11TH INTERNATIONAL CONFERENCE
ON CRITICAL INFORMATION
INFRASTRUCTURES
SECURITY

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Cyber Security Investment in the Age of Big Data:
Reassessment of the Gordon-Loeb Model and Application to Critical Infrastructure Protection

Dimitri Percia David[ab], Marcus Matthias Keupp[b], Solange Ghernaouti[a], and Alain Mermoud[ab]

[a] *Swiss Cybersecurity Advisory and Research Group, University of Lausanne*
[b] *Military Academy at ETH Zurich*

UNIL | Université de Lausanne
HEC Lausanne

MILAK MILITÄRAKADEMIE AN DER ETH ZÜRICH

Agenda

Introduction	2’
The economics of information security	
Investigating investment dynamics in cybersecruity	
Extending the GL model	8’
The impact of Big Data Analytics on the GL model	
Suggesting a multi-period model	
Relaxing the assumption of continuity	
Application to Critical Infrastructure Protection	2’
Concluding comments	2’
Further research	1’
Q&A and discussion	5’

Introduction

Economics of Information Security as a complementary approach

Cyber Security issues = bad incentives + bad design

Introduction

Investigating investment dynamics in cybersecruity

Yes, BUT...

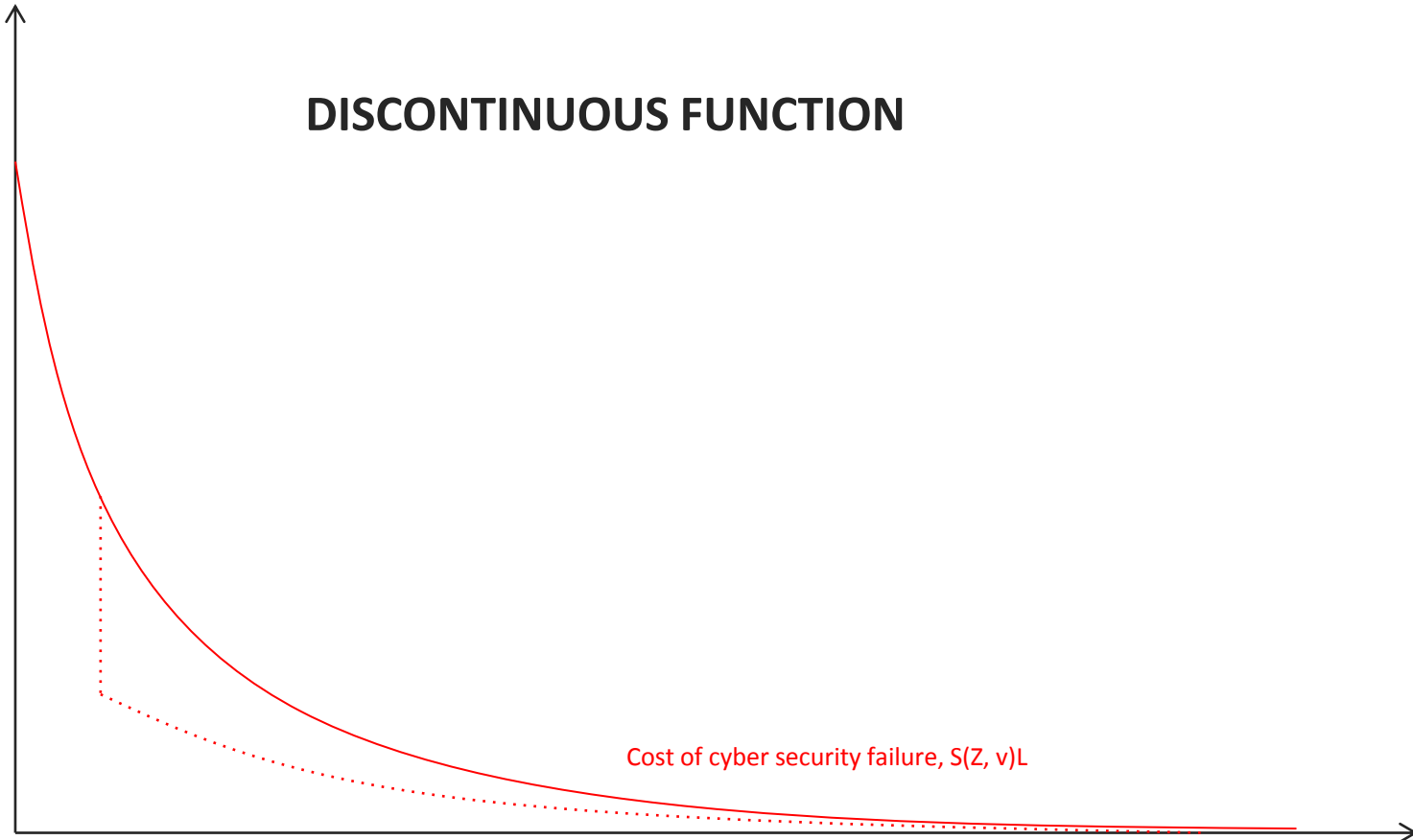
SINGLE PERIOD MODEL

Introduction

Investigating investment dynamics in cybersecruity

MULTI-PERIOD MODEL

DISCONTINUOUS FUNCTION



Extending the GL model

The impact of Big Data Analytics on the GL model

Security Analytics: from bad signatures to bad actions

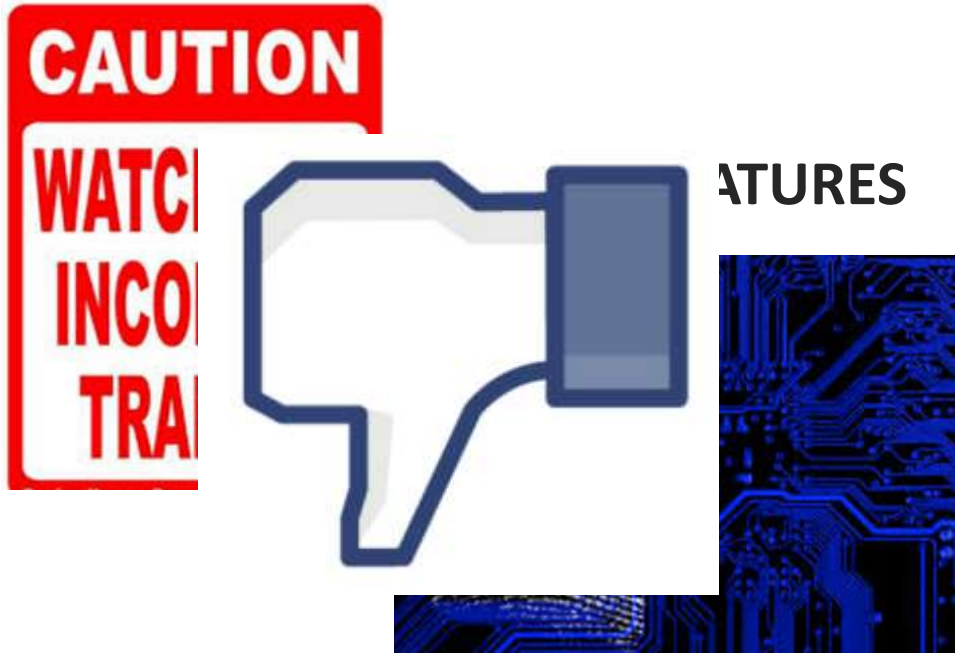
MINIMIZING COSTS

CONVENTIONAL CYBERSECURITY MEANS = **LIMITED SUCCESS**

Extending the GL model

The impact of Big Data Analytics on the GL model

Security Analytics: from bad signatures to bad actions



BAD ACTIONS

Extending the GL model

The impact of Big Data Analytics on the GL model

From resilience to anticipation: the next generation of information technologies

Real time analytics

Dynamic detection

Early warnings

EARLY WARNING PROJECT

Extending the GL model

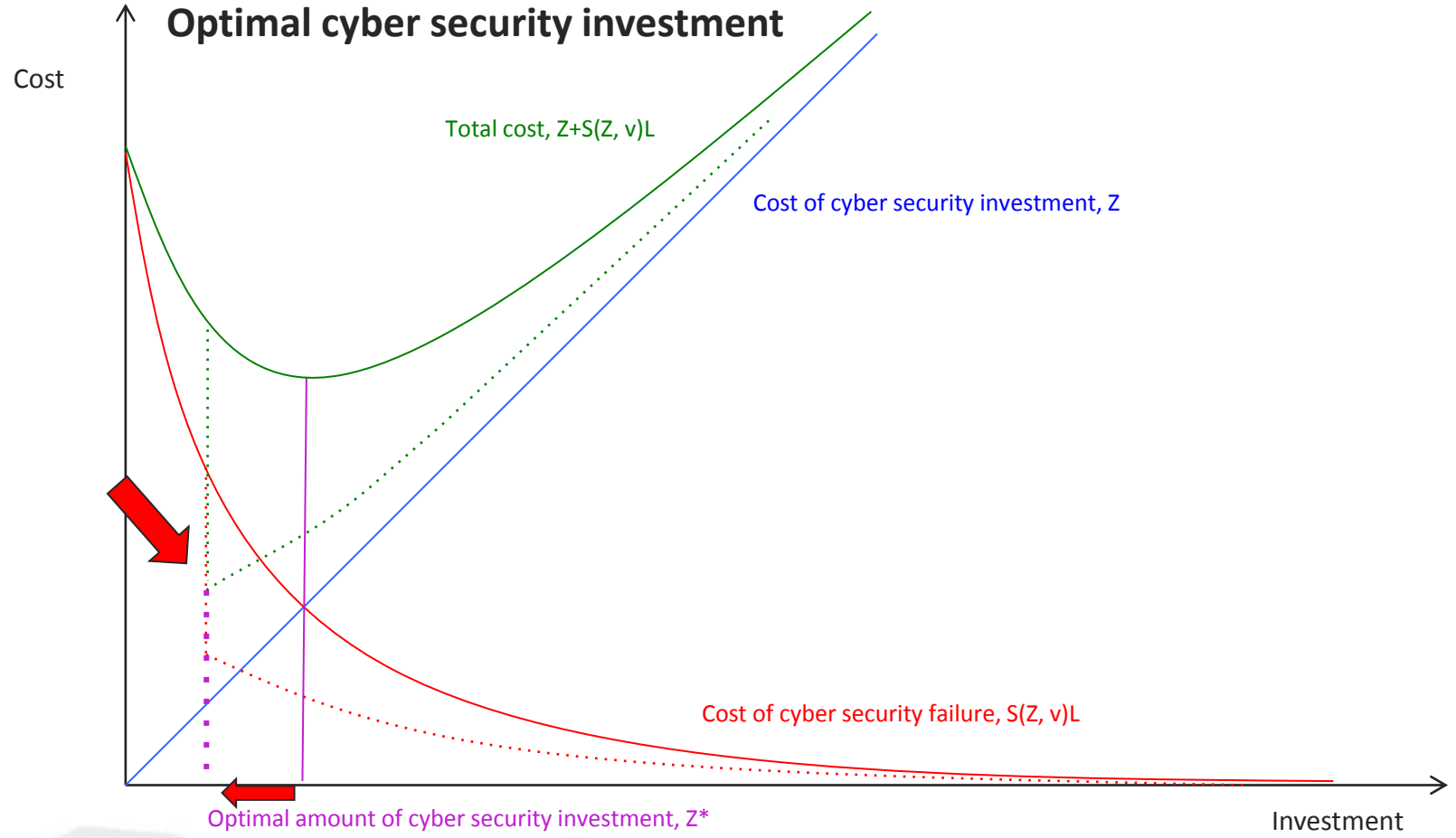
1st impact: Suggesting a multi-period model

$$Max\ ENBIS(z) = [v - S(z, v)]\, L - z$$

$$Max\ ENBIS(z_i) \left\{ \sum_{i=1}^{n} [v_i - S_i(z_i, v_i)]\, L_i - z_i \right\}$$

Extending the GL model

2nd impact: Relaxing the assumption of continuity



Extending the GL model

2nd impact: Relaxing the assumption of continuity

Proposition 1. *If BDA is employed for producing cyber security, then investments in cyber security will decrease from* $\sum_{i=1}^{n} z_i(v_i) \leq \sum_{i=1}^{n} \frac{1}{e} v_i L_i$ *to* $\sum_{i=1}^{n} z_i(v_i) \ll \sum_{i=1}^{n} \frac{1}{e} v_i L_i$ *due to greater efficiency of BDA compared to conventional tools.*

Application to CIP

An urgent need for efficiency and effectiveness improvement

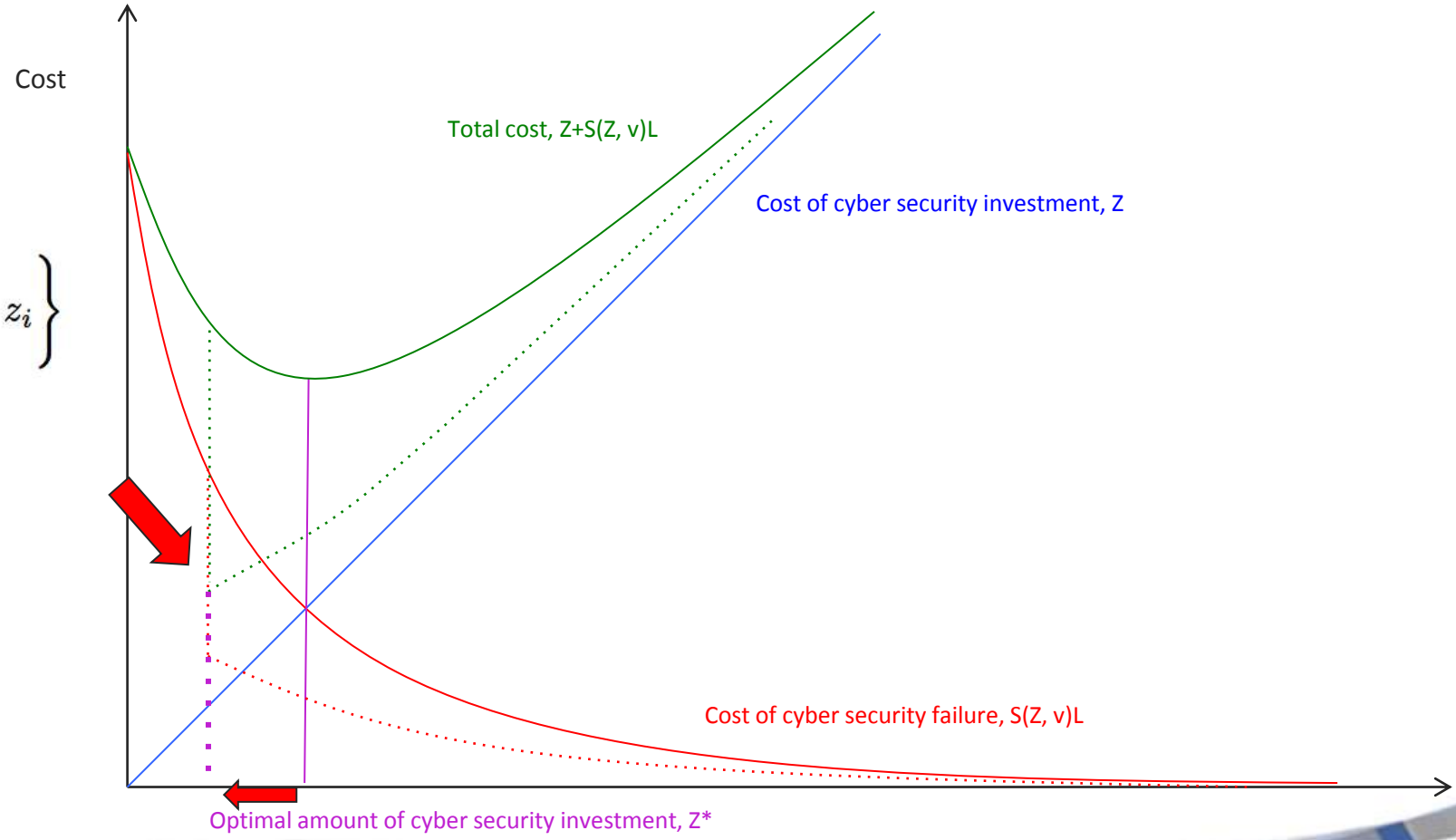
Effectiveness is...
"Doing the right thing"

Efficiency is
"Doing the thing right"

Concluding comments

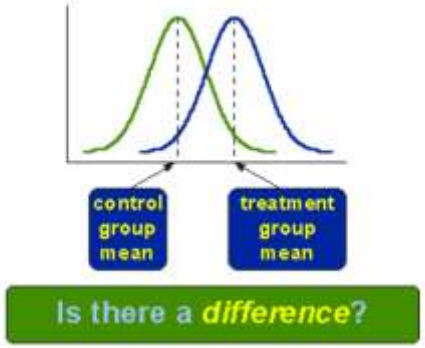
Extending the GL model for radically innovative and disruptive technologies

$$Max\ ENBIS(z_i)\left\{\sum_{i=1}^{n}\left[v_i - S_i(z_i, v_i)\right] L_i - z_i\right\}$$

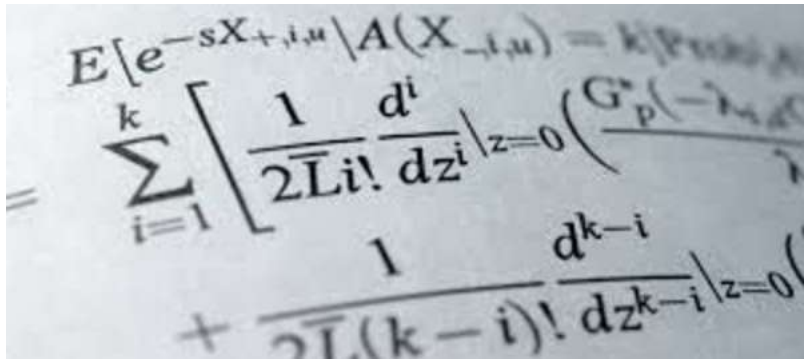


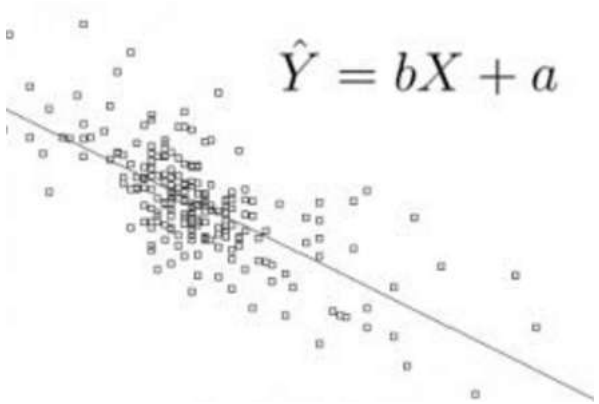
Further research

A game theory experiment for collecting data



An econometric model for testing our hypothesis





Q&A and discussion