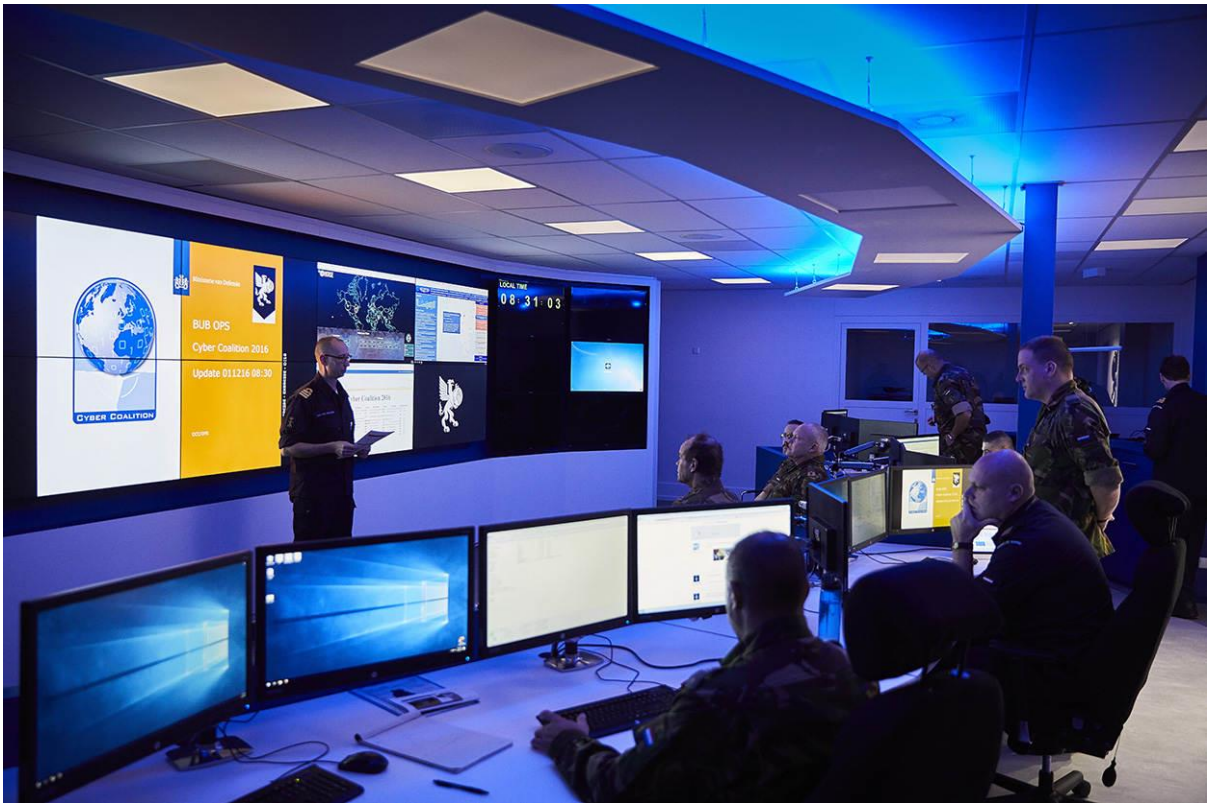
POLICY BRIEFING



Cyber fraud on Individuals: A Sorry Tale

Plenty of 'facts' but not enough figures

Antonis Papasavva, Henry Skeoch, Arianna Trozze

Overview

Increased availability of household internet connections and reduced computer hardware prices in the 1990s resulted in the integration of the internet into much of modern life. The increase in connectivity brought many societal benefits but also presented new opportunities for criminal revenue generation, particularly fraud targeted at individuals. We conducted a systematic literature review that examines the quantitative cost of cyberfraud to individuals worldwide. We found the body of literature to be underdeveloped, specifically in relation to data reliability and availability, as well as methodological rigour. We recommend well-publicised inter-governmental victim reporting databases; employing traditional economic modelling; and public-private sector cooperation to apply existing technical and analytical methods to other areas of cybercrime.

Method

We searched a range of academic literature databases using a list of carefully defined search terms, following our proposed systematic literature review protocol.[1] We used a Preferred Reporting Items for Systematic Reviews and Meta-Analysis flow diagram (PRISMA) to refine the list of articles. The PRISMA process entails four distinct phases: identification, screening, eligibility and inclusion; all necessary steps for a systematic literature review.

Ultimately, 25 studies were deemed eligible for inclusion in this systematic literature review. These studies provide quantitative samples and assess the global criminal revenue from cyber-fraud targeting individuals.

Key Findings

- Research quantifying the cost of cyber fraud against individuals is **underdeveloped**.
- Studies purporting to provide quantitative estimates tended to use **unreliable data and methods.**
- We identify the following primary issues in the literature: **data availability and methodological rigour**.

Recommendations

- Create and publicise **inter-governmental victim reporting databases**.
- Utilise **traditional economic modelling** to arrive at quantitative estimates.
- Use **public-private partnerships** to apply existing technical and analytical methods to other areas of cybercrime.

Results

Our study uses a classification proposed by Professor David Wall[2] to categorise cybercrime. Table 1 outline examples proposed by Wall for each type of crime. Table 2 lists the estimated criminal revenue reported in each of the 25 studies reviewed.

[1] See protocol https://bit.ly/2KqF7Pn

[2] David Moher et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement". In: Annals of internal medicine 151.4 (2009), pp. 264-269.

Crime Type	Crime against machines	Crime using machines	Crimes in the machine
Opportunities			
Cyber-Assisted	Telecommunications network abuse	Frauds	Cyber-stalking
Cyber-Enabled	Viruses	Identity Theft	Hate Speech
Cyber-Dependent	Denial of Service	Phishing	Online Grooming

Table 1: The Wall Classification Matrix for Cybercrimes

Author	Publication Year	Countries	Estimated Criminal Revenue
Hinde	2001	France, Germany, UK	USD 265-378mn
Oates	2001	USA	USD 500bn pa
Foltz	2008	USA	USD 1.4-100mn
Chambers & Turksen	2010	Jamaica, UK	GBP 52.5mn
Naruedomkol et al.	2010	Thailand	N/A
Moore	2010	Unspecified	USD 0.4-20.00 per card USD 10-100 per bank account
Pratt et al.	2010	USA (FL)	N/A
Blanco Hache & Ryder	2011	UK	USD 400bn pa, GBP 13.9-30bn
Watters et al.	2012	Australia	
Heinonen et al.	2012	USA	USD 3.56mn
Keene	2012	Virtual	JPY 150mn
Land	2013	Australia	AUD 2bn
Anderson et al.	2013	Global, UK	N/A
Lamberger et al.	2013	Slovenia	USD 41bn
Dobovsek et al.	2013	Slovenia	N/A
Pearce et al.	2014	Global	USD 100k per day
Naylor	2015	USA	USD 375-575bn
Levi	2016	Various Developed	N/A
Mathew	2016	Europe	GBP 1.2bn pa
Adewumi & Akinyelu	2017	Global	USD 32bn, GBP 183.2mn
Asgary et al.	2017	Turkey	N/A
Levi et al.	2017	UK	GBP 55mn
Cross	2018	Australia	AUD 340mn
Holub & O'Connor	2018	Global	N/A
Umlauf & Mochizuki	2018	Global	N/A

Table 2: Estimated criminal revenue discussed in reviewed literature

Findings and Recommendations

Our review suggested that the literature quantifying the cost of cyber fraud against individuals is underdeveloped. Studies purporting to provide quantitative estimates on a range of crimes are often broad, leading to unsubstantive estimates. Estimates are generally more meaningful when they address more specific categories rather than cybercrime more generally. Without accurate quantitative estimates of the impact of specific types of cyber fraud on individuals, we are unable to develop appropriate interventions and mitigations. In particular, estimates of the direct (i.e., loss to individuals), indirect (any other financial losses incurred as a result of the crime), and defensive (costs incurred defending against said crimes) costs are critical.[1]

Most papers cite estimates from other sources rather than conducting their own robust quantitative analyses of the impact of cyber fraud on individuals. While some papers offered 'real-world' analysis, the majority of the studies relied merely on secondary sources or tended to be speculative.

Policy Recommendations

1. Raise public awareness of how to report cyber fraud.

2. Develop consistent international databases to improve data quality and allow analysis using robust statistical methods.

3. Encourage the private sector to share aggregated cyber fraud preventative and remediative costs.

Key Issues: Methods

1. Overall lack of statistical rigour.

2. Studies often failed to use systematic approaches to sampling.

3. Some studies merely cited estimates from other sources.

4. Sample sizes varied greatly or were undisclosed.

[3] Ross Anderson et al. "Measuring the Changing Cost of Cybercrime". In: Boston, 2019, p. 32.

Acknowledgments. This project was funded by the UK EPSRC grant EP/S022503/1 that supports the Centre for Doctoral Training in Cybersecurity delivered by UCL's Departments of Computer Science, Security and Crime Science, and Science, Technology, Engineering and Public Policy.

Antonis Papasavva: antonis.papasavva@ucl.ac.uk
Henry Skeoch: henry.skeoch.19@ucl.ac.uk
Arianna Trozze: arianna.trozze@ucl.ac.uk

ucl.ac.uk