	62.0	62.0	62.0	62.0
Daily compensation (max.)	196.0	196.0	196.0	196.0
Daily compensation (avg.)	129.0	129.0	145.0	144.0
Daily avg. opportunity-cost	190.9	190.9	174.9	175.9
Nb. of service days	390.0	280.0	413.0	600.0
Total avg. opportunity-cost	74 451.0	53 452.0	72 233.7	105 540.0

Table II.6: **Aggregated Opportunity-Cost**

Archetype considered	**Student/apprentice**			
	CivServ	Private	NCO	Officer
Fringe benefits	−21 060.0	−14 980.0	−32 337.9	−50 100.0
Leisure	0.0	53 939.2	98 207.3	178 794.0
Income	11 310.0	8120.0	−46 256.0	−66 600.0
Total	−9750.0	47 079.2	19 613.4	62 094.0

Archetype considered	**Young professional**			
	CivServ	Private	NCO	Officer
Fringe benefits	−21 060.0	−14 980.0	−32 337.9	−50 100.0
Leisure	0.0	76 876.8	139 982.7	254 826.0
Income	44 343.0	31 836.0	40 350.1	59 220.0
Total	23 283.0	93 732.8	147 994.9	263 946.0

Archetype considered	**Skilled professional**			
	CivServ	Private	NCO	Officer
Fringe benefits	−21 060.0	−14 980.0	−32 337.9	−50 100.0
Leisure	0.0	101 427.2	184 685.8	336 204.0
Income	74 451.0	53 452.0	72 233.7	105 540.0
Total	53 391.0	139 899.2	224 581.6	391 644.0

References

1. Alcaraz, C. & Zeadally, S. Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. *International Journal of Critical Infrastructure Protection* **8,** 53–66 (2015).
2. Allen, M. L'armée, toujours une école de cadres pour l'économie? *Swissinfo.* (2016) (July 10, 2016).
3. Angrist, D. Estimating the Labor Market Impact of Voluntary Military Service Using Social Security Data on Military Applicants. *Econometrica* **66,** 249–288 (1998).
4. Armed Forces Health Surveillance Center (AFHSC). Deaths while on active duty in the U.S. Armed Forces, 1990-2011. *MSMR* **19,** 2–5 (2012).
5. Asch, B. J. *et al. Cash Incentives and Military Enlistment, Attrition, and Reenlistment* (RAND National Defense Research Institute, Santa Monica, USA, 2010).
6. Banzhaf, H. S. & Walsh, R. P. Do People Vote with Their Feet? An Empirical Test of Tiebout. *American Economic Review* **98,** 843–863 (2008).
7. Becker, G. S. A Theory of the Allocation of Time. *The Economic Journal* **75,** 493–517 (1965).
8. Bellais, R., Foucault, M. & Oudot, J.-M. *Économie de la défense* 128 pp. ISBN: 978-2-7071-8223-4 (La Découverte, Paris, France, 2014).
9. Ben-Dor, G. *et al.* I versus We: Collective and Individual Factors of Reserve Service Motivation during War and Peace. *Armed Forces & Society* **34,** 565–592 (2008).
10. Bénabou, R. & Tirole, J. Intrinsic and Extrinsic Motivation. *The Review of Economic Studies* **70,** 489–520 (2003).
11. Bingley, P., Lundborg, P. & Lyk-Jensen, S. V. *Estimating Family Spillovers: Evidence from a Draft Lottery* 2015.
12. Boockmann, B. & Vaubel, R. The Theory of Raising Rivals' Costs and Evidence from the International Labour Organisation. *The World Economy* **32,** 862–887 (2009).
13. Buchanan, J. M. in *The New Palgrave Dictionary of Economics* (eds Durlauf, S. N. & Blume, L. E.) 4710–4713 (Palgrave Macmillan, London, UK, 2008). ISBN: 978-1-349-58802-2.
14. Buffat, A. *La mise en oeuvre de la réforme de l'armée suisse « Armée XXI »: les changements vécus à l'interne* Master Thesis (University of Lausanne, Lausanne, Switzerland, 2005).
15. Bühlman, F., Beetschen, M., David, T., Ginalski, S. & Mach, A. *Transformation des élites en Suisse* (Social Change in Switzerland, Université de Lausanne, 2015).
16. Cellini, S. R. & Kee, J. E. in *Handbook of Practical Program Evaluation* (eds Newcomer, K. E., Hatry, H. P. & Wholey, J. S.) 4th ed., 636–672 (Jossey-Bass & Pfeiffer Imprints, Hoboken, USA, 2015).
17. Church, R. L., Scaparra, M. P. & Middleton, R. S. Identifying Critical Infrastructure: The Median and Covering Facility Interdiction Problems. *Annals of the Association of American Geographers* **94,** 491–502 (2004).
18. Clarke, A. C. The Use of Leisure and its Relation to Levels of Occupational Prestige. *American Sociological Review* **21,** 301–307 (1956).
19. Dandeker, C. & Strachan, A. Soldier Recruitment to the British Army: A Spatial and Social Methodology for Analysis and Monitoring. *Armed Forces & Society* **19,** 279–290 (1993).

20. Dertouzos, J. N. *Cost-Effectiveness of Military Advertising: Evidence from 2002-2004* OCLC: 320143725 (RAND Corporation, Santa Monica, USA, 2009).

21. Dixon, P. Britain's 'Vietnam Syndrome'? Public Opinion and British Military Intervention from Palestine to Yugoslavia. *Review of International Studies* **26,** 99–121 (2000).

22. Elder Jr., G. H., Johnson, M. K. & Crosnoe, R. in *Handbook of the Life Course* 3–19 (Springer, Boston, USA, 2003). ISBN: 978-0-306-48247-2.

23. Geiser, U. Swiss voters endorse army conscription. *Swissinfo.* (2019) (Sept. 22, 2013).

24. Gibson, J. L., Griepentrog, B. K. & Marsh, S. M. Parental Influence on Youth Propensity to Join the Military. *Journal of Vocational Behavior* **70,** 525–541 (2007).

25. Gigerenzer, G. & Selten, R. *Bounded Rationality: The Adaptive Toolbox* (MIT press, 2002).

26. Gigon, A. L'armée veut retrouver son aura dans l'économie. *Swissinfo.* (2016) (May 21, 2010).

27. Gorman, L. & Thomas, G. W. Enlistment Motivations of Army Reservists: Money, Self-Improvement, or Patriotism? *Armed Forces & Society* **17,** 589–599 (1991).

28. Government, S. *Arbeitslosenzahlen [Unemployment statistics]* (State Secretariat of Economic Affairs, Swiss Confederation, Bern, Switzerland, 2010).

29. Government, S. *Armeeauszählung 2016 [Armed Forces Census 2016]. Operations Staff of the Armed Forces* (Swiss Federal Department of Defense, Bern, Switzerland, 2016).

30. Government, S. *Betriebsübliche Arbeitszeit nach Wirtschaftsabteilungen (NOGA 2008), in Stunden pro Woche [Normal Workweek in the Private Sector According to NOGA 2008 Classification in Hours Per Week]* (Swiss Federal Office of Statistics, Neuchâtel, Switzerland, 2016).

31. Government, S. *Erwerbsausfallentschädigungen, Infoblatt 6.01 [Compensatory Payments, Information Sheet 6.01]* (Federal Compensation Office, Swiss Confederation, Bern, Switzerland, 2015).

32. Government, S. *Finanzielle Entschädigung Von Armeeangehörigen Im Dienst [Financial Compensation of Armed Forces Personnel on Duty]. Operations Staff of the Armed Forces* (Swiss Federal Department of Defense, Bern, Switzerland, 2012).

33. Government, S. *Haushaltseinkommen Und –Ausgaben [Household Income and Expenses]* (Swiss Federal Office of Statistics, Neuchâtel, Switzerland, 2016).

34. Government, S. *Jahresstatistik ZIVI [Annual Statistics for the Civilian Service]* (Administrative Office for the Civilian Service, Bern, Switzerland, 2016).

35. Government, S. *Standardisiertes Bruttoerwerbseinkommen der Hochschulabsolvent/Innen: Stand fünf Jahre und ein Jahr nach Studienabschluss [Standardized Gross Income of University Graduates: Situation Five and One Year(S) after Graduation]* (Swiss Federal Office of Statistics, Neuchâtel, Switzerland, 2015).

36. Haltiner, K. W. in *Soldat-ein Berufsbild im Wandel* (eds Klein, P., Kuhlmann, J. & Rohde, H.) Klein, P., Kuhlmann, J., & Rohde, H., 112 (Deutscher Bundeswehr-Verlag, Bonn, Germany, 1993). ISBN: 978-3-559-99000-8.

37. Haltiner, K. W. in *Schweizer Armee heute und in Zukunft: Das Aktuelle Standardwerk über die Schweizerische Landesverteidigung: Forschungsstelle für Sicherheitspolitik und Konfliktanalyse FSK* (ed Carrel, L. F.) 435–447 (Ott-Verlag, Thun, Switzerland, 1996). ISBN: 978-3-7225-6853-9.

38. Haltiner, K. & Meyer, R. Aspects of the Relationship between Military and Society in Switzerland. *Armed Forces & Society* **6,** 49–81 (1979).

39. Henning, C. A. *Army Officer Shortages: Background and Issues for Congress* (Congressional Research Service, Washington, USA, 2006).

40. Herder, P. M. & Thissen, W. A. H. in *Critical Infrastructures State of the Art in Research and Application* (eds Thissen, W. A. H. & Herder, P. M.) 1–8 (Springer, Boston, USA, 2003).

41. Hershatter, A. & Epstein, M. Millennials and the World of Work: An Organization and Management Perspective. *Journal of Business and Psychology* **25,** 211–223 (2010).

42. Hofstetter, P. *Survey on the Working Hours of Militia Officers in the Swiss Armed Forces (unpublished database)* (University of Zurich, Zurich, Switzerland, 2016).

43. Hosek, J. R. & Peterson, C. E. *Enlistment Decisions of Young Men.* RAND/R-3238-MIL (Rand corp., Santa Monica, 1985).

44. Juster, F. T. & Stafford, F. P. The Allocation of Time: Empirical Findings, Behavioral Models, and Problems of Measurement. *Journal of Economic Literature* **29,** 471–522 (1991).

45. Keller, K., Poutvaara, P. & Wagener, A. Military Draft and Economic Growth in Oecd Countries. *Defence and Peace Economics* **20,** 373–393 (2009).

46. Kohen, A. I. *Attrition from Military and Civilian Jobs: Insights from the National Longitudinal Surveys* Final Report BATT-TR-638 (Battelle Memorial Institute, Columbus, USA, 1984).

47. Kohn, A. Why Incentive Plans Cannot Work. *Harvard Business Review* **71,** 54–60 (1993).

48. Korb, L. J. & Duggan, S. E. An All-Volunteer Army? Recruitment and its Problems. *PS: Political Science & Politics* **40,** 467–471 (2007).

49. Kriesi, H. Military Service and Social Change in Switzerland. *Armed Forces & Society* **2,** 218–226 (1976).

50. Lee, D. R. & McKenzie, R. B. Reexamination of the Relative Efficiency of the Draft and the All-Volunteer Army. *Southern Economic Journal* **58,** 644–654 (1992).

51. Levin, M. & Satarov, G. Corruption and Institutions in Russia. *European Journal of Political Economy* **16,** 113–132 (2000).

52. Lewis, M. R. Army Transformation and the Junior Officer Exodus. *Armed Forces & Society* **31,** 63–93 (2004).

53. Malizard, J. Opportunity Cost of Defense: An Evaluation in the Case of France. *Defence and Peace Economics* **24,** 247–259 (2013).

54. Moskos, C. C. From Institution to Occupation: Trends in Military Organization. *Armed Forces & Society* **4,** 41–50 (1977).

55. Moteff, J. & Parfomak, P. *Critical Infrastructure and Key Assets: Definition and Identification* (Library of Congress Washington DC, Congressional Research Service, Washington, DC, 2004).

56. Musgrave, R. A. & Musgrave, P. B. *Public Finance in Theory and Practice* 5th ed. ISBN: 978-0-07-044127-9 (McGraw-Hill College, New York, USA, 1989).

57. Nielsen, H. Bounded Rationality in an Imperfect World of Regulations: What if Individuals are not Optimizing. *Organization Science* **2,** 439–448 (2012).

58. Oi, W. Y. The Economic Cost of the Draft. *The American Economic Review* **57,** 39–62 (1967).

59. Ouyang, M. Review on Modeling and Simulation of Interdependent Critical Infrastructure Systems. *Reliability Engineering & System Safety* **121,** 43–60 (2014).

60. Owen, J. D. The Demand for Leisure. *Journal of Political Economy* **79,** 56–76 (1971).

61. Perri, T. Deferments and the Relative Cost of Conscription. *The B.E. Journal of Economic Analysis & Policy* **10,** 103 (2010).

62. Peuker, M. *Motivation of Swiss Army Career Officers: Implications of Generational Characteristics for Attracting and Recruiting Career Officer Candidates* Master's thesis (University of Fribourg, Fribourg, Switzerland, 2012). 20–50.

63. Popper, M. Leadership in Military Combat Units and Business Organizations: a Comparative Psychological Analysis. *Journal of Managerial Psychology* **11,** 15–23 (1996).

64. Rinaldi, S. M., Peerenboom, J. P. & Kelly, T. K. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems Magazine* **21,** 11–25 (2001).

65. Salop, S. C. & Scheffman, D. T. Raising Rivals' Costs. *The American Economic Review* **73,** 267–271 (1983).

66. Santos, J. R., Haimes, Y. Y. & Lian, C. A Framework for Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies: Linking Cybersecurity Metrics to the Modeling of Macroeconomic Interdependencies. *Risk Analysis* **27,** 1283–1297 (2007).

67. Simon, H. A. A behavioral model of rational choice. *The quarterly journal of economics* **69,** 99–118 (1955).

68. Snyder, W. P. Officer Recruitment For the All-Volunteer Force: Trends and Prospects. *Armed Forces & Society* **10,** 401–425 (1984).

69. Soomro, Z. A., Shah, M. H. & Ahmed, J. Information Security KManagement Needs More Holistic Approach: A Literature Review. *International Journal of Information Management* **36,** 215–225 (2016).

70. Suman, M. G. M. Shortage of Officers is the Root-Cause. *Indian Defence Review* (May 29, 2015).

71. Szvircsev Tresch, T. The Transformation of Switzerland's Militia Armed Forces and the Role of the Citizen in Uniform. *Armed Forces & Society* **37,** 239–260 (2011).

72. Szvircsev Tresch, T. & Merkulova, N. Vorzeitiges Ausscheiden Aus Dem Berufskader Der Armee. *Allgemeine Schweizerische Militärzeitschrift* **12,** 42–43 (2012).

73. Szvircsev Tresch, T. *et al. Sicherheit 2018: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend* (Center for Security Studies (CSS), ETH Zürich; Militärakademie (MILAK) an der ETH Zürich, Birmensdorf, 2018).

74. Szvirczev Tresch, T., Wenger, A., Würmli, S., Pletscher, M. & Wenger, U. *Sicherheit. Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend. Editions for the years 2008 through 2017* (Center for Security Studies and Military Academy at the Federal Institute of Technology Zurich, Zurich, Switzerland, 2008).

75. Taylor, J. K., Clerkin, R. M., Ngaruiya, K. M. & Velez, A.-L. K. An Exploratory Study of Public Service Motivation and the Institutional–Occupational Model of the Military. *Armed Forces & Society* **41,** 142–162 (2015).

76. Warner, J. T. & Asch, B. J. The Record and Prospects of the All-Volunteer Military in the United States. *Journal of Economic Perspectives* **15,** 169–192 (2001).

77. Warner, J., Simon, C. & Payne, D. The Military Recruiting Productivity Slowdown: the Roles of Resources, Opportunity Cost and the Tastes of Youth. *Defence and Peace Economics* **14,** 329–342 (2003).

78. Werner, C. Gifts, Bribes, and Development in Post-Soviet Kazakstan. *Human Organization* **59,** 11–22 (2000).

79. Wrzesniewski, A. *et al.* Multiple Types of Motives Don't Multiply the Motivation of West Point Cadets. *Proceedings of the National Academy of Sciences* **111,** 10990–10995 (2014).

80. Yariv, D. *The Integration of High Ranks Retired Military Officers into the Civilian Sector and the Congruence Between Military and Civilian Careers (* unpublished master's thesis (Tel-Aviv University, Tel-Aviv, Israel, 1980).

Part III

Knowledge-Resource Absorption

'An investment in knowledge pays the best interest.'

— Benjamin Franklin

Knowledge Absorption for Cyber-Security

The Role of Human Beliefs

Percia David Dimitri[1,2]; Keupp Marcus[2]; Mermoud Alain[1,2]

[1] University of Lausanne, Faculty of HEC, Department of Information Systems
[2] ETH Zurich, Military Academy, Department of Defense Economics

Journal article under publication in *Computers in Human Behavior*

- Submitted on January 3, 2019;
- Revised (major revisions) and resubmitted on May 2, 2019;
- Revised (minor revisions) and resubmitted on September 3, 2019;
- Revised (minor revisions) and resubmitted on December 4, 2019;
- Accepted on January 7, 2020.

N.B.: For the purpose of harmonizing some technical notions throughout this thesis, minor adaptations were implemented.

Abstract

We investigate how human beliefs are associated with knowledge absorption for producing cyber-security. We propose a novel measure of knowledge absorption, by using the individual level of analysis. As organizational learning requires individual learning, we argue that knowledge absorption should be apprehended on the individual level and should focus on human interaction. Following this logic, cyber-security production might be associated with the extent to which organizations' members can absorb tacit knowledge required for this production. Framing this argument in the *knowledge-based view of the firm* and *transaction-cost economics*, we employ psychometric methods for analyzing a sample of 262 members of an information-sharing and analysis center. The results show that human beliefs are associated with individuals' knowledge absorption for producing cyber-security. Resource belief, knowledge-absorption belief, and reciprocity belief are associated with knowledge absorption. To the best of our knowledge, this is the first human-involved empirical contribution that analyzes knowledge absorption in a private setting, where sensitive information is shared and absorbed for producing the tacit-knowledge of cyber-security. We contribute to the *security economics* literature by emphasizing that cyber-security is not only a technical issue, therefore strengthening the proposition that economics and psychology are useful for producing cyber-security. Finally, we define paths for future research.

Keywords— cyber-security, security economics, information sharing, organizational learning, knowledge-based view, tacit knowledge, knowledge absorption.

Contents of Part III

1 Introduction

For both public and private organizations, effective cyber-security is required to prevent business interruption and thus to ensure operational continuity [51, 52, 59, 90, 130, 141]. The production of such cyber-security is a knowledge-intensive task [12, 71].[1] Despite the fact that hardware and software components required for this defense are relatively homogeneous and readily available at low cost or even for free [2, 68], highly specialist knowledge is required to combine and deploy these components effectively for organizational defense – for instance, by designing resilient systems architectures and implementing them efficiently [41, 84]. Hence, cyber-security is a complex capability that is not readily created by the purchasing of technological components; rather, it is the skilled knowledge of how to organize and orchestrate these components that creates the actual defense [2, 68, 148]. Furthermore, due to the swift technological evolution and short technology life-cycles of these components, knowledge required to produce cyber-security becomes obsolete [21, 26, 92, 153]. Organizations are hence under continuous pressure to update existing and acquire novel knowledge to keep up with the evolution of cyber-threats [11, 20, 21, 26, 32, 82, 92, 116, 120, 128, 138, 153].

Any organization that has to organize cyber-security might thus be interested in a continuous absorption of such specialist knowledge. Knowledge absorption is an organizational capability to transfer, integrate, and utilize new knowledge obtained from external sources [29, 60, 61, 106, 144].[2] Prior research suggests that if the organization succeeds at this knowledge absorption, the investment cost for any given level of information security is reduced [54], as are inefficient duplications of effort [46]. Furthermore, the effectiveness of security solutions improves [107, 119].

As organizations can absorb knowledge only by the learning of their existing members or the recruitment of new members [95, 127], our study of knowledge absorption puts the individual level of analysis to the fore. After all, it is humans who learn and develop specialist knowledge, and who use this knowledge to orchestrate the technical components for effective cyber-defense. Therefore, it is not surprising that recent research has emphasized

[1] In this article, the term *knowledge* refers to the established definition of [91]. In their seminal work, [91] proposed four different types of knowledge: (1) *know-what*, (2) *know-why*, (3) *know-how*, (4) *know-who*. (1) is related to knowledge about 'facts', and thus is close to what is generally called an 'information' – e.g., an individual who knows what a dynamic-programming algorithm is, has a knowledge that is classified as a *know-what* [91]. (2) refers to scientific knowledge. This kind of knowledge is central for technology development. An individual who knows how to develop a dynamic-programming algorithm, has a knowledge related to a *know-why* [91]. (3) is related to the capacity (i.e., skills) to do something. An individual who has a *know-why* is not necessarily competent when it comes to operationalize such a *know-why*. The capacity to translate a *know-why* into a concrete application is a knowledge that is classified as a *know-how*, even though a *know-how* does not necessarily presuppose a *know-why*. For instance, an individual who can successfully implement a dynamic-programming algorithm has a knowledge that is classified as a *know-how*. Typically, a *know-how* is developed and kept within organizations, giving them a competitive advantage [91]. Finally, (4) is related to social skills (i.e., 'soft skills'). *Know-who* is related to information about who knows what, as well as who knows how to do what. It involves the capacity to develop social relationships that ultimately enables to get access to and use their knowledge efficiently [91].

[2] The concept of *knowledge absorption* is well established in the literature. As early as 1989, Cohen and Levinthal proposed that performance differentials between firms can be traced to these firms' varying capabilities to absorb knowledge from beyond the boundary of the firm [29]. In a subsequent seminal article, they developed the concept of knowledge absorption as an organizational capability to 'recognize the value of new, external knowledge, assimilate it, and apply it to commercial ends.' [30]. As a result, there is now a large and mature theory of knowledge absorption on both the firm and the individual level of analysis (see [146], for an excellent meta-analysis). Any firm which lacks such a capability to absorb and integrate knowledge from sources beyond the boundary faces significant impediments as it attempts to innovate or perform better than the competition [133]. Grant [60, 61] expanded this firm-level argument to the individual level of analysis when he proposed that organizations can only realize such absorption by the individual efforts of their members – i.e., by the learning efforts of human beings – or by recruiting novel members who have specialized knowledge.

that any understanding of cyber-security is incomplete unless the association of individual action and cyber-security outcomes is studied [2, 3, 4, 57, 82]. However, few such studies exist to date. A recent overview of the related literature by Laube and Böhme [82] suggests that almost all research on cyber-security information exchange (and subsequent knowledge absorption) is characterized by the following limitations. First, the overwhelming majority of this literature does not analyze individuals, but analyzes impersonal information such as log-files [48, 49, 93, 96, 98]. Much literature is also restricted to pure game theory or simulation [23, 47, 54, 57, 63, 66, 80, 94, 125]. Second, a cyber-security context often requires sensitive and classified information that is unlikely to be shared or disseminated by public channels [13, 54, 66, 82, 99, 155]. Third, the knowledge required to build cyber-security is expert knowledge and hence is highly tacit, i.e., bound in personal experience.[3] Such tacit knowledge is not only hard to describe objectively (e.g., by documentation in manuals or textbooks), but it can also not readily be transferred among individuals, unless by intense social interaction between sender and recipient [103, 114, 126]. Although some work on cyber-security studies the transfer of explicit knowledge that can be documented in forums and databases (e.g., [158]) and [119]), we are not aware of any empirical work that would analyze the transfer and absorption of tacit knowledge in a cyber-security context. This lack of attention constitutes an important research gap [151]. Fourth and finally, even if the absorption of tacit knowledge requires human interaction, the social process alone does not necessarily imply that knowledge is actually absorbed. Human interaction can be futile if the possessor of any knowledge is unable or unwilling to transfer it to other individuals. To the best of our knowledge, the existing literature focuses on attitudes, motivations and contexts that influence an individual's propensity to (not) share information [73, 100, 111, 119, 137, 140, 149, 152, 160]. In contrast, we are not aware of any contribution that measures the extent to which (i.e., the success with which) actual knowledge absorption for cyber-security has occurred as a result of social interaction.

The purpose of our paper is to address all of these limitations. We study the extent to which an individual successfully absorbs knowledge in a private, collaborative setting in which sensitive, non-public and tacit knowledge required to build cyber-security is absorbed through information sharing. Hence, both the focus and the unit of analysis are on the individual level. Recent work has highlighted that the study of such collaborative-information sharing should lead to a better understanding of cyber-security [82]. We go one step further by not only studying elements associated with such information sharing, but also its outcomes in terms of individual knowledge absorption.

We first build a framework that is anchored in the knowledge-based view of the firm (KBV), arguing that the absorption of tacit knowledge is associated with human beliefs (Section 2). Using ordered probit regression, we then test this model with psychometric data from 262 members of the closed user group of MELANI-net, the national information sharing and analysis center (ISAC) in Switzerland (Section 3). Our results suggest that resource belief, usefulness belief, and reciprocity belief are positively associated with knowledge absorption, whereas belief in hard rewards is not (Section 4). We discuss the implications of our findings and provide recommendations for future research and managerial practice (Section 5).

[3] A *tacit knowledge* is distinguished from *codified knowledge* (i.e., classical knowledge) in the sense that *tacit knowledge* cannot be easily transferred through information infrastructures [126]. *Codified knowledge* is related to a process of conversion and reduction that simplifies the transmission, storage, verification and reproduction of knowledge [126]. As such, codified knowledge can be transferred across organizations at relatively low costs [35, 126]. In contrast with *codified knowledge*, *tacit knowledge* is notoriously difficult to transfer as it does not constitute an explicit kind of knowledge [35, 126]. Typically, the *know-how* and the *know-who* types of knowledge are rather implicit and therefore tacit [35, 126]. The only way to transfer *tacit knowledge* is to engage in social/human interaction [114].

2 Theoretical Framework and Hypotheses

In this section, we present our hypotheses related to potential associations between human beliefs and knowledge absorption.

The KBV suggests that knowledge is a valuable, scarce, and imperfectly imitable resource and hence is a significant source of competitive advantage for organizations [9, 50, 60, 61, 77, 102, 110, 131]. More specifically, specialist knowledge is a significant contributor to processes, products and/or services innovation [60, 61, 121, 122, 139]. Hence, an organization must continuously absorb specialist knowledge to be able to generate innovations that can provide cyber-security for its IT components and systems architecture.

Organizational knowledge absorption is the result of individual (i.e., human) learning. An organization absorbs knowledge only by the learning of its current members, or by the inclusion of new members [60, 61, 95, 127]. In this article, we focus on the learning of existing organization members.[4] In this perspective, novel organizational knowledge is created by the individual knowledge absorption of these members [14].

However, for any individual member, knowledge absorption from beyond the boundary of the organization is not a free activity. Typically, an individual incurs significant transaction costs before any economic exchange is completed. Such costs include time spent and financial resources dedicated to receiving information, making decisions, and the process of interacting with others [156]. In the context of an ISAC, these costs are incurred once the individual begins to interact with others, as intensive social interaction is required for a successful transfer of tacit knowledge between any two individuals [78, 103, 114, 135, 136]. Prior research also suggests that if information sharing takes too much time, is too laborious, or requires too much effort, an individual engages less in knowledge transfer, and the amount of knowledge transferred is reduced [39, 40, 90, 158]. Furthermore, the knowledge might be classified or irrelevant from the individual's perspective. We therefore propose that before making any specific assessment, the individual might estimate whether or not the knowledge present in the ISAC is generally worth the transaction cost required to absorb this knowledge. Unless this assessment is positive, the individual is unlikely to engage in any profound interaction at all.

2.1 H1: Resource Belief

When individuals must make such considerations, they typically use cues and heuristics to simplify the decision-making process [53, 109]. By such cues, objective and impersonal assessment is replaced by a subjective, belief-based assessment of whether or not the information to be received is useful at all [78, 114, 145]. Whenever such a belief is present, individuals are more prone to engage in social interactions that precede knowledge absorption [88]. Hence, knowledge absorption might be positively associated with the extent to which the individual believes the knowledge available in the ISAC constitutes a valuable, rare, and imperfectly imitable asset – i.e., a resource [9] – that is worth absorbing (resource belief). Hence,

H1: *Knowledge absorption is positively associated with resource belief.*

H1 is therefore related to the individual's belief that the transaction costs of knowledge sharing will be outweighed by the benefits that will come from such a social interaction (i.e., knowledge sharing); such benefits being concertized by knowledge absorption resulting from knowledge sharing.

[4] We consider the discussion of recruiting strategies for novel members beyond our scope, because this context would transcend both the individual level of analysis and the boundary of the firm. As a recall, recruiting strategies were analyzed in Part II of this thesis.

2.2 H2: Usefulness Belief

While this resource belief might induce the individual to interact with others at all, it does not necessarily imply the knowledge available is directly applicable for the specific job tasks the individual is charged with. For example, ISAC participants might exchange information that is useful to the industry or the organization in general, but that information might offer no specific guidance for any particular job task.

Prior research suggests that individuals do not necessarily act altruistically – i.e., only in the interest of the organization [101]. Goal-alignment theory suggests that individual and organizational goals are not necessarily congruent [70, 89]. Consequently, an individual would not only consider the general usefulness of any knowledge available from other ISAC members – i.e., whether or not this knowledge constitutes a resource that is worth the transaction cost – but also the extent to which this knowledge is specifically useful for any particular job task.

As the job performance evaluation of the individual might be considered as a specific contribution to organizational cyber-security, the individual has an incentive to study the specific usefulness of any information with this job-related assessment in mind [45, 90, 101]. Hence, knowledge absorption might be positively associated with the extent to which individuals believe the knowledge available in the ISAC specifically contributes to fulfilling their job tasks (usefulness belief). Hence,

H2: *Knowledge absorption is positively associated with usefulness belief.*

If H1 is related to the individual's fundamental assessment that determines if engaging in knowledge sharing is worth it (i.e., the transaction costs of such a social interaction will be outweighed by the benefits coming from the resulting knowledge absorption in general), H2 reaches one step further by suggesting that knowledge absorption might be useful for the individual's job tasks.

2.3 H3: Reward Belief

Further, goal alignment theory also suggests that the individual might choose to not disclose the specialist knowledge absorbed to other members of the organization. Typically, individuals align their behavior with their return goals; hence they expect to be rewarded whenever they exhibit behavior that is in the organization's interest [101].

Unless individuals believe that the organization will provide such rewards, they might choose to exploit their ISAC membership on an individual basis (e.g., by hoarding knowledge to make oneself irreplaceable in the organization, by starting up a firm or by selling private consultancy services to the industry). Hence, the individual would not absorb knowledge in the interest of the organization, but rather in the interest of private business. To solve this incentivization problem, organizations typically offer 'hard rewards' whenever knowledge is absorbed and shared for the benefit of the organization. Such rewards include job promotions, greater job security, salary increases, or more power and responsibility in the organization [14, 24, 74, 118]. For example, Buckman Laboratories distinguishes its 100-top information-sharers at an annual conference located at a resort [129]. Lotus Development, an IBM division, rewards employees for information sharing activities [33]. Prior research suggests that such rewards positively contribute to individuals' hours worked, dedication, and performance [38, 55].

Therefore, the more individuals believe they will receive such 'hard rewards' for successful knowledge absorption (reward belief), the more they should be likely to concentrate on realizing such absorption. Hence,

H3: *Knowledge absorption is positively associated with reward belief.*

If H2 is related to the individual's assessment that determines if engaging in knowledge sharing will help the fulfillment of their job tasks (i.e., the transaction costs of such a social interaction will be outweighed by the benefits coming from the resulting knowledge absorption in terms of job tasks fulfilment), H3 suggests that knowledge absorption might be fostered if such absorption is compensated by rewards delivered by the organization.

2.4 H4: Reciprocity Belief

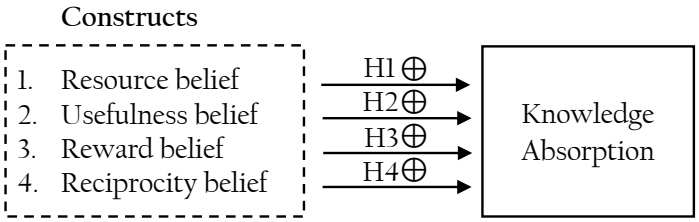
Given that knowledge is a valuable, scarce and imperfectly imitable resource [9, 50, 60, 61, 77, 102, 110, 131], the value of a unit of cyber-security knowledge is proportional to the incremental cyber-security enhancement that this unit is supposed to provide [15, 58]. As individuals are probably aware that any knowledge they share delivers such benefits to others, they might expect to receive adequate knowledge in return. Typically, humans prefer such equitable exchanges over any other arrangement [5, 16, 79], and they punish those who defect from this principle of equity or refuse to reciprocate when another individual provides something valuable [17, 43, 44, 143]. For example, reciprocal fairness is an important variable in the design of peer-selection algorithms in peer-to-peer (P2P) networks. As a result, the operators of such networks have developed ways to remove 'leechers' who demand information without providing any [150]. The extent to which an individual can absorb tacit knowledge by social exchange might depend on the extent to which this individual is willing to reciprocate whenever they receive information from others [157].

Therefore, unless the individual believes that original knowledge sharing will be reciprocated (reciprocity belief), they might terminate social interaction with others. As such interaction is a prerequisite of effective absorption, any prior level of knowledge absorption would significantly decrease. Hence,

H4: *Knowledge absorption is positively associated with reciprocity belief.*

The following illustration summarizes the different constructs – i.e., the set of independent variables and their respective hypothesis –, and emphasizes their association with the dependent variable, i.e., knowledge absorption.

Figure III.1: **Knowledge-Absorption Model**



Notes to Figure III.1: Each construct and its respective hypothesis (H1 to H4) are potentially positively associated with the dependent variable – i.e., knowledge absorption.

By testing the above-mentioned model, we suggest to explore with which intensity (if at all) the variable of *knowledge absorption* is associated with the individual's beliefs.

3 Data and Methods

In this section, we present the sampling context and population of this study, how we measured our independent variable, items and constructs, how we implemented the questionnaire in order to measure our items and constructs, as well as how we proceeded with our analysis.

3.1 Sampling Context and Population

As our theoretical reasoning focuses on knowledge absorption by social interaction, the sampling context must fit this research interest. We therefore collected our data from the closed user-group of MELANI-net – the Swiss national information sharing and analysis center (ISAC). An ISAC is a nonprofit organization that brings together cyber-security managers in person to facilitate interpersonal information exchange between critical-infrastructure providers (CIP).[5] Both the survey and the related dataset we exploit are identical to those described in [97].

This setting is particularly useful for our context as individuals in the closed user-group participate on behalf of their organizations, share highly sensitive and classified information in a private and exclusive setting, and interact socially as they share and absorb tacit knowledge. The 424 members of the closed user-group are all managers and specialists who must provide cyber-security for their respective organizations. They come from both private and public CIP. They have to undergo government identification and clearance procedures, as well as background checks before being admitted for ISAC membership. There is no interaction whatsoever between these members and the public, and no external communication to the public or any publication of relevant knowledge is made. Hence, this setting matches our proposition that the knowledge needed to produce cyber-security is not only classified and difficult to identify, but also tacit and grounded in personal experience, such that social interaction between individuals is required to transfer it.

Whenever a particular individual has shared information about a threat that is of interest to other members of this closed user group, individuals can contact each other by an internal message board. They do so by commenting on the initial information shared, in order to establish a first contact that then leads to further social exchange between the individuals. Once contact is made by a short reply about the threat information, to share detailed security information, the individuals involved in the conversation meet on their own initiative (e.g., informally over lunch, in group meetings, or small industry-specific conferences, but always from an individual to another). Each individual decides for themselves if they want to meet, with whom, and by what means. They also freely decide about the extent of the information shared (if any). MELANI-net officials neither force nor encourage individuals to interact; both in terms of social interaction in general and regarding the sharing of any particular unit of information.

3.2 Measures

Our study follows individuals who self-report about their beliefs. We therefore chose a psychometric approach to operationalize our constructs [104].

Dependent Variable

We introduce a novel ordinal indicator to capture individual knowledge absorption. It asks respondents to state which amount of exclusive information they receive through security information exchange with the other participants inside the ISAC. We believe that this operationalization is congruent with the concept of knowledge absorption for the following reasons.

Information processing research in both business research, information science and mathematics suggests that knowledge is created from information. More specifically, knowledge emerges from information by purposeful combination of such information inside the individual's mind [67, 76, 85, 103]. Our construct takes this precedence into account

[5] For a general introduction to the concept of an ISAC and illustrative examples, see [115] and [40]. For a detailed description of MELANI-net, its organization and history, see [22].

by asking the respondent to concentrate on the specialist information provided by others. Unless such information is provided by others in the first place (i.e., if absorption fails), the individual lacks relevant information, such that the desired knowledge cannot be constructed. In essence, knowledge absorption requires the combination of external, new information with internal, existing knowledge [154].

Moreover, tacit knowledge – on which our article focuses since it is this type of knowledge that is primarily required to build cybersecurity – must rely on rare, valuable and 'hard to get' knowledge outside the boundary of the firm. Our construct takes this point into account by putting 'exclusive' information to the fore that cannot be obtained unless by social interaction with other ISAC participants. We thus capture two important aspects of knowledge absorption: The knowledge in question is located beyond the boundary of the firm, and some human activity is required to absorb it.

Finally, our measure incorporates a third important aspect, namely the idea that absorption must be effective. The respondent states the extent to which they receive knowledge from others. That implies the transfer has been successful, i.e., the individual has obtained and understood information. This effectiveness aspect of knowledge absorption is highlighted by [159] who note that a measure of knowledge absorption should not just focus on the context and process of absorption – on which the majority of the knowledge absorption literature concentrates – but should also take the effectiveness of the transfer into account.

Our empirical measure is an ordinal indicator that can take on five discrete values. The respondent uses this indicator to estimate the extent to which they have received exclusive knowledge as a result of interacting with the other participants inside the ISAC. One might think of this indicator as a percentage calculation: Take all the exclusive information a given individual receives during a particular time-frame. What percentage of that exclusive information was obtained as a result of interacting with others inside the ISAC? Hence, it is not an *individual* perception, attitude or belief that is recorded, but rather a performance figure. As our pre-tests suggested that the individual might find it difficult to provide exact percentage figures, we specified broader value categories instead.

It is worthwhile to note that there is a dearth of empirical measures for knowledge absorption by individuals in the literature, and therefore we believe that our paper makes an empirical contribution in this respect. The majority of the literature on knowledge absorption has focused on organizational absorption, i.e., it has taken the firm as the unit of analysis. As a result, many extent empirical measures of knowledge absorption are proxy measures that are detached from individual (human) action. Examples of such measures are the firm's R&D intensity [29, 30], patent cross-citation indicators [56, 108], or the number of engineers the firm employs [72].

The problem with these measures is that they do not take into account that it is human beings – and not organizations – who absorb knowledge. Even if they do, they focus on organizational context, disposition, and behavior, but not on realized absorption. For example, the multi-item scale proposed by Ter Wal et al. [137] focuses on the individual disposition towards knowledge absorption and the extent to which the individual engages in social interaction congruent with this disposition. By contrast, this scale does not consider the extent to which knowledge absorption actually occurs, i.e., the extent to which the individual actually receives information and realizes actual absorption.

Hence, we believe that while our proposed indicator is far from being perfect or exhaustive, it can capture individual knowledge absorption and thus can possibly provide a steppingstone for future researchers who might build on and expand our approach.

Constructs

To measure the different beliefs we hypothesized, extant psychometric scales were used. Adaptions of these scales to our population context were kept to a minimum. Table III.1 on page 110 details all constructs, their sources, item composition and wording, dropped items (if any), factor loadings; and Cronbach alphas.

Controls

To capture respondent heterogeneity, we controlled for gender, age, and education level. Gender was coded dichotomously (male, female). Age was captured by four mutually exclusive categories (21-30, 31-40, 41-50, 50+ years). Education level was captured by six mutually exclusive categories (none, bachelor, diploma, master, PhD, other).[6]

We further captured the respondent's hierarchical position in the organization (employee, chief employee – i.e., intermediary supervisor position –, middle management, management, member of the board, other), as this position might influence both the propensity of sharing knowledge as such, and the intensity with which knowledge is actually shared [18].

We also controlled for the number of years the individual had experience with collaborative-information sharing (prior information sharing experience: not in charge, less than 1, 1 to 3, 3 to 6, over 6), as such experience is significantly associated with information sharing intention [83].

Further, the extent to which the respondent can absorb knowledge can co-evolve with the length of ISAC membership, as individuals gain more insight over time and develop interpersonal relationships. Hence, we controlled for membership duration and calculated it as the difference between 2017 and the year the individual became an ISAC member.

Also, individual experience from past social interactions can influence the respondent's beliefs [64, 147]. We therefore asked respondents to state whether or not they had already participated in prior ISAC meetings and events (dichotomously coded yes/no).

Sympathy and antipathy in peer relations might influence the extent to which individuals interact and learn; hence, the quality of any peer relation might influence the extent to which knowledge absorption can occur [27, 31]. We therefore asked respondents to rate their individual perception of the personal relationships they had with their peers among ISAC members (very friendly, friendly, neutral, unfriendly, very unfriendly).

We also asked respondents to rate their potential individual contribution by indicating the extent to which they felt they (generally) had much information to share (strongly agree, agree, neutral, disagree, strongly disagree). We insert this control into the model as an individual's intention to share knowledge might be associated with how much the individual knows already. Further, individuals who have little to share might receive less information from their peers as these feel less compelled to reciprocate if they receive little in the first place [25, 34].

Finally, we controlled for the industry heterogeneity (government, banking/finance, energy, health, all other industries) by logging each respondent's self-reported affiliation. This information was used to construct dichotomous indicators ('dummy variables') that group respondents into the five industry categories, government, banking & finance, energy, health, and all other industries. Each dummy variable takes on the value 1 if a respondent is affiliated with a particular industry, and has a value of 0 otherwise.

[6] For instance, an individual who has a master's degree has necessarily a bachelor's degree, and therefore will be flagged only in the master's degree category. The term *diploma* refers to the Swiss *CFC*, i.e., a *Federal Certificate of Competence*, which is a diploma awarded for an apprenticeship of 3 to 4 years and successful completion of a final examination.

3.3 Implementation

Data for all variables was collected from individual respondents by a questionnaire instrument. We followed the procedures and recommendations of Dillman, Smyth, and Christian [37] for questionnaire design, pretest, and implementation. Likert-scaled items were anchored at 'strongly disagree' (1) and 'strongly agree' (5) with 'neutral' as the midpoint (3). The questionnaire was first developed as a paper instrument. It was pretested with seven different focus groups from academia and the cyber-security industry. The feedback obtained was used to improve the visual presentation of the questionnaire and to add additional explanations. This feedback also indicated that respondents could make valid and reliable assessments. Within the closed user-group, both MELANI-net officials and members communicate with each other in English. Switzerland has four official languages, none of which is English, and all constructs we used for measurement were originally published in English. We therefore chose to implement the questionnaire in English to rule out any back-translation problems. Before implementation, we conducted pretests to make sure respondents had the necessary language skills. The cover page of the survey informed respondents about the research project and our goals, and it also made clear that we had no financial or business-related interests. We followed Podsakoff et al.[112], as far as this was possible for a cross-sectional research design, to alleviate common method bias concerns from the onset.

The paper instrument was then implemented as a web-based survey by using the *Select-Survey* software provided by the Swiss Federal Institute of Technology Zurich (ETH). For reasons of data security, the survey was hosted on the proprietary servers of this university. The management of MELANI-net invited all closed user-group members to respond to the survey by sending an anonymized access link, such that the anonymity of respondents was guaranteed at all times. Respondents could freely choose whether or not to reply. As a reward for participation, respondents were offered, free of charge, a research report that summarized the responses. Respondents could freely choose to save intermediate questionnaire completions and to return to the survey and complete it at a later point in time.

The online questionnaire and the reminders were sent to the population by the Deputy Head of MELANI-net, together with a letter of endorsement. The survey link was sent in an e-mail describing the authors, the data, contact details for IT support, the offer of a free report, and the scope of our study. Data collection began on October 12, 2017 and ended on December 1, 2017. Two reminders were sent on October 26 and November 9, 2017. Of all 424 members, 262 had responded when the survey was closed, for a total response rate of 62%.

3.4 Analysis

Upon completion of the survey, the data were exported from the survey server, manually inspected for consistency, and then converted into a *STATA* dataset (Vol. 15) on which all further statistical analysis was performed. Post-hoc tests suggested no significant influence of response time on any measure. There was no significant over-representation of individuals affiliated with any particular organization, thus suggesting no need for a nested analytical design.

By calculating item-test, item-rest, and average inter-item correlations, the validity of each construct was tested [65]. The reliability was measured by Cronbach alpha. We performed iterative principal component factor analysis with oblique rotation until total variance explained was maximized and each item clearly loaded on one factor. During this process, four items were dropped because they did not meet these criteria. Table III.2 on page 111 details the results of this procedure, and Table III.1 on page 110 documents the

dropped items. The high direct factor-loadings and low cross-loadings of the final four factors we identified indicate a high degree of convergent validity [65]. All of these have an eigenvalue above unity. The first factor explained 19.1% of the total variance, suggesting the absence of significant common method variance in the sample [113]. To construct the scale values, individual item scores were added, and this sum was divided by the number of items in the scale [117, 142].

Our dependent construct is ordered and categorical, therefore we estimated an ordered probit model. A comparison with an alternative ordered logit estimation confirmed the original estimations and indicated that the ordered probit model slightly better fit the data. The model was estimated with robust standard errors to neutralize any potential heteroscedasticity. For the controls age, industry, and education, a benchmark category was automatically selected during estimation (cf. footnote *b* of Table III.5 on page 113). Consistent with the recommendation of Cohen et al. [28], we incrementally built all models by entering only the controls in a baseline model first, then, we added the main effects. In both estimations, we mean-centered all measures before entering them into the analysis. Model fit was assessed by repeated comparisons of Akaike and Bayesian information criteria between different specifications.

4 Results

Table III.3 on page 111 provides summarized descriptive statistics . 95% of respondents are male, 32% are below and 68% above the age of 40. Practitioners without a formal degree constitute 20% of the sample, whereas 68% have a certificate of competence or a bachelor degree. Only 4.6% have a master degree or a PhD. The majority of the sample is composed of two groups: employees or intermediate supervisors (42% of respondents), and middle or line managers (51%). Only 2.7% are top managers or board members. 43% of respondents have up to three years of experience with collaborative information sharing, and 48% have more than three years of such experience. 52% had already participated in one of more prior ISAC meetings or event.

Since our dependent variable is ordinal, a monotonic correlation analysis is necessary. Moreover, data for ordinal variables need not be distributed normally. Table III.4 on page 112 therefore provides Spearman rather than Pearson correlations. For the sake of brevity, correlates for controls are omitted. Table III.5 on page 113 documents the final best-fitting model, together with its diagnostic measures.

H1 is supported. Resource belief is positively associated with knowledge absorption at $p < 0.05$. This suggests that whenever an individual believes valuable knowledge can be acquired, they are more willing to invest the transaction cost for tacit knowledge absorption and are able to absorb such knowledge to a greater extent.

H2 is supported. Usefulness belief is positively associated with knowledge absorption at $p < 0.01$. This finding is in line with our theoretical expectation that individuals seek knowledge absorption not for its own sake, but in order to augment the efficiency and effectiveness of their cyber-security production.

H3 is not supported. Reward belief is not significantly associated with knowledge absorption. In context with the above findings for H1 and H2, this signals that the individual's decision to participate in a knowledge-transfer process is primarily intrinsically motivated. Moreover, this non-finding might be due to the fact that Wang and Hou [152] introduce their measure of reward belief (which we adapted for our study) in the context of public information-sharing and absorption, implying that in a private setting of knowledge absorption, intrinsic motivations for absorption might outweigh extrinsic ones.

H4 is supported. Reciprocity belief is significantly associated with the extent to which

the individual absorbs knowledge at $p < 0.01$. This finding is in line with our theoretical expectation that knowledge absorption is ultimately the result of reciprocated human interaction.

Although all control variables and industry dummy variables capture variance, only one of them is significant at $p < 0.05$. We find that knowledge absorption is not associated with an individual's job position, prior information-sharing experience, size of the organization that employs an individual, quality of peer relationships, potential individual contribution, an individual's gender, age, education level, industry affiliation, or length of ISAC membership. These non-findings do not only alleviate concerns about unobserved heterogeneity among respondents, but the non-significance of the industry dummies also alleviates concerns of over-representation of a particular industry or firm among the responses.

The one significant effect we do find suggests that participation in prior ISAC events (such as group meetings, conferences, and industry-specific talks) is positively associated with knowledge absorption. This finding suggests that knowledge absorption positively evolves over time, as individuals build social relationships during such events.

5 Discussion

In this last section, we present our concluding comments, the policy recommendations resulting from concluding comments, we discuss the limitations of this study and suggest paths for further research.

5.1 Concluding comments

In this article, we argue that the production of organizational cyber-security is associated with the extent to which the members of this organization, i.e., human beings, can absorb the tacit knowledge required for this production. Framing this argument in the knowledge-based view of the firm and transaction cost economics, we empirically show that human beliefs are significantly associated with the extent to which an individual absorbs knowledge.

To the best of our knowledge, our study is the first empirical contribution that analyzes knowledge absorption in a private setting, where sensitive knowledge required for cyber-security products and services is shared and absorbed. Prior to our approach, scholars analyzed human interaction in the context of cyber-security, but almost exclusively in public settings. We develop this empirical literature by focusing on tacit knowledge-transfer in a private setting, thus suggesting this research design corresponds more closely with both the type of knowledge required to produce cyber-security and the transmission channels by which this sensitive and classified knowledge is shared.

We also contribute to filling the significant gap that Laube and Böhme [82] note in their tabulation of the recent literature. Through this research, we help to extend the literature on the economics of information security by suggesting that cyber-security is not solely a technical issue. Whereas many technological solutions to cyber-security have been proposed, few of these are successful unless an economic perspective is adopted [2, 4]. Our study therefore strengthens the proposition that interdisciplinary approaches which attempt to integrate thinking from economics and psychology when considering cyber-security are useful [4, 52]. For the same reason, we suggest that a proper understanding of subjective human beliefs and behaviors can complement the analysis of objective data such as log files. We argue that humans consider the transaction costs of knowledge absorption before they engage in any related activities. We therefore caution future research from depicting humans as neutral 'tools' that work only for the production of a public good or social welfare [58]. Instead, in this study, we contribute to resolving the paradox that humans are

often reluctant to provide cyber-security knowledge, despite the fact that they are aware that the absorption of this knowledge by others is conducive to producing individual and collective cyber-security [39, 40, 54, 57, 100].

We propose to interpret effective knowledge absorption as the result of a multi-stage decision-making process. Our findings suggest that individuals first consider the transaction cost of social exchange that precedes knowledge absorption (resource belief). If this decision is affirmative, they begin social interaction, absorb some first knowledge elements, and assess the extent to which these are relevant for their job tasks (usefulness belief). Once they believe so, they likely adapt their social behavior in order to facilitate further knowledge absorption, i.e., they reciprocate to maintain the exchange process (reciprocity belief). As a result, collaborative and collective knowledge sharing perpetuates. While we can only propose such a process, and while we cannot establish any sequential or causal order with the data we have, future research might test this proposition from a longitudinal perspective.

5.2 Considerations for Policy Recommendations

Our results also have implications for ISAC managers. The organizational design of an ISAC is relevant as it influences the behavior of the participants [124]. ISAC managers can attempt to increase participation rates by emphasizing that, in their ISAC, transaction costs of participation are low, participants bring valuable knowledge assets to the table, and interpersonal exchange is facilitated. At the same time, they should be careful to reduce transaction costs by only novel, technology-enabled forms of organization. For example, recommendations to construct distributed ISACs by adopting methods from cryptology and secure distributed computation (e.g., Ezhei and Ladani [42]) might be useful if the goal is the quick absorption of explicit knowledge. However, the high demands that tacit knowledge absorption puts on the intensity of social, i.e., close interactions of individuals might reduce the value of such technology-based solutions. Hence, and somewhat ironically, the more sensitive the technological knowledge is to cyber-security, the less likely this knowledge will be shared inside the cyber-sphere.

Also, the specialists who absorb knowledge by participating in ISAC meetings and other forms of social exchange do not need to be the same people as those who are generally in charge of organizing the production of cyber-security. Our results should caution those who organize the production of cyber-security to not rely on monetary or career incentives as they attempt to give incentives to the group. Although many organizations have created reward systems to encourage their employees to share information with others [10], we find no support for the hypothesis that knowledge absorption is associated with reward belief. Hence, goal alignment between individual and organizational interests is unlikely to be produced by the promise of monetary and career rewards. Hence, managers should concentrate on measures that reduce transaction cost by facilitating social exchange, helping to establishing long-term human relationships, and emphasizing the usefulness of knowledge absorption for the individual's personal job.

5.3 Limitations and Paths for Further Research

Finally, our research design has some limitations that future research could help relax.

First, we studied a single, centrally organized ISAC in one country. Hence, future research should generalize our approach to alternative models of ISAC organizations and explore diverse national and cultural settings by replicating our study with different ISACs and nation states. We believe our approach is conducive to such generalization as neither our theoretical framework, nor any one of our measurement constructs, nor the empirical measures we used to operationalize these are context specific to any particular national

or cultural context. Our measures and the theory in which they are grounded represent fundamental aspects of human economic decision-making that, in our view, should apply globally. At the same time, this focus implies a limitation of scope. Our study does not deliver a multidimensional account of information sharing, nor do we attempt to introduce dyadic settings. Our perspective is that of an individual who self-reports on the extent to which they have realized knowledge absorption. Future work could therefore build on our approach by studying dyadic aspects of knowledge absorption.

Second, much prior research analyzed associations between human attitudes and intentions on the one hand and human behavior on the other hand [73, 111, 119, 152]. Although this research is useful, our study goes one step further by associating beliefs with a performance outcome on the individual level, i.e., the extent to which an individual has effectively absorbed knowledge as a result of the social exchange with other ISAC participants. Future studies could continue our line of work by expanding our setting to the organizational level of analysis, studying how and why tacit knowledge, individually absorbed, contributes to the production of organizational cyber-security. Furthermore, the organizational context could moderate or even impede this production as the 'not-invented- here' syndrome could obstruct the integration of knowledge from beyond the boundary of the firm into the internal cyber-security production processes [7, 8, 69, 75, 87], as could political divergences, processual impediments, and organizational bureaucracy. Today, the microfoundations of the organizational processes by which individually acquired tacit cyber-security knowledge is combined with other knowledge assets and material resources into actual cyber-security are largely unknown. Future research might study both the resource configuration and the combination process of these assets to a greater extent in order to bridge the research gap between individual knowledge absorption and organizational cyber-security.

Third, the ability of our dependent construct to measure effective knowledge absorption is limited. While we believe this measure is useful to capture individual absorption, it is also an ordinal indicator. If knowledge absorption is the organizational (or individual) capability to transfer, integrate, and utilize new knowledge obtained from external sources [29, 60, 61, 106, 144], a more profound measurement approach should reflect such terms, e.g., by considering the transfer, integration, and use of information. Moreover, the measure represents not an objective performance figure, but an individual perception of a quantity. Future research should therefore expand and refine our measure. For example, receiving exclusive information through security-information exchange is a necessary but not sufficient condition for effective knowledge absorption, as an integration of the newly absorbed information with prior individual knowledge is required [67, 76, 85, 103]. Future measures could take such differences between initial absorption and intra-organizational transfer of knowledge into account. However, as such a multi-step process of absorption cannot be readily measured by psychometric methods, our dependent measure should be seen as a first step towards providing such full measurement. Furthermore, we suggest that any such future measures should be conceptualized on the individual level of analysis, as individual learning typically precedes organizational learning. While our ordinal indicator of knowledge absorption is far from being exhaustive, it is worthwhile to note that few empirical measures study individual absorption. Much work still uses measures defined at the organizational level, such as R&D intensity [19, 29, 30, 62, 86, 123], patent cross-citation indicators [56, 108] or the number of engineers the firm employs [72].

Fourth, by adopting a factor analysis and psychometric methodologies that capture data in a single period, this research is based on a cross-sectional framework, implying we could only identify associations, but not causal links [6]. Thus, future research should study the interaction of ISAC members over time, e.g., by using time-series regressions that link knowledge-absorption outcomes in later periods to interactions in prior periods [1, 36, 132].

Table III.1: **Constructs**

Measure [Publication]	Type	Item	Text	Fact. l.	Cr. α
Dependent					
Knowledge absorption	Ordered categorical indicator	n/a	Which amount of exclusive information do you receive through security information exchange with MELANI?	n/a	n/a
(Novel)			* Very Small * Small * Neutral * Large * Very Large		
Independent					
Resource belief ([105])	Likert scale	RES1	I believe that people in my network give credit for each other's knowledge where it is due	dropped	0.82
		RES2	I believe that people in my network respond when I am in need	0.81	
		RES3	I believe that people in my network use each other's knowledge appropriately	0.82	
		RES4	I believe that my requests for knowledge will be answered	0.86	
		RES5	I believe that people in my network share the best knowledge that they have	dropped	
Usefulness belief ([134])	Likert scale	US1	SIS would decrease the time needed for my job responsibilities	0.85	0.71
		US2	SIS would increase the effectiveness of performing job tasks	0.86	
		US3	Considering all aspects, SIS would be useful	0.64	
Reward belief ([152])	Likert scale	HR1	I expect to be rewarded with a higher salary in return for sharing knowledge with other participants	0.91	0.81
		HR2	I expect to receive monetary rewards (i.e., additional bonus) in return for sharing knowledge with other participants	0.90	
		HR3	I expect to receive opportunities to learn from others in return for sharing knowledge with other participants	dropped	
		HR4	I expect to be rewarded with an increased job security in return for sharing knowledge with other participants	0.73	
Reciprocity belief ([81])	Likert scale	NOR1	I believe that it is fair and obligatory to help others because I know that other people will help me some day	dropped	0.8
		NOR2	I believe that other people will help me when I need help if I share knowledge with others through MELANI	0.82	
		NOR3	I believe that other people will answer my questions regarding specific information and knowledge in the future if I share knowledge with others through MELANI	0.87	
		NOR4	I think that people who are involved with MELANI develop reciprocal beliefs on give and take based on other people's intentions and behavior	0.79	

Table III.2: **Final Set of Factor Loadings After Oblique Rotation** [a]

Item	Loading on oblimin-rotated factor				
	factor 1	factor 2	factor 3	factor 4	uniqueness
HR1	0.91				0.14
HR2	0.90				0.18
HR4	0.73				0.44
US1				0.85	0.26
US2				0.86	0.22
US3				0.64	0.39
NOR2			0.82		0.26
NOR3			0.87		0.21
NOR4			0.79		0.36
RES2		0.81			0.28
RES3		0.82			0.28
RES4		0.86			0.24
Eigenvalue	2.29	2.29	2.22	1.94	
Proportion of variance explained	19.10%	19.05%	18.48%	16.20%	
Cumulative variance explained	19.10%	38.16%	56.64%	72.84%	

[a] Blank cells represent factor loadings (x) such as $|x| < 0.3$.

Table III.3: **Descriptive Statistics**

Variable	Obs	Mean	Std. Dev.	Min	Max
Knowledge absorption	260	3.13	0.86	1	5
Resource belief	190	3.82	0.52	1.67	5
Usefulness belief	208	3.78	0.62	1.67	5
Reward belief	195	2.16	0.75	1	4
Reciprocity belief	195	3.89	0.61	1.67	5
Size of the organization	260	4.57	0.90	1	5
Quality of peer relationships	260	3.93	0.70	3	5
Potential individual contribution	243	3.07	0.91	1	5
Membership duration	260	6.05	5.35	0	17

Table III.4: **Correlation Analysis** [a]

	Knowledge absorption	Resource belief	Usefulness belief	Reward belief	Reciprocity belief
Knowledge absorption	1				
Resource belief	0.2860^{***}	1			
Usefulness belief	0.2779^{***}	0.2042^{**}	1		
Reward belief	0.0258	−0.1568	−0.0602	1	
Reciprocity belief	0.3543^{***}	0.3500^{***}	0.2489^{***}	−0.0001	1

[a] ρ: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Table III.5: **Results of Model Estimation** (Ordered Probit Regression) [a, b]

Knowledge absorption		
Constructs	**coefficient**	**(robust std. error)**
Resource belief	0.4256*	(0.1695)
Usefulness belief	0.4167**	(0.1601)
Reward belief	0.0973	(0.1203)
Reciprocity belief	0.4012**	(0.1525)
Control variables		
Position in the organization	−0.0769	(0.0567)
Prior information sharing experience	−0.1285	(0.0934)
Size of the organization	0.0412	(0.0916)
Participation in prior ISAC events	0.4267*	(0.2000)
Quality of peer relationships	0.3066	(0.1706)
Potential individual contribution	−0.0377	(0.1009)
Gender	0.4955	(0.3388)
Age 21-30	0.0116	(0.4230)
Age 31-40	−0.3392	(0.2386)
Age 41-50	−0.3595	(0.2060)
Education none	−0.2416	(0.4354)
Education Master	−0.0153	(0.4207)
Education Bachelor	−0.1350	(0.4003)
Education PhD	−0.4339	(0.4700)
Membership duration	−0.0130	(0.0196)
Government	0.5862	(0.3693)
Banking & Finance	0.5474	(0.3486)
All other industries	0.5160	(0.3636)
Energy	0.5717	(0.3900)
Health	0.4981	(0.4362)
Log pseudolikelihood	−204.23	
Pseudo R^2	0.1385	
Wald χ^2 *(24 d.f.)*	83.95	
$p>\chi^2$	0.000***	
Observations [c]	188	

[a] Two-tailed tests: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.
[b] Age category "above 50", education category "other" and the IT industry serve as respective control variable benchmarks.
[c] The difference between the number of respondents (= 262) and the number of observations of the model (= 188) is due to our conservative estimation approach that prefers list-wise deletion over imputation or modification.

References

1. Amemiya, T. *Advanced Econometrics* (Harvard university press, 1985).
2. Anderson, R. *Why Information Security is Hard – an Economic Perspective* in *Seventeenth Annual Computer Security Applications Conference* Annual Computer Security Applications Conference (ACSAC) (IEEE, New Orleans, USA, 2001), 358–365. ISBN: 0-7695-1405-7.
3. Anderson, R. & Fuloria, S. in *Economics of Information Security and Privacy* (eds Moore, T., Pym, D. & Ioannidis, C.) 55–66 (Springer, Boston, USA, 2010). ISBN: 978-1-4419-6967-5.
4. Anderson, R. & Moore, T. The Economics of Information Security. *Science* **314,** 610–613 (2006).
5. Andreoni, J. Cooperation in Public-Goods Experiments: Kindness or Confusion? *The American Economic Review* **85,** 891–904 (1995).
6. Antonakis, J., Bendahan, S., Jacquart, P. & Lalive, R. On Making Causal Claims: A Review and Recommendations. *The Leadership Quarterly* **21,** 1086–1120 (2010).
7. Antonelli, C. Localized Technological Change, New Information Technology and the Knowledge-Based Economy: The European Evidence. *Journal of Evolutionary Economics* **8,** 177–198 (1998).
8. Antons, D. & Piller, F. T. Opening the Black Box of "Not Invented Here": Attitudes, Decision Biases, and Behavioral Consequences. *Academy of Management Perspectives* **29,** 193–217 (2015).
9. Barney, J. Firm Resources and Sustained Competitive Advantage. *Journal of Management* **17,** 99–120 (1991).
10. Bartol, K. M. & Srivastava, A. Encouraging Knowledge Sharing: The Role of Organizational Reward Systems. *Journal of Leadership & Organizational Studies* **9,** 64–76 (2002).
11. Bauer, J. M. & van Eeten, M. J. G. Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options. *Telecommunications Policy* **33,** 706–719 (2009).
12. Ben-Asher, N. & Gonzalez, C. Effects of Cyber Security Knowledge on Attack Detection. *Computers in Human Behavior* **48,** 51–61 (2015).
13. Bisogni, F. *Data Breaches and the Dilemmas in Notifying Customers* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'15)* Workshop on the Economics of Information Security (WEIS'15) (Delft, Netherlands, 2015).
14. Bock, G. W. & Kim, Y.-G. Breaking the Myths of Rewards: An Exploratory Study of Attitudes about Knowledge Sharing. *Information Resources Management Journal (IRMJ)* **15,** 14–21 (2002).
15. Bodin, L. D., Gordon, L. A., Loeb, M. P. & Wang, A. Cybersecurity Insurance and Risk-Sharing. *Journal of Accounting and Public Policy* **37,** 527–544 (2018).
16. Bolton, G. E. & Ockenfels, A. ERC: A Theory of Equity, Reciprocity, and Competition. *American Economic Review* **90,** 166–193 (2000).
17. Brosnan, S. F. & de Waal, F. B. M. Monkeys reject unequal pay. *Nature* **425,** 297–299 (2003).
18. Cai, S., Goh, M., De Souza, R. & Li, G. Knowledge Sharing in Collaborative Supply Chains: Twin Effects of Trust and Power. *International Journal of Production Research* **51,** 2060–2076 (2013).

19. Camisón, C. & Forés, B. Knowledge Absorptive Capacity: New Insights for its Conceptualization and Measurement. *Journal of Business Research* **63,** 707–715 (2010).

20. Cardenas, A. A., Manadhata, P. K. & Rajan, S. P. Big Data Analytics for Security. *IEEE Security & Privacy* **11,** 74–76 (2013).

21. Casas, P., Soro, F., Vanerio, J., Settanni, G. & D'Alconzo, A. *Network Security and Anomaly Detection With Big-DAMA, a Big Data Analytics Framework* in *IEEE 6th International Conference on Cloud Networking (CloudNet'17)* IEEE 6th International Conference on Cloud Networking (CloudNet'17) (2017), 1–7.

22. Cavelty, M. D. *Cybersecurity in Switzerland* ISBN: 978-3-319-10620-5 (Springer, Cham, Switzerland, 2014).

23. Cavusoglu, H., Raghunathan, S. & Yue, W. T. Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems* **25,** 281–304 (2008).

24. Centers, R. & Bugental, D. E. Intrinsic and Extrinsic Job Motivations Among Different Segments of the Working Population. *Journal of Applied Psychology* **50,** 193–197 (1966).

25. Chang, H. H. & Chuang, S.-S. Social Capital and Individual Motivations on Knowledge Sharing: Participant Involvement as a Moderator. *Information & Management* **48,** 9–18 (2011).

26. Chen, H., Chiang, R. H. L. & Storey, V. C. Business Intelligence and Analytics: From Big Data to Big Impact. *MIS Quarterly* **36,** 1165–1188 (2012).

27. Chow, W. S. & Chan, L. S. Social Network, Social Trust and Shared Goals in Organizational Knowledge Sharing. *Information & Management* **45,** 458–465 (2008).

28. Cohen, J., Cohen, P., West, S. G. & Aiken, L. S. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences* 3rd ed. ISBN: 978-0-8058-2223-6 (Taylor & Francis, Didcot, UK, 2002).

29. Cohen, W. M. & Levinthal, D. A. Innovation and Learning: The Two Faces of R&D. *The Economic Journal* **99,** 569–596 (1989).

30. Cohen, W. M. & Levinthal, D. A. Absorptive Capacity: A New Perspective on Learning and Innovation. *Administrative Science Quarterly* **35,** 128–152 (1990).

31. Coolahan, K., Fantuzzo, J., Mendez, J. & McDermott, P. Preschool Peer Interactions and Readiness to Learn: Relationships Between Classroom Peer Play and Learning Behaviors and Conduct. *Journal of Educational Psychology* **92,** 458 (2000).

32. Cui, B. & He, S. *Anomaly Detection Model Based on Hadoop Platform and Weka Interface* in *10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'16)* 10th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS'16) (2016), 84–89.

33. Davenport, T. H. & Glaser, J. Just-in-Time Delivery Comes to Knowledge Management. *Harvard business review* **80,** 107–111 (2002).

34. Davenport, T. H., Prusak, L., *et al. Working Knowledge: How Organizations Manage What They Know* (Harvard Business Press, 1998).

35. David, P. A. Knowledge, Property, and the System Dynamics of Technological Change. *The World Bank Economic Review* **6,** 215–248 (1992).

36. Davidson, R., MacKinnon, J. G., *et al.* Estimation and Inference in Econometrics. *OUP Catalogue* (1993).

37. Dillman, D. A., Smyth, J. D. & Christian, L. M. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method* 4th ed. ISBN: 978-1-118-45614-9 (John Wiley & Sons, Hoboken, USA, 2014).

38. Encinosa, W. E., Gaynor, M. & Rebitzer, J. B. The Sociology of Groups and the Economics of Incentives: Theory and Evidence on Compensation Systems. *Journal of Economic Behavior & Organization* **62,** 187–214 (2007).

39. ENISA. *Incentives and Barriers to Information Sharing* (European Union Agency for Network and Information Security, Heraklion, Greece, 2010).

40. ENISA. *Information Sharing and Analysis Centres (ISACs): Cooperative Models* (European Union Agency for Network and Information Security, Attiki, Greece, 2018).

41. Etzioni, A. Cybersecurity in the Private Sector. *Issues in Science and Technology* **28,** 58–62 (2011).

42. Ezhei, M. & Ladani, B. Information Sharing vs. Privacy: a Game Theoretic Analysis. *Expert Systems with Applications* **88,** 327–337 (2017).

43. Fehr, E. & Gächter, S. Altruistic Punishment in Humans. *Nature* **415,** 137–140 (2002).

44. Fehr, E. & Gächter, S. Fairness and Retaliation: The Economics of Reciprocity. *Journal of Economic Perspectives* **14,** 159–181 (2000).

45. Feldman, M. S. & March, J. G. Information in Organizations as Signal and Symbol. *Administrative Science Quarterly* **26,** 171–186 (1981).

46. Feledi, D., Fenz, S. & Lechner, L. Toward Web-based Information Security Knowledge Sharing. *Information Security Technical Report* **17,** 199–209. ISSN: 1363-4127 (2013).

47. Fielder, A., Panaousis, E., Malacaria, P., Hankin, C. & Smeraldi, F. *Game Theory Meets Information Security Management* in *ICT Systems Security and Privacy Protection* IFIP International Information Security Conference (eds Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A. & Sans, T.) **428** (Springer, Berlin, Heidelberg, Germany, 2014), 15–29. ISBN: 978-3-642-55415-5.

48. Flegel, U. *Pseudonymizing Unix Log Files* in *Infrastructure Security* International Conference on Infrastructure Security (Springer, Berlin, Heidelberg, Germany, 2002), 162–179. ISBN: 978-3-540-45831-9.

49. Forte, D. V. The "Art" of Log Correlation: Tools and Techniques for Correlating Events and Log Files. *Computer Fraud & Security* **2004,** 15–17 (2004).

50. Foss, N. J. More Critical Comments on Knowledge-Based Theories of the Firm. *Organization Science* **7,** 519–523 (1996).

51. Fransen, F., Smulders, A. & Kerkdijk, R. Cyber Security Information Exchange to Gain Insight into the Effects of Cyber Threats and Incidents. *e&i Elektrotechnik und Informationstechnik* **132,** 106–112 (2015).

52. Furnell, S. & Clarke, N. Power to the People? The Evolving Recognition of Human Aspects of Security. *Computers & Security* **31,** 983–988 (2012).

53. Gabaix, X., Laibson, D., Moloche, G. & Weinberg, S. Costly Information Acquisition: Experimental Analysis of a Boundedly Rational Model. *American Economic Review* **96,** 1043–1068 (2006).

54. Gal-Or, E. & Ghose, A. The Economic Incentives for Sharing Security Information. *Information Systems Research* **16,** 186–208 (2005).

55. Gaynor, M., Rebitzer, J. B. & Taylor, L. J. *Incentives in HMOs* w8522 (National Bureau of Economic Research, Cambridge, USA, 2001).

56. George, G., Zahra, S. A., Wheatley, K. K. & Khan, R. The Effects of Alliance Portfolio Characteristics and Absorptive Capacity on Performance: A Study of Biotechnology Firms. *The Journal of High Technology Management Research* **12,** 205–226 (2001).

57. Gordon, L. A., Loeb, M. P. & Lucyshyn, W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* **22,** 461–485 (2003).

58. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, L. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* **6,** 24–30 (2015).

59. Gordon, L. A., Loeb, M. P. & Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security* **7,** 49–59 (2016).

60. Grant, R. M. Prospering in Dynamically-Competitive Environments: Organizational Capability as Knowledge Integration. *Organization Science* **7,** 359–467 (1996).

61. Grant, R. M. Toward a Knowledge-Based Theory of the Firm. *Strategic Management Journal* **17,** 109–122 (S2 1996).

62. Griffith, R., Redding, S. & van Reenen, J. R&D and Absorptive Capacity: Theory and Empirical Evidence. *Scandinavian Journal of Economics* **105,** 99–118 (2003).

63. Grossklags, J., Christin, N. & Chuang, J. *Secure or Insure?: A Game-Theoretic Analysis of Information Security Games* in *Proceeding of the 17th International Conference on World Wide Web* 17th international conference on World Wide Web (ACM Press, Beijing, China, 2008), 209–218. ISBN: 978-1-60558-085-2.

64. Haemmerli, B., Raaum, M. & Franceschetti, G. Trust Networks Among Human Beings: Analysis, Modeling, and Recommendations. *Effective Surveillance for Homeland Security,* 21–50 (2013).

65. Hair, J. F. *Multivariate Data Analysis* 5th ed. (Pearson Education India, Taramani, India, 2006).

66. Hausken, K. Information Sharing Among Firms and Cyber Attacks. *Journal of Accounting and Public Policy* **26,** 639–688 (2007).

67. Hiebert, J. & Lefevre, P. Conceptual and Procedural Knowledge in Mathematics: An Introductory Analysis. *Conceptual and Procedural Knowledge: The Case of Mathematics* **2,** 1–27 (1986).

68. Hofmann, A. & Ramaj, H. Interdependent Risk Networks: the Threat of Cyber Attack. *International Journal of Management and Decision Making* **11,** 312–323 (2011).

69. Huber, G. P. Transfer of Knowledge in Knowledge Management Systems: Unexplored Issues and Suggested Studies. *European Journal of Information Systems* **10,** 72–79 (2001).

70. Hume, D. *A Treatise of Human Nature* ISBN: 978-0-19-875172-4 (Oxford University Press, New York, USA, 2000).

71. Jakobson, G. *Mission Cyber Security Situation Assessment Using Impact Dependency Graphs* in *14th International Conference on Information Fusion* (2011), 1–8.

72. Jane Zhao, Z. & Anand, J. A Multilevel Perspective on Knowledge Transfer: Evidence From the Chinese Automotive Industry. *Strategic Management Journal* **30,** 959–983 (2009).

73. Jeon, S., Kim, Y.-G. & Koh, J. An Integrative Model for Knowledge Sharing in Communities-of-Practice. *Journal of Knowledge Management* **15,** 251–269 (2011).

74. Kalleberg, A. L. Work Values and Job Rewards: A Theory of Job Satisfaction. *American Sociological Review* **42,** 124–143 (1977).

75. Katz, R. & Allen, T. J. Investigating the Not Invented Here (NIH) Syndrome: a Look at the Performance, Tenure, and Communication Patterns of 50 R&D Project Groups. *R&D Management* **12,** 7–20 (1982).

76. Knight, G. A. & Liesch, P. W. Information Internalisation in Internationalising the Firm. *Journal of Business Research* **55,** 981–995 (2002).

77. Kogut, B. The Network as Knowledge: Generative Rules and the Emergence of Structure. *Strategic Management Journal* **21,** 405–425 (2000).

78. Kogut, B. & Zander, U. Knowledge of the Firm and the Evolutionary Theory of the Multinational Corporation. *Journal of International Business Studies* **24,** 625–645 (1993).

79. *Handbook of the Economics of Giving, Altruism and Reciprocity* (eds Kolm, S.-C. & Mercier-Ythier, J.) (Elsevier, Amsterdam, Netherlands, 2006). ISBN: 978-0-08-047821-0.

80. Kunreuther, H. & Heal, G. Interdependent Security. *Journal of Risk and Uncertainty* **26,** 231–249 (2003).

81. Kwahk, K.-Y. & Park, D.-H. The Effects of Network Sharing on Knowledge-sharing Activities and job Performance in Enterprise Social Media Environments. *Computers in Human Behavior* **55,** 826–839 (B 2016).

82. Laube, S. & Böhme, R. Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys (CSUR)* **50,** 77 (2017).

83. Lee, C. S. & Ma, L. News Sharing in Social Media: The Effect of Gratifications and Prior Experience. *Computers in Human Behavior* **28,** 331–339 (2012).

84. Lee, J., Bagheri, B. & Kao, H.-A. A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems. *Manufacturing Letters* **3,** 18–23 (2015).

85. Li, Y. & Kettinger, W. J. An Evolutionary Information-Processing Theory of Knowledge Creation. *Journal of the Association for Information Systems* **7,** 25 (2006).

86. Liao, S.-H., Fei, W.-C. & Chen, C.-C. Knowledge Sharing, Absorptive Capacity, and Innovation Capability: an Empirical Study of Taiwan's Knowledge-Intensive Industries. *Journal of Information Science* **33,** 340–359 (2007).

87. Lichtenthaler, U. & Ernst, H. Attitudes to Externally Organising Knowledge Management Tasks: a Review, Reconsideration and Extension of the NIH Syndrome. *R&D Management* **36,** 367–386 (2006).

88. Lichtenthaler, U. & Ernst, H. Developing Reputation to Overcome the Imperfections in the Markets for Knowledge. *Research Policy* **36,** 37–55 (2007).

89. Lindenberg, S. & Foss, N. Managing Joint Production Motivation: The Role of Goal Framing and Governance Mechanisms. *Academy of Management Review* **36,** 500–525 (2011).

90. Luiijf, E. & Klaver, M. *On the Sharing of Cyber Security Information* in *Critical Infrastructure Protection IX* International Conference on Critical Infrastructure Protection. **466** (Springer, Cham, Switzerland, 2015), 29–46. ISBN: 978-3-319-26567-4.

91. Lundvall, B.-ä. & Johnson, B. The Learning Economy. *Journal of Industry Studies* **1,** 23–42 (1994).

92. Mahmood, T. & Afzal, U. *Security Analytics: Big Data Analytics for Cybersecurity: a Review of Trends, Techniques and Tools* in *2013 2nd National Conference on Information Assurance (NCIA)* 2013 2nd National Conference on Information Assurance (NCIA) (IEEE, Rawalpindi, Pakistan, 2013), 129–134. ISBN: 978-1-4799-1288-9.

93. Maillart, T., Zhao, M., Grossklags, J. & Chuang, J. Given Enough Eyeballs, All Bugs Are Shallow? Revisiting Eric Raymond With Bug Bounty Programs. *Journal of Cybersecurity* **3,** 81–90 (2017).

94. Manshaei, M. H., Zhu, Q., Alpcan, T., Bacşar, T. & Hubaux, J.-P. Game Theory Meets Network Security and Privacy. *ACM Computing Surveys* **45,** 25 (2013).

95. March, J. G. Exploration and Exploitation in Organizational Learning. *Organization Science* **2,** 71–87 (1991).

96. Masud, M. M., Al-Khateeb, T., Khan, L., Thuraisingham, B. & Hamlen, K. W. *Flow-based Identification of Botnet Traffic by Mining Multiple Log Files* in *2008 First International Conference on Distributed Framework and Applications* First International Conference on Distributed Framework and Applications (IEEE, Penang, Malaysia, 2008), 200–206. ISBN: 978-1-4244-2313-2.

97. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M. & Percia David, D. To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing. *Journal of Cybersecurity* **5,** (in print (2019).

98. Moore, T. W. & Clayton, R. The Impact of Public Information on Phishing Attack and Defense. *Communications and Strategies,* 45–68 (2011).

99. Moran, T. & Moore, T. *The Phish-Market Protocol: Securely Sharing Attack Data between Competitors* in *Financial Cryptography and Data Security* International Conference on Financial Cryptography and Data Security (Springer, Berlin, Heidelberg, Germany, 2010), 222–237. ISBN: 978-3-642-14577-3.

100. Naghizadeh, P. & Liu, M. *Inter-temporal Incentives in Security Information Sharing Agreements* in *2016 Information Theory and Applications Workshop (ITA)* 2016 Information Theory and Applications (ITA) (IEEE, La Jolla, USA, 2016), 1–8. ISBN: 978-1-5090-2529-9.

101. Nagin, D. S., Rebitzer, J. B., Sanders, S. & Taylor, L. J. Monitoring, Motivation, and Management: The Determinants of Opportunistic Behavior in a Field Experiment. *American Economic Review* **92,** 850–873 (2002).

102. Nickerson, J. A. & Zenger, T. R. A Knowledge-Based Theory of the Firm—The Problem-Solving Perspective. *Organization Science* **15,** 617–632 (2004).

103. Nonaka, I. & Takeuchi, H. *The Knowledge-Creating Company : How Japanese Companies Create the Dynamics of Innovation* 1st ed. ISBN: 978-0-19-509269-1 (Oxford University Press, New York, USA, 1995).

104. Nunnally, J. C. & Bernstein, I. H. *Psychometric Theory* 3rd ed. ISBN: 978-0-07-047849-7 (McGraw-Hill, New York, USA, 1994).

105. Ou, C. X. J., Davison, R. M. & Wong, L. H. M. Using Interactive Systems for Knowledge Sharing: the Impact of Individual Contextual Preferences in China. *Information & Management* **53,** 145–156 (2016).

106. Park, B. I. Knowledge Transfer Capacity of Multinational Enterprises and Technology Acquisition in International Joint Ventures. *International Business Review* **20,** 75–87 (2011).

107. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* **42,** 165–176 (2014).

108. Peri, G. Determinants of Knowledge Flows and Their Effect on Innovation. *Review of Economics and Statistics* **87,** 308–322 (2005).

109. Petty, R. E. & Cacioppo, J. T. in *Communication and Persuasion* 1–24 (Springer, New York, USA, 1986). ISBN: 978-1-4612-4964-1.

110. Phelan, S. E. & Lewin, P. Arriving at a Strategic Theory of the Firm. *International Journal of Management Reviews* **2,** 305–323 (2000).

111. Pi, S.-M., Chou, C.-H. & Liao, H.-L. A study of Facebook Groups Members' Knowledge Sharing. *Computers in Human Behavior* **29,** 1971–1979 (2013).

112. Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y. & Podsakoff, N. P. Common Method Biases in Behavioral Research: a Critical Review of the Literature and Recommended Remedies. *Journal of Applied Psychology* **88,** 879–903 (2003).

113. Podsakoff, P. M. & Organ, D. W. Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management* **12,** 531–544 (1986).

114. Polanyi, M. Tacit Knowing: Its Bearing on Some Problems of Philosophy. *Reviews of Modern Physics* **34,** 601–616 (1962).

115. Powner, D. A. *Critical Infrastructure Protection Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities: Report to Congressional Requesters.* (DIANE Publishing, 2005).

116. Ransbotham, S., Kane, G. C. & Lurie, N. H. Network Characteristics and the Value of Collaborative User-Generated Content. *Marketing Science* **31,** 369–547 (2012).

117. Reinholt, M., Pedersen, T. & Foss, N. J. Why a Central Network Position Isn't Enough: The Role of Motivation and Ability for Knowledge Sharing in Employee Networks. *Academy of Management Journal* **54,** 1277–1297 (2011).

118. Ryan, R. M. & Deci, E. L. Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemporary Educational Psychology* **25,** 54–67 (2000).

119. Safa, N. S. & Von Solms, R. An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior* **57,** 442–451 (2016).

120. Sait, S. Y., Bhandari, A., Khare, S., James, C. & Murthy, H. A. Multi-Level Anomaly Detection: Relevance of Big Data Analytics in Networks. *Sadhana* **40,** 1737–1767 (2015).

121. Scarbrough, H. Knowledge Management, HRM and the Innovation Process. *International Journal of Manpower* **24,** 501–516 (2003).

122. Schilling, M. A. *Strategic Management of Technological Innovation* 3rd ed. ISBN: 978-0-07-128957-3 (McGraw-Hill Education, New York, USA, 2010).

123. Schmidt, T. Absorptive Capacity—One Size Fits All? A Firm-Level Analysis of Absorptive Capacity for Different Kinds of Knowledge. *Managerial and Decision Economics* **31,** 1–18 (2010).

124. Sedenberg, E. M. & Dempsey, J. X. Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs. *Computing Research Repository* (2018).

125. Shiva, S., Roy, S. & Dasgupta, D. *Game Theory for Cyber Security* in *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10* The Sixth Annual Workshop on Cyber Security and Information Intelligence Research (ACM Press, Oak Ridge, USA, 2010), 34–37. ISBN: 978-1-4503-0017-9.

126. Siesfeld, T., Cefola, J. & Neef, D. *The Economic Impact of Knowledge* (Routledge, 2009).

127. Simon, H. A. Bounded Rationality and Organizational Learning. *Organization Science* **2,** 125–134 (1991).

128. Singh, J. & Nene, M. J. A Survey on Machine Learning Techniques for Intrusion Detection Systems. *International Journal of Advanced Research in Computer and Communication Engineering* **2,** 4349–4355 (2013).

129. Singh, K. *Organisation Change and Development* Google-Books-ID: rQLjYrAcKWkC. ISBN: 978-81-7446-442-2 (Excel Books, New Delhi, India, 2005).

130. Skopik, F., Settanni, G. & Fiedler, R. A Problem Shared is a Problem Halved: a Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing. *Computers & Security* **60,** 154–176 (2016).

131. Spender, J.-C. Making Knowledge the Basis of a Dynamic Theory of the Firm: Making Knowledge. *Strategic Management Journal* **17,** 45–62 (S2 1996).

132. Stock, J. H., Watson, M. W., *et al. Introduction to Econometrics* (Addison Wesley Boston, 2003).

133. Szulanski, G. Exploring Internal Stickiness: Impediments to the Transfer of Best Practice Within The Firm. *Strategic Management Journal* **17,** 27–43 (1996).

134. Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M. & Rohani, V. A. Evaluation Model for Knowledge Sharing in Information Security Professional Virtual Community. *Computers & Security* **43,** 19–34 (2014).

135. Teece, D. in *Technological and Organizational Factors in the Theory of the Multinational Enterprise* Mark Casson, 51–62 (George Allen & Unwin, London, UK, 1983).

136. Teece, D. J. Technology Transfer by Multinational Firms: the Resource Costs of Transferring Technological Know-How. *The Economic Journal* **87,** 242–261 (1977).

137. Ter Wal, A. L., Criscuolo, P. & Salter, A. Making a Marriage of Materials: The Role of Gatekeepers and Shepherds in The Absorption of External Knowledge and Innovation Performance. *Research Policy* **46,** 1039–1054 (2017).

138. Terzi, D. S., Terzi, R. & Sagiroglu, S. *Big Data Analytics for Network Anomaly Detection from Netflow Data* in *International Conference on Computer Science and Engineering (UBMK'17)* International Conference on Computer Science and Engineering (UBMK'17) (2017), 592–597.

139. Tether, B. S. & Tajar, A. Beyond Industry–University Links: Sourcing Knowledge for Innovation from Consultants, Private Research Organisations and the Public Science-Base. *Research Policy* **37,** 1079–1095 (2008).

140. Tosh, D. K., Shetty, S., Sengupta, S., Kesan, J. P. & Kamhoua, C. A. *Risk Management Using Cyber-Threat Information Sharing and Cyber-Insurance* in *Game Theory for Networks* International Conference on Game Theory for Networks (Springer, Cham, Switzerland, 2017), 154–164. ISBN: 978-3-319-67540-4.

141. Tounsi, W. & Rais, H. A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks. *Computers & Security* **72,** 212–233 (2018).

142. Trevor, C. O. & Nyberg, A. J. Keeping Your Headcount When All About You Are Losing Theirs: Downsizing, Voluntary Turnover Rates, and The Moderating Role of HR Practices. *Academy of Management Journal* **51,** 259–276 (2008).

143. Tricomi, E., Rangel, A., Camerer, C. F. & O'Doherty, J. P. Neural Evidence for Inequality-Averse Social Preferences. *Nature* **463,** 1089–1091 (2010).

144. Tsai, W. Knowledge Transfer in Intraorganizational Networks: Effects of Network Position and Absorptive Capacity on Business Unit Innovation and Performance. *Academy of management journal* **44,** 996–1004 (2001).

145. Van den Bosch, F. A. J., Volberda, H. W. & de Boer, M. Coevolution of Firm Absorptive Capacity and Knowledge Environment: Organizational Forms and Combinative Capabilities. *Organization Science* **10,** 551–568 (1999).

146. Van Wijk, R., Jansen, J. J. & Lyles, M. A. Inter-and Intra-Organizational Knowledge Transfer: A Meta-Analytic Review and Assessment of its Antecedents and Consequences. *Journal of management studies* **45,** 830–853 (2008).

147. Vázquez, D. F., Acosta, O. P., Spirito, C., Brown, S. & Reid, E. *Conceptual Framework for Cyber Defense Information Sharing Within Trust Relationships* in *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (2012), 1–17.

148. Von Solms, R. & van Niekerk, J. From Information Security to Cyber Security. *Computers & Security* **38,** 97–102 (2013).

149. Wagner, T. D., Palomar, E., Mahbub, K. & Abdallah, A. E. A Novel Trust Taxonomy for Shared Cyber Threat Intelligence. *Security and Communication Networks* **2018,** 1–11 (2018).

150. Wang, J. H., Wang, C., Yang, J. & An, C. A Study on Key Strategies in P2P File Sharing Systems and ISPs' P2P Traffic Management. *Peer-to-Peer Networking and Applications* **4,** 410–419 (2011).

151. Wang, S. & Noe, R. A. Knowledge Sharing: a Review and Directions for Future Research. *Human Resource Management Review* **20,** 115–131 (2010).

152. Wang, W.-T. & Hou, Y.-P. Motivations of Employees' Knowledge Sharing Behaviors: A Self-Determination Perspective. *Information and Organization* **25,** 1–26 (2015).

153. Wang, Y., Wang, Y., Liu, J. & Huang, Z. *A Network Gene-Based Framework for Detecting Advanced Persistent Threats* in *Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC'14)* Ninth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC'14) (2014), 97–102.

154. Ward, T. B. Cognition, Creativity, and Entrepreneurship. *Journal of Business Venturing* **19,** 173–188 (2004).

155. Weiss, N. E. *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (Congressional Research Service, Washington, USA, 2014).

156. Williamson, O. E. The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology* **87,** 548–577 (1981).

157. Xiong, L. & Liu, L. PeerTrust: Supporting Reputation-Based Trust for Peer-to-Peer Electronic Communities. *IEEE Transactions on Knowledge and Data Engineering* **16,** 843–857 (2004).

158. Yan, Z., Wang, T., Chen, Y. & Zhang, H. Knowledge Sharing in Online Health Communities: a Social Exchange Theory Perspective. *Information & Management* **53,** 643–653 (2016).

159. Yao, Z., Yang, Z., Fisher, G. J., Ma, C. & Fang, E. E. Knowledge Complementarity, Knowledge Absorption Effectiveness, and New Product Performance: The Exploration of International Joint Ventures in China. *International Business Review* **22,** 216–227 (2013).

160. Zibak, A. & Simpson, A. *Cyber Threat Information Sharing: Perceived Benefits and Barriers* in *Proceedings of the 14th International Conference on Availability, Reliability and Security* (2019), 85.

Conclusion

'If I have seen further, it is by standing on the shoulders of giants.'

— Isaac Newton

Contents of the Conclusion

1 Contributions

This section presents the contributions of my thesis under two sub-sections. In the first one, I emphasize the specific contributions of each article, and I present how they respond to their respective research sub-question. In the second sub-section, I emphasize some broader and more general insights related to the joint contribution of my three articles (synthesis).

1.1 Answers to Research Questions

This thesis began with the premise that critical infrastructure providers (CIP) are at risk whenever the security of their information systems (IS) is threatened, as security incidents that follow might lead to large-scale economic and societal damages. In the introductory section, I argued that an effective defense against such IS-security incidents requires an IS-defense capability – i.e., the organizational ability to purposefully acquire, combine and deploy resources to neutralize security incidents before they occur or immediately after they have occurred [2, 70, 94]. I inferred that whenever CIPs have problems related to security incidents, their IS-defense capability is insufficient. I finally argued that this insufficiency can be traced to either an inefficient combination of resources or to obstacles that impede organizations from acquiring these resources in the first place. My thesis focused on this latter aspect by identifying specific research gaps and related research sub-questions, attempting to provide some answers to these sub-questions.

Through my three research sub-questions, I explored specific aspects and problems that organizations would have to overcome as they attempt to acquire material, human, and knowledge resources – which are all required to build an IS-defense capability [10, 66, 89, 94]. More specifically, I asked how they would acquire each of the resource categories. My thesis structured this exploration into three separate articles, each of which deals with a particular approach angle – determined by specific research gaps – in order to acquire each resource categories. These research angles and their contributions related to specific resource-categories acquisition are summarized in the three following sub-sections.

Part I: Material-Resource Investment

My first research sub-question focused on how, if at all, CIPs must adapt current investment models in order to acquire technologies (material resources) required to build an IS-defense capability. In prior research, such investment was primarily modeled by the information-security investment model of Gordon and Loeb (e.g., [43]; for a systematic literature review, see Table i.2 on page i.2). This model and its extant extensions provide two contributions: (1) they calculate an optimal financial amount that an organization should invest in order to protect its assets (e.g., [12, 44, 62, 67, 97]), and (2) they provide analytical means in order to recommend a choice of technologies that an organization should invest in [22, 43].

In the introductory chapter, my literature review related to the Gordon-Loeb (GL) model and its extensions (Table i.2 on page i.2) suggested that while this model is useful, it also has significant limitations. The works I reviewed assume a single-period setup, a continuous security-breach probability function (SBPF), or both. I argued that this static analysis might be inappropriate for environments in which technology evolves (and obsolesces) fast. I suggested that such an environment requires an investment approach that can account for technological discontinuity and dynamic – rather than discrete – investment. To the best of my knowledge, to date, no such model exists in the literature.

Therefore, the first article of my thesis offers an extension of the GL model that considers multiple investment periods and relaxes the assumption of a continuous SBPF. I determine the optimal level of IS-security investment through the maximization of the expected net benefit in information-security function (ENBIS). The optimal level of IS-security investment

is obtained when the difference between benefits and costs are maximized [43, 45] – i.e., where the marginal benefits of IS-security investment are equivalent to the marginal cost of potential losses due to IS-security incidents. Also, my extension of the GL model provides a theoretical framework in order to analyze the expected net benefits of the implementation of any given novel technology over time. Hence, my model allows CIPs to determine if any novel technology generates a greater ENBIS. If so, CIPs might consider this novel technology as disruptive and *vice versa*.

Further, as I conceptualized a SBPF with productivity parameters, CIPs can calculate the optimal investment that should be used to invest in IS-defense technologies. Finally, my model allows CIPs to select among such technologies according to their marginal contribution to IS-security productivity.

All in all, these extensions allow CIPs to adapt their investment to a dynamic environment and discontinuous technology evolution, both in terms of technology selection and efficiency of investment.

Part II: Human-Resource Recruitment

My second research sub-question focused on how CIPs can attract the human resources required to build an IS-defense capability. In the introduction of this thesis, I summarized the economic literature that suggests specialized human staff is required in order to build an IS-defense capability (e.g., [57, 81]). In particular, the specialist knowledge that new organizational members bring with them helps organizations to adapt to new IS-incidents and stay competitive [87]. I exemplified the organizational problems that follow whenever such specialists cannot be recruited by considering the case of armed forces.

Therefore, the second article of my thesis offers an opportunity-cost analysis of specialists-recruitment problems in the context of the Swiss Armed Forces (SAF). While this organization provides cyber-defense for the government and secondary support for other critical infrastructures (CI), it witnesses significant problems to recruit human specialists [7, 92]. Since such specialists are hired as staff and warrant officers, I produced an opportunity-cost analysis that attempts to explain recruitment problems as a result of economic, rather than sociological or psychological problems. My systematic literature review on the matter (Table i.3 on page i.3) presented in the introductory chapter of this thesis suggested that sociological and psychological analysis fall short to explain these recruitment problems within the SAF. Therefore, my opportunity-cost analysis added an economic explanation to this literature.

I modeled decision alternatives both within and outside a military organization, taking private sector employment of IT specialists as the reference point. I then monetized opportunity-costs of leisure, fringe benefits, and private sector income not compensated. The results suggested that the opportunity cost of enlisting in the armed forces *vis-à-vis* the private sector employment is prohibitively high for IT-specialists, which explains the persistent staff deficit. Worse, an officer career is also the least attractive option among all service alternatives within the armed forces. There is hence a threat of adverse selection for military organizations, in the sense that enlisting as a specialist will only be attractive to those employed in low-paying industries or those unable to compete for higher-paying jobs in the private sector. As a result, the qualification level of human personnel is lower than required, and hence the IS defense-capability suffers from this situation.

This analysis provides some answers to my second research question, suggesting that as long as organizations cannot overcome such effects, they cannot properly acquire the necessary human resources required to build an IS-defense capability. At the same time, this article makes suggestions on how such obstacles might be overcome, implying that any IS-defense capability would be strengthened by these suggestions. While such suggestions are elaborated in the specific context of armed forces, I believe this context provides a

drastic example of a more general type of problems that any given CIP probably faces. As civilian CIPs are competing for specialists with the private sector, or within the private sector, they might face similar recruitment problems, and hence the suggestions I presented in Part III might be transferable to their contexts.

First, I advise armed forces to accept that the opportunity cost of enlistment grows with IT-specialists' age, career development, and professional qualification. Hence, recruiting policies for IT specialists should target candidates during graduate studies or professional training as for this cohort, opportunity cost is low while the marginal utility of salary increases is high. The same issue probably applies to any given CIP, as poaching IT specialists might be prohibitively expensive once these have begun a career track in the private sector.

Second, any attempt to counter under-staffing of IT specialists by monetary incentives is probably unsuccessful as it undermines intrinsic motivation [16, 60]. Further, the generation born between 1985 and 2000 ('millennials') puts greater emphasis on the work-leisure trade-off and assigns less importance to monetary fringe benefits and status [55]. As a result, specialists should be attracted by non-monetary opportunities – e.g., technological challenges not available in the private sector outside a CIP context such as electronic warfare or cyber-attacks by professionally equipped state actors. Another option would be to offer subsidized or free tertiary education. For example, in the United States, the GI Bill largely waives the cost of studying for a degree once military personnel have completed their duty. This program reached record levels in 2009 as nearly 95% of eligible personnel involved in the program actually used it once they left the military [15]. Also, empirical evidence suggests that spending a fixed budget on recruitment rather than on salary increases is a much more efficient way to win over qualified staff [29].

Third, any attempt to force IT specialists to enlist is *de jure* impossible for civilian CIPs, but neither is this a promising option for armed forces. As my study found that an officer position is also the worst amongst all military service alternatives, applying 'raising rival's costs' tactics [23, 79] – e.g., making the civilian service more unattractive *vis-à-vis* other service options, are unlikely to succeed. Rather, both armed forces and CIPs should try to broaden the recruitment base – e.g., by relaxing the requirement that only men or only citizens can serve in the armed forces.

Part III: Knowledge-Resource Absorption

My third research sub-question focused on how CIPs can succeed at absorbing external knowledge that is required to build an IS-defense capability. I used the theory of the *knowledge-based view of the firm* to suggest that tacit and specialist knowledge is a key ingredient for an IS-defense capability. I further argued that organizational learning often requires absorbing new knowledge from beyond the boundary of the firm [66, 87], such that the more an organization succeeds at this absorption, the more effective its IS-defense capability is (e.g., [32, 36, 74, 77, 78]). Finally, I argued that this knowledge absorption is particularly difficult in a CIP context as the required knowledge is likely tacit and not readily available by public channels.

Therefore, the third article in this thesis presents an empirical study that analyzes a dataset of 262 members of an information-sharing and analysis center (ISAC) who share highly sensitive and classified information by interpersonal exchange. Using econometric and psychometric methods, and modeling the absorption problem using the theory of *transaction cost economics*, I hypothesize associations between human belief and knowledge-absorption outcomes.

This analysis provides an answer to my third research question, suggesting that organizations can acquire tacit and specialized knowledge if they can master knowledge absorption from external sources. As I identified significant associations between knowledge absorption

and human belief, I suggest that such an absorption does not happen randomly, but that productive social behavior, in particular reciprocal exchange of information, is required for such an absorption. I argue that the extent to which an individual engages in information sharing is a function of their individual knowledge-absorption expectation – i.e., the benefit they expect from sharing information. Thus, my work extends prior approaches [68] by not only focusing on describing such a knowledge exchange, but also on describing the outcomes of such an exchange in terms of knowledge absorbed.

Moreover, these findings have implications for ISACs managers. I framed my study in *transaction cost economics*, suggesting that individuals consider the transaction cost of social exchange that precedes knowledge absorption, and thus this cost likely influences their decision of whether or not to participate in such an exchange in the first place. Since the organizational design of an ISAC influences the behavior of its members [84], ISACs managers should strive to minimize such transaction costs. At the same time, the absorption of tacit and specialized knowledge requires intensive and interpersonal interaction, implying that decentralized or automated ways of organizing information exchange are probably not productive. I join the authors of [68] in predicting that the more relevant technological knowledge is for IS defense, the less likely this knowledge will be shared inside the cyber-sphere.

Finally, my results caution organizations to not incentivize their members by monetary incentives. Although many organizations have created reward systems to encourage their employees to share information with others [11], I find no support for the hypothesis that knowledge absorption is associated with reward belief.

1.2 Synthesis

While each of the three articles of this thesis addressed a particular research sub-question, broader and more general insights can be emphasized by linking the contributions of each article.

First, I followed the recommendation to pry open the 'black box' of organizations as they acquire and combine resources to produce capabilities [94]. I followed this call by studying organizations and their members, rather than relying on more objective but impersonal data analysis of log-files, incident reports, etc. I believe that my approach is productive as it offers the reader an integrative view of the different resources that an IS-defense capability requires. Moreover, organizations that are not satisfied with their current IS-defense capability are offered a structured analytical framework by which they might spot weaknesses in a particular category that they can then address. For example, an organization might invest in adopting multi-period settings and technological discontinuities, and also participate in ISACs meeting, but it might have problems finding IT specialists. In this case, such an organization would have the necessary material and knowledge resources, but not the human resources, such that it might use my findings to develop novel recruitment strategies.

Second, I attempted to generate an integrative view of the different resources needed to build an IS-defense capability that future research might build on. In particular, future work might use my thesis as an entry point to further explore each resource category in greater depth – e.g., by exploring additional aspects of resources acquisition that are not captured by my three articles. I emphasized that security incidents in IS are at least as often caused by inappropriate organizational design and human behavior as they are caused by inefficient IT design [6]. My thesis partially addresses this problem from the onset by adopting the definition of IS as socio-technical systems (STS) that integrate technologies (material resources), human agents who employ such technologies (human

resources) and their tacit and specialist knowledge (knowledge resources) [13, 38]. I have therefore explored the acquisition of each of these resources through targeted aspects related to research gaps. While this approach certainly has limitations as to the depth with which each resource category was studied, it also offers the advantage of greater generalizability. As future research follows the above call of [94], a closer focus on any resource category implies that the influence of the organizational context grows and hence makes results more context-specific to the particular organization that was studied. I therefore believe that my approach should go ahead with a study that looks at all resource categories and that focus on identifying generalizable results before each category is explored in greater detail.

I therefore designed the three articles with a focus on generalizability rather than specificity. In the first article, the extension to the GL model I proposed is derived by formal modeling. Neither this technique nor the results are bound to the idiosyncrasies of any particular organization or investment policy. This approach is consistent with the recommendation that an investment model should be generalizable to any context [82].

In the second article, I study a particular armed-forces organization, but I believe that my findings are also generalizable to other armed forces, and to CIPs in general. First, my opportunity-cost estimates probably represent a lower boundary of actual opportunity cost, as due to the Swiss goverenment doctrines of neutrality and non-involvement in international armed conflict, the SAF have a defensive and isolationist nature. This implies that other armed forces might have to take into account additional opportunity costs that are unlikely to materialize in the Swiss context – e.g., mortality risk, geographic mobility, or effects related to job tenure. As a result, my study probably represents a baseline case that many other armed forces can employ, taking into account their particular additional cost factors on top of my estimates. Moreover, while I do study armed forces, I believe the findings are also applicable to other CIPs as both types of organization face significant competition from the private sector. The solutions to this recruitment problem I proposed are not context-specific to armed forces, but they rather strive to influence IT-specialists' decision at a time where their opportunity cost is still low.

In the third article, I studied a particular ISAC, but none of the constructs I used to operationalize and test my hypothesis is specific to any industry, cultural or national context. On the contrary, I used well-established constructs from the prior literature (Table III.1 on page 110) that represent fundamental aspects of human belief and human interaction. As these are rooted in human nature and psychology as such, rather than in the behavior of any particular cohort of human beings or social groups, I believe my findings can be considered representative for a wide range of ISACs. These might certainly differ with respect to organization, language, and membership rules; yet, I suggest that human interaction inside any particularly ISAC might reproduce the transaction-cost considerations I have set out in my third article.

Third, all in all, my thesis focuses on IS defense in the context of CIs, in which any security breach might lead to significant economic and societal losses that far exceeds losses in the private sector due to IS incidents. If the measures I proposed in this context help organizations to acquire each of the three resource categories, they might be also useful in a context that faces less extreme risks.

Fourth, from a broader perspective, my thesis attempted to respond to the call that IS research should be enriched with both theoretical concepts and empirical methods from economics. I emphasized that building an IS-defense capability requires more than technology development, thus responding to the call that the study of IS defense requires an approach that should integrate economic perspectives and go far beyond technical design. Further, methodologically, much of the literature on IS defense has focused on risk

management and operations research methods [98]. While this approach is productive, it can be strengthened by complementing it with methods of economic analysis [3, 6, 21, 35, 78, 96]. My thesis therefore applies microeconomic theory and formal modeling in the first and second articles, and transaction cost economics and econometric analysis in the third article.

2 Limitations

The overarching framework of this thesis – as well as each of the three articles that compose it – have inherent limitations related to the respective approaches and the methodologies employed. Such limitations are already described either in the introduction or in the respective discussion sections of each article. However, these limitations are also listed here as reading them successively helps to emphasize the overall limitations of this thesis.

2.1 Overarching Framework

The choice of the overarching methodology – i.e., the organizational capability approach – on which this thesis is based represents an important choice of focus. Alternatives to this approach could have been to pursue the extension of the traditional literature – namely a risk-management approach and/or a operations-research approach – of IS defense for CIPs. However, my approach attempts to respond to the research call that the understanding of any capability production is incomplete unless the 'black box' of the organization is pried open [94]. Also, I followed recommendations of [3, 5, 6, 21, 35] who argue that organizations and human action and behavior must be studied in order to reach a deeper understanding of IS security. The organizational capability framework allows me to explore the three resources components in great detail, whereas extending the traditional literature would involve a higher level of abstraction and hence the loss of much contextual information that is useful to understand any capability production – especially when this latter is related to human action and behavior.

Also, as argued in the introduction of this thesis, the acquisition of material, human, and knowledge resources is a necessary – yet not sufficient – condition in order to build an IS-defense capability. Such an acquisition of the above-mentioned resources might be studied under different aspects. In this thesis, the study of material-resource acquisition was investigated under an investment focus and by a utility-maximization methodology, the study of human-resource acquisition was investigated under a recruitment focus and by an opportunity-cost framework, and the study of knowledge-resource acquisition was investigated under a knowledge-absorption focus and by a factor analysis and a psychometric methodology. However, the study of the acquisition of the three resources mentioned above might have been done by other approaches and methodologies. For instance, material-resource acquisition might have been studied by focusing on R&D instead of investment and studied with alternative methodologies such as the risk-based return on investment and/or net-present value (e.g., [9]), game-theory (e.g., [36]) or simulation (e.g., [54]). Also, the study of human-resource acquisition might have been made under a focus based on intrinsic and extrinsic motivation factors and with methodologies coming from social psychology (e.g., [93]), or by focusing on socio-demographic factors related to enlistment in an organization (e.g., [40]). Finally, the study of knowledge-resource acquisition might have been made under the focus of impersonal information analysis using game theory or simulation (e.g., [61], or log-files analysis (e.g., [37]), or through other channels than inter-organizational contexts and with alternative methodologies that do not imply knowledge absorption. Consequently, I do not pretend that I adopted a framework that captures the whole problematic of resources acquisition. Rather, I focused on targeted aspects of resources acquisition that

were determined by the nature of the respective research gaps found in the literature. The fact that targeted aspects of resources acquisition were investigated – and not the whole problematic of resources acquisition in general – is a limitation that should be emphasized.

Also, I study three specific aspects related to material-, human-, and knowledge-resources acquisition. An alternative approach would have been to concentrate on just the acquisition of one resource, and thus exploring this one category in greater detail. However, the deconstruction an IS-defense capability into three resources-requirements categories implies that it is consequential to study all of these. The literature I cited in Section 2 suggests quite unanimously that all three resources are required to produce an IS-defense capability, and I therefore decided to opt for a holistic approach. Therefore, a complete understanding of this capability requires the study of all resources. I then argue that as long as an organization merely has only one or any two of these resources, such an organization will experience problems with the production of an IS-defense capability.

Another decision regarding research focus is the use of three different organizational contexts to study the three resource categories. An alternative approach would have been to study all three resource categories in a single organizational context. However, such an approach would have entailed to study a single organization and the evolution of its IS-defense capability. Thus, the generalizability of the findings would have been limited. Further, any profound study of knowledge absorption should involve looking beyond the boundary of the organization and hence study human interaction; else, knowledge absorption could only be studied on the receiving end in the particular organization, and much contextual information about motivations to (not) interact with others in an attempt to absorb information could not be collected.

Additionally, a central idea of this thesis is to transfer theory and analytical concepts from economics into the IS domain in order to contribute to research questions that IS research struggles to answer [5, 6, 21, 31, 35]. This implies that my methodological approach is interdisciplinary; it combines thinking from IS security, microeconomics, and organizational-capability research. An alternative approach would have been to produce a number of field studies that are specific to the particular research tradition in any of these fields. But then, again, I would have missed out on the opportunity to infuse IS research with thoughts from economics, as there are few studies that span a bridge between these domains [31]. As a result of this interdisciplinary setup, my empirical approach entails the use of multiple methods. An alternative approach would have been to consistently use a single method in all three articles while still studying different contexts and resource categories. For example, as I use formal modeling in the first article of my thesis that studies material-resource investment, I could also have specified formal models of specialist staff recruitment and knowledge absorption. But that again would have meant missing out in-depth insights coming from different contexts, as human behavior and knowledge absorption can hardly be captured by formal models [14, 20, 42]. This thesis makes a compromise in this regard as I am studying human behavior both formally – by assuming rational choice and utility maximization of human agents in my second article as I study staffing problems – and under a human action and behavior perspective – providing much contextual information about actual human behavior in my third article as I study knowledge absorption.

2.2 Part I

My first article formally modeled an extension to the GL model, but it did not simulate or empirically test my suggested extension. I decided to leave this operationalization to future research as I wanted to focus on the generalizability of the model.

Any empirical operationalization requires a specification of the productivity parameters α_i and β_i of each technology considered for investment [69]. Moreover, decisions must be

made about which technologies are considered disruptive (and when), implying that a value threshold for the dummy variable d_i (that takes the value 0 when no disruptive technology is used, and 1 otherwise) must be determined.[1] Such choices make the model more specific to particular assumptions about technological and productivity contexts. Hence, I suggest my model should be operationalized by a series of different simulations instead of empirical tests – as they require the specification of productivity parameters α_i and β_i and the dummy variable d_i.

Given the fact that (1) specifications of such simulations and/or empirical tests would require multiple cases and thus multiple articles, and given the fact that (2) the research scope that I wanted to provide in this thesis is based on all three resource categories, such simulations and/or empirical tests are too ambitious to be explored in a single thesis. Nevertheless, I recommend that future research simulates, tests and develops further the model I proposed. For instance, it would be relevant to run a Monte Carlo simulation using equation I.2 by: (1) defining the domain of possible inputs of this equation – including the not numerically-defined thresholds of α_i, β_i and d_i, (2) randomly generating inputs from a probability distribution over the domain, (3) performing a deterministic computation on the inputs, (4) aggregating the results for both the productivity parameters α_i, β_i and the dummy variable d_i. With an increasing level of sampling complexity (e.g., path-spaces models with an increasing time horizon), proposition 1 and proposition 2 of the third article of my thesis could be tested. Therefore, such a simulation could determine respective thresholds and numerical values of α_i, β_i and d_i in order to determine (1) the conditions for a decrease in the optimal amount of investment in cyber-security, and (2) the conditions for a discountinuity in the SBPF.

2.3 Part II

My second article implicitly accepts assumptions from economic theory that future research could help relax.

Any opportunity-cost analysis is framed in neoclassical economic thought; it thus assumes that individuals maximize individual utility and make rational choices [86]. In the context of my research, this 'homo economicus' assumption might be questionable for two reasons. First, when it comes to making personal career choices, individuals might exhibit bounded, rather than perfect, rationality [41]. Hence, individuals might prefer imprecise estimates, partial information, social cues, projections, and assumptions over precise calculation as they evaluate relative magnitudes of costs [71]. My analysis could be refined by introducing weights or scaling factors that can take such bounded rationality into account – e.g., by adopting a conjoint-analysis methodology. Such weights or scaling factors require an extensive field survey in order to determine how individuals make their career decisions – i.e., what factors are predominantly important in shaping their decisions. Second, I assumed that IT specialists are ideologically neutral; implying they would evaluate and compare service alternatives inside and outside armed forces organizations as they would consider different career choices in the private sector. However, as both armed forces and many CIPs operate in a public sector and a national-security context, individuals might have ideological reservations to enlist. On the other hand, using the reverse argument, a particular type of individuals might enjoy the culture of armed forces and the public-sector context. Such ideological influence would increase the opportunity cost of enlistment for the first type, but reduce it for the second type of individuals. Future research should take this differentiation into account through the implementation a field survey in order to determine how the ideology of individuals influences their respective opportunity costs related to the enlistment in the military.

[1] Concerning the aforementioned productivity parameters and the dummy variable, please refer to equation I.2 on page 52.

2.4 Part III

My third article is a cross-sectional study, implying I could only identify associations, but not causal links [8]. Therefore, future research should study the interaction of ISAC participants over time – e.g., by using time-series regressions that link knowledge-absorption outcomes in later periods to interactions in prior periods [1, 28, 90].

Also, I proposed a novel measure of knowledge absorption that puts individual absorption to the fore, as much prior research used measures that aggregate individual absorption into organizational measures, such as R&D intensity [24, 26, 49, 64, 83], patent cross-citation indicators [39, 75], or the number of engineers the firm employs [58]. While I believe this measure is useful to capture individual absorption, it is also an ordinal indicator and hence its ability to measure effective knowledge absorption is limited. If knowledge absorption is the organizational (or individual) capability to transfer, integrate, and utilize new knowledge obtained from external sources [25, 46, 48, 73, 95], a more profound measurement approach should reflect such terms – e.g., by considering the transfer, integration, and use of information. Moreover, the measure represents not an objective performance figure, but an individual perception of a quantity. Future research should therefore expand and refine my measure by measuring the knowledge differential before and after enlisting in an ISAC – while controlling for all other factors related to knowledge absorption.

Also, receiving exclusive information through security-information exchange is a necessary but not sufficient condition for effective knowledge absorption, as an integration of the newly absorbed information with prior individual knowledge is required [56, 59, 63, 72]. As those specialists who absorb knowledge by participating in ISAC meetings and other forms of social exchange do not need to be identical to those who are generally in charge of organizing the production of IS defense. Future measures could take such differences between initial absorption and intra-organizational transfer of knowledge into account. However, as such a multi-step process of absorption cannot be readily measured by psychometric methods, my dependent measure should be seen as a first step towards providing such full measurement.

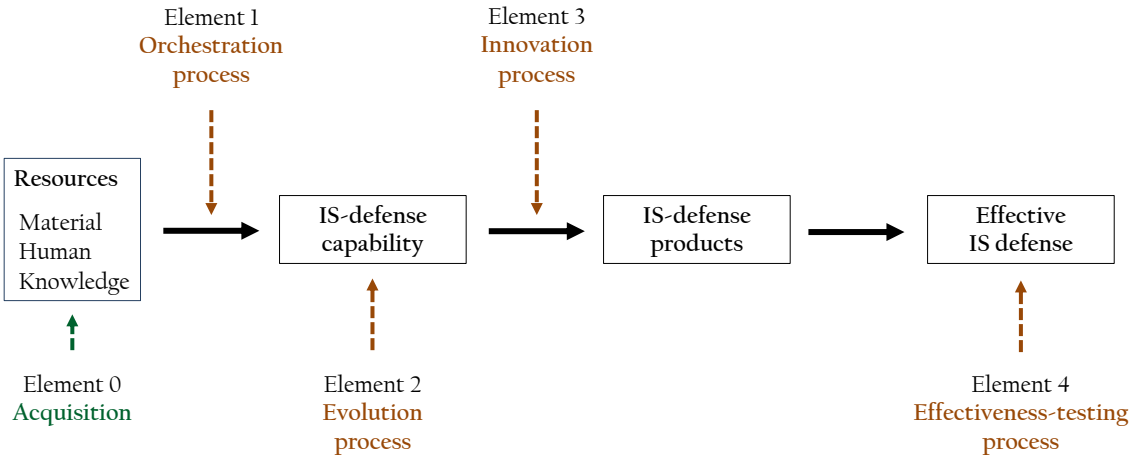
3 Paths for Further Research

My thesis has merely explored the very first point (labelled 'Element 0' in Figure IV.1) of a line of elements that stretches from the acquisition of resources required for an IS-defense capability to the effectiveness of IS defense. Figure IV.1 provides a visual overview of this line, and structures my ideas with respect to how my results might lead to a research agenda.

3.1 Element 1: Orchestration Process

In the introductory section of my thesis, I argued that problems encountered with an IS-defense capability can be due to a lack of required resources. However, I also noted that even if an organization has (or has access to) all required resources, it might still fail to combine/orchestrate them. As resources endowment precedes resources combination, I focused on the former question. This implies that I addressed the very first 'box' of the line that Figure IV.1 defines; and future research could now focus on the second concern (labelled 'Element 1' in Figure IV.1). The resource-orchestration process – i.e., purposeful combination of resources by organizational routines – is a prerequisite for any organizational capability [18, 27, 47, 52, 88]. This implies that once a CIP has secured all three resource categories, this organization must orchestrate them in order to build an IS-defense capability. Such orchestration is specific to the organization, in particular, its

Figure IV.1: **Proposed Research Agenda**



Notes to Figure IV.1: Each element (ranging from 1 to 4) is a proposed research project (c.f., the following paragraphs). In my thesis, I explored targeted aspects of 'Element 0'.

organizational processes and governance [10, 65]. The processes by which this orchestration happens are termed *microfoundations* in economics research; their study focuses on what managers do inside organizations as they orchestrate resources. Microfoundations are hence an aggregation of individual-level routines and interactions by which a capability is actually created [10, 33]. Hence, a study of human actions and social interactions associated with building an IS-defense capability could expand my findings by focusing more on the individual (micro) level of analysis. As my thesis emphasized generalizability, it did not study such combination processes, but future research might apply a more detailed focus. For example, both longitudinal qualitative studies of particular organizations as well as more abstract simulations of resource-combination processes could be carried out (see [99, 100] for illustrations of such methodological approaches).

3.2 Element 2: Evolution of IS-Defense Capability

Organizational capabilities are not static, they evolve as organizations, products, markets, and customer demand change [51, 53]. This implies that an IS-defense capability is also changing as technologies evolve and both attackers and defenders alternate their strategies and actions. Resources combination is therefore not a singular activity, rather, resources bases must be reconfigured continuously as the organization adapts to changing environments. This adaption requires both investing into novel and extant resources as well as changing organizational processes [80, 85]. My thesis has a static research concept and therefore does not take such dynamic or evolutionary perspectives into account. Hence, future research should dynamize my perspective, studying how organizations acquire and adapt their resources base over time as they adapt their IS-defense capability to changing threat environments and customers demand.

3.3 Element 3: Innovation Process

Organizational capabilities are a central prerequisite for the development of innovative processes, products and/or services [46, 48, 91, 94]. It is these processes (e.g., threat detection processes such as intrusion-detection systems (IDS), and handling procedures such as multi-modal bio-metric authentication of systems' users), products (e.g., technological applications such as hard- and software) and/or services (e.g., early warning services based on technologies such as machine learning) that provide the basis for actual defense [4].

Prior research described many of these processes, products and/or services [98], but the link between resources inputs and products outputs is still missing. I therefore predict that organizations that can acquire the three types of resources and orchestrate them efficiently will outperform other organizations in terms of IS-defense effectiveness. I invite future research to test this prediction.

3.4 Element 4: IS-Defense Effectiveness

My thesis began with the construction of an overarching argument that links resources endowments to performance outcomes: organizations must acquire three types of resources and orchestrate them in order to be able to develop innovative processes, products and/or services, which provide actual defense for the organization's IS. A test of this proposed link requires linking resources endowments to IS-defense performance differentials. Therefore, both operationalizations of IS defense (e.g., number of attacks defended, time by which breaches are neutralized) and inter-organizational studies of performance differentials are required. I suggest that organizations with a low level of IS-defense effectiveness probably experience difficulties at acquiring one or more of the constitutive resources components that I analyzed. Future work could build on my decomposition by associating different resources endowments with different capability levels in an attempt to understand how and why such differences give rise to different IS-defense capabilities, and, as a result, performance differentials between organizations [10, 94]. Prior research argued on conceptual grounds that differences in organizational capabilities should be associated with differences in organization performance [19, 30]. For example, [17] found superior IT capabilities to be associated with high-profit ratios. Hence, stronger IS-defense capabilities can be associated with superior performance as these capabilities mitigate the systemic risk of IS failure and hence economic losses. I believe that future research regarding this overarching link is productive since much prior work suggests that CIPs differ significantly as to their IS-defense capability [34, 50, 76, 98]. As both organizations and academic research strive to find ways and means to improve IS defense, they should study the reasons for such performance differentials.

References

1. Amemiya, T. *Advanced Econometrics* (Harvard university press, 1985).
2. Amit, R. & Schoemaker, P. J. Strategic assets and organizational rent. *Strategic Management Journal* **14,** 33–46 (1993).
3. Anderson, R. *Why Information Security is Hard – an Economic Perspective* in *Seventeenth Annual Computer Security Applications Conference* Annual Computer Security Applications Conference (ACSAC) (IEEE, New Orleans, USA, 2001), 358–365. ISBN: 0-7695-1405-7.
4. Anderson, R. J. *Security Engineering: A Guide to Building Dependable Distributed Systems* (John Wiley & Sons, 2010).
5. Anderson, R. & Fuloria, S. in *Economics of Information Security and Privacy* (eds Moore, T., Pym, D. & Ioannidis, C.) 55–66 (Springer, Boston, USA, 2010). ISBN: 978-1-4419-6967-5.
6. Anderson, R. & Moore, T. The Economics of Information Security. *Science* **314,** 610–613 (2006).
7. Anex, A. L'armée peine à recruter des cyber-spécialistes, plus séduits par Google. *RTS Info* (Oct. 2017).
8. Antonakis, J., Bendahan, S., Jacquart, P. & Lalive, R. On Making Causal Claims: A Review and Recommendations. *The Leadership Quarterly* **21,** 1086–1120 (2010).
9. Arora, A., Krishnan, R., Nandkumar, A., Telang, R. & Yang, Y. *Impact of Vulnerability Disclosure and Patch Availability - An Empirical Analysis* in *Third Workshop on the Economics of Information Security* Third Workshop on the Economics of Information Security. **24** (2004), 1268–1287.
10. Barney, J. & Felin, T. What Are Microfoundations? *Academy of Management Perspectives* **27,** 138–155 (2013).
11. Bartol, K. M. & Srivastava, A. Encouraging Knowledge Sharing: The Role of Organizational Reward Systems. *Journal of Leadership & Organizational Studies* **9,** 64–76 (2002).
12. Baryshnikov, Y. *IT Security Investment and Gordon-Loeb's 1/e rule* in *2012 Workshop on the Ecopnomics of Information Security* Workshop on the Ecopnomics of Information Security (2012).
13. Baxter, G. & Sommerville, I. Socio-technical Systems: From design Methods to Systems Engineering. *Interacting with Computers* **23,** 4–17 (2011).
14. Becker, P. H. Common Pitfalls in Published Grounded Theory Research. *Qualitative Health Research* **3,** 254–260 (1993).
15. Bellais, R., Foucault, M. & Oudot, J.-M. *Économie de la défense* 128 pp. ISBN: 978-2-7071-8223-4 (La Découverte, Paris, France, 2014).
16. Bénabou, R. & Tirole, J. Intrinsic and Extrinsic Motivation. *The Review of Economic Studies* **70,** 489–520 (2003).
17. Bharadwaj, A. S. A Resource-based Perspective on Information Technology Capability and Firm Performance: an Empirical Investigation. *MIS Quarterly,* 169–196 (2000).
18. Bhatt, G. D. Organizing knowledge in the knowledge development cycle. *Journal of knowledge management* **4,** 15–26 (2000).
19. Bhatt, G. D. & Grover, V. Types of Information Technology Capabilities and Their Role in Competitive Advantage: an Empirical Study. *Journal of Management Information Systems* **22,** 253–277 (2005).

20. Blumer, H. Symbolic interactionism. *Contemporary Sociological Theory* **62** (2012).

21. Böhme, R. *The Economics of Information Security and Privacy* ISBN: 978-3-642-39498-0 (Springer, Berlin, Heidelberg, 2013).

22. Bojanc, R. & Jerman-Blažič, B. A Quantitative Model for Information-Security Risk Management. *Engineering Management Journal* **25,** 25–37 (2013).

23. Boockmann, B. & Vaubel, R. The Theory of Raising Rivals' Costs and Evidence from the International Labour Organisation. *The World Economy* **32,** 862–887 (2009).

24. Camisón, C. & Forés, B. Knowledge Absorptive Capacity: New Insights for its Conceptualization and Measurement. *Journal of Business Research* **63,** 707–715 (2010).

25. Cohen, W. M. & Levinthal, D. A. Innovation and Learning: The Two Faces of R&D. *The Economic Journal* **99,** 569–596 (1989).

26. Cohen, W. M. & Levinthal, D. A. Absorptive Capacity: A New Perspective on Learning and Innovation. *Administrative Science Quarterly* **35,** 128–152 (1990).

27. Collis, D. J. Research Note: How Valuable are Organizational Capabilities? *Strategic Management Journal* **15,** 143–152 (1994).

28. Davidson, R., MacKinnon, J. G., *et al.* Estimation and Inference in Econometrics. *OUP Catalogue* (1993).

29. Dertouzos, J. N. *Cost-Effectiveness of Military Advertising: Evidence from 2002-2004* OCLC: 320143725 (RAND Corporation, Santa Monica, USA, 2009).

30. Doherty, N. F. & Terry, M. The Role of IS Capabilities in Delivering Sustainable Improvements to Competitive Positioning. *The Journal of Strategic Information Systems* **18,** 100–116 (2009).

31. Falco, G. *et al.* Cyber Risk Research Impeded by Disciplinary Barriers. *Science* **366,** 1066–1069 (2019).

32. Feledi, D., Fenz, S. & Lechner, L. Toward Web-based Information Security Knowledge Sharing. *Information Security Technical Report* **17,** 199–209. ISSN: 1363-4127 (2013).

33. Felin, T., Foss, N. J., Heimeriks, K. H. & Madsen, T. L. Microfoundations of Routines and Capabilities: Individuals, Processes, and Structure. *Journal of Management Studies* **49,** 1351–1374 (2012).

34. Fisher, R. & Norman, M. Developing Measurement Indices to Enhance Protection and Resilience of Critical Infrastructure and Key Resources. *Journal of Business Continuity & Emergency Planning* **4,** 191–206 (2010).

35. Furnell, S. & Clarke, N. Power to the People? The Evolving Recognition of Human Aspects of Security. *Computers & Security* **31,** 983–988 (2012).

36. Gal-Or, E. & Ghose, A. The Economic Incentives for Sharing Security Information. *Information Systems Research* **16,** 186–208 (2005).

37. Gay, S. Strategic news bundling and privacy breach disclosures. *Journal of Cybersecurity* **3,** 91–108. ISSN: 2057-2085. `https://academic.oup.com/cybersecurity/article/3/2/91/4775012` (2019) (June 1, 2017).

38. Geels, F. W. From Sectoral Systems of Innovation to Socio-technical Systems. *Research Policy* **33,** 897–920 (2004).

39. George, G., Zahra, S. A., Wheatley, K. K. & Khan, R. The Effects of Alliance Portfolio Characteristics and Absorptive Capacity on Performance: A Study of Biotechnology Firms. *The Journal of High Technology Management Research* **12,** 205–226 (2001).

40. Gibson, J. L., Griepentrog, B. K. & Marsh, S. M. Parental Influence on Youth Propensity to Join the Military. *Journal of Vocational Behavior* **70,** 525–541 (2007).

41. Gigerenzer, G. & Selten, R. *Bounded Rationality: The Adaptive Toolbox* (MIT press, 2002).

42. Goerger, S. R., McGinnis, M. L. & Darken, R. P. A Validation Methodology for Human Behavior Representation Models. *The Journal of Defense Modeling and Simulation* **2,** 39–51 (2005).

43. Gordon, L. A. & Loeb, M. P. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)* **5,** 438–457 (2002).

44. Gordon, L. A., Loeb, M. P., Lucyshyn, W. & Zhou, L. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* **34,** 509–519 (2015).

45. Gordon, L. A., Loeb, M. P. & Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security* **7,** 49–59 (2016).

46. Grant, R. M. Prospering in Dynamically-Competitive Environments: Organizational Capability as Knowledge Integration. *Organization Science* **7,** 359–467 (1996).

47. Grant, R. M. The Resource-based Theory of Competitive Advantage: Implications for Strategy Formulation. **33,** 114–135 (1991).

48. Grant, R. M. Toward a Knowledge-Based Theory of the Firm. *Strategic Management Journal* **17,** 109–122 (S2 1996).

49. Griffith, R., Redding, S. & van Reenen, J. R&D and Absorptive Capacity: Theory and Empirical Evidence. *Scandinavian Journal of Economics* **105,** 99–118 (2003).

50. Haimes, Y. Y. On the definition of vulnerabilities in measuring risks to infrastructures. *Risk Analysis: An International Journal* **26,** 293–296 (2006).

51. Helfat, C. E. Stylized Facts, Empirical Research and Theory Development in Management. *STtrategic Organization* **5,** 185–192 (2007).

52. Helfat, C. E. Know-how and Asset Complementarity and Dynamic Capability Accumulation: the Case of R&D. *Strategic Management Journal* **18,** 339–360 (1997).

53. Helfat, C. E. & Peteraf, M. A. The Dynamic Resource-Based View: Capability Lifecycles. *Strategic Management Journal* **24,** 997–1010 (2003).

54. Herath, H. S. & Herath, T. C. Investments in Information Security: A Real Options Perspective With Bayesian Postaudit. *Journal of Management Information Systems* **25,** 337–375 (2008).

55. Hershatter, A. & Epstein, M. Millennials and the World of Work: An Organization and Management Perspective. *Journal of Business and Psychology* **25,** 211–223 (2010).

56. Hiebert, J. & Lefevre, P. Conceptual and Procedural Knowledge in Mathematics: An Introductory Analysis. *Conceptual and Procedural Knowledge: The Case of Mathematics* **2,** 1–27 (1986).

57. Hoffman, L., Burley, D. & Toregas, C. Holistically Building the Cybersecurity Workforce. *IEEE Security & Privacy* **10,** 33–39 (2012).

58. Jane Zhao, Z. & Anand, J. A Multilevel Perspective on Knowledge Transfer: Evidence From the Chinese Automotive Industry. *Strategic Management Journal* **30,** 959–983 (2009).

59. Knight, G. A. & Liesch, P. W. Information Internalisation in Internationalising the Firm. *Journal of Business Research* **55,** 981–995 (2002).

60. Kohn, A. Why Incentive Plans Cannot Work. *Harvard Business Review* **71,** 54–60 (1993).

61. Laube, S. & Böhme, R. The Economics of Mandatory Security Breach Reporting to Authorities. *Journal of Cybersecurity* **2,** 29–41 (2016).

62. Lelarge, M. Coordination in Network Security Games: a Monotone Comparative Statics Approach. *IEEE Journal on Selected Areas in Communications* **30,** 2210–2219. ISSN: 0733-8716 (2012).

63. Li, Y. & Kettinger, W. J. An Evolutionary Information-Processing Theory of Knowledge Creation. *Journal of the Association for Information Systems* **7,** 25 (2006).

64. Liao, S.-H., Fei, W.-C. & Chen, C.-C. Knowledge Sharing, Absorptive Capacity, and Innovation Capability: an Empirical Study of Taiwan's Knowledge-Intensive Industries. *Journal of Information Science* **33,** 340–359 (2007).

65. Makadok, R. Toward a Synthesis of the Resource-based and Dynamic-capability Views of Rent Creation. *Strategic Management Journal* **22,** 387–401 (2001).

66. March, J. G. Exploration and Exploitation in Organizational Learning. *Organization Science* **2,** 71–87 (1991).

67. Matsuura, K. in *Managing Information Risk and the Economics of Security* (ed Johnson, M. E.) 99–119 (Springer, Boston, USA, 2009). ISBN: 978-0-387-09762-6.

68. Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M. & Percia David, D. To Share or Not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing. *Journal of Cybersecurity* **5,** (in print (2019).

69. Moore, T., Kenneally, E., Collett, M. & Thapa, P. *Valuing Cybersecurity Research Datasets* in *Proceedings of the Workshop on the Economics of Information Security (WEIS'19)* Workshop on the Economics of Information Security (WEIS'19) (University of Cambridge, UK, 2019), 1–27.

70. Nelson, R. R. & Winter, S. G. The Schumpeterian tradeoff revisited. *The American Economic Review* **72,** 114–132 (1982).

71. Nielsen, H. Bounded Rationality in an Imperfect World of Regulations: What if Individuals are not Optimizing. *Organization Science* **2,** 439–448 (2012).

72. Nonaka, I. & Takeuchi, H. *The Knowledge-Creating Company : How Japanese Companies Create the Dynamics of Innovation* 1st ed. ISBN: 978-0-19-509269-1 (Oxford University Press, New York, USA, 1995).

73. Park, B. I. Knowledge Transfer Capacity of Multinational Enterprises and Technology Acquisition in International Joint Ventures. *International Business Review* **20,** 75–87 (2011).

74. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. & Jerram, C. Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* **42,** 165–176 (2014).

75. Peri, G. Determinants of Knowledge Flows and Their Effect on Innovation. *Review of Economics and Statistics* **87,** 308–322 (2005).

76. Petit, F. *et al. Resilience Measurement Index: an Indicator of Critical Infrastructure Resilience* tech. rep. (Argonne National Lab.(ANL), Argonne, IL (United States), 2013).

77. Rocha Flores, W., Antonsen, E. & Eling, M. Information Security Knowledge Sharing in Organizations: Investigating the Effect of Behavioral Information Security Governance and National Culture. *Computers & Security* **43,** 90–110 (2014).

78. Safa, N. S. & Von Solms, R. An Information Security Knowledge Sharing Model in Organizations. *Computers in Human Behavior* **57,** 442–451 (2016).

79. Salop, S. C. & Scheffman, D. T. Raising Rivals' Costs. *The American Economic Review* **73,** 267–271 (1983).

80. Sarker, S. & Sarker, S. Exploring Agility in Distributed Information Systems Development Teams: an Interpretive Study in an Offshoring Context. *Information Systems Research* **20,** 440–461 (2009).

81. Scarbrough, H. Knowledge Management, HRM and the Innovation Process. *International Journal of Manpower* **24,** 501–516 (2003).

82. Schatz, D. & Bashroush, R. Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers* **19,** 1205–1228 (2017).

83. Schmidt, T. Absorptive Capacity—One Size Fits All? A Firm-Level Analysis of Absorptive Capacity for Different Kinds of Knowledge. *Managerial and Decision Economics* **31,** 1–18 (2010).

84. Sedenberg, E. M. & Dempsey, J. X. Cybersecurity Information Sharing Governance Structures: An Ecosystem of Diversity, Trust, and Tradeoffs. *Computing Research Repository* (2018).

85. Setia, P., Setia, P., Venkatesh, V. & Joglekar, S. Leveraging digital technologies: How information quality leads to localized capabilities and customer service performance. *MIS Quarterly* **37,** 565–590 (2013).

86. Simon, H. A. A behavioral model of rational choice. *The quarterly journal of economics* **69,** 99–118 (1955).

87. Simon, H. A. Bounded Rationality and Organizational Learning. *Organization Science* **2,** 125–134 (1991).

88. Sirmon, D. G., Hitt, M. A. & Ireland, R. D. Managing firm resources in dynamic environments to create value: Looking inside the black box. *Academy of Management Review* **32,** 273–292 (2007).

89. Sirmon, D. G., Hitt, M. A., Ireland, R. D. & Gilbert, B. A. Resource orchestration to create competitive advantage: Breadth, depth, and life cycle effects. *Journal of management* **37,** 1390–1412 (2011).

90. Stock, J. H., Watson, M. W., *et al. Introduction to Econometrics* (Addison Wesley Boston, 2003).

91. Szulanski, G. Exploring Internal Stickiness: Impediments to the Transfer of Best Practice Within The Firm. *Strategic Management Journal* **17,** 27–43 (1996).

92. Szvircsev Tresch, T. *et al. Sicherheit 2018: Aussen-, Sicherheits- und Verteidigungspolitische Meinungsbildung im Trend* (Center for Security Studies (CSS), ETH Zürich; Militärakademie (MILAK) an der ETH Zürich, Birmensdorf, 2018).

93. Taylor, J. K., Clerkin, R. M., Ngaruiya, K. M. & Velez, A.-L. K. An Exploratory Study of Public Service Motivation and the Institutional–Occupational Model of the Military. *Armed Forces & Society* **41,** 142–162 (2015).

94. Teece, D. J. A Capability Theory of the Firm: an Economics and (Strategic) Management Perspective. *New Zealand Economic Papers* **53,** 1–43 (2019).

95. Tsai, W. Knowledge Transfer in Intraorganizational Networks: Effects of Network Position and Absorptive Capacity on Business Unit Innovation and Performance. *Academy of management journal* **44,** 996–1004 (2001).

96. Von Solms, R. & van Niekerk, J. From Information Security to Cyber Security. *Computers & Security* **38,** 97–102 (2013).

97. Willemson, J. *Extending the Gordon and Loeb Model for Information Security Investment* in *2010 International Conference on Availability, Reliability and Security* 2010 International Conference on Availability, Reliability, and Security (ARES) (IEEE, Krakow, Poland, 2010), 258–261. ISBN: 978-1-4244-5879-0.

98. Yusta, J. M., Correa, G. J. & Lacal-Arántegui, R. Methodologies and Applications for Critical Infrastructure Protection: State-of-the-art. *Energy Policy* **39,** 6100–6119 (2011).

99. Zott, C. Dynamic Capabilities and the Emergence of Intraindustry Differential Firm Performance: Insights from a Simulation Study. *Strategic Management Journal* **24,** 97–125 (2003).

100. Zott, C. & Huy, Q. N. How Entrepreneurs Use Symbolic Management to Acquire Resources. *Administrative Science Quarterly* **52,** 70–105 (2007).

Appendix

'Gutta cavat lapidem.'

— Ovid

Contents of the Appendix

1 Supplement to the Introduction

The following table has been retrieved from Yusta et al., 2011, and recompiled according to IS defense for CIP.

Table a.1: **Description of Platforms Developed for Defending IS of CIPs**

Platform	Acronym	Brief Description	Development Entity
	ATHENA	Software tool. Analysis of interdependent infrastructure networks, including political, military, economic and social aspects. Athena incorporates several sophisticated reasoning algorithms that allow to study the dependence between nodes.	On Target Technologies, Inc. Sponsored by National Laboratories for the U.S. Air Force.
Critical infrastructures interdependencies Integrator		Software tool. Estimates times and costs required to restore a part or the whole set of critical infrastructures in order to return to normality, after an operational interruption.	Argonne National Laboratories
Critical infrastructure modelling system	CIMS	Software tool. Geo-referenced simulation scenarios, to perform sensitivity analysis in decision-making. It facilitates assess risks of infrastructure, including policies, regulations and response plans.	Idaho National Laboratories. Sponsored by U.S. Air Force Laboratories.
Critical infrastructure protection decision support system	CIP/DSS	Software tool. Allows comparing the effectiveness of strategies to reduce the probability of a risk, based upon the study of scenarios that represent the impacts. The model is designed to help analysts and policy makers in the evaluation and selection of the most effective strategies in reducing risk, taking into account the potentially affected infrastructure, the measures of impact and likelihood of an incident.	Argonne National Laboratories

Table a.1 continued from previous page

Platform	Acronym	Brief Description	Development Entity
Critical infrastructure simulation by interdependent agents	CISIA	Software tool. Simulation through a set of interdependent agents with non-linear relationships. It analyzes the short-term effects of decisions on infrastructure, in terms of propagation of faults and performance degradation of the system. Very useful in the analysis of origin and response to emergencies.	University of New Brunswick (Canada)
Agent-based simulation model of the U.S. economy	COMM-ASPEN	Software tool. Agent-based simulation of the effects of both market decisions and interruptions of telecommunications infrastructure in the economy.	Sandia National Laboratories
Distributed engineering workstation.	DEW	Software tool. Intended for asset management, operating procedures, events, planning in short and long term. Suited for spotting and analysis of inter-dependencies in large power systems. There are also applications in hydraulic systems of ships.	Electrical Distribution Design, Inc. Sponsored by DOE and the U.S. Department of Defence
Procedimiento informatico-logico para el analisis de riesgos	EAR-PILAR	Software tool. Characterisation of the assets (spotting, clustering, rating and analyzing dependencies), characterisation of risks, evaluation of safeguards. The tool assesses impact and risk, as well as cumulative, potential and residual effects by enabling the analysis of these risks.	National Cryptology Centre Spain
Electricity market complex adaptive system	EMCAS	Software tool. Simulation through agents, to investigate potential operational and economic impacts on the electrical system, as affected by various external events.	Argonne National Laboratories. Sponsored by ADICA Consulting
Financial system infrastructure	FINSIM	Software tool. Allows representation of U.S. economic services, functioning as complex system decentralised, with autonomy from the interaction of multiple decision nodes, or agents. It applies to scenarios of crisis affecting the banking payment system, the use of plastic money, the federal funds market and the interactions between these entities.	Los Alamos National Laboratories. Sponsored by U.S. Department of Homeland Security

Table a.1 continued from previous page

Platform	Acronym	Brief Description	Development Entity
Failure modes and effects analysis	FMEA-FMECA	Working Methodology. Set of procedures for analyzing potential failures in a system, based upon the severity or the effect of system failures. It is widely used by manufacturing organizations at various stages of product life cycle, and it is also used in the service industry. FMECA is a variant of FMEA.	
	FORT-FUTURE	Software tool. It runs multiple dynamic simulations, evaluating a set of alternatives. Additionally, it is supported on GIS with applications to transportation systems, electricity, water systems, etc.	
Fault tree analysis	FTA	Working Methodology. This deductive technique focuses on a particular accidental event (risk) and provides a method to determine the causes leading to the manifestation of a risk within a system. It provides qualitative results by searching for quantitative critical paths in terms of probability of components failure in a system.	
	GORAF	Software tool. It allows to spot the most critical resources within an infrastructure. It proposes metrics that represent the economic losses and strategic metrics with the outcome of malfunctioning of a resource (usually combined with the tool CISI).	University of New Brunswick (Canada)
	CERT Government Initiatives	Working Methodology. The teams in these initiatives are directly related to the defence ministries in countries where they are deployed. Some cases of successful implementation of these programs are available on the GOVCERT.nl (Netherlands), COLCERT (Colombia), CERT.br (Brazil), Es-CERT (Spain), etc.	

Table a.1 continued from previous page

Platform	Acronym	Brief Description	Development Entity
Hazardous operations	HAZOP	Working Methodology. Set of risk identification techniques based on inductive assumption that the risks, accidents or operations problems, occur as a result of misuse of process variables with respect to the normal operating parameters in a given system and a particular stage.	
Inoperability input– output model	IIM	Software tools. Suite of analytical models to determine the impact of an attack on an infrastructure and the cascading effects on all other interconnected infrastructures (in economic and operating issues). The tool allows representing a system recovery after an attack or event and also allows a temporal analysis in recovery mode.	Sandia National Laboratories and Los Alamos National Laboratories. Sponsored by U.S. Department of Homeland Security
	INTEPOINT VU	Software tool. Allows analysis of planning responses to intentional and unintentional events in infrastructure, taking into account the social and behavioural patterns of the population. (Multi-agent system, combined with a geographical information system of the area being analyzed).	Intepoint LLC. Sponsored by U.S. Department of Defence
	LUND	Working Methodology. Sets the relationships between each of the nodes that make up a system of roads or rail interconnected transport infrastructure. (Grounded Network theory).	University of Lund (Sweden). Sponsored by the International Energy Agency
Metodologia de ana lisis y gestion de riesgos de los sistemas de informacion	MARGERIT	Working Methodology. Focused on digital information, data networks and computer systems protection, in order to determine how much value is at stake and the importance of protecting information.	Higher Council for Electronic Administration of Spain
Methodology for inter-dependencies assessment	MIA	Working Methodology. Used to identify critical interdependencies of the systems that are subject to vulnerabilities.	European Commission

Table a.1 continued from previous page

Platform	Acronym	Brief Description	Development Entity
Multi-network interdependent critical infrastructure program for analysis of lifelines	MUNICIPAL	Software tool. Allows understanding adverse events that affect the interdependence of civil infrastructure as well as responses to events of termination of the provision of health, safety and economic welfare of its citizens. (Databases with information on critical infrastructure connection, and geographic information system).	Rensselaer Polytechnic Institute (US)
Network security risk assessment model	NSRAM	Software tool. Simulation and analysis of large networks in terms of failures or structural damage. It accurately simulates the severity of network failures, and considers the repair variables (time, cost and repair priorities).	James Madison University
Risk maps		Working methodology. Allows carrying out an inventory risk, in an orderly and systematic. For this purpose, risks are analyzed and described along with their possible consequences. This methodology is widely accepted in the spotting of risks due to its simplicity and adaptability to all sectors.	
Urban infrastructure suite	UIS	Software tools. Represents the behavioural simulation of urban infrastructure, its inhabitants, the effects of interdependencies, and the dynamics of their interconnections.	Los Alamos National Laboratories. Sponsored by U.S. Department of Homeland Security

2 Supplement to the Articles

2.1 Officer Selection-Process Related to Part II

The following description details how conscripted-officer candidates are identified in the SAF.

The candidate's potential for a conscripted-officer career is analyzed with respect to the prerequisites of the future function. To be nominated for further selection procedures, a candidate must meet the following conditions:

(A) Has good qualifications in the areas of personal skills and social skills;

(B) Is personally aware of future officer duties;

(C) Has a military performance evaluation score of at least 3 (out of maximum of 5);

(D) Has a physical fitness score of at least 3 (out of maximum of 5);

(E) Shows exemplary attitude and behavior;

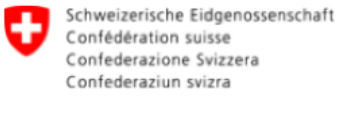
(F) Possesses official certification for any current or completed academic studies or professional training.

With very few exceptions, candidates who meet these criteria are identified during boot camp by senior officers. Eligible candidates who accept to serve as an officer are then invited to an assessment-center-based qualification procedure that tests the candidate's leadership capabilities, personals skills and development capacity, as well as their social, instructive and technical competence. Any candidate could be subject to extensive background screening and long-term security checks. Once the qualification process is complete, results are assessed by senior unit leaders who then make proposals to the SAF's head of recruiting in order to decide which candidates to recruit for officer careers. These candidates are then sent to the Military Academy for further academic studies, language courses, and military training.

2.2 Online Questionnaire of Part III

Incentives and Security Information Sharing

This study is endorsed by :



Pascal Lamia
Head of MELANI

pascal.lamia@isb.admin.ch
058 463 45 06

PD Dr. Marcus M. Keupp
Head of Defense Management

mkeupp@ethz.ch
058 484 82 47

Alain Mermoud, PhD candidate
Study leader

alain.mermoud@milak.ethz.ch
058 484 82 99

You can verify the authenticity of this study and the identity of the authors on the official website of their institutions

Pascal Lamia (Swiss Confederation)
Marcus Matthias Keupp (Military Academy at ETH Zurich)
Alain Mermoud (Military Academy at ETH Zurich)

Or by calling MELANI +4158 46 34506

Dear member of the MELANI closed circle,
Sehr geehrte Mitglieder des "Geschlossenen Kundenkreises" (GK),
Chers membres du cercle fermé,

We are doing a research study in the domain of human aspects of security information sharing in organisations. We would like to understand your incentives and barriers to cybersecurity-relevant information sharing with the Swiss Reporting and Analysis Centre for Information Assurance (MELANI). Your responses will be extremely valuable to build a safer and more resilient Cyberspace. Please find below some information on:

The authors
- This survey is being conducted by the military academy at ETH Zurich with the support of MELANI
- Data collection is led by PD Dr. Marcus M. Keupp and his assistant Alain Mermoud, who is a PhD candidate at the University of Lausanne

The data
- All your responses are collected in Switzerland and treated strictly anonymously

- The collected data will be deleted after all analyses have been performed
- This survey is purely academic and has no financial or business-related interest

Your reward
- You will receive a free study which will support your organisation in the security information sharing process
- Upon request, you will be delivered with a precise picture of how your organisation compares to others. If you decide to receive this reward, only your e-mail address will be disclosed to the study leader.

The questionnaire
- The template is responsive, but we strongly recommend to answer the survey on a desktop or laptop with a trustworthy Internet connection
- The questionnaire takes about 15-20 minutes to complete
- The questionnaire is only available in English, but the study leader can support you in French and German
- Please direct any questions directly to alain.mermoud@milak.ethz.ch or +4158 484 82 99

Definition and scope
- Security information sharing is an activity consisting of sharing cybersecurity-relevant information between cybersecurity stakeholders. For the sake of brevity, we will refer to this activity as "security information sharing" (SIS) throughout the questionnaire
- Organisations typically exchange information on vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence, best practices, early warnings, and expert advices and insights (Luiijf & Klaver, 2015)
- Please note that this study attempts to capture your SIS activities with MELANI only. Please ignore other SIS activities, such as SIS with other Information Sharing and Analysis Centers (ISACs) or bilateral SIS
- The unit of analysis is yourself. **Please answer the questions based on your personal experiences, and not on behalf of your organisation!**

Incentives and Security Information Sharing

Controls

Control variables are necessary to eliminate distortions.

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

1. Gender*
   - ◯ Male
   - ◯ Female
   - ◯ Other, please specify
   - [ ]

2. What is your mother tongue?*
   - ◯ German
   - ◯ French
   - ◯ English
   - ◯ Italian
   - ◯ Other, please specify
   - [ ]

3. What is your age group?*
   - ◯ Below 21
   - ◯ 21 to 30
   - ◯ 31 to 40
   - ◯ 41 to 50
   - ◯ above 50

4. Which education level did you achieve?*
   - ◯ No education
   - ◯ Diploma
   - ◯ Bachelor
   - ◯ Master
   - ◯ PhD
   - ◯ Other, please specify
   - [ ]

5. What is your position in your organisation?*
   - ◯ Employee
   - ◯ Chief employee
   - ◯ Middle management
   - ◯ Management
   - ◯ Member of the board
   - ◯ Other, please specify
   - [ ]

6. In which field does your organisation operate?*
   - Chemical / Pharmaceutical

- ( )
- ( ) Banking & Finance
- ( ) Administration
- ( ) Energy
- ( ) Telecommunication / IT
- ( ) Insurance
- ( ) Transport and logistic
- ( ) Industry
- ( ) Health
- ( ) Other, please specify

7. Fow how many years have you overseen Security Information Sharing (SIS)?*
   ( ) Not in charge ( ) less than 1 ( ) 1 to 3 ( ) 3 to 6 ( ) over 6

8. What is the workload related to SIS in your organisation (in full-time equivalent)?*
   ( ) 0
   ( ) 0-1
   ( ) 1-2
   ( ) 2-3
   ( ) over 3

9. How would you rate your general level of IT knowledge*
   ( ) Excellent ( ) Good ( ) Neutral ( ) Fair ( ) Poor

10. How many people work in your organisation?*
    ( ) 1 ( ) 1 - 20 ( ) 20 - 100 ( ) 100 - 250 ( ) over 250

11. In which year did your organisation become a member of MELANI?*
    -- Please Select --

12. Have you participated in MELANI workshops / events?*
    -- Please Select --

13. What is the level of IT outsourcing in your organisation?*
    ( ) Very Significant ( ) Significant ( ) Neutral ( ) Insignificant ( ) Very Insignificant

14. What is the level of internationalisation of your organisation (shareholding, clients, subsidiaries, etc.)?*
    ( ) Very Significant ( ) Significant ( ) Neutral ( ) Insignificant ( ) Very Insignificant

15. What is your level of satisfaction with MELANI services?*
    ( ) Very Satisfied ( ) Satisfied ( ) Neutral ( ) Dissatisfied ( ) Very Dissatisfied

16. How are your personal relationships with your peers (other MELANI participants)?*
    ( ) Very Friendly ( ) Friendly ( ) Neutral ( ) Unfriendly ( ) Very Unfriendly

17. Which amount of exclusive information do you receive through SIS with MELANI?
    ( ) Very Small ( ) Small ( ) Neutral ( ) Large ( ) Very Large

Incentives and Security Information Sharing

Frequency

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

18. Generally, I have a lot of information to share*
Strongly Agree Agree Neutral Disagree Strongly Disagree

19. I frequently share my experience about information security with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

20. I frequently share my information security knowledge with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

21. I frequently share my information security documents with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

22. I frequently share my expertise from my information security training with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

23. I frequently talk with others about information security incidents and their solutions in MELANI workshops*
Strongly Agree Agree Neutral Disagree Strongly Disagree

24. I share a new information with other participants*
- Never
- Rarely, in less than 10% of the chances when I could have
- Occasionally, in about 30% of the chances when I could have
- Sometimes, in about 50% of the chances when I could have
- Frequently, in about 70% of the chances when I could have
- Usually, in about 90% of the chances I could have
- Every time

Incentives and Security Information Sharing

Intensity

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

25. How often do you comment on shared information?*
- Never
- Rarely, in less than 10% of the chances when I could have
- Occasionally, in about 30% of the chances when I could have
- Sometimes, in about 50% of the chances when I could have
- Frequently, in about 70% of the chances when I could have
- Usually, in about 90% of the chances I could have
- Every time

26. How intensely do you react to the comments of other participants?*
- Not at all
- Little
- Moderate
- Significant
- Always

27. I often react to comments in the community*

Strongly Agree Agree Neutral Disagree Strongly Disagree

28. I often use the community to provide comments*
Strongly Agree Agree Neutral Disagree Strongly Disagree

29. I comment in the community as much as possible*
Strongly Agree Agree Neutral Disagree Strongly Disagree

30. I am very interested in sharing knowlege with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

31. I usually spend a lot of time reacting to comments*
Strongly Agree Agree Neutral Disagree Strongly Disagree

32. I usually actively share my knowledge with MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Value of information

Please answer the questions based on your personal experiences and not on behalf of your organisation!

33. I believe SIS is a useful behavioral tool to safeguard the organization's information assets*
Strongly Agree Agree Neutral Disagree Strongly Disagree

34. My SIS has a positive effect on mitigating the risk of information security breaches*
Strongly Agree Agree Neutral Disagree Strongly Disagree

35. SIS is a wise behavior that decreases the risk of information security incidents*
Strongly Agree Agree Neutral Disagree Strongly Disagree

36. SIS would decrease the time needed for my job responsibilities*
Strongly Agree Agree Neutral Disagree Strongly Disagree

37. SIS would increase the effectiveness of performing job tasks*
Strongly Agree Agree Neutral Disagree Strongly Disagree

38. Considering all aspects, SIS would be useful*
Strongly Agree Agree Neutral Disagree Strongly Disagree

39. I can’t seem to find the time to share knowledge in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

40. It is laborious to share knowledge in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

41. It takes me too much time to share knowledge in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

42. The effort is high for me to share knowledge in the community*

Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Reciprocity

Please answer the questions based on your personal experiences and not on behalf of your organisation!

43. I believe that it is fair and obligatory to help others because I know that other people will help me some day*
Strongly Agree Agree Neutral Disagree Strongly Disagree

44. I believe that other people will help me when I need help if I share knowledge with others through MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

45. I believe that other people will answer my questions regarding specific information and knowledge in the future if I share knowledge with others through MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

46. I think that people who are involved with MELANI develop reciprocal beliefs on give and take based on other people's intentions and behavior*
Strongly Agree Agree Neutral Disagree Strongly Disagree

47. I expect to be rewarded with a higher salary in return for sharing knowledge with other participants*
Strongly Agree Agree Neutral Disagree Strongly Disagree

48. I expect to receive monetary rewards (i.e. additional bonus) in return for sharing knowledge with other participants*
Strongly Agree Agree Neutral Disagree Strongly Disagree

49. I expect to receive opportunities to learn from others in return for sharing knowledge with other participants*
Strongly Agree Agree Neutral Disagree Strongly Disagree

50. I expect to be rewarded with an increased job security in return for sharing knowledge with other participants*
Strongly Agree Agree Neutral Disagree Strongly Disagree

51. My acts of knowledge sharing and seeking strengthen the ties of obligation between existing participants*
Strongly Agree Agree Neutral Disagree Strongly Disagree

52. My acts of knowledge sharing and seeking create the obligations with other members within MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

53. My acts of knowledge sharing and seeking expand the scope of my association with other members within MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

54. My acts of knowledge sharing and seeking will encourage cooperation among MELANI participants in the future*
Strongly Agree Agree Neutral Disagree Strongly Disagree

55. My acts of knowledge sharing and seeking create strong relationships with members who have common interests within MELANI*
Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Institutional design

Please answer the questions based on your personal experiences and not on behalf of your organisation!

56. A centralized sharing model - such as a relational database like a forum - would allow me to engage in more SIS activities*
Strongly Agree Agree Neutral Disagree Strongly Disagree

57. A decentralized sharing model - such as a distributed database like blockchain - would encourage me to engage in more SIS activities*
Strongly Agree Agree Neutral Disagree Strongly Disagree

58. Formalization would allow me to engage in more SIS activities*
Formalization is the extent to which work roles are structured in an organization, and the activities of the employees are governed by rules and procedures.
Strongly Agree Agree Neutral Disagree Strongly Disagree

59. Standardization would allow me to engage in more SIS activities*
Standardization is the process of implementing and developing technical standards based on the consensus of different parties.
Strongly Agree Agree Neutral Disagree Strongly Disagree

60. SIS is of value in my organization*
Strongly Agree Agree Neutral Disagree Strongly Disagree

61. The management appreciates employees for their SIS*
Strongly Agree Agree Neutral Disagree Strongly Disagree

62. The management awards employees for their SIS*
Strongly Agree Agree Neutral Disagree Strongly Disagree

63. The management encourages employees to utilise SIS*
Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Reputation

Please answer the questions based on your personal experiences and not on behalf of your organisation!

64. Sharing knowledge can enhance my reputation in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

65. I get praises from others by sharing knowledge in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

66. I feel that knowledge sharing improves my status in the community*
Strongly Agree Agree Neutral Disagree Strongly Disagree

67. I can earn some feedback or rewards through knowledge sharing that represent my reputation and status in the

community*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

68. My colleagues respect me when I share my information security knowledge*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

69. The others have a positive opinion when I share my information security knowledge*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

70. The management asked me to help others in terms of information security*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

71. Employees have a positive image about me due to their evaluation of my information security knowledge*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

Incentives and Security Information Sharing

Trust

Please answer the questions based on your personal experiences and not on behalf of your organisation!

72. I believe that my colleague's information security knowledge is reliable*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

73. I believe that my colleague's information security knowledge is effective*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

74. I believe that my colleague's information security knowledge mitigates the risk of information security breaches*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

75. I believe that my colleague's information security knowledge is useful*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

76. I believe that my colleagues would not take advantage of my information security knowledge that we share*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

77. I believe that people in my network give credit for each other's knowledge where it is due*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

78. I believe that people in my network respond when I am in need*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

79. I believe that people in my network use each other's knowledge appropriately*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

80. I believe that my requests for knowledge will be answered*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

81. I believe that people in my network share the best knowledge that they have*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

Incentives and Security Information Sharing

You are almost at the end of the survey

Please answer the questions based on your personal experiences and not on behalf of your organisation!

82. SIS satisfies my desire for acquiring information security skills*
Strongly Agree Agree Neutral Disagree Strongly Disagree

83. SIS satisfies my sense of curiosity*
Strongly Agree Agree Neutral Disagree Strongly Disagree

84. I enjoy it when I gain knowledge about information security through knowledge sharing*
Strongly Agree Agree Neutral Disagree Strongly Disagree

85. I feel pleasure when I share my knowledge about information security*
Strongly Agree Agree Neutral Disagree Strongly Disagree

86. I am interested in SIS*
Strongly Agree Agree Neutral Disagree Strongly Disagree

87. I have the necessary knowledge about information security to share with the other staff*
Strongly Agree Agree Neutral Disagree Strongly Disagree

88. I have the ability to share information security knowledge to mitigate the risk of information security breaches*
Strongly Agree Agree Neutral Disagree Strongly Disagree

89. SIS is an easy and enjoyable task for me*
Strongly Agree Agree Neutral Disagree Strongly Disagree

90. I have the useful resources to share SIS with the other employees*
Strongly Agree Agree Neutral Disagree Strongly Disagree

91. I am willing to share my information security knowledge because of its potential to reduce cyber risks*
Strongly Agree Agree Neutral Disagree Strongly Disagree

92. I will share my information security experiences with my colleagues to increase their cyber threat awareness*
Strongly Agree Agree Neutral Disagree Strongly Disagree

93. I will inform the other staff about new methods and software that can reduce the risk of information security*
Strongly Agree Agree Neutral Disagree Strongly Disagree

94. I will share the report on information security incidents with others, in order to reduce the risk*
Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Last page

Please answer the questions based on your personal experiences and not on behalf of your organisation!

95. According to your experience, the number of participants in the MELANI closed circle is*

Very Small | Small | Neutral | Large | Very Large

96. I prefer to engage in SIS activities that involves participants from the entire Critical Infrastructure closed circle ("Geschlossene Kundenkreis" / "cercle fermé")*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

97. I prefer to engage in SIS activities that involves participants from my industry*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

98. I prefer to engage in SIS activities that involves participants from the MELANI staff only*

Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree

99. Do you want to leave a general comment on this study?
For instance, you can describe your personal incentives and barriers to engage in SIS activities or your favorite service provided by MELANI.

100. Upon request, you will be delivered with a precise picture of how your organisation compares to others. If you decide to receive this reward, please enter your e-mail address below. It will only be disclosed to the study leader.

Again, thank you very much for your cooperation! Best regards,
Alain Mermoud, PhD candidate
Study leader
alain.mermoud@milak.ethz.ch
+4158 484 82 99

3 Other Related Scientific Contributions

Related scientific contributions that are intrinsically linked to my PhD, but not explicitly discussed in this manuscript, are presented here. They are related to (1) additional scientific publications that I co-authored, (2) the blind reviewing of scientific works, and (3) assistantship and supervision of academic research.

3.1 Additional Publications

During the last four years, I have co-authored four publications related to security-information sharing (SIS) research projects. As presented in Part III of this manuscript, SIS constitutes an effective means for an organization to learn from its members. Such a learning process is related to the acquisition of cyber-security-relevant information for protecting critical infrastructures (CIs). SIS is therefore an interesting subject of study that helps us to defend IS of CIPs. These additional four publications are presented hereunder, and are based on the same online questionnaire that I analyzed in Part III of this thesis.

Journal Paper: Journal of Cybersecurity

The following journal paper was first published in the post-proceedings of the *17th Annual Workshop on the Economics of Information Security*, held in Innsbruck, Austria, on June 18-20, 2018. This paper was later readapated, revised and resubmitted for publication in the *Journal of Cybersecurity* on February 28, 2019:

> Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2019). *To Share or Not to Share: A Behavioral Perspective on Human Participation in Security-Information Sharing*, Vol. 5, No. 1. Journal of Cybersecurity (in print).

Abstract

Security-information sharing (SIS) is an activity whereby individuals exchange information that is relevant for analysis in order to prevent cyber-security incidents. However, despite technological advances and increased regulatory pressure, human individuals still seem reluctant to share security information. To date, few contributions have addressed this research gap. We adopt an interdisciplinary approach, and we propose a behavioral framework that theorizes how and why human behavior and SIS can be associated. We use psychometric methods to test these associations, analyzing a unique sample of 262 human Information Sharing and Analysis Centre (ISAC) members who share real security information. We also provide a dual empirical operationalization of SIS by introducing the measures of SIS frequency and intensity. We find significant associations between human behavior and SIS. Thus, we contribute to clarifying why SIS, though beneficial, is underutilized by pointing to the pivotal role of human behavior for economic outcomes. Hence, we add to the growing field of the economics of information security. By the same token, we inform managers and regulators about the significance of human behavior, as they propagate goal alignment and shape institutions. Finally, we define a broad agenda for future research on SIS.

Keywords— security-information sharing; psychometrics; economics of information security; behavioral economics; behavioral psychology.

Conference Paper and Post-Proceedings: WEIS 2018

The following conference paper was presented at the *17th annual Workshop on the Economics of Information Security* (WEIS 18), held in Innsbruck, Austria, on the June 18-20, 2018:

> Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). *Incentives for Human Agents to Share Security Information: A Model and an Empirical Test.* In Proceedings of the 17th Workshop on the Economics of Information Security (WEIS), Innsbruck, Austria.

This paper was accepted as a full paper, among 22 other full paper reviewed and selected from a total of 57 submissions.

Abstract

In this paper, we investigate the role of incentives for security-information sharing (SIS) between human agents working in institutions. We present an incentive-based SIS system model that is empirically tested with an exclusive dataset. The data was collected with an online questionnaire addressed to all participants of a deployed Information Sharing and Analysis Center (ISAC) that operates in the context of critical infrastructure protection (N=262). SIS is measured with a multidimensional approach (intensity, frequency) and regressed on five specific predicators (reciprocity, value of information, institutional barriers, reputation, trust) that are measured with psychometric scales. We close an important research gap by providing, to the best of our knowledge, the first empirical analysis on previous theoretical work that assumes SIS to be beneficial. Our results show that institutional barriers have a strong influence on our population, i.e., SIS decision makers in Switzerland. This lends support to a better institutional design of ISACs and the formulation of incentive-based policies that can avoid non-cooperative and free-riding behaviours. Both frequency and intensity are influenced by the extent to which decision makers expect to receive valuable information in return for SIS, which supports the econometric structure of our multidimensional model. Finally, our policy recommendations support the view that the effectiveness of mandatory security-breach reporting to authorities is limited. Therefore, we suggest that a conducive and lightly regulated SIS environment – as in Switzerland – with positive reinforcement and indirect suggestions can "nudge" SIS decision makers to adopt a productive sharing behaviour.

Keywords— security-information sharing; incentives; psychometrics; economics of information security; behavioral economics.

Conference Paper and Post-proceeding: CRITIS 2018

The following conference paper was presented at the *13th International Conference on Critical Information Infrastructure Security* (CRITIS 2018), held in Kaunas, Lithuania, on October 24-26, 2018:

> Mermoud, A., Keupp, M. M., & Percia David, D. (2019). *Governance Models Preferences for Security-Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection.* In Lectures Notes in Computer Science (pp. 179-190). Springer, Cham.

This paper was accepted as a full paper, among 16 other full papers and 3 short papers reviewed and selected from a total of 61 submissions.

Abstract

Empirical studies analyzed the incentive mechanisms for sharing security information between human agents, a key activity for critical infrastructure protection. However, recent research shows that most Information Sharing and Analysis Centers do not perform optimally, even when properly regulated. Using a meso-level of analysis (i.e., information sharing organizations), we close an important research gap by presenting a theoretical framework that links institutional economics and security-information sharing. We illustrate this framework with a dataset collected through an online questionnaire addressed to all critical infrastructures (N=262) that operates at a Swiss Reporting and Analysis Centre for Information Security. Using descriptive statistics, we investigate how institutional rules offer human agents an institutional freedom to design an efficient security-information sharing artifact. Our results show that a properly designed artifact can positively reinforce human agents to share security information and find the right balance between three governance models: (a) public–private partnership, (b) private, and (c) government-based. Overall, our work lends support to a better institutional design of security-information sharing and the formulation of policies that can avoid non-cooperative and free-riding behaviors that plague cyber-security.

Keywords— economics of information security; security-information sharing; new institutional economics; information sharing and analysis center; critical infrastructure protection; information assurance.

Conference Paper and Post-Proceedings: CRITIS 2016

The following conference paper was presented at the *11th International Conference on Critical Information Infrastructure Security* (CRITIS 2016), held in Paris, France, on October 10-12, 2016. It has been later published in the post-proceedings of the aforementioned conference:

Mermoud, A., Keupp, M. M., Ghernaouti, S., & Percia David, D. (2016). *Using Incentives to Foster Security-Information Sharing and Cooperation: a General Theory and Application to Critical Infrastructure Protection.* In International Conference on Critical Information Infrastructures Security (pp. 150-162). Springer, Cham.

This paper was accepted as long paper among 22 other full papers and 8 short papers reviewed and selected from a total of 58 submissions.

Abstract

There is a conspicuous lack of investment in cyber-security. Various measures have been proposed to mitigate this. Investment models theoretically demonstrate the potential application of security-information sharing (SIS) to critical-infrastructure protection (CIP). However, the free-rider problem remains a major pitfall, preventing the full potential benefits of SIS from being realized. We closed an important research gap by providing a theoretical framework that

links incentives with voluntary SIS. We apply this framework to CIP through a case study of the Swiss Reporting and Analysis Centre for Information Security, and we use the SIS model to analyze the incentive mechanisms that most effectively support SIS for CIP. Our work contributes to an understanding of the free-rider problem that plagues the provision of the public good that is cyber-security, and we offer clues to its mitigation.

Keywords— cyber-security economics; free-rider problem; security-information sharing; information assurance.

3.2 Reviewer for a Scientific Journal

The second article presented in Part II of this manuscript was published in *Armed Forces & Society*. Given the military recruitment aspects of this publication, I was asked to blind review a manuscript that was submitted for publication in this same journal.

3.3 Assistantship and Supervision

Working in parallel with my research projects, I was also involved in the assistenship of a lecturer, the editing of two books and one supervision of one's bachelor thesis.

PhD Assistant at the University of Lausanne

During the autumn semester of 2017, I was a PhD assistant for the lecture entitled *Cybercrime and Cyberpower* given by Prof. Dr. Solange Ghernaouti. This lecture is part of the *Master of Law in Legal Issues, Crime and Security of Information Technologies*. During this semester, I lectured five sessions and assisted the students in their seminars and presentations.

Assistant Editor of the Book *The Security of Critical Infrastructures*

As a scientific collaborator and researcher at the Military Academy of ETH Zurich, I assisted the editor PD Dr. Marcus Matthias Keupp in the coordination and editing of the book *The Security of Critical Infrastructures*, published by Springer in late 2019. In this respect, various synergies were developed with the experts in the domain of CIP, which helped me to shape the structure of my thesis.

Assistant Editor of the Book *Defense Economics*

Before assisting the coordination and editing of the the book *The Security of Critical Infrastructures*, my efforts were directed also editing the book entitled *Defense Economics* published by Springer in early 2019. The application of the capability theory in the defense and security domains were developed in this book, which eventually helped me apply the same theory to IS defense for CIP.

Bachelor Thesis Supervision

During the autumn semester of 2018 and the spring semester of 2019, I supervised the bachelor's thesis of Florain Mauri, a student at the Military Academy of ETH Zurich. His bachelor's thesis was methodologically related to the research project presented in Part II of this manuscript.

Research subject– As part of its commitments/support to third parties, the Swiss Army supports various events such as the *2016 Federal Wrestling Festival* in Estavayer, the

Patrouille des Glaciers and other events. In the context of such a service, the diversity of costs, their extent and aggregation are only rarely identified and analyzed. Consequently, there is a lack of overall vision, transparency, and clarity regarding the impact of such costs on public finances.

These various costs are of a direct or indirect nature, borne by the Swiss Army and/or generated by it and involving municipalities, cantons or other departments. These costs are divided into different types: operational and/or logistical. They also involve Loss of Earnings Insurance (APG/EO) and generate competition for local companies, thus causing them to lose revenue (opportunity-cost). The wide range of costs of such a commitment/support to third parties thus far exceeds the costs of the rehearsal courses and the company's accounting.

To our knowledge, a global vision of finance and a rigorous approach to cost accounting, as well as a systematic review of the various costs generated by such commitments to/support of third parties, have never been the subject of a scientific study. By studying the case of the *2016 Federal Wrestling Festival* in Estavayer, this bachelor's thesis sheds light on the opportunity-cost that such a commitment to/support of third parties generates for public finances – at the three political levels: municipal, cantonal, federal.
Research question(s)– In order to investigate the research topic described above, it is necessary to address the following question:

> *What is the aggregate cost – borne by public finances, and considered as a opportunity-cost – of the commitment to/support of third parties that the Swiss Army generated during the 2016 Federal Wrestling Festival in Estavayer?*

From this main question flow the following underlying questions:

- *What are the different costs generated by the commitment to/support of third parties provided by the Swiss Army for the 2016 Federal Wrestling Festival in Estavayer? And which public finance bodies are involved?*
- *What is the cost and opportunity borne by local companies as a result of the fact that they are not used to provide the services as they are performed by the engagement to/support of third parties offered by the Swiss Army?*
- *What is the cost and opportunity borne by companies that employ militiamen absent during military service?*
- *By cascade effect, what is the opportunity-cost borne by the tax offices on these first two opportunity costs (lack of tax revenue)?*
- *What is the opportunity-cost borne by the three political levels: communal, cantonal, and federal?*

4 Research Dissemination

During the last two years of my PhD research, I took the opportunity to disseminate my research through diverse occasions: Three positions as an invited lecturer at Swiss universities, two talks for practitioners, and six white papers gave me the occasion to spread my research results among students and practitioners.

4.1 Invited Lecturer, Swiss Federal Institute of Technology (ETHZ)

During the autumn semester of 2018, I was invited as a lecturer for the lecture entitled *Defense Economics II*, at ETH Zurich. This lecture is part of the bachelor degree in political science and is a prerequisite for professional military officers of the Swiss Armed Forces.

The theme of my lecture was entitled *Geopolitics and Geoeconomics of Information Systems*. I analyzed central concepts related to the III^{rd} and IV^{th} industrial revolutions such as its novel means of production, systemic risks, CIP, numerical sovereignty, numerical hegemony strategies and the Power to Coerce (P2C). The focus was then put on how to acquire and maintain political and/or economic power in the Information Age.

4.2 Invited Lecturer, University of Lausanne (UNIL)

During my assignment as a PhD assistant at the Department of Information Systems (HEC Lausanne) in the autumn semester of 2017, I gave three lectures inspired by the academic field of the *Economics of Information Security*. This lecture is part of the Master of Law in Legal Issues, Crime and Security of Information Technologies.

My lecture was entitled *What can Economics bring to the Security of Information Systems*. I analyzed the central concepts related to the alignment of incentives between principals and agents, what is takes for designing efficient information systems under a socio-technical perspective, and some aspects related to the numerical footprint and privacy concerns.

4.3 Invited Lecturer, University of Geneva (UNIGE)

I was also invited as lecturer for the *MAS Sécurité globale et résolution de conflits* at the Univesity of Geneva at three different occasions in 2018 and 2019.

My lecture was entitled *Smart Power in the Information Age*. Similarly to the lecture I gave at ETH Zurich, I analyzed the central concepts related to the III^{rd} and IV^{th} industrial revolutions, such as their novel means of production, systemic risks, CIP, numerical sovereignty, numerical hegemony strategies and the Power to Coerce (P2C). The focus was, however, put on what it takes for governments to apply economical, political and diplomatic pressure in order to acquire and maintain political and/or economic power through smart power methods related to the Information Age.

4.4 Invited Talks

During my four years as a PhD candidate, I was also invited to give a few talks related to my research projects:

- On February 17, 2016, for the *Höhere Stabsoffiziere* (HSO) Seminar, gathering all senior staff officers of the Swiss Armed Forces – in the rank of brigadier (one-star general), major general (two-star general), or lieutenant general (three-star general) –, held in Bern, Switzerland;
- On December 6, 2016, in French, for the *Association suisse de la sécurité de l'information* (CLUSIS) held in Geneva, Switzerland;
- On December 13, 2016, for the 30^{th} *De Nouvelles Architectures pour les Communications* (DNAC 2016) held at *Télécom ParisTech*, in Paris, France;
- On October 19, 2017, for the 1^{st} *Cyber-Security in Networking Conference* (CSNet'17) held in Rio de Janeiro, Brazil.

4.5 Practitioners' Magazines and Newspapers

During these four years, I also had the opportunity to write several vulgarized articles for information professionals and security experts:

- Percia David, D. & Mermoud, A. (2016). *La LRens, pour réduire le vide stratégique numérique*, in Le Temps (21.09.2016);
- Mermoud, A., & Percia David, D. (2016). *L'intelligence économique : Du renseignement militaire au renseignement privé*, in Revue Militaire Suisse (RMS+), No 4;
- Percia David, D. & Mermoud, A. (2016). *L'attractivité du service militaire : garantie d'un système sécuritaire efficace*, in Revue Militaire Suisse (RMS+), No 6;
- Keupp M.M., Mermoud, A., & Percia David, D. (2017). *Pour une approche économique de la cybersécurité*, in Military Power Revue, No 1;
- Keupp M.M., Mermoud, A., & Percia David, D. (2018). *Teile und herrsche: Cybersicherheit durch Informationsaustausch*, in Allgemeine Schweizerische Militärzeitschrift (ASMZ), No 7;
- Keupp M.M., Percia David, D. & Mermoud, A. (2018). *Teile und herrsche: Cybersicherheit durch Fusionszentren*, in Allgemeine Schweizerische Militärzeitschrift (ASMZ), No 13;
- Percia David, D., & Mermoud, A. (2018). *La souveraineté du renseignement : un besoin stratégique grandissant*, in Revue Militaire Suisse (RMS+), No 6;
- Mermoud, A., & Percia David, D. (2018). *Produire du renseignement grâce au partage d'information*, in Revue Militaire Suisse (RMS+), No 6;
- Percia David, D. & Mermoud, A. (2018). *Les fusion centers: le renseignement sous stéroïdes?*, in Revue Militaire Suisse (RMS+), No 6.
- Percia David, D. & Mermoud, A. (2019). *Canvas pour le développement d'une capacité de cyberdéfense*, in Revue Militaire Suisse (RMS+), No 6.

Dimitri PERCIA DAVID

Chemin de Bellerive 1
1007 Lausanne (VD), Switzerland
+41 79 442 48 30 – dimitri.percia.david@gmail.com
ORCID: 0000-0002-9393-1490

March 1st, 1986
Single
Swiss, Brazilian

Goal: Develop and Orchestrate Cyber-Security Capabilities for Critical-Infrastructure Protection

As a researcher in information systems at HEC Lausanne and at ETH Zurich, my goal is to provide actionable novelties in the field of information-systems security for critical-infrastructure protection.

Adopting a socio-technical perspective of information systems, I apply microeconomics to the field of information-systems security, and I mobilize strategic management theories related to organizational capabilities.

My research focus is based on the development of an information-systems defense capability – through the investment in effective technologies, cost-benefit analysis of human-resource recruitment, and the analysis of human behavior in tacit knowledge acquisition related to cyber-security.

PROFILE

RESEARCH EXPERIENCE
- 8 scientific publications (double blind peer-reviewed)
- Defining novel and relevant research questions
- Elaborating empirical studies and surveys
- Delivering strategic insights based on research results

DATA ANALYSIS EXPERIENCE
- Providing data mining and metadata analysis
- Delivering econometric, quantitative, statistical analysis
- Qualitative, sociological analysis, survey research methods

ECONOMIST AND POLITICAL-SCIENTIST BACKGROUND
- Providing applied macro-/microeconomic analysis
- Delivering performance measurement and benchmarking
- Providing in-depth international-relations analysis
- Deep knowledge in economic and political issues

MANAGEMENT EXPERIENCE
- Leadership Training Center certifications (Swiss Army)
- Managing a team of 240 stakeholders (captain)
- Mobilizing resources efficiently and effectively
- Planning, organizing and leading efforts towards goals

COMMUNICATION SKILLS
- Delivering concise and clear management insights
- International exposure – collaboration with 4 continents
- Proactive communication oriented

ORGANIZATIONAL SKILLS
- Prioritizing on urgency and importance criteria
- Planning and delivering on time
- Coping under pressure

WORK EXPERIENCES

SCIENTIFIC COLLABORATOR/LECTURER — 2015 – today
Military Academy at ETH Zurich, attached to the Swiss Federal Department of Defense– Birmensdorf
Providing in-depth economic analysis and contributing to independent researches on cyber-security

- Assistant for the Defense-Economics lecture at the ETH Zurich;
- Cost-benefit analysis within the Swiss Armed Forces;
- Researcher on cyber-security-capabilities development for critical infrastructure.

TRADING INTELLIGENCE / ECONOMETRICIAN — 2013 – 2015
Cargill International SA (Alvean) – Geneva
Providing trading-intelligence insights leading to more informed investment decisions

- Applied quantitative research aiming to deliver timely and actionable trading insights;
- Econometric forecast of fuel consumption and impacts assessment on related markets;
- Statistical assessment of soft-commodities diversion for meeting biofuels demand;
- Monitoring economic policies and measuring their potential impact on trade;
- Long-term consumption and price-elasticity of demand analysis;
- Report writing on applied-research results and conclusions.

MARKET ANALYST 2012 – 2013
Platts (inc. Kingsman) – Lausanne
Consultancy-based analysis and reports writing on the international sugar market

· Quantitative and qualitative economic/financial market analysis;
· Data-mining and cluster analysis;
· Consultancy and reports production for customers.

INVITED RESEARCHER 2011 – 2012
Center for the Study of Development Strategies – Rio de Janeiro
Econometric researcher focused on crime impact on economic growth

· Public policy recommendations in macroeconomic*;*
· Consultancy based on the impact of crime on the formal economic growth.

CAVALRY OFFICER (Captain, Company commander, NATO OF-2) 2006 - today
Armored Task Force of the Swiss Army – Thun
Leading and managing a battle-tank company of 190 soldiers 14 officers and 35 sergeants

· Captain (company commander)
· Recognized as best officer candidate among 68 participants – Pz/Art OS 22-1.

EDUCATION

UNIVERSITÉ DE LAUSANNE, Switzerland – HEC, Faculty of Business and Economics 2015 - 2019
· PhD in Information Systems: *Three Articles on the Economics of Information-Systems Defense Capability: Material-, Human-, and Knowledge-Resources Acquisition for Critical Infrastructures.*

UNIVERSIDADE ESTADUAL DO RIO DE JANEIRO, Brazil – Faculty of Economic Sciences 2011 - 2012
· Master Thesis in Applied Econometrics: *The Detrimental Impact of Crime on the Formal Economic Growth: Evidence from Rio de Janeiro.*

UNIVERSITÉ DE NEUCHÂTEL, Switzerland – Faculty of Economic Sciences 2010 - 2012
· Master of Science in Applied Economics, Major in Economic Policy.

UNIVERSITÉ DE LAUSANNE, Switzerland – Faculty of Political Science 2006 - 2009
· Bachelor of Arts in Political Science, Major in International Relations.

LEADERSHIP TRAINING CENTER, Switzerland – Swiss Army 2006 - 2012
· Leadership training for Army leaders and managers;
· Certificates in communication and information, conflict management, group command, command techniques, psychology of command, self-knowledge.

LANGUAGES

FLUENT
· English: C1
· French: mother tongue
· Portuguese: mother tongue

ADVANCED
· German: B1

BASICS
· Italian: C1 as passive, B2 as active
· Spanish: C1 as passive, A2 as active

COMPUTER SKILLS

· EViews
· R
· Stata
· MS Office
· HTML
· LaTeX

EXTRACURRICULAR ACTIVITIES

· Alpinism, *trad* climbing, ice climbing, dry tooling, backcountry skiing, "Patrouille des Glaciers"; 2000 - today
· Captain of the Riviera Saints, American Football Team with three consecutive champion titles; 2007 - 2012
· Scuba diving, adventure travelling, yoga. 2008 – today

REFERENCES

Upon request.

Index