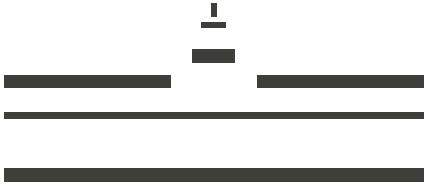


Westfälische
Wilhelms-Universität
Münster

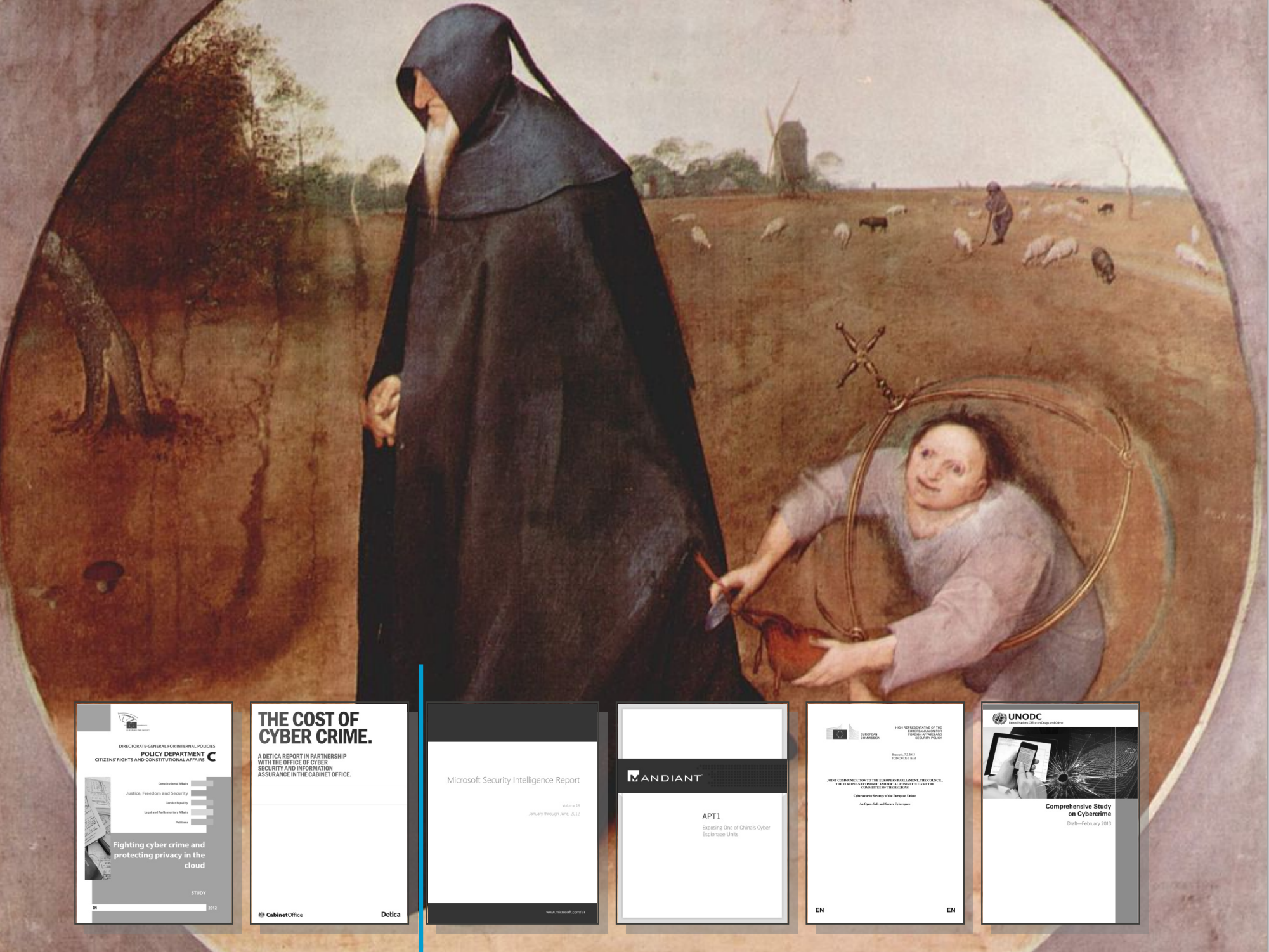
Measuring the Cost of Cybercrime

IMF 2013 Keynote, Nürnberg

living.knowledge
WWU Münster

Rainer Böhme

12 March 2013



DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Constitutional Affairs
Justice, Freedom and Security
Gender Equality
Legal and Parliamentary Affairs
Petitions

Fighting cyber crime and protecting privacy in the cloud

STUDY

EN 2012

THE COST OF CYBER CRIME.

A DETICA REPORT IN PARTNERSHIP WITH THE OFFICE OF CYBER SECURITY AND INFORMATION ASSURANCE IN THE CABINET OFFICE.

CabinetOffice Detica

Microsoft Security Intelligence Report

Volume 13
January through June, 2012

www.microsoft.com/sir

MANDIANT

APT1

Exposing One of China's Cyber Espionage Units

EUROPEAN COMMISSION

HIGH REPRESENTATIVE OF THE EUROPEAN UNION FOR FOREIGN AFFAIRS AND SECURITY POLICY

Brussels, 7.2.2013
JOIN(2013) 1 final

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

Cybersecurity Strategy of the European Union:

An Open, Safe and Secure Cyberspace

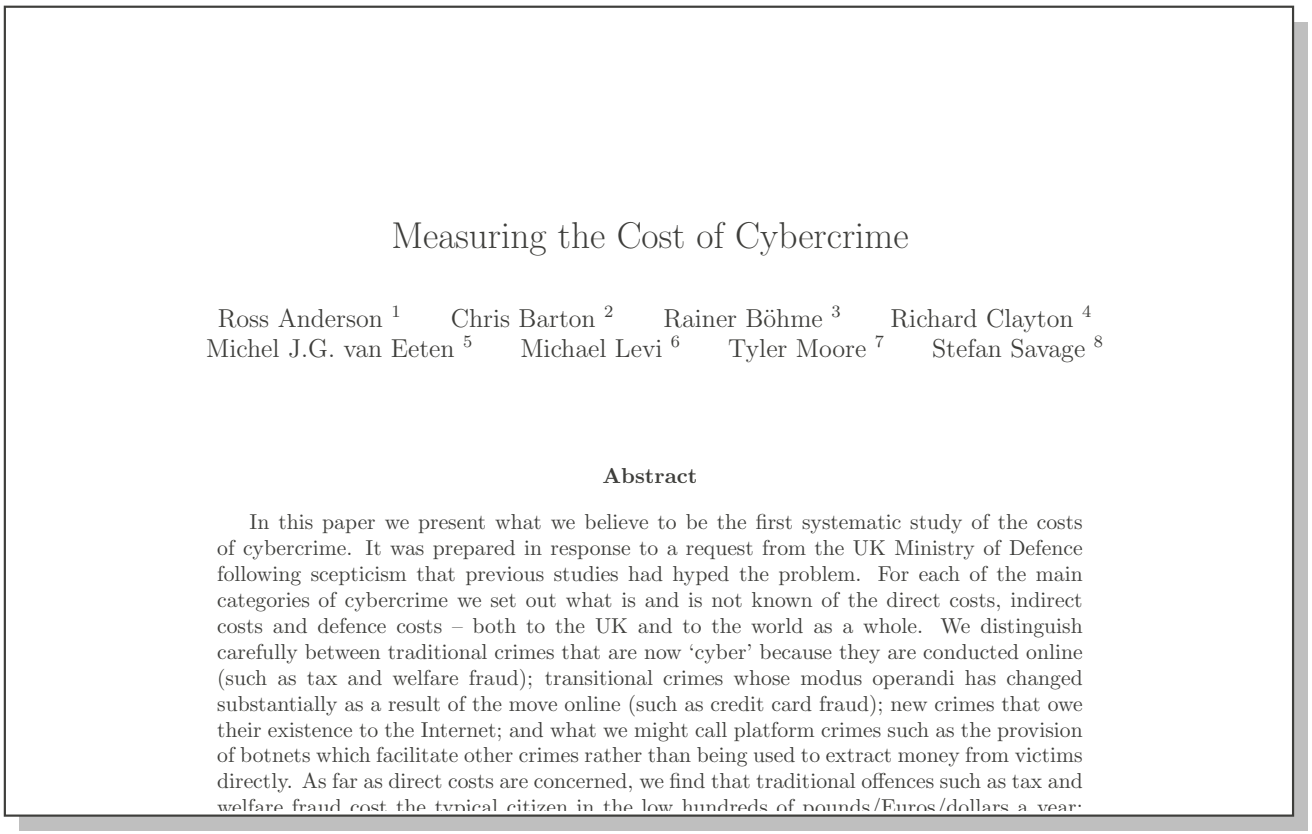
EN EN

UNODC
United Nations Office on Drugs and Crime

Comprehensive Study on Cybercrime

Draft—February 2013

We decided to write one, too:



Measuring the Cost of Cybercrime

Ross Anderson [1] Chris Barton [2] Rainer Böhme [3] Richard Clayton [4]
Michel J.G. van Eeten [5] Michael Levi [6] Tyler Moore [7] Stefan Savage [8]

Abstract

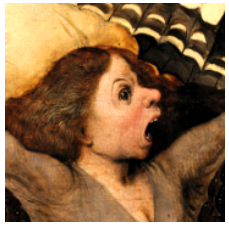
In this paper we present what we believe to be the first systematic study of the costs of cybercrime. It was prepared in response to a request from the UK Ministry of Defence following scepticism that previous studies had hyped the problem. For each of the main categories of cybercrime we set out what is and is not known of the direct costs, indirect costs and defence costs – both to the UK and to the world as a whole. We distinguish carefully between traditional crimes that are now 'cyber' because they are conducted online (such as tax and welfare fraud); transitional crimes whose modus operandi has changed substantially as a result of the move online (such as credit card fraud); new crimes that owe their existence to the Internet; and what we might call platform crimes such as the provision of botnets which facilitate other crimes rather than being used to extract money from victims directly. As far as direct costs are concerned, we find that traditional offences such as tax and welfare fraud cost the typical citizen in the low hundreds of pounds/Euros/dollars a year;

Workshop on the Economics of Information Security (WEIS) 2012

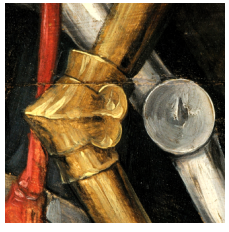
Quantifying cybercrime

Triangulation approach

Police-recorded crime statistics



Victimization surveys



Technology-based cybersecurity indicators

Translating incidents to costs

- Prioritize policy initiatives
- Evaluate efficiency of countermeasures

The figures in our heads

- In 2009 AT&T's Ed Amoroso testified before the US Congress that global cybercrime profits topped $ 1 trillion.
- That is 1.6 % of world GDP.
- In 2011 Detica's figure (£27 Bn) is 2 % of UK GDP.
- Not only are the figures eye-poppingly large, it is often unclear what is being measured.
- Amoroso spoke of cybercrime "profits", while Detica describes "losses".

Quote from a widely cited industry source

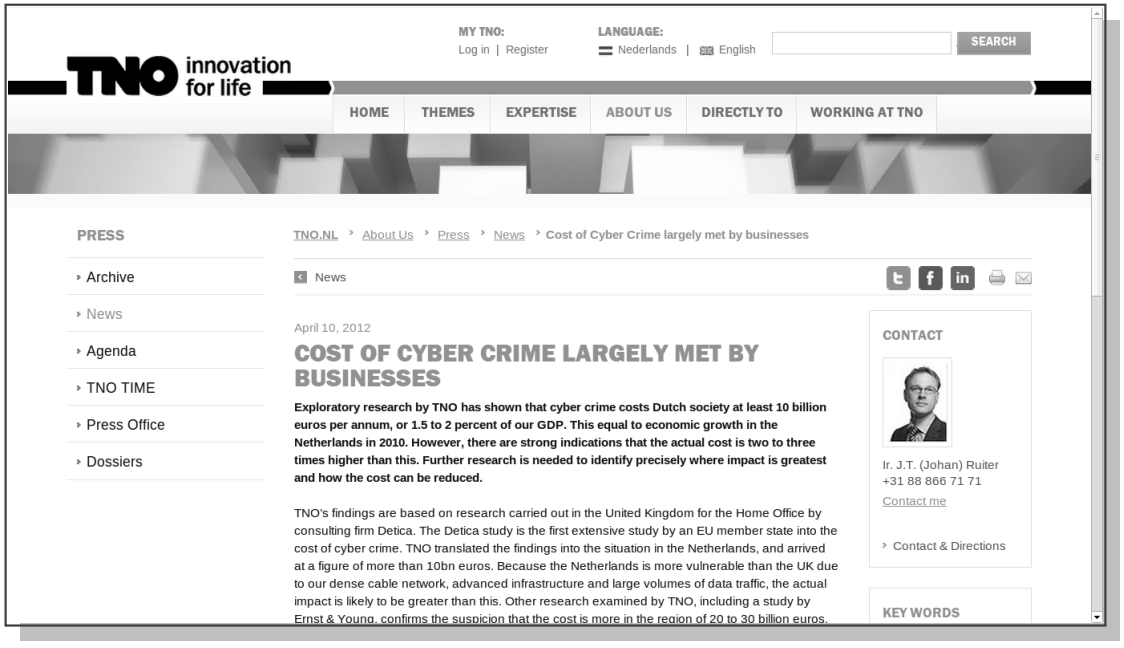
"**Methodology**

[. . .] A team of researchers combined manual search methods with advanced search tools including [vendor's own product], which specialises in turning large amounts of structured and unstructured data into intelligence.

The research team compiled a comprehensive evidence review of over 7,000 documentary sources, including public, private and 'grey' documentation."

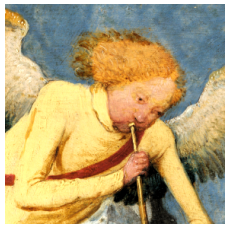
Truth by repetition

Poorly-sourced estimates get “laundered” by derivative reports that use the estimates without critically examining the methodology.



- In spring 2012 TNO scaled the 2 % GDP figure to the Netherlands.
- Surprise, surprise! German intelligence sources estimated the cost of cybercrime to € 50 billion p. a. in late summer 2012.

Games people play



Consumers

Are concerned; pay the bill

Government

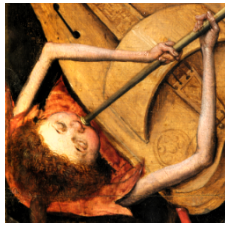
Spends public money; wants to stay in power

Security industry

Needs customers; smells defense budgets

Other industry

“Keep out of my way!”



Academia

Wants research grants

But can we do better?

- It is one thing to point out flaws, but it is quite another to produce a more reliable estimate of cybercrime losses.
- The UK Ministry of Defence challenged us to produce a more accurate estimate.
- We documented our attempt to measure cybercrime losses using publicly available data.
- Our methodology is bottom-up: we count what we know, knowing that we undercount what we cannot measure.

The Blind Leading the Blind

Cybercrimes we considered

- Online banking fraud
- Fake antivirus
- ‘Stranded traveler’ scams
- ‘Fake escrow’ scams
- Advance-fee fraud
- Infringing pharmaceuticals
- Copyright-infringing software
- Copyright-infringing music and video

} “Genuine” cybercrime

- Online payment card fraud
- In-person payment card fraud
- PABX fraud
- Industrial cyber-espionage and extortion

} Transitional cybercrime

- Welfare fraud
- Tax and tax filing fraud

} Traditional crime becoming “cyber”

A working definition of cybercrime

We adopt the European Commission's proposed definition:

Traditional forms of crime

such as fraud or forgery, though committed over electronic communication networks and information systems;

Publication of illegal content

over electronic media (e.g., child sexual abuse material or incitement to racial hatred);

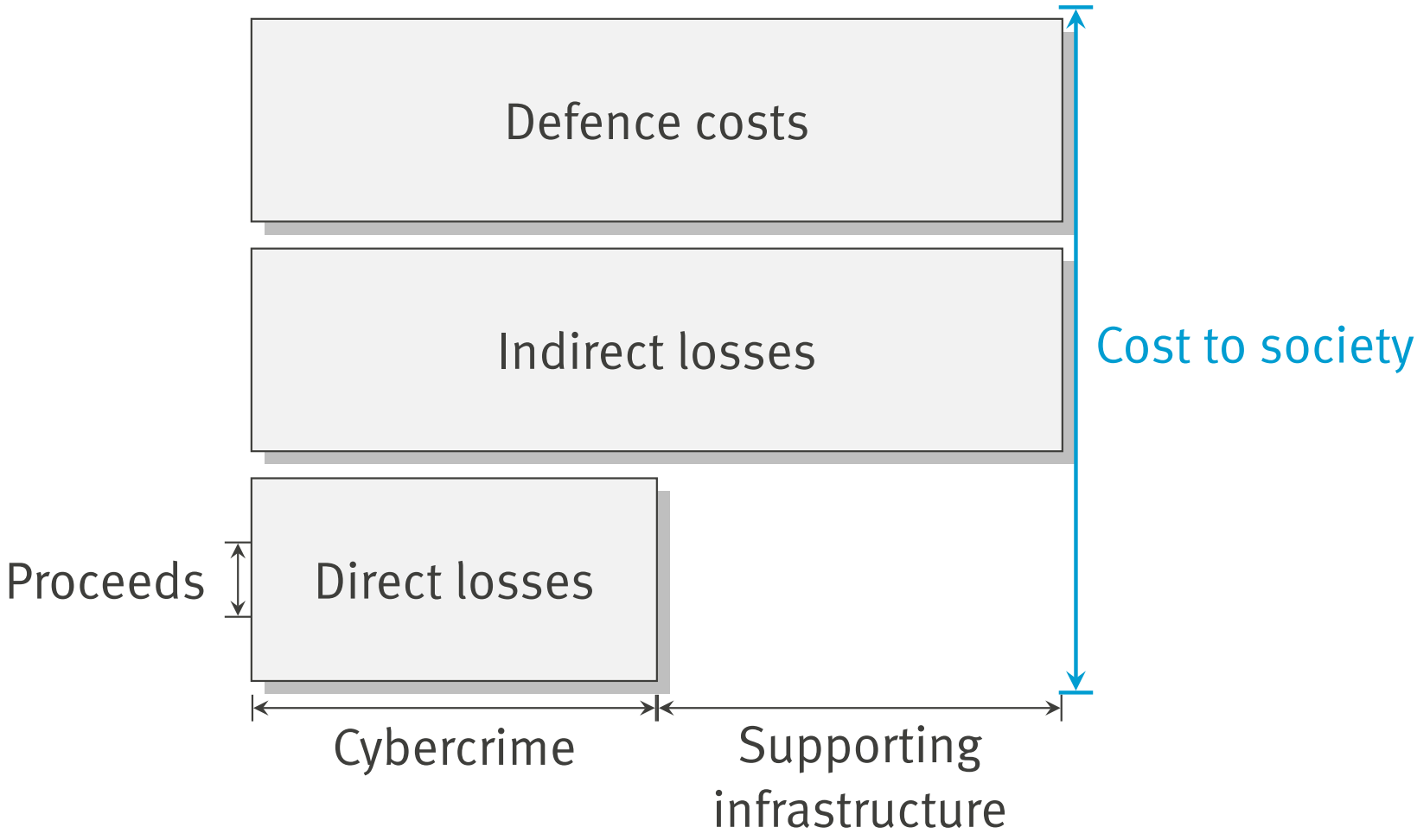
Crimes unique to electronic networks

e.g., attacks against information systems, denial of service and hacking.

COM (2007) 267

- The boundary between traditional and cybercrimes is fluid.

Framework for analysing the cost of cybercrime



Indirect and defense costs outweigh direct losses

Cybercrime cost category	Estimate
Direct losses	
– genuine cybercrime (e.g., phishing, advanced-fee fraud)	$ 2–3 Bn
– online payment card fraud	$ 4 Bn
Indirect costs	
– cybercriminal infrastructure (e.g., malware cleanup)	$ 10 Bn
– loss of confidence in online transactions	$ 30 Bn
Defense costs	
– cybercriminal infrastructure (e.g., antivirus)	$ 15 Bn
– payment card and online banking security measures	$ 4 Bn

Global estimates for 2010. Source: Measuring the Cost of Cybercrime, WEIS 2012.

- See our report for details and limitations.

Cost per citizen

Traditional crime becoming “cyber”

such as tax and welfare fraud

… a few hundred €/$/£ per year

Transitional cybercrime

such as payment card fraud

… a few tens €/$/£ per year

“Genuine” cybercrime

such as fake antivirus

… a few tens €/$/£ per year

(but the vast bulk are indirect and defense costs)

Our report's conclusions

- Today's cybercriminals are best compared to metal thieves: relatively small proceeds cause tremendous social costs.

- Every €/$/£ spent on better law enforcement seems to be more efficient than one spent on protection technology.

- As social interactions move online, there will soon be hardly any crime not involving a cyber component.

  So the real question is how a networked society can protect its institutions and values despite a base rate of criminal activity.

Drivers of indirect costs

- The European Commission's speechwriting unit conducts regular surveys of EU citizens on a range of topics.
- In Spring 2012 they ran a survey asking about citizens' concerns about and reactions to cybercrime using face-to-face interviews: 26,593 EU residents (18K Internet users) age 15+.
- The report provides descriptive statistics on how experiences with cybercrime varied across 27 EU Member States.
- We were granted access to micro-data on responses in order to conduct a secondary analysis.
- We focus on the relationship between experiences and concerns over cybercrime and the resulting actions taken by consumers.

Analytical approach

Intent
to bank or shop less because of cybercrime

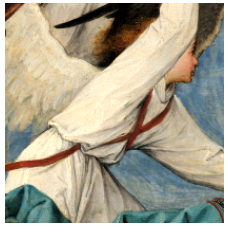
Experience with cybercrime
e.g., falling victim to identity theft, receiving phishing emails

Concern over cybercrime

e.g., concern over security of online payments

Exposure to news about cybercrime

e.g., read newspaper articles



Proficiency
e.g., educational attainment, online expertise, running antivirus

- Method: logistic regression model with country fixed effects

Dependent variables

"Has concern about security issues made you change the way you use the Internet in any of the following ways ?"

Indicator	EU27	DE
Less likely to buy goods online	17.5	13.4
Less likely to bank online	14.4	9.0
Less likely to participate online (summary of:)	63.0	74.3
– Less likely to give personal information on websites	36.3	50.8
– Only visit websites you know and trust	33.5	33.1
– Do not open emails from people you don't know	42.8	56.5

$N = 18,133$ EU residents, Internet users, age 15+

Eurobarometer Special 390, March 2012

Explanatory variables (1)

Indicator	EU27	DE
Experience with cybercrime		
Personal experience (at least "occassionally") with ...		
– Identity theft	8.0	6.1
– Phishing/advance-fee fraud spam	37.4	40.0
– E-commerce fraud	12.2	13.5

$N = 18,133$ EU residents, Internet users, age 15+

Eurobarometer Special 390, March 2012

Explanatory variables (2)

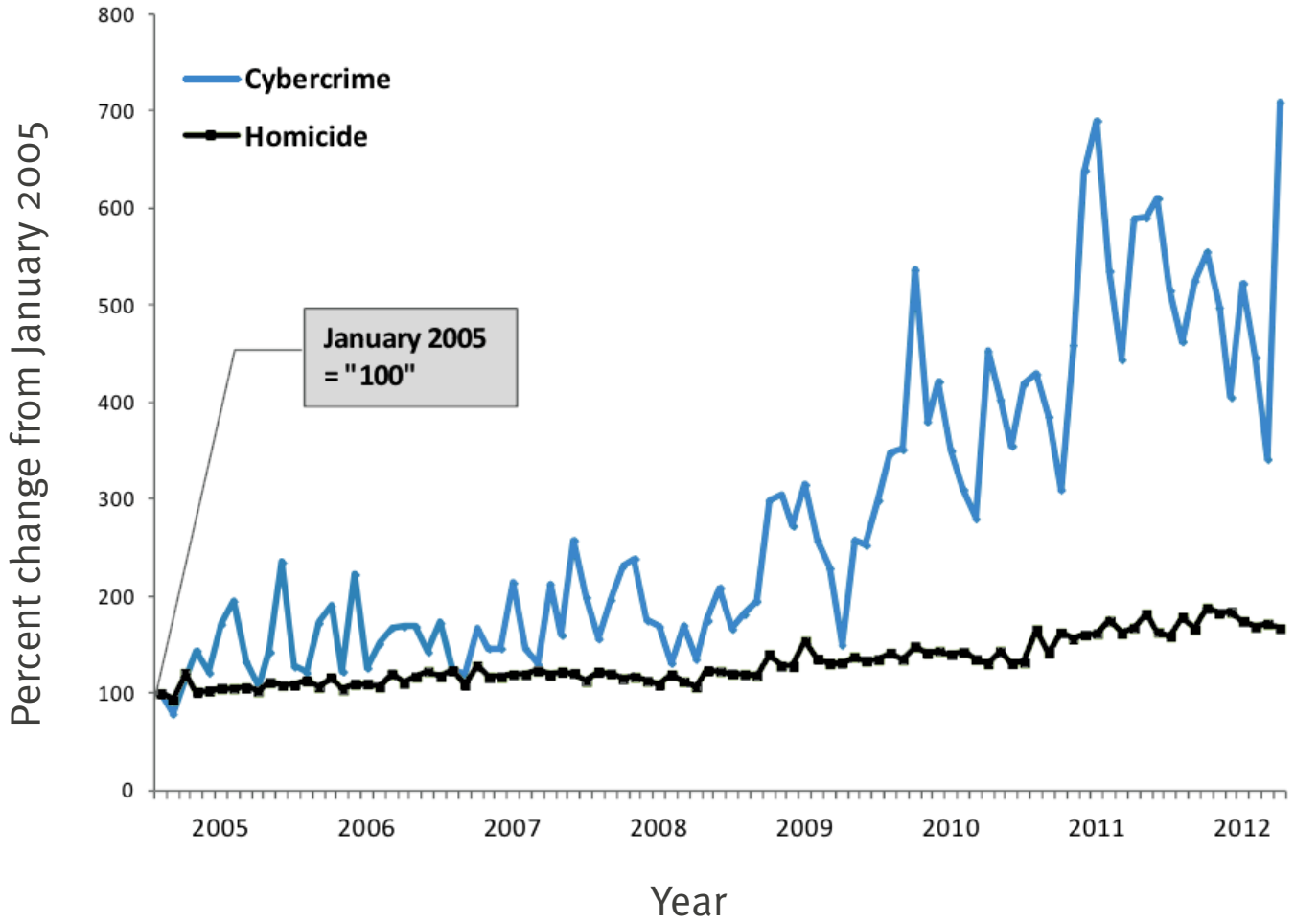
Indicator	EU27	DE
Concerns about cybercrime		
Personally (at least "fairly") concerned about ...		
– Identity theft	63.3	53.4
– Phishing/advance-fee fraud spam	50.2	47.9
– E-commerce fraud	51.7	41.7
Generally concerned about ...		
– Security of online payments	37.1	32.6
– Misuse of personal data	39.7	58.3

$N = 18,133$ EU residents, Internet users, age 15+

Eurobarometer Special 390, March 2012

Cybercrime makes the news

Relative frequency of global news reports 2005–2012



Source: UNODC calculations from Dow Jones Factiva, 2013

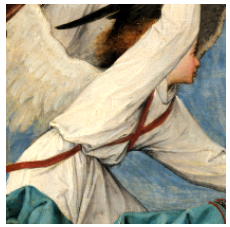
Explanatory variables (3)

Indicator	EU27	DE
Exposure to news about cybercrime		
On television	66.5	72.2
On radio	22.9	28.5
In the newspapers	33.3	48.8
On the Internet	33.9	36.5
From friends, family or colleagues	25.5	30.8
Not heard anything about cybercrime (spontaneous)	14.8	8.5

$N = 18,133$ EU residents, Internet users, age 15+

Eurobarometer Special 390, March 2012

Control variables



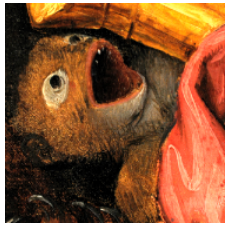
Indicator	EU27	DE
Proficiency indicators		
Internet access more than once a day	54.2	49.0
Bank online	47.8	48.4
Buy goods or services online	52.0	68.5
Feel confident about Internet skills	67.7	72.7
Feel informed about the risks of cybercrime	51.1	48.4
Changed at least one password in the past 12 months	48.4	44.2
Use different passwords for different sites	24.8	36.6
Antivirus installed	50.7	71.9
Higher education	46.5	41.8
Perceived social status above median	51.3	52.5

$N = 18,133$ EU residents, Internet users, age 15+

Hypotheses

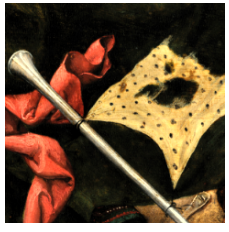
H1 – Supported with evidence

Falling victim to cybercrime reduces online participation, in particular online banking and shopping.



H2 – Supported with strong evidence

Expressing concern over cybercrime reduces online participation, in particular online banking and shopping.



H3 – Supported only for online banking

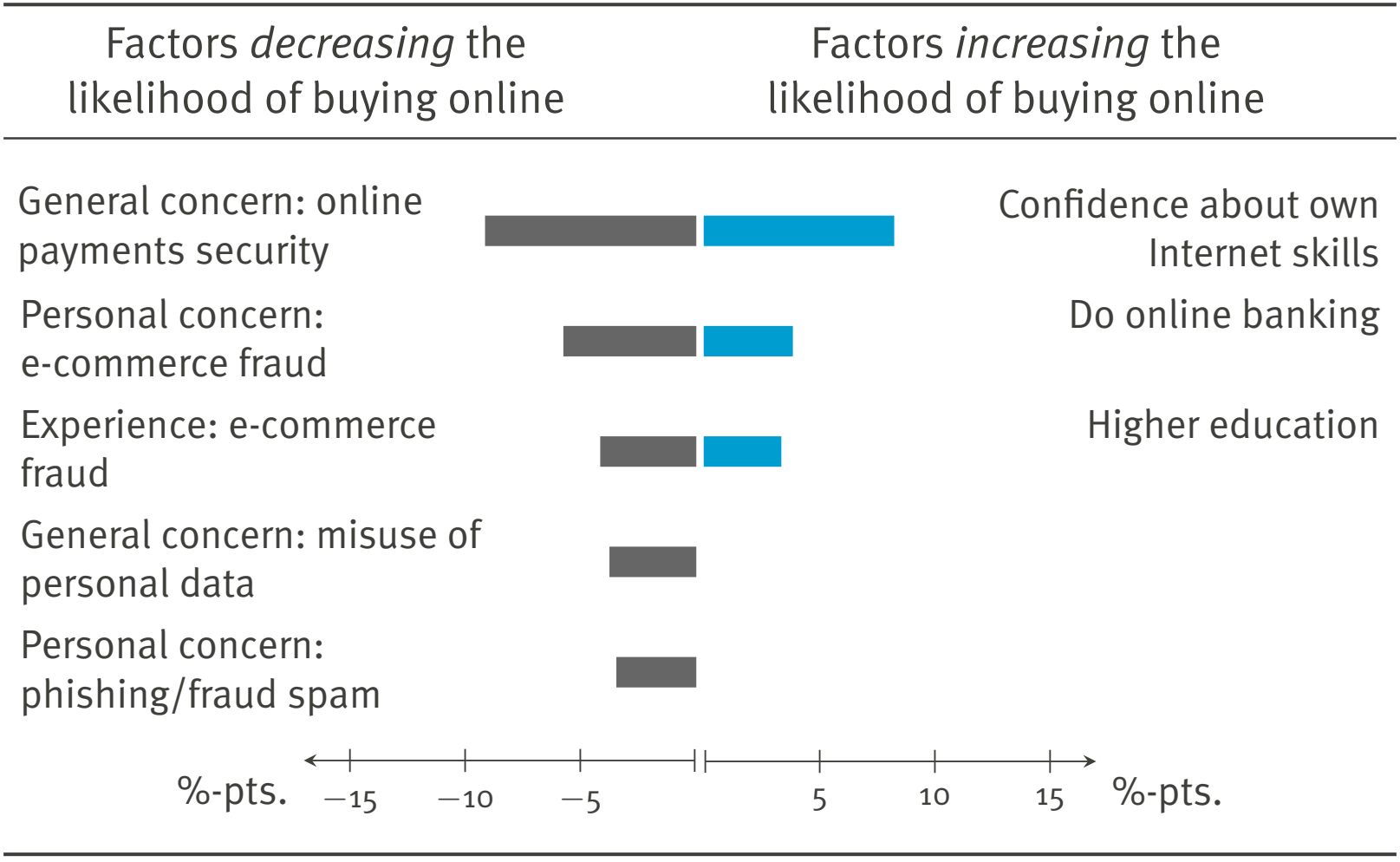
Exposure to cybercrime in the news media reduces online participation, in particular online banking and shopping.

H4 – Some support for e-commerce fraud

Falling victim to one form of cybercrime reduces participation in unrelated forms of online activity.

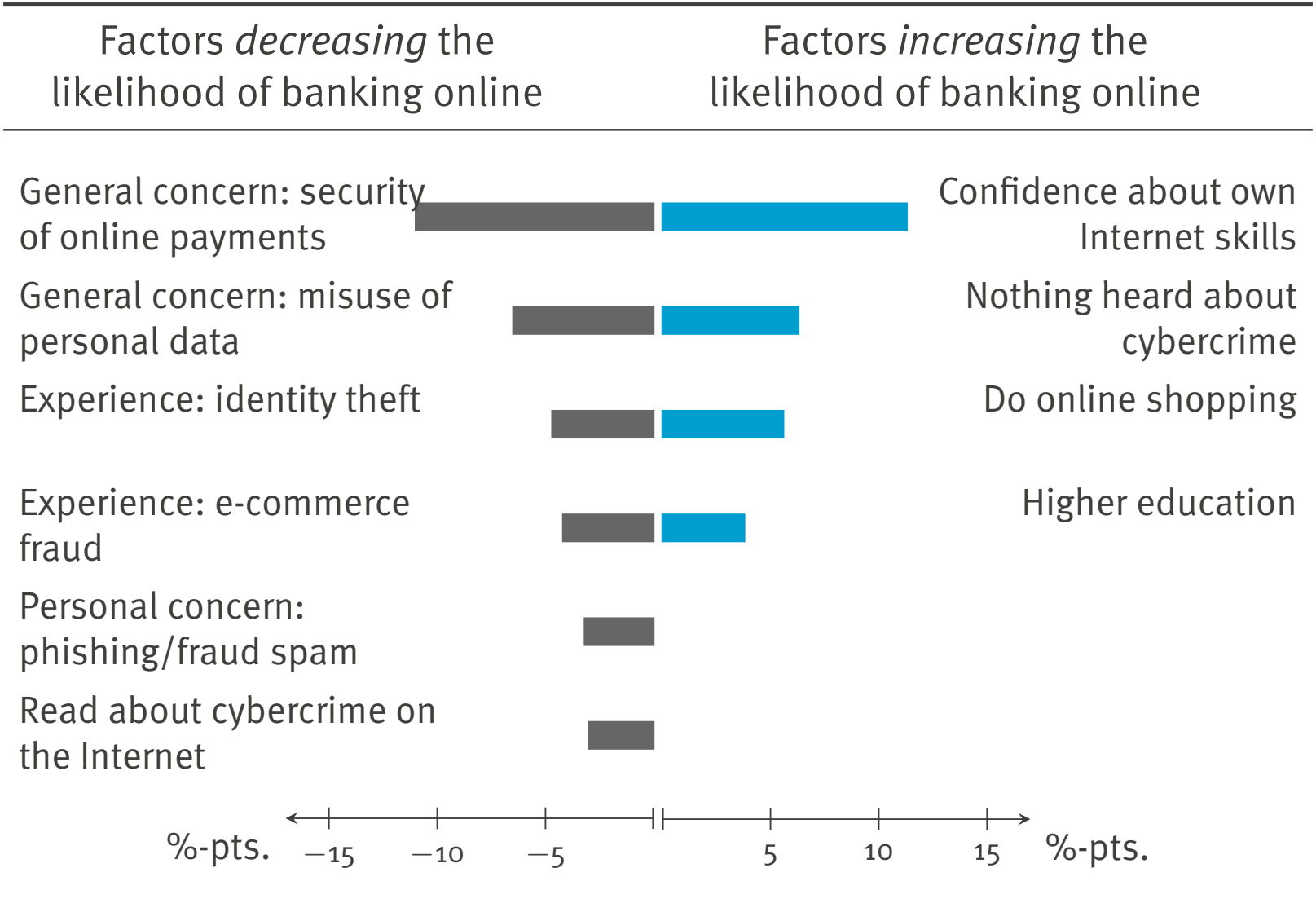
Source: Böhme & Moore 2012

Likelihood of shopping online



Böhme & Moore 2012 (based on Eurobarometer Special 390)

Likelihood of banking online



Böhme & Moore 2012 (based on Eurobarometer Special 390)

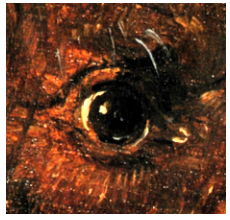
Drivers of indirect costs

One important and unexpected result

Concern about cybercrime inhibits online participation more than direct **experience** with cybercrime does.

- People may find the experience of cybercrime to be less painful than their worst fears.
- Regardless of what is driving the result, its implications are clear: assuaging society's concerns over cybercrime could make a greater impact than allocating further resources on assisting victims.
- Since experiencing cybercrime is relatively rare, this calls into question the use of frightening narratives for the purpose of awareness raising.

State-sponsored cyber-espionage



“We spy because you bribe.”

Allegations of espionage have always accompanied international trade talks, often as cover for protectionist behavior.

The myths conflate different threats. But it remains very hard to map the incidents we observe to tangible losses.

The “shareconomy” needs a Kerckhoffs’ principle for business models.

Importantly, tensions about cyber-espionage must not

- thwart cooperation in the prosecution of (other) cybercrime,
- militarize the cyberspace further.

Militarization of cyberspace

Traditional Indicator	Online Parallel
1) Extortion techniques	- Threats to close down systems by malware attacks - Use of compromising browser records for blackmail obtained by key logging software
6) Sex & prostitution	- Creation of online pornography empires - Links between escort sites, trafficking and organised groups
7) Violence	- Attacks on carding forums to take over rival operations - Willingness to use violence to acquire identification or other digital currencies

BAE/Detica 2012

Worrisome narratives:

- linking violence to objectively less serious (intangible) offenses,
- branding cybercrime as “organized crime”; there is a difference between gangs and a mafia.

After all, there is no violence in “cyber” alone.

Responsibility lasts on engineers who connect “cyber” to physical force.

A slippery slope

Article 15

Implementation and enforcement

1. Member States shall ensure that the competent authorities have all the powers necessary to investigate cases of non-compliance of public administrations or market operators with their obligations under Article 14 and the effects thereof on the security of networks and information systems.

2. Member States shall ensure that the competent authorities have the power to require market operators and public administrations to:

   (a) provide information needed to assess the security of their networks and information systems, including documented security policies;

   (b) undergo a security audit carried out by a qualified independent body or national authority and make the results thereof available to the competent authority.

COM (2013) 48 final (7 Feb 2013)

After recent German and EC policy initiatives on cybersecurity, it seems that the European version of breach disclosure laws . . .

1. is ten years late,
2. blurs the boundary between police and intelligence,
3. is designed as a oneway street, and
4. empowers the wrong actors.

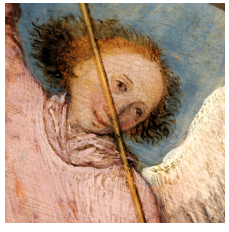
Recommendations to cybersecurity professionals

Question common narratives.

Be careful not to propagate “truth” by repetition.

Gather facts.

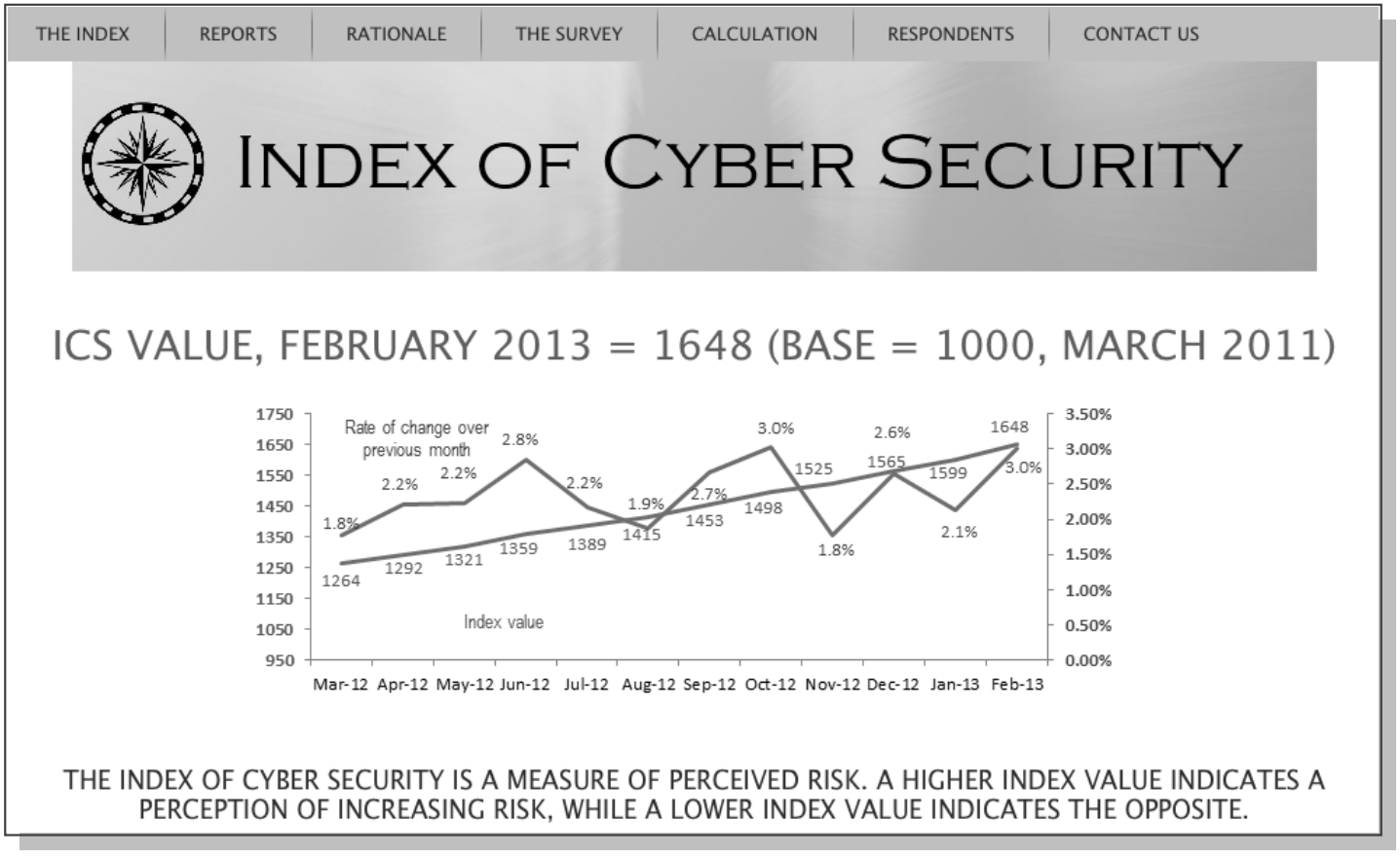
Refine measurements and make them transparent.



The world needs cyber-pacifists.

- Yes, we have to deal with cybercrime, but let us take it with professional distance and responsibility for society at large.

Cybersecurity professionals' sentiment indicators



Dan Geer & Mukul Pareek

- Help us to bring this index to the German-speaking community.

[Advertisement]

Survey-based sentiment indicators exist for:

- purchase managers (PMI),
- financial analysts (ZEW),
- professional economic forecasters (SPF), etc.

Why not regularly ask a panel of information security professionals to construct a **forward-looking** sentiment indicator?

We use a **short questionnaire**, asking for general observations of **changes in perceived attack intensity**. No breach disclosure!

Respondents will be privately recruited industry practitioners with operational responsibilities for managing information security risks.

Take a flyer and contact us if you think you are eligible.
Forward them to suitable colleagues.

Thank you.

Resources

- Ross Anderson, Chris Barton, Rainer Böhme, Richard Clayton, Michel J. G. van Eeten, Michael Levi, Tyler Moore, Stefan Savage (2012): **Measuring the Cost of Cybercrime**. *Workshop on the Economics of Information Security (WEIS)*, Berlin, June 25–26.
  `http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf`

- Rainer Böhme, Tyler Moore (2012): **How Do Consumers React to Cybercrime ?** *APWG eCrime Researchers Summit*, Puerto Rico, October 22–25.
  `http://lyle.smu.edu/~tylerm/ecrime12eurobar.pdf`

- Comments and questions: **rainer.boehme @ uni-muenster.de**

Epilogue

- Color on the slides is reserved to Pieter Bruegel the Elder (1525–1559)
- Detail squares form a bigger picture: The Fall of the Rebel Angels

Detailed digital reproduction thanks to the Google art project.